Version imprimée de la documentation Relution

Manuel Relution

Pour la version 26.4.0

Dernière mise à jour: 2026-10-21 14:01 UTC

Disponible en ligne sur hub.relution.io

Table des matières

1. Relution Cloud
2. On Premises Installation
    1. Installation
    2. Stockage objet
    3. After installation
    4. Base de connaissances
3. Product information
4. Commencer
5. Général
    1. Tableau de bord
    2. Relution Apps
    3. Gestion des applications
    4. Gestion des utilisateurs
    5. Gestion des appareils
    6. Administration Apple
6. Apple iOS
    1. Enrôler des appareils
    2. Supervision
    3. Actions
    4. Paramètres
    5. Politiques
    6. Base de connaissances
7. Apple tvOS
    1. Enrôler les appareils
    2. Actions
    3. Policies
    4. Base de connaissances

Pour la version 26.4.0

8. Apple macOS
    1. Enrôler les appareils
    2. Actions
    3. Politiqus
    4. Base de connaissances
9. Apple visionOS
    1. Inscrire les appareils
    2. Actions
    3. Politiques
10. Apple watchOS
    1. Inscrire les appareils
    2. Actions
    3. Politiques
11. Éducation
    1. Apple dans l'éducation
12. Android Enterprise
    1. Enrôler les appareils
    2. Actions
    3. Politiques
    4. Base de connaissances
13. Android Classic
    1. Enrôler les appareils
    2. Actions
    3. Politiques
    4. Base de connaissances
14. Whiteboards
    1. Android classique
    2. Android Enterprise
15. Windows
    1. Enrôler les appareils
    2. Actions
    3. Policies
    4. Windows Apps
    5. opsi
    6. Base de connaissances
16. Linux
17. Paramètres
    1. Licences
    2. TeamViewer
    3. Accès conditionnel

Pour la version 26.4.0

Relution Cloud

Relution propose une offre cloud performante, qui comprend l'exploitation du logiciel sous forme de solution de serveur cloud virtualisé. Cet hébergement s'effectue dans un environnement cloud conforme au RGPD et garantit la sécurité et la protection de toutes les données traitées. Grâce à l'installation automatique des mises à jour, le logiciel reste toujours à jour et sécurisé. De plus, l'infrastructure assure à la plateforme Relution une haute disponibilité de 99,5 % hors fenêtre de maintenance, garantissant ainsi une utilisation fiable à tout moment.

Informations générales

Les informations générales suivantes s'appliquent à l'exploitation du Relution Cloud.

Fenêtre de maintenance

La maintenance des serveurs Relution Cloud a lieu du lundi à 17h00 au mardi à 4h00 CE(S)T. Des restrictions temporaires peuvent survenir pendant cette période.

Mises à jour de Relution

Les mises à jour de Relution sont annoncées au préalable via la newsletter → et sont effectuées le jour annoncé entre 16h00 et 19h00 CE(S)T. Aucune interruption de service n'a lieu pendant ces mises à jour.

Pour la version 26.4.0

Réception des e-mails

S'assurer que les e-mails provenant de `no-reply@relution.io` et `no-reply@mail.relution.io` peuvent être reçus. Ces adresses sont utilisées comme expéditeurs pour les échanges de courriels des serveurs cloud.

Adresses IP de la passerelle

Les adresses de passerelle à partir desquelles les serveurs Relution Cloud envoient des requêtes sont disponibles de deux manières :

1. Via DNS : les adresses IP sont publiées sous forme d'enregistrements DNS A sous le FQDN `gateway.<nom-du-cluster>.relution.io`, par exemple `gateway.eu.relution.io` pour le cluster `eu`. Les pare-feux prenant en charge les règles basées sur un FQDN peuvent utiliser directement ce nom d'hôte dans leurs autorisations.
2. Sous forme de liste JSON : les adresses sont également publiées sous forme lisible par machine à l'adresse https://repo.relution.io/other/relution-cloud-gateways.json.

Les deux sources sont régulièrement mises à jour de manière automatisée. Si une autorisation basée sur l'adresse IP est nécessaire pour l'accès à, par exemple, LDAP, la source correspondante doit être consultée régulièrement et l'autorisation mise à jour ; une solution automatisée ou l'utilisation de règles de pare-feu basées sur un FQDN est recommandée.

Limites et quotas

Voir l'article Limites et quotas →.

Variantes de l'offre Relution Cloud

L'offre cloud de Relution est proposée en deux variantes afin de répondre de manière flexible à différents besoins :

Hébergement partagé sur live.relution.io

Dans le modèle hébergement partagé, une organisation est mise à disposition sur `live.relution.io` au sein d'un serveur partagé. Cette variante offre une solution économique pour les organisations ayant des besoins moins complexes. Un accès de test peut être créé directement via l'aperçu « Prix et démo » sur le site relution.io →.

Dedicated Server

Pour les organisations nécessitant un contrôle et une personnalisation maximaux, un Dedicated Server exploité exclusivement est disponible. Celui-ci permet une infrastructure propre et des possibilités d'extension adaptées aux besoins spécifiques de l'entreprise. Ces serveurs sont mis à disposition sous une URL suivant le schéma `<nom-du-serveur>.<nom-du-cluster>.relution.io`, par exemple `acme.eu.relution.io`.

Pour la version 26.4.0

Le `<nom-du-serveur>` est soumis aux restrictions suivantes :

- Maximum 20 caractères
- Uniquement des caractères alphanumériques (minuscules) ou `-`
- Doit commencer par une lettre
- Doit se terminer par un caractère alphanumérique

Mise en service initiale

Les informations suivantes sont nécessaires pour la mise en service initiale :

- Nom de serveur souhaité, donnant le domaine `<nom-du-serveur>.<nom-du-cluster>.relution.io`
- Nombre approximatif d'appareils devant être gérés sur le serveur
- Nom et adresse e-mail du compte administrateur système à créer

Déroulement de la mise en service initiale :

1. Le service commercial Relution demande la création du serveur avec les données décrites ci-dessus
2. Le serveur est créé dans le cluster SaaS Relution correspondant
3. Une notification est envoyée à l'adresse de contact du client
4. Une réinitialisation du mot de passe est effectuée pour le compte administrateur système par une personne ayant accès à la boîte e-mail
5. Connexion et acceptation du contrat de licence utilisateur final (CLUF)
6. Signature numérique du contrat de sous-traitance (AVV) dans le cadre du règlement général sur la protection des données (RGPD) sur le portail Relution
7. Recommandation fortement conseillée : mettre en place l'authentification multifacteur (MFA) → pour l'administrateur système

En option, un accès pour le support Relution → peut ensuite être configuré.

Domaine personnalisé pour Dedicated Server

Sur demande, un domaine personnalisé peut également être utilisé pour la variante Dedicated Server. Pour cela, une entrée DNS CNAME correspondante doit être configurée pour le domaine, pointant vers `<nom-du-serveur>.<nom-du-cluster>.relution.io`. Le domaine personnalisé (par exemple `relution.nomclient.de`) pointe alors vers l'instance Relution Cloud (par exemple `nomclient.eu.relution.io`).

Extension VPN Site-to-Site pour Dedicated Server

Pour la variante Dedicated Server, l'extension VPN Site-to-Site est également disponible, permettant un accès sécurisé aux infrastructures spécifiques du client, comme les services intranet. Cette extension propose les fonctionnalités suivantes :

- Connexion des services intranet au serveur cloud Dedicated
- Jusqu'à 10 Go de trafic par mois
- Garantie d'une disponibilité de 99,5 %

Comme prérequis pour la mise en place, l'équipement distant côté client (passerelle VPN) doit prendre en charge IPSec IKEv2 avec EAP-PSK.

Ces options permettent aux organisations d'étendre leur infrastructure informatique de manière individuelle et de s'adapter pleinement à leurs besoins spécifiques.

Relution Shield en exploitation SaaS

En tant qu'extension supplémentaire pour Dedicated Server, Relution propose avec Relution Shield → une extension performante en exploitation SaaS. Avec Relution Shield, une configuration road-warrior pour les terminaux peut être mise en œuvre, offrant une solution sécurisée et flexible pour l'accès aux ressources internes. Cette extension comprend notamment :

- Contrôle d'accès basé sur des certificats, garantissant une sécurité élevée pour les connexions des terminaux
- Vérification de conformité pour contrôler les paramètres de sécurité des appareils connectés
- Utilisation du tunnel Site-to-Site pour accéder aux ressources internes de l'organisation

Cette extension est idéale pour les utilisateurs mobiles et en télétravail qui ont besoin d'un accès sécurisé à haute sécurité à l'infrastructure interne.

Pour la version 26.4.0

Limites et quotas

Ce chapitre décrit les quotas et limites standard de l'offre Relution Cloud. Sauf accord contraire, les valeurs s'appliquent à tous les tenants et à tous les modes de déploiement.

Catégorie	Shared (`live.relution.io`)	Dedicated Server
Taille maximale de téléversement	1 Go par fichier	1 Go par fichier
Limite de stockage	10 Go par tenant	100 Go par serveur
Actions par appareil et par jour	50 actions (moyenne sur 7 jours)	50 actions (moyenne sur 7 jours)

Taille de téléversement

La taille maximale de téléversement définit la taille qu'un seul fichier peut atteindre lors d'un téléversement vers le cloud.

- Sur Shared (`live.relution.io`), la limite est de 1 Go.
- Sur les serveurs dédiés, la limite est également de 1 Go. Cette limite peut être augmentée sur demande.

Si un fichier dépasse cette limite, le téléversement est refusé.

Pour la version 26.4.0

Limite de stockage

La limite de stockage définit la quantité maximale d'espace de stockage disponible pour les organisations ou les serveurs.

- Sur live.relution.io (Shared), chaque tenant dispose de jusqu'à 10 Go d'espace de stockage.
- Sur les serveurs dédiés, chaque serveur dispose de jusqu'à 100 Go d'espace de stockage.

Limite d'actions par appareil et par jour

Pour garantir la stabilité du système, le nombre d'actions par appareil et par jour est limité.

- Un maximum de 50 actions par appareil et par jour en moyenne sur 7 jours est couvert par le quota.

Si cette limite est dépassée de manière durable, le système peut appliquer des restrictions ou des limitations temporaires.

Migration vers Relution Cloud

Les installations Relution peuvent être facilement transférées vers le cloud Relution.
Pour une migration réussie, seules quelques étapes doivent être suivies et des configurations spécifiques sont nécessaires.

Conditions préalables

Les composants suivants sont nécessaires pour la migration vers le cloud Relution :

- Une sauvegarde récente de la base de données Relution
- Le compartiment de stockage S3, s'il est utilisé dans l'installation sur site existante

Ces deux composants sont fournis dans le cloud par l'équipe chargée de l'infrastructure Relution.

> L'URL de l'instance Relution utilisée jusqu'à présent doit également pointer vers la nouvelle instance cloud après la migration, généralement via une entrée DNS CNAME vers la nouvelle adresse cible (par exemple, nomclient.relution.io).

Pour la version 26.4.0

Exécution

Avant la migration, il est impératif de contacter l'assistance Relution.
Si la migration a déjà été demandée, l'équipe d'assistance dispose généralement d'un ticket correspondant, ce qui lui permet d'accompagner le processus de manière ciblée. Tout d'abord, une sauvegarde SQL de la base de données actuelle est créée et mise à la disposition de l'assistance Relution. Ensuite, la nouvelle instance cloud est configurée et la base de données est importée. La durée dépend de la taille de la base de données et peut prendre plusieurs heures.

Pendant ou après l'importation, l'entrée DNS CNAME est configurée:
l'URL précédente (par exemple relution.nomdelclient.de) renvoie alors vers la nouvelle instance cloud Relution (par exemple nomdelclient.relution.io).

Remarque: les terminaux n'ont pas besoin d'être réenregistrés après la migration. Le fonctionnement se poursuit sans interruption : tous les profils MDM, applications et certificats sont conservés.

Résumé : étapes de la migration

1. Contacter l'assistance Relution
2. Fixer un rendez-vous pour la sauvegarde et la migration
3. Mettre à disposition la base de données (et le cas échéant le bucket S3) en concertation avec l'assistance
4. Configurer l'entrée DNS CNAME vers la nouvelle instance Cloud

Sauvegardes et récupération

Cet article décrit les mesures de sauvegarde et de récupération pour les instances Cloud Dedicated → exploitées par Relution.

> Pour les instances auto-hébergées, la responsabilité des sauvegardes incombe à l'exploitant concerné.

Relution met en œuvre une stratégie de sauvegarde à plusieurs niveaux afin de garantir la disponibilité et l'intégrité des données clients. Toutes les mesures sont régulièrement vérifiées et améliorées.

Base de données

La base de données Relution fonctionne dans une configuration à haute disponibilité avec réplication automatique. Ainsi, la défaillance d'une seule instance de base de données ne devrait pas entraîner de perte de données. D'autres mesures techniques détectent et corrigent de manière proactive les problèmes au niveau matériel avant qu'ils ne puissent entraîner une perte de données.

Par ailleurs, les modifications de la base de données sont continuellement sauvegardées à l'extérieur et complétées régulièrement par des sauvegardes complètes. Cela permet une récupération à un instant précis (Point-in-Time Recovery) dans la période de conservation allant jusqu'à 90 jours.

Conformément au principe 3-2-1, les sauvegardes sont créées à l'aide de deux méthodes indépendantes, une copie étant stockée chez un prestataire indépendant sur un site géographiquement distinct. Toutes les données sont chiffrées au repos avec des clés spécifiques au client.

Pour la version 26.4.0

Stockage d'objets

Les données du stockage d'objets sont versionnées et peuvent être restaurées avec la base de données.

RPO et RTO

Indicateur	Valeur	Explication
RPO (Recovery Point Objective)	≤ 5 minutes	Dans le pire des cas, jusqu'à 5 minutes de modifications de la base de données peuvent être perdues.
RTO (Recovery Time Objective)	≤ 3 heures (pendant les heures ouvrables)	Délai cible pour restaurer le service après une panne.

Les sauvegardes sont-elles conservées séparément ?

Oui. Les sauvegardes de la base de données suivent le principe 3-2-1 ; une copie est stockée chiffrée chez un prestataire indépendant sur un site géographiquement distinct.

Puis-je demander une restauration individuelle en tant que client ?

Contacter le support Relution pour discuter d'une restauration. Sur demande, une récupération à un instant précis (Point-in-Time Recovery) dans la période de conservation est également possible. Une restauration à la demande du client est facturée.

La période de conservation peut-elle être adaptée ?

Oui. La période de conservation peut être adaptée selon les besoins (contre un supplément). Contacter le support Relution à ce sujet.

Quelles données sont couvertes par la sauvegarde ?

La sauvegarde couvre toutes les données persistantes de l'instance Relution.

Pour la version 26.4.0

Exigences du système

Le matériel suivant est nécessaire pour faire fonctionner un serveur Relution requis :

- 2 cœurs de CPU
- 4 Go de RAM
- 1 carte réseau
- 10 GiB HDD/SSD
- Espace de stockage supplémentaire pour les données de l'utilisateur, le système d'exploitation et d'autres applications et programmes

Stockage des ressources externes

Nous recommandons l'utilisation d'un stockage de ressources externe dans generel, en particulier dans les cas suivants :

- Installation et gestion des applications natives sur les appareils Windows
- Si des applications natives d'une taille supérieure à 50 Mo ou, en général, un grand nombre d'applications natives sont utilisées
- Serveurs avec plus de 5 000 appareils

Relution prend en charge la configuration d'un système de stockage séparé compatible S3 comme minIO.
Plus d'informations sont disponibles sur Installation minIO →

Pour la version 26.4.0

Matériel recommandé

En fonction du nombre d'appareils gérés, nous recommandons l'équipement matériel suivant :

- Jusqu'à 150 appareils
- 150 à 1 000 appareils
- 1 000 à 5 000 appareils
- 5 000 à 10 000 appareils
- 10 000 à 30 000 appareils
- 30 000 à 50 000 appareils

Système d’exploitation

Les systèmes d’exploitation suivants sont pris en charge :

- Alma Linux ou Rocky Linux Version 9 ou 10
- Red Hat Enterprise Linux (RHEL) version 9 ou ultérieure
- Ubuntu Server dans la version LTS actuelle

Installation de Docker (recommandée)

- Versions actuelles de Docker et de Docker Compose.

Installation native

Les logiciels suivants sont recommandés pour l’exécution d’un serveur Relution. recommandé :

- Java 21
  - AdoptOpenJDK 21 est recommandé.
- NGINX 1.8 ou plus récent
- Serveur de base de données pris en charge.

pour la version 26.4.0

Bases de données prises en charge

Relution prend en charge les serveurs de base de données suivants :

- MariaDB LTS version minimale 10.11 ou plus récente
- PostgreSQL 14.0 ou plus récent

> Les versions 10.4.9 et 10.4.10 de MariaDB contiennent un bogue sérieux qui pourrait rendre Relution inutilisable après le redémarrage du service. Utiliser MariaDB 10.4.11 ou une version supérieure, ou 10.4.8 ou une version inférieure.

Pour utiliser le portail web de Relution, l’un des navigateurs suivants est requis, dans sa dernière version :

- Chrome
- Firefox
- Safari

Appareils et plateformes gérés

- Android 7 ou version ultérieure
- iOS 15 ou ultérieur
- iPadOS 15 ou version ultérieure
- macOS 10.12 ou version ultérieure
- tvOS 12.0 ou version plus récente
- Windows 10 Professionnel/Education ou plus récent

Réseau

- Connexion directe à l'internet
- Pas de serveur proxy entre Relution et Internet
- Un certificat SSL provenant d'une autorité de certification de confiance
    - Dans la configuration standard de Relution, Traefik obtient un certificat Let's Encrypt via le port 80

Accès Internet

Les ports suivants doivent être ouverts sur le pare-feu pour les connexions entrantes et sortantes de/vers l'internet.

la version 26.4.0

Port	Type	Direction	Source	Nécessaire	Description
80	TCP	Entrant	All	Oui	Redirection vers HTTPS
443	TCP	Inbound	All	Oui	Pour l'accès à internet et la communication client-serveur
7800	TCP	Entrant/Sortant	Nœud de cluster	Oui	Nécessaire pour la communication entre les nœuds de cluster
8099	TCP	Entrant	Réseau local	Non	Nécessaire pour le suivi de l'état de santé
2197	TCP	Entrant/Sortant	Associé/Nommé	Non[1]	Services de notification push d'Apple (APNS)
443	TCP	Outbound	-	Oui	par exemple, service SMS, serveur de licences, VPP, DEP, ...
123	UDP	Outbound	-	Yes	NTP (serveur de temps)

[1] Requis pour la communication entre les appareils iOS et Apple Push Notification Services (APNS) jusqu'à la version 4.70. Requis comme solution de repli dans les versions ultérieures.

Exigences réseau Apple

Pare-feu Si le pare-feu prend en charge les noms d'hôtes, il est possible d'utiliser la plupart des services Apple en autorisant les connexions sortantes vers `*.apple.com`. Si le pare-feu ne peut être configuré qu'avec des adresses IP, autoriser les connexions sortantes vers les plages d'adresses IP suivantes appartenant à Apple, en fonction de la version IP.

```
Pour IPv4, vous pouvez autoriser les connexions sortantes vers 17.0.0.0/8.
Pour IPv6, vous pouvez autoriser les connexions sortantes vers les plages réseau
suivantes:
2403:300::/32
2620:149::/32
2a01:b740::/32
```

Proxy HTTP L'utilisation des services Apple via un proxy nécessite d'appliquer `désactiver l'inspection des paquets` ainsi que l'authentification pour le trafic entrant et sortant vers les hôtes listés. Les exceptions à cette règle sont mentionnées ci-dessus. Toute tentative d'inspecter le contenu des communications cryptées entre les appareils Apple et les services entraînera une perte de connexion pour garantir la sécurité de la plateforme et la confidentialité des utilisateurs. Exigences réseau Apple →

Exigences réseau Google

Exigences réseau Google →

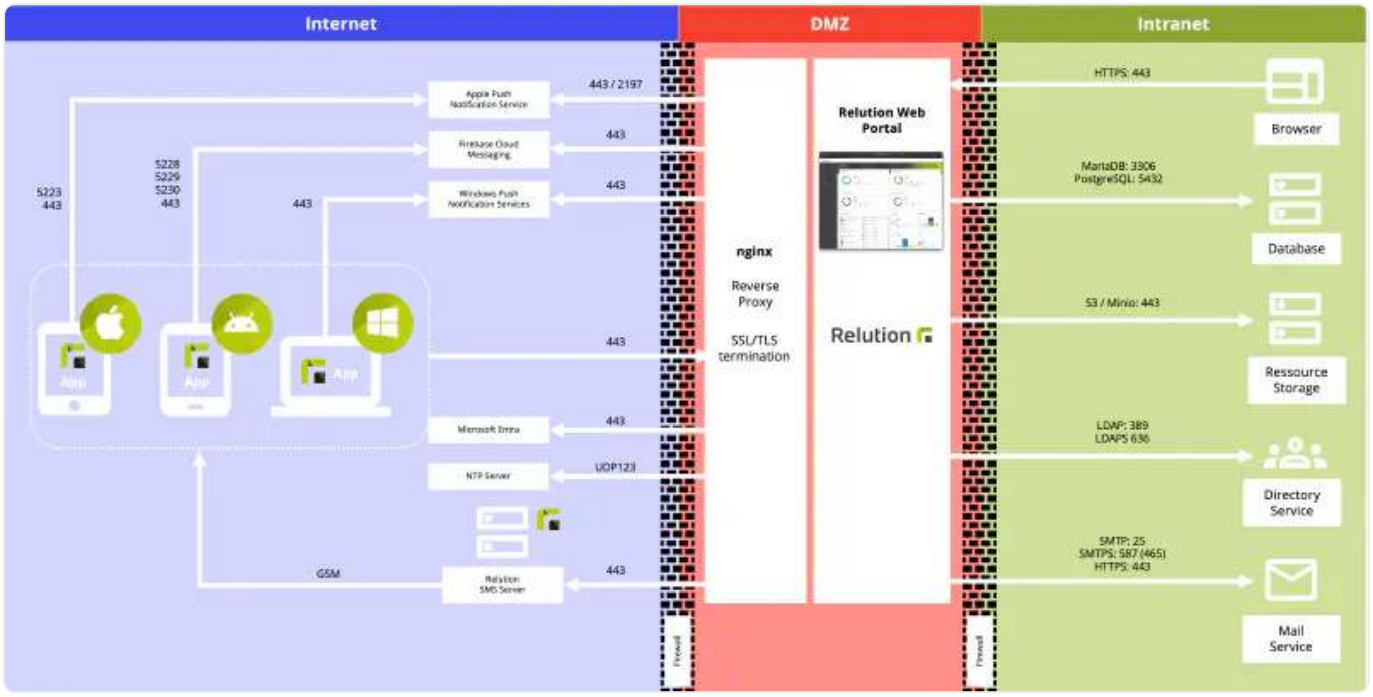
Pour la version 26.4.0

Réseau interne

Le service Relution utilise ces ports pour communiquer avec des services externes (base de données, service d'annuaire, serveur de messagerie). La configuration exacte dépend des services utilisés et du fait que les services fonctionnent sur des serveurs séparés (recommandé).

Si les serveurs se trouvent sur le même réseau, aucune configuration supplémentaire du pare-feu n'est nécessaire. Tous les ports sont des ports TCP.

Port	Description
25	Serveur de messagerie (SMTP)
389	Service d’annuaire (LDAP)
587	Serveur de messagerie (SMTPS)
636	Service d’annuaire (LDAPS)
3306	MariaDB/MySQL
5432	PostgreSQL



Appareils mobiles

Lorsque les appareils mobiles sont connectés aux réseaux internes, des ports entrants et sortants supplémentaires doivent être ouverts pour que les appareils puissent se connecter aux serveurs Apple, Microsoft ou Google afin de recevoir des messages push. Pour communiquer avec Relution, le port HTTPS par défaut 443 est nécessaire. En fonction des fonctionnalités à utiliser sur les appareils, des ports supplémentaires peuvent être nécessaires, qui peuvent être trouvés dans la documentation du fabricant. Lorsque les appareils sont connectés aux données mobiles, aucune configuration supplémentaire n’est nécessaire.

Liens connexes :

- Utiliser les produits Apple sur les réseaux d’entreprise →
- Ports TCP et UDP utilisés par les logiciels Apple →
- Apple technotes →
- Apple Classroom →
- Firebase Cloud Messaging →
- Firebase Cloud Messaging ASN of 15169 →

Port	Type	Direction	Description
443	TCP	Outbound	HTTPS, par exemple Relution, Google FCM, Microsoft WNS, Apple Push Notification Service,…
443	UDP	Outbound	QUIC, e.g. iCloud Private Relay, Google services
5223	TCP	Inbound/Outbound	Service de notification push d’Apple[1]
5228-5230	TCP	Outbound	Google Firebase Cloud - Firebase Cloud Messaging (FCM)
3283	TCP	Inbound/Outbound	Apple Remote Desktop (par ex. Apple Classroom App)
3283	UDP	Inbound/Outbound	Apple Remote Desktop (par ex. Apple Classroom App)
3284	TCP	Entrant/Sortant	Partage de documents Apple Classroom
3285	TCP	Inbound/Outbound	Apple Classroom App

Pour la

Avant l'installation

Avant de commencer l’installation, il est recommandé de consulter cette liste de contrôle afin de vérifier que l’infrastructure répond aux exigences minimales et qu’elle est correctement configurée.

Il est possible d’héberger plusieurs services sur la même machine (pour des raisons de sécurité, nous recommandons d’héberger chaque service sur un serveur distinct).
Par exemple: il est possible d’héberger plusieurs services sur la même machine : Si Relution et le proxy inverse `nginx` sont installés sur la même machine, `le serveur qui exécute Relution` et `le serveur qui exécute nginx` se réfèrent à la même machine physique. Dans ce cas, le serveur doit répondre aux exigences des deux services.

Matériel

Le serveur qui exécute Relution a les exigences minimales suivantes →.

Système d’exploitation

Le serveur sur lequel Relution est exécuté utilise un système d’exploitation recommandé → la version du système d’exploitation est conforme ou supérieure à la version minimale prise en charge.

Pour la version 26.4.0

Base de données

Le serveur sur lequel Relution s’exécute dispose d’un accès réseau à un serveur de base de données pris en charge. Ce guide contient des instructions sur l’installation de MariaDB si un nouveau serveur de base de données doit être installé.

Infrastructure réseau

Le serveur qui exécute le proxy inverse `nginx` est configuré pour héberger un service disponible sur Internet. Il possède une adresse IP publique et un nom DNS public par exemple `mdm.example.com`. Lorsque des services sont hébergés sur plusieurs serveurs internes, ils peuvent résoudre leurs noms d’hôte respectifs.

L’adresse IP publique doit être statique. Les adresses IP dynamiques ne sont pas prises en charge. Exceptions : Le serveur est hébergé par un fournisseur de services en nuage, comme Amazon Web Services (AWS) ou Microsoft Azure, qui fournit l’infrastructure DNS nécessaire.

Exigence

- Le serveur dispose d'un accès direct à l'internet
- Le serveur dispose d'une adresse IP statique
- Le serveur dispose d'un nom DNS public
- Le DNS interne est correctement configuré et fonctionne

Configuration du pare-feu

Le pare-feu est configuré pour accepter les requêtes HTTP(S) entrantes provenant d'appareils mobiles et de navigateurs web.

Requête

- Le reverse proxy est accessible depuis l'Internet via HTTP (80)
- Le proxy inverse est accessible depuis l'internet via HTTPS (443)
- Relution peut se connecter à l'Internet (80, 443, 5223, 123 UDP)
- Relution peut se connecter au serveur SMTP
- Relution peut se connecter au serveur de base de données.
  En option:
- Relution peut se connecter à LDAP via le port 389 ou 636.

Pour la version 26.4.0

Certificats

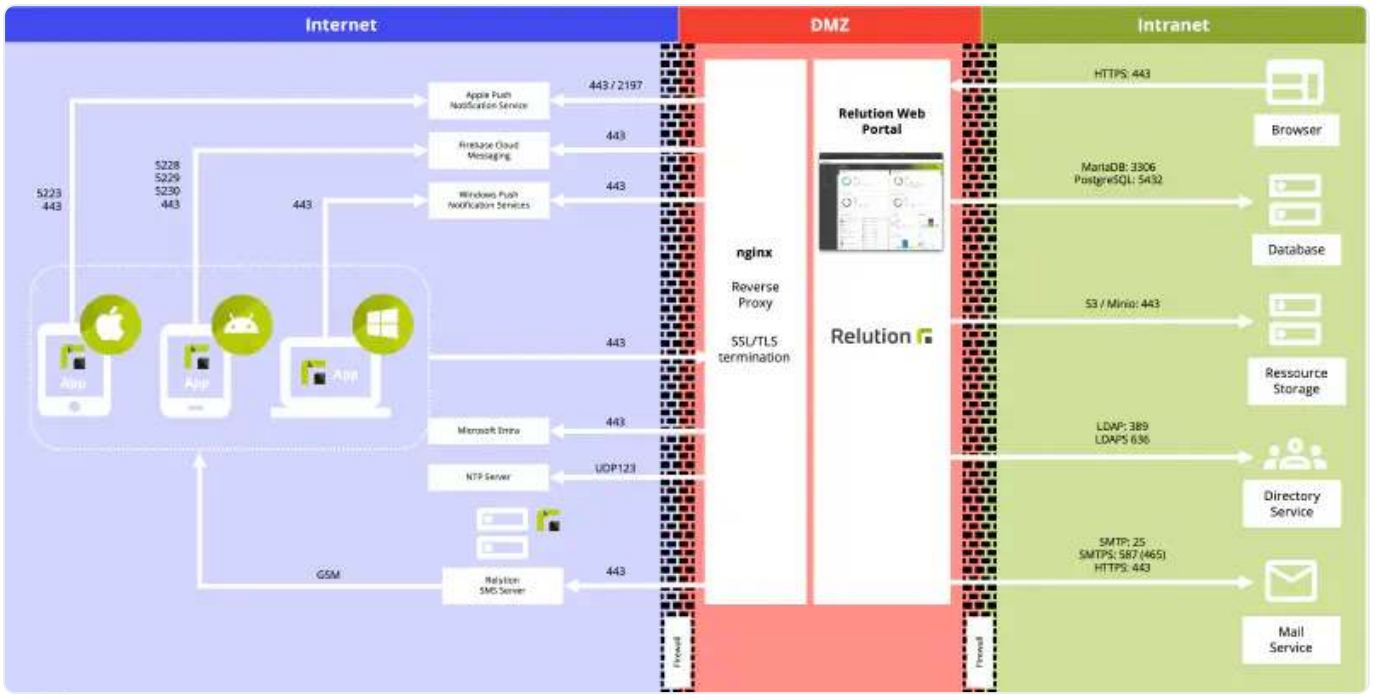
Le protocole HTTPS nécessite un certificat SSL valide délivré par une autorité de certification (CA) de confiance.

- Les certificats auto-signés ne fonctionnent pas, car les appareils mobiles ne leur font pas confiance par défaut
- Les certificats de Let's Encrypt → fonctionnent et sont gratuits.

Une liste des autorités de certification connues, basée sur la part de marché et l'utilisation, est disponible sur W3Techs →.

...

> Relution est livré avec un certificat APNS valide qui est utilisé. Dans ce cas, le certificat sera également mis à jour lors de la mise à jour de Relution. La mise à jour automatique pour les propres certificats APNS utilisés n'est pas disponible et doit être organisée séparément.



Pour la version 26.4.0

Docker (Recommandé)

Ce guide s'applique à Rocky / Alma Linux 9 et 10 ainsi qu'à Ubuntu Server (version LTS actuelle).
(État Déc. 2025). Nous recommandons l'utilisation de Linux pour le système hôte.

Ce guide couvre l'installation et la configuration d'une instance Relution de base, qui s'exécute dans des conteneurs Docker.

Prérequis

Avant de commencer, s'assurer que les exigences suivantes sont remplies :

- La machine hôte peut se connecter à Internet.
- Disposer des droits `root` ou `sudo`.
- Optionnel : Un certificat SSL valide pour l'URL.

> Les certificats auto-signés ne fonctionnent pas, car les appareils mobiles ne leur font pas confiance. Il est possible d'installer manuellement le certificat racine sur un appareil, mais cette procédure n'est pas recommandée en raison de l'effort considérable. Les certificats de Let's Encrypt → ont été testés et fonctionnent.

Pour la version 26.4.0

Préparation

En cas de familiarité avec `vim`, il peut être défini comme éditeur par défaut. Ignorer cette section pour continuer à utiliser l'éditeur standard.

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

Aperçu

L'installation est divisée en étapes principales suivantes :

1. Installer Docker et Docker Compose.
2. Configurer les Conteneurs.
3. Configurer Traefik ou nginx.

Installation de Docker et Docker Compose

Pour exécuter Relution dans un conteneur Docker, `Docker` et `docker compose` doivent d'abord être installés.

Installer Docker

Suivre ces commandes pour 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
```

Pour Ubuntu Server, les commandes suivantes s'appliquent (dépôt Docker selon la documentation Docker →) :

```
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
```

S'assurer de démarrer et d'activer le service Docker après l'installation afin qu'il soit disponible après un redémarrage du système.

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

Les images minimales et cloud de RHEL, AlmaLinux et Rocky Linux 10 (EL10) ne contiennent pas le paquet `kernel-modules-extra`, ce qui empêche le service Docker de démarrer. Dans ce cas, exécuter les étapes décrites dans Docker ne démarre pas sur EL10 → avant le premier démarrage de Docker. Sur EL9, cela n'est pas nécessaire.

Configuration des Conteneurs

Créer un répertoire pour les fichiers de configuration Relution, par exemple pour `docker compose`.

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

compose.yaml

Télécharger le fichier :

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

Modifier le fichier :

```
vim /opt/relution/compose.yaml
```

Adapter le fichier à l'environnement. Au moins l'espace réservé suivant doit être remplacé :

Demande	Satisfait
Un certificat SSL et une clé valides sont disponibles	

Espace Réservé	Description
`%POSTGRES_PASSWORD%`	Le mot de passe de l'utilisateur de la base de données Relution

application.yml

Télécharger le fichier :

```
wget https://raw.githubusercontent.com/relution-io/relution-setup/master/docke
    --directory-prefix=/opt/relution
```

Modifier le fichier :

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

Adapter le fichier à l'environnement. Les espaces réservés suivants doivent être remplacés :

26.4.0

Espace Réservé	Description
`%EXT_HOSTNAME_URL%`	L'adresse externe du serveur Relution, par exemple `https://mdm.example.com`
`%POSTGRES_PASSWORD%`	Le mot de passe de l'utilisateur de la base de données Relution
`%SYSTEM_ADMIN_PASSWORD%`	Le mot de passe initial de l'administrateur système. À changer après la première connexion, puis à supprimer de cette ligne.
`%SYSTEM_ADMIN_EMAIL%`	L'adresse e-mail de l'administrateur système

Remarque sur les Mots de Passe : Le fichier Compose définit trois services : `database`, `relution` et `traefik`. Utiliser des mots de passe aléatoires sécurisés pour les mots de passe (par exemple, avec `pwgen -snc 48 1`). En cas de remplacement de l'espace réservé du mot de passe dans un conteneur (par exemple, `%POSTGRES_PASSWORD%`), s'assurer d'utiliser le même mot de passe dans l'`application.yml`.

Persistance des Données : La configuration standard mappe les répertoires de données PostgreSQL au système hôte. Relution stocke toutes ses données dans la base de données, aucune configuration supplémentaire n'est donc requise. S'assurer d'inclure PostgreSQL dans la stratégie de sauvegarde.

Configuration de Traefik (Proxy Inverse)

Traefik est utilisé comme proxy inverse pour permettre l'accès à Relution tout en fournissant le chiffrement SSL/TLS. Sans Traefik ou un proxy similaire, l'accès à Relution n'est possible que localement via localhost.

Création Automatique de Certificats (Let's Encrypt)

Télécharger le fichier de configuration Traefik et l'adapter à l'environnement :

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

Dans le fichier `/opt/relution/configs/traefik/relution.yaml`, l'espace réservé `external.url` doit être remplacé par l'URL externe réelle sous laquelle Relution doit être accessible :

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

```
http:
  routers:
    relution:
      rule: Host(`external.url`) # Remplacer l'espace réservé
```

L'URL externe ici est spécifiée sans le préfixe `https://`, contrairement à l'`application.yml`.

Démarrage de Relution

Accéder au répertoire Relution et démarrer les conteneurs Docker :

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

Ceci téléchargera les images et démarrera les services. Il faudra peut-être un certain temps avant que les services ne soient disponibles.

Pour afficher la sortie du journal d'un conteneur spécifique (par exemple, Relution) :

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

Arrêt

Pour arrêter et supprimer les conteneurs (les images sont conservées) :

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

Statiques traefik Certificats

Télécharger le fichier de configuration pour les certificats statiques :

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

Dans le fichier `/opt/relution/configs/traefik/relution.static_cert.yaml`, l'espace réservé `external.url` doit être remplacé par l'URL externe réelle sous laquelle Relution doit être accessible :

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

```
http:
  routers:
    relution:
      rule: Host(`external.url`) # Remplacer l'espace réservé
```

La chaîne de certificats et la clé privée correspondante doivent être placées sous `server.pem` et `server.key` dans le répertoire `/opt/relution/certs/static`.

De plus, le bloc `traefik:` dans le `compose.yml` doit être ajusté :

```
...
  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 comme Alternative à Traefik (Proxy Inverse)

> Nginx est utilisé comme proxy inverse pour permettre l'accès à Relution tout en fournissant le chiffrement SSL/TLS. Sans Nginx ou un proxy similaire, l'accès à Relution n'est possible que localement via localhost.

Télécharger le fichier de configuration nginx :

```
wget https://raw.githubusercontent.com/relution-io/relution-setup/master/docke
    --directory-prefix=/opt/relution
```

Remplacer le bloc `traefik:` dans le `compose.yaml` par ce bloc `nginx:` :

```
  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.co
      - "/opt/relution/server.pem:/etc/nginx/server.pem"
      - "/opt/relution/server.key:/etc/nginx/server.key"
```

Pour une sécurité accrue, l'utilisation de meilleurs paramètres DH est recommandée.

1. Générer la clé :

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

2. Ajuster `relution-nginx.conf` : Ajouter la ligne (et activer `ssl_stapling` si nécessaire) :

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

3. Étendre les Volumes `compose.yaml` : Ajuster les `Volumes` du conteneur nginx pour inclure les paramètres DH :

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

La configuration s'attend à ce que le certificat SSL et la clé se trouvent dans `/opt/relution/server.pem` et `/opt/relution/server.key`. Sinon, ajuster les `Volumes` du conteneur nginx en conséquence.

Conversion du Certificat SSL →

Pour la version 26.4.0

En cas d'utilisation de la Secure Mail Gateway, le chemin `/Microsoft-Server-ActiveSync` dans la configuration nginx doit pointer vers le service SMG et non vers Relution. Voir Secure Mail Gateway →.

Si nginx (ou un autre reverse proxy) s'exécute sur un serveur différent de celui de Relution, cela peut entraîner, à partir de Relution 26.4.0, le message `L'accès est interdit` lors de la connexion, car la requête du proxy n'est par défaut pas considérée comme fiable. De plus, l'en-tête `proxy_set_header X-Forwarded-Proto $scheme;` doit être correctement défini dans la configuration nginx. Pour la solution, voir Connexion : L'accès est interdit →.

Mise à Jour de Relution

Pour mettre à jour les services, utiliser les commandes suivantes :

```
cd /opt/relution/
docker compose pull # Télécharge la dernière image
docker compose up -d # Arrête et redémarre les conteneurs
```

Le service Relution ne sera pas disponible tant que le redémarrage du conteneur ne sera pas terminé.

En cas de problèmes de démarrage avec Relution, envoyer le journal complet sous forme de fichier Zip au support. Le support est payant.

Pour la version 26.4.0

SSL Certificates - Certbot

Certbot est une solution gratuite pour l'émission de certificats SSL/TLS via Let's Encrypt, qui permet une connexion HTTPS sécurisée pour les sites web. Par rapport aux fournisseurs payants, qui impliquent souvent un travail administratif supplémentaire et des coûts récurrents, Certbot offre une alternative automatisée et gratuite qui simplifie la gestion des certificats et prend en charge les renouvellements continus.

Installation

Il est recommandé d'installer Certbot → nativement sur l'hôte, d'obtenir des certificats une fois via Certbot et de l'intégrer en tant que volume dans le conteneur nginx.

1. Installer Certbot

Prérequis: → ALMA / Rocky Linux ou Ubuntu Server comme hôte → Docker installé selon les instructions → Relution configuré selon les instructions

Sous Alma / Rocky Linux, Certbot s'installe avec la commande suivante :

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

Sous Ubuntu Server :

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

2. Arrêter Nginx

Nginx doit être arrêté temporairement car Certbot en mode `--standalone` démarre brièvement son propre serveur web sur le port 80.

our la version 26.4.0

```
docker stop docker_nginx
```

3. Créer un certificat

Démarrer Certbot et suivre les instructions de l'assistant.

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

4. Ajuster le chemin du certificat

Dans `docker-compose.yml`, le chemin vers les certificats SSL créés doit être ajusté.

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

> Si Nginx est démarré avec les volumes (chemin vers les certificats) dans le fichier docker-compose.yml et que les certificats ne sont pas présents, Docker créera des dossiers au lieu de fichiers. Ces dossiers doivent être supprimés pour que les certificats puissent être créés au démarrage de Docker.

5. Démarrer le conteneur Docker

Si les certificats sont créés avec succès, tous les conteneurs peuvent être démarrés et vérifiés.

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

6. Pré- et post-hooks

Pour le renouvellement, des pre- et post-hooks peuvent être configurés dans Certbot pour arrêter puis redémarrer le conteneur nginx. Les hooks ne sont exécutés que si Certbot détermine, lors de l'appel à Renwal, que les certificats doivent effectivement être remplacés. Certbot est généralement configuré pour s'exécuter deux fois par jour et vérifier si un remplacement est nécessaire. Les certificats sont valables pendant 90 jours.

En fonction du système hôte, Certbot devrait déjà mettre en place automatiquement un renouvellement (par exemple sous la forme d'un service systemd + timer). L'appel peut alors être étendu en conséquence par ces crochets, par exemple

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

Les pre- et post-hooks seraient alors en conséquence :

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

Les hooks peuvent également pointer vers des fichiers de script qui contiennent l'appel réel, ce qui est généralement plus clair.

Important: Lors du premier essai, il est toujours recommandé d'utiliser `--dry-run` afin que Let's Encrypt ne soit pas bloqué pendant plusieurs jours par un trop grand nombre de tentatives ratées. Dans un environnement productif, cela doit bien sûr être supprimé, sinon il n'y aura pas de certificat.

Docker - 1000 à 5000 appareils

Pour un nombre d'appareils compris entre 1000 et 5000, il est recommandé d'exploiter le serveur d'application et le serveur de base de données séparément.

La configuration de base des serveurs ainsi que l'installation des paquets logiciels requis sont décrites en détail dans le Guide d'installation Docker général →.

Ce guide décrit les fichiers de configuration nécessaires avec des commentaires explicatifs pour faciliter l'adaptation, et vient en complément du guide d'installation Docker général.

Exigences matérielles et architecture

1x Serveur d'application

- 2 cœurs CPU
- 4 Go de RAM
- Environ 30 Go d'espace disque SSD

1x Serveur de base de données

- 4 cœurs CPU
- 8 Go de RAM
- Environ 100 Go d'espace disque SSD

Pour la version 26.4.0

Serveur App

Le serveur d'applications nécessite les deux fichiers suivants.

compose.yaml

```
services:
  relution:
    image: relution/relution:latest
    restart: unless-stopped
    container_name: relution
    environment:
```

```
      TZ: "Europe/Berlin"
    expose:
      - "8080"
      - "8099"
    ports: # Extern freigegebener Port der Applikation zum testen // deaktivie
      - "8080:8080" # Extern freigegebener Port der Applikation zum testen //
    volumes:
      - "./application.yml:/opt/relution/application.yml"

networks:
  relution-network:
```

application.yml

```
relution:
  system:
    admin:
      password: $Platzhalter # Initiales Passwort hier setzen und nach der ers
      email: $Platzhalter # Alternative zum Benutzernamen "Admin" und zum zurü
  server:
    externalURL: https://$Platzhalter # Ersetzen durch die URL unter der der S
  database:
    type: postgresql
    url: jdbc:postgresql://$Platzhalter:5432/relution?currentSchema=public # I
    username: relution # Benutzername der Datenbank
    password: $Platzhalter # Passwort der relution Datenbank = POSTGRES_PASSWO
```

Le mot de passe indiqué dans l'application.yml sera de nouveau nécessaire par la suite lors de la configuration de la base de données dans le compose.yaml

Serveur DB

Un fichier compose distinct est utilisé pour le serveur de base de données.

compose.yaml

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

volumes:
  postgresql:

networks:
  relution-network:
```

Surveillance avec Grafana

Relution fournit une variété de métriques qui peuvent être visualisées à l'aide de Grafana. Ci-dessous, nous avons fourni une configuration de base pour une installation Docker et deux tableaux de bord. Ces configurations peuvent être adaptées selon les besoins spécifiques.

> Prometheus, Grafana et les tableaux de bord individuels ne sont pas maintenus par Relution Support.

Activer les métriques Prometheus dans Relution

Depuis Relution 26.4, Relution n'expose par défaut que le point de terminaison health pour des raisons de sécurité ; le point de terminaison Prometheus (`/actuator/prometheus`) est désactivé. Pour que les métriques soient disponibles, la section suivante doit être ajoutée au fichier de configuration `application.yml` du serveur Relution :

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

Un redémarrage du serveur Relution est nécessaire pour que la modification prenne effet.

Fichiers et répertoires nécessaires

Comme indiqué, les configurations sont disponibles et peuvent être téléchargées ici →.

Fichiers

- docker-compose.yml
  - Contient les configurations des conteneurs Docker `Prometheus` et `Grafana`.
- prometheus.yml
  - Contient la configuration de `Prometheus`.
- .env
  - Contient les variables `GF_SECURITY_ADMIN_USER` et `GF_SECURITY_ADMIN_PASSWORD`. Pour un fonctionnement productif, il est recommandé de changer le mot de passe.

Sous-dossier

- Tableaux de bord Exemples de tableaux de bord : Les fichiers de configuration pour deux exemples de tableaux de bord sont inclus. Ces tableaux de bord sont automatiquement importés dans le conteneur Grafana Docker.
- Provisionnement Configurations de base : Les fichiers de configuration pour la source de données Prometheus et les deux exemples de tableaux de bord sont inclus. Ces configurations peuvent être adaptées selon les besoins.

Pour la version 26.4.0

Intégration du fichier docker-compose.yml

Le fichier docker-compose.yml décrit ici peut être utilisé de deux manières :

- Autonome Le fichier peut être utilisé en tant que fichier autonome.
- Contenu Le contenu du fichier peut être inclus dans un fichier docker-compose.yml existant.

Dans notre exemple, le contenu du fichier est inclus dans le fichier `docker-compose.yml` existant. Dans ce cas, il est important que les fichiers et les répertoires des volumes soient à l'endroit approprié et aient les permissions correctes. Dans notre `docker-compose.yml`, les conteneurs mariadb, Relution et nginx sont présents, donc les lignes deux à quatre n'ont été insérées que pour l'orientation.

> Show full configuration example

Dans le fichier `docker-compose.yml`, les ports pour Prometheus et Grafana sont définis à 9090 et 3000 respectivement. Cette section peut être insérée dans le fichier `docker-compose.yml` existant pour l'exemple.

Ajustement du fichier .env

Pour des raisons de sécurité, il est recommandé d'ajuster le paramètre password.

```
GF_SECURITY_ADMIN_USER=admin
GF_SECURITY_ADMIN_PASSWORD=motdepasse
```

Paramètres de la base de données prometheus.yml

```yaml
global:
 # Intervalle d'analyse par défaut
  scrape_interval: 15s

scrape_configs:
 # Job pour récupérer les métriques Prometheus
  - job_name: "prometheus"
    scrape_interval: 5s
    static_configs:
      - targets: ["localhost:9090"]

  - job_name: "relution"
 # Job pour récupérer les métriques de l'application
    metrics_path: "/actuator/prometheus"
    scrape_interval: 5s
    static_configs:
 # Appeler le docker host à l'intérieur du conteneur
      - targets: ["relution:8099"]
```

Dans notre configuration concrète, la dernière ligne doit contenir le nom du conteneur et le port 8099, dans ce cas `relution:8099`. Avec la commande `docker ps`, le nom et le port du conteneur utilisé peuvent être vérifiés et ajustés si nécessaire. Lorsque les conteneurs sont téléchargés et démarrés avec `docker compose down` ou docker `compose up -d`, l'interface Grafana est accessible sous `IP du serveur` et `port 3000`. Deux tableaux de bord sont maintenant disponibles.

Tableaux de bord

Tableau de bord du serveur Relution :

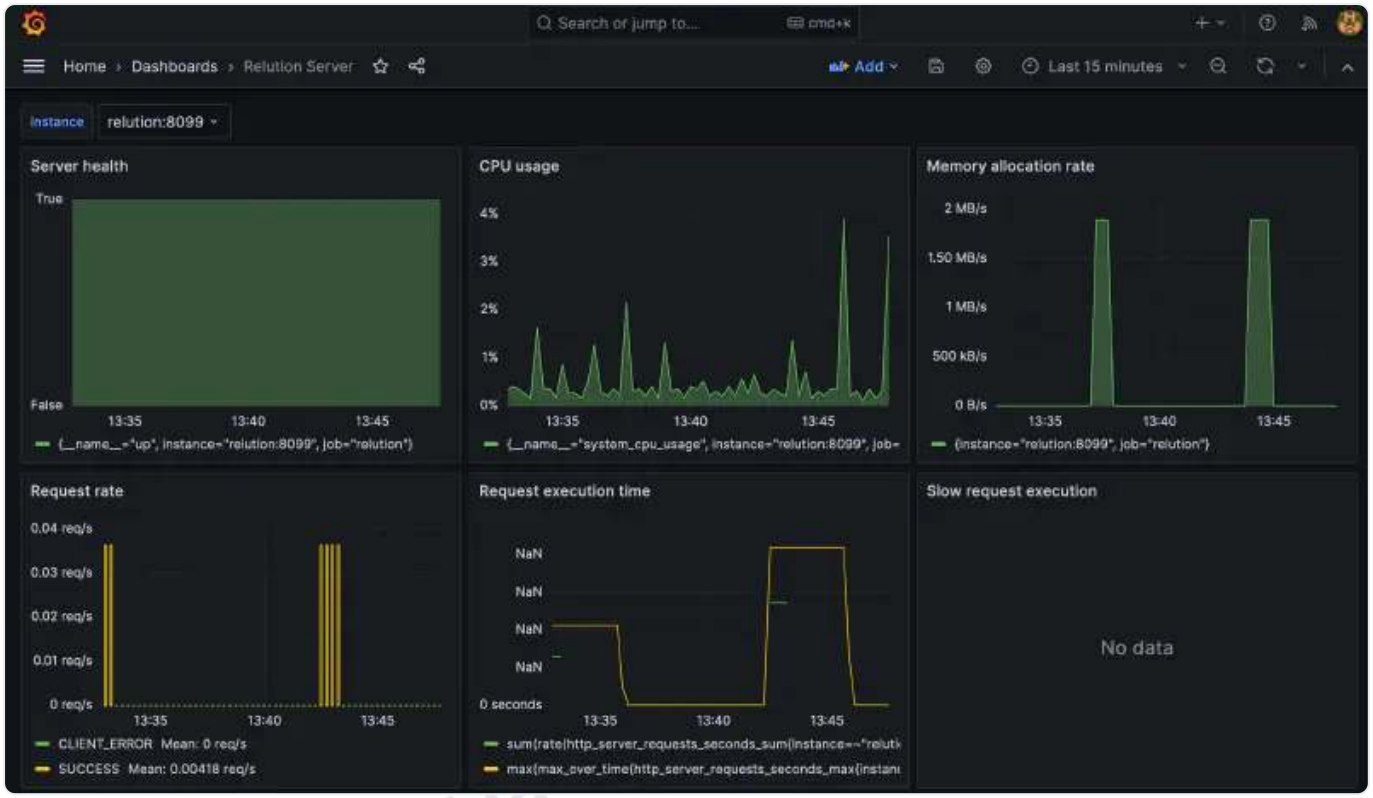


Tableau de bord par défaut de Spring Boot :



Voici la configuration et le guide SSH traduits en français, structurés en Markdown.

Pour la version 26.4.0

Configuration pour Serveur Distant

Dans ce scénario, Grafana est également exploité via un conteneur Docker. Des ajustements spécifiques sont nécessaires pour lire correctement les métriques. La différence majeure avec la configuration locale est que ce setup communique avec l'instance Relution via HTTPS.

Préparation dans Relution

Avant de démarrer les conteneurs, un utilisateur correspondant doit être créé dans Relution :

- Organisation : L'utilisateur doit impérativement être créé au sein de l'Organisation Globale.
- Autorisation : Attribuer à l'utilisateur le droit Health Check (ou État du système).
- Authentification : L'accès doit se faire via Basic Authentication.
- Les comptes utilisateurs avec OIDC (Single Sign-On) ne fonctionnent pas pour cet usage.
- L'authentification multifacteur (MFA) doit être désactivée pour ce compte.

Téléchargement et Extraction

Télécharger les fichiers de configuration préparés :
Grafana Setup →

Extraire l’archive dans le répertoire choisi sur le serveur cible.

Adaptation des fichiers de configuration

Fichier : compose.yml

Modifier les variables d’environnement pour l’accès administratif à l’interface Grafana :

- `GF_SECURITY_ADMIN_USER` : Le nom d’utilisateur administrateur choisi.
- `GF_SECURITY_ADMIN_PASSWORD` : Un mot de passe sécurisé pour la connexion à Grafana.

Fichier : prometheus.yml

Ce fichier définit la connexion à l’interface Relution. Remplacer les espaces réservés par les données spécifiques :

Paramètre	Description
`$SERVER_URL`	L’URL externe du serveur Relution (important : sans le préfixe `https://`).
`username`	Le nom d’utilisateur créé à l’étape 1 dans Relution.
`password`	Le mot de passe correspondant de l’utilisateur.

Déploiement

Une fois la configuration terminée, les conteneurs peuvent être démarrés. Exécuter la commande suivante dans le répertoire :

```
docker compose up -d
```

Remarques sur l’accès :

- Grafana est accessible par défaut via le port 3000.
- Selon la sécurisation du serveur, l’accès est possible directement via l’IP/domaine ou de manière sécurisée via un tunnel SSH.

Pour accéder à Grafana en toute sécurité via un tunnel SSH, la redirection de port peut être utilisée. Ceci est particulièrement utile si le port 3000 est bloqué par le pare-feu du serveur.

Établir le tunnel SSH

Exécuter la commande suivante dans un terminal local (Windows PowerShell, macOS ou Linux) :

```
ssh -L 3000:localhost:3000 nom_utilisateur@ip-de-votre-serveur
```

Explication des paramètres :

- `-L 3000:localhost:3000` : Redirige le port 3000 de la machine locale vers le port 3000 du serveur distant.
- `nom_utilisateur` : L'utilisateur SSH sur le serveur.
- `ip-de-votre-serveur` : L'adresse IP ou le nom d'hôte du serveur distant.

Accès à l'interface

1. Laisser la fenêtre du terminal avec la connexion SSH active ouverte.
2. Ouvrir un navigateur web.
3. Saisir dans la barre d'adresse : `http://localhost:3000`
4. Se connecter avec les identifiants définis dans le fichier `compose.yml` (`GF_SECURITY_ADMIN_USER` et `GF_SECURITY_ADMIN_PASSWORD`).

Pour la version 26.4.0

Relution Files Bridge

L'application Relution Files pour iOS et Android peut accéder à des partages SMB et WebDAV. La Relution Files Bridge permet de mettre à disposition des partages SMB ou DFS sous forme de WebDAV. La Relution Files Bridge peut être exploitée confortablement en tant que conteneur Docker.

Installation

Sur le serveur destiné à être utilisé comme Relution Files Bridge, créer dans le répertoire `/opt/rfb` un fichier compose.yml et y ajouter ce contenu :

```
services:
  relution-smb-bridge:
 # Bitte schauen Sie auf https://hub.docker.com nach der aktuellen Versionsnum
    image: relution/relution-smb-bridge:1.0.1
    restart: unless-stopped
    ports:
      - '8080:8080'
    environment:
      TZ: "Europe/Berlin"
```

Exploitation avec https

Si la connexion doit également être établie via https, il est possible de placer un reverse proxy devant la Files Bridge. Celui-ci peut également être exploité dans le même fichier compose.yaml. Dans l'exemple, un Traefik est utilisé.

Le fichier devrait alors ressembler à ceci :

> Show full configuration example

Utiliser comme fichier de configuration pour Traefik le même fichier que celui utilisé pour l'exploitation de Relution, et l'adapter en conséquence :

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

Adapter la ligne 4 avec l'adresse externe et la ligne 15 avec le nom du conteneur `relution-smb-bridge` en conséquence.

Démarrage et exploitation

Démarrer les conteneurs avec :

```
docker compose up -d
```

Accès au partage

Pour la version 26.4.0

Si le partage DFS utilisait un chemin tel que `smb://mein-fileserver.intra/data`, la configuration dans Relution Files doit être la suivante :

1. Nom : au choix
2. Protocole : WebDAV
3. Chemin : https://adresse-des-relution-files-bridge-servers/mein-fileserver.intra/data
4. Nom d'utilisateur : Domaine\Utilisateur
5. Mot de passe

La Relution Files Bridge transmettra alors la requête, reçue en tant que requête WebDAV, au serveur sous forme de requête SMB / DFS.

Cluster HA (avancé)

Pour installer Relution dans une configuration de haute disponibilité, il est possible de mettre en place un cluster. Dans ce cluster, plusieurs instances Relution (nœuds d'application) sont démarrées et se connectent toutes à la même base de données. Un équilibreur de charge doit distribuer le trafic vers ces nœuds en utilisant la méthode round-robin.

> La configuration d'un cluster à haute disponibilité ne doit être entreprise que par des administrateurs expérimentés.

Prérequis

Pour établir un cluster, toutes les instances Relution doivent résider sur le même réseau. Les nœuds doivent pouvoir communiquer entre eux via leur nom d'hôte et le port TCP 7800. Pour plus d'informations, se référer aux conditions requises pour le réseau →.

Toutes les instances de Relution doivent utiliser les mêmes fichiers de configuration (par exemple, `application.yml`) ou les mêmes variables d'environnement. La seule exception est lorsque le nom d'hôte ne peut pas être déterminé, auquel cas la variable d'environnement `EXTERNAL_IP` peut être utilisée pour définir l'adresse IP de l'instance à travers laquelle d'autres instances Relution peuvent y accéder.

Pour la version 26.4.0

Fonctionnalité

Lorsqu'une instance Relution est démarrée, elle se connecte à la base de données et écrit son nom d'hôte dans la table `JGROUPSPING`. Par la suite, toutes les entrées de la table sont chargées et l'instance établit une connexion avec d'autres instances via le port TCP 7800. L'état du cluster est régulièrement contrôlé via la table de la base de données. Si une instance devient inaccessible, ses entrées sont supprimées de la base de données.

Vérification de l'état de la grappe

Il existe plusieurs façons de vérifier l'état de la grappe.

1. Portail du système

Pour un environnement en grappe, nous recommandons d'activer le portail système. Le portail système fournit une vue d'ensemble des nœuds enregistrés dans la grappe. Pour qu'il fonctionne pleinement, il faut que les nœuds communiquent entre eux via le port `8099`. Pour plus de détails sur l'activation du portail système et l'exposition des points de terminaison actuator, voir Activation du portail système →.

2. Point de terminaison métrique

Il est possible de vérifier la métrique `counter_cluster_size_total` en accédant au point de terminaison de l'API pour Prometheus à l'adresse `https://127.0.0.1:8099/actuator/prometheus`. Cette métrique indique le nombre de nœuds enregistrés avec succès dans le cluster. Depuis Relution 26.4, ce point de terminaison requiert d'être activé dans `application.yml` sous `management.endpoints.web.exposure.include` (par exemple `prometheus` ou `metrics`), voir Activation des points de terminaison actuator →.

Pour la version 26.4.0

Relution Shield (Add-on)

Relution Shield permet un accès sécurisé depuis Internet à l'intranet interne de l'organisation et combine réseau privé virtuel (VPN), infrastructure à clé publique (PKI) et UEM - MDM. Pour plus d'informations : Relution Shield →.

Pour la mise à niveau depuis Relution Shield 1.x, voir Mise à niveau de 1.x vers 2.x →

Conditions préalables

> L'installation de Relution Shield est exigeante et demande de l'attention et du temps. Vérifier soigneusement les commandes et les configurations avant de les enregistrer – porter une attention particulière aux variables qui doivent être définies.

Pour la version 26.4.0

Serveur d'application Relution

Le serveur d'application Relution existant, sur lequel Relution Shield est configuré et les profils VPN des appareils sont gérés.

1. Serveur Relution (version 5.26+)
2. Une organisation cible sur le serveur avec une licence Relution Shield

Serveur Relution Shield

Un serveur séparé sur lequel Relution Shield est installé en tant que composant VPN.

- Ubuntu 22.04+
  - Vérifier la version : `lsb_release -a`
- Les ports UDP 500 et 4500 doivent être libres et accessibles depuis l'extérieur
  - Ouverts lors de la configuration du pare-feu (`ufw allow 500,4500/udp`)
    Vérifier le statut : `sudo ufw status verbose`
- Trafic sortant vers toutes les cibles qui doivent être protégées par Relution Shield
- Trafic sortant via HTTPS vers le serveur Relution
- Le serveur doit être accessible depuis Internet
- Recommandé : entrée DNS publique
  - p. ex. `vpn.mondomaine.fr`

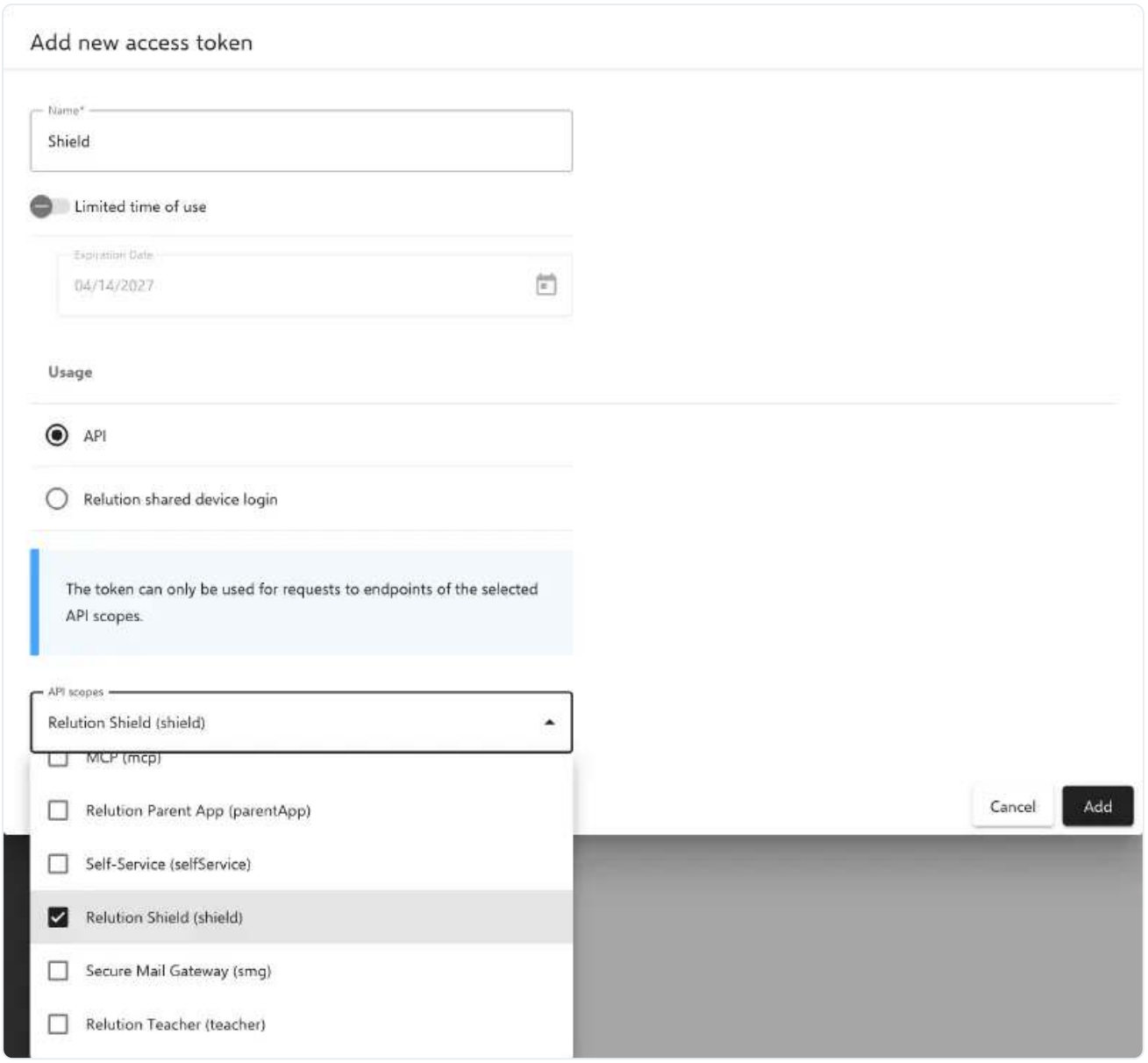
Création d’un utilisateur technique et d’un jeton d’accès API

Nouveau dans 26.5

1. Créer une nouvelle autorisation avec le rôle Relution Shield Access Check : sous `Home` → `Utilisateurs` → `Autorisations` → `Ajouter`, activer le point `Relution Shield Access Check` dans la section Appareils
2. Créer un nouvel utilisateur sans mot de passe (désactiver l’authentification par mot de passe) dans l’organisation cible

   > Si l’utilisateur est créé dans l’organisation `Global`, Relution Shield peut effectuer les contrôles d’accès pour toutes les organisations du serveur Relution (nécessite Relution Shield 2.0 ou plus récent).
3. Attribuer à l’utilisateur l’autorisation nouvellement créée
4. Créer un jeton d’accès API pour l’utilisateur et désactiver la durée de validité : sous Utilisation, choisir l’option API et, dans le champ Portées d’API, activer l’entrée Relution Shield (shield)

Pour la version 26.4.0



5. Enregistrer l’utilisateur

À partir de Relution 26.5, un jeton d’accès API n’est valable que pour les portées d’API sélectionnées. Relution Shield nécessite uniquement la portée Relution Shield (shield). Si elle manque, le serveur Relution refuse le contrôle d’accès. Relution Shield traite ce refus comme un serveur injoignable : avec la valeur par défaut `RELUTION_SERVER_NOT_REACHABLE_ALLOW_DEVICE=true`, les appareils disposant d’un certificat valide sont admis sans contrôle d’accès, et le journal affiche `Relution: Could not retrieve status, temporarily accepting …`.

Les jetons d’accès API créés avant la mise à jour vers Relution 26.5 reçoivent automatiquement toutes les portées d’API lors de la mise à jour et continuent de fonctionner sans changement.

Paramètres requis

1. Relution Host : nom d'hôte du serveur Relution
   p. ex. `mdm.mondomaine.fr`
2. Jeton API Relution : jeton d'accès API avec la portée d'API Relution Shield (shield), voir l'étape précédente
   Création d'un utilisateur technique et d'un jeton d'accès API →
3. VPN CIDR : la plage d'adresses IP privées à partir de laquelle Relution Shield attribue une adresse IP interne aux appareils connectés, p. ex. `10.1.0.0/16`. Cette plage ne doit pas chevaucher le réseau existant.
4. Interface réseau : nom de l'interface réseau utilisée par le serveur Relution Shield, p. ex. `eth0` – vérifier via `ip a`
5. Relution Shield Host : nom d'hôte de Relution Shield
   p. ex. `vpn.mondomaine.fr`
6. Serveurs DNS : les adresses IP des serveurs DNS internes du réseau, p. ex. `10.1.0.1,10.1.0.2`. Elles sont communiquées aux appareils connectés afin que les noms d'hôtes internes (p. ex. ressources intranet) puissent être résolus.

Installation

Pour la version 26.4.0

1. Exécuter la commande suivante :

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

2. Installer Docker, y compris docker-compose (pas via **`snap`**)
   Guide d'installation de Docker →

3. Créer le répertoire d'installation et le répertoire de conformité :

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

4. Créer le fichier d'environnement `/opt/relution-shield/.env` :

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

Remplacer l'espace réservé `<%Relution Host%>` par le nom d'hôte réel, p. ex. `RELUTION_HOSTNAME=mdm.mondomaine.fr`

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

Si le jeton d'accès API appartient à un utilisateur de l'organisation `Global`, le scope global doit être activé pour le contrôle d'accès
(nécessite Relution Shield 2.0 ou plus récent) :

```
RELUTION_ACCESS_CHECK_SCOPE=global
```

5. Pare-feu Ubuntu `ufw`

    1. Définir la politique de transfert par défaut dans `/etc/default/ufw` sur `DEFAULT_FORWARD_POLICY="ACCEPT"` :

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

    ```
    DEFAULT_FORWARD_POLICY="ACCEPT"
    ```

    2. Autoriser SSH et les ports UDP IPSec requis :

    ```
    ufw allow ssh
    ```

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

3. Insérer les lignes suivantes au début du fichier `/etc/ufw/before.rules` – avant les lignes obligatoires contenant `*filter` :

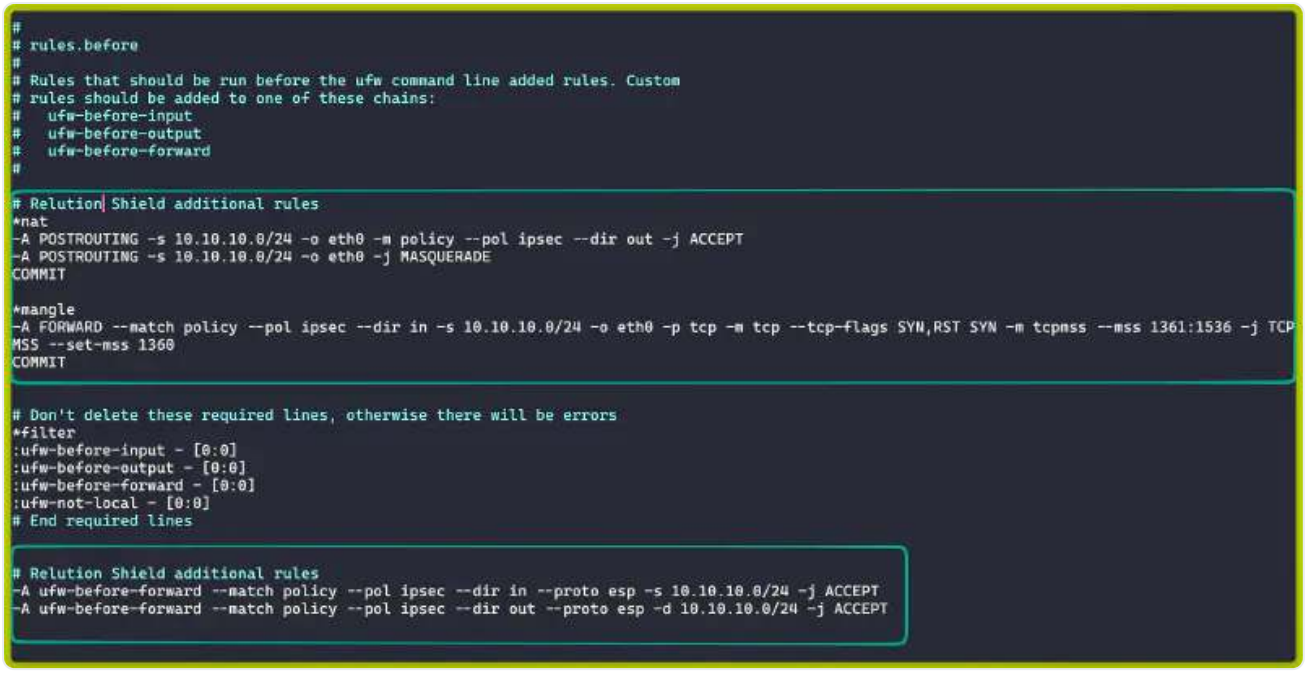
```
vi /etc/ufw/before.rules
```

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

*mangle
-A FORWARD --match policy --pol ipsec --dir in -s <%VPN CIDR%> -o <%Net
COMMIT
```

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

Remplacer `<%VPN CIDR%>` et `<%Network interface%>` aux trois endroits.



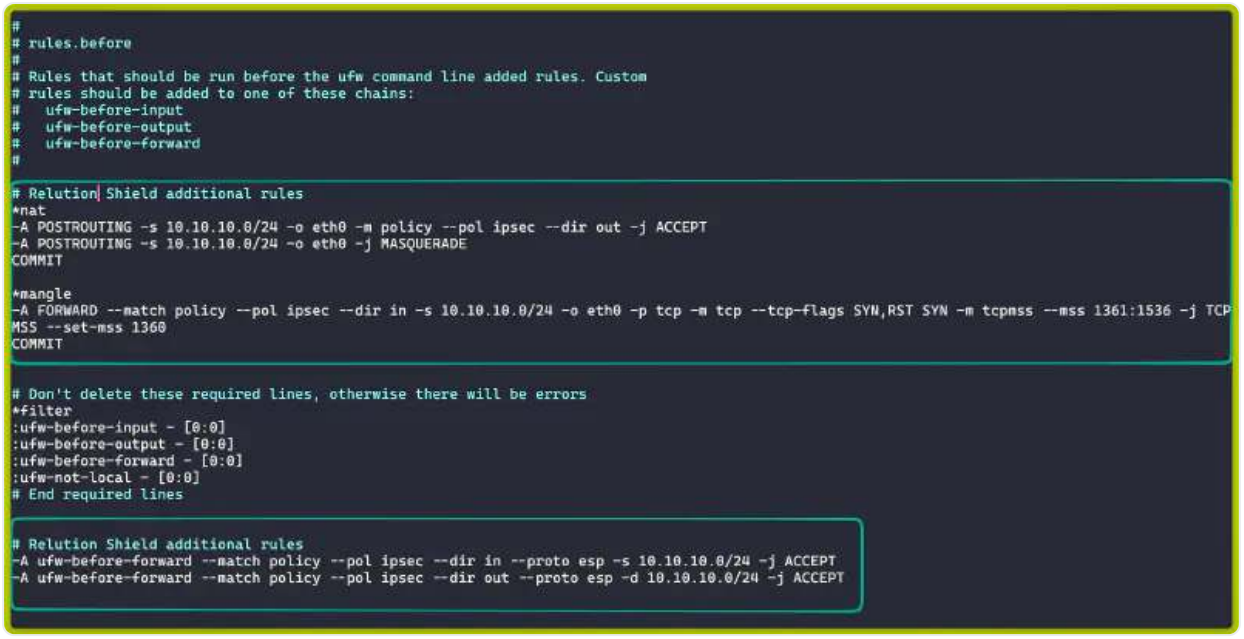
1. Insérer les lignes suivantes à la fin du fichier `/etc/ufw/before.rules` – après les lignes obligatoires contenant `*filter` :

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

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

```
# Relution Shield additional rules
-A ufw-before-forward --match policy --pol ipsec --dir in --proto esp
-A ufw-before-forward --match policy --pol ipsec --dir out --proto esp
```

Remplacer `<%VPN CIDR%>` aux deux endroits.



2. Insérer les lignes suivantes à la fin du fichier `/etc/ufw/sysctl.conf` :

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

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

3. Redémarrer le pare-feu Ubuntu :

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

6. Préparer la configuration de Relution Shield :

    1. Créer les certificats et clés nécessaires :

```
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
```

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

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

Une ligne s'affiche dans le terminal plugin 'tpm': failed to load···, indiquant qu'un plugin TPM est manquant.
Ce message peut être ignoré. Il ne s'agit pas d'une erreur.

Remplacer l'espace réservé `<%Relution Shield Host%>`, p. ex. `"CN=ca.vpn.mondomaine.fr"` :

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

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

```
# 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 \
```

Pour la version 26.4.0

```
         --dn "CN=<%Relution Shield Host%>" --san "<%Relution Shield Hos
         --flag serverAuth --flag ikeIntermediate --outform pem \
    >  pki/certs/server-cert.pem
```

Le message d'erreur TPM suivant peut être ignoré :

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

```
# Prepare Key Pair archive, will be needed for Relution later
openssl pkcs12 -export -out "pki/ca.<%Relution Shield Host%>.p12" -inke
```

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

Pour la version

La clé privée de l'autorité de certification (CA) doit être conservée en lieu sûr : en cas de vol, la sécurité de l'infrastructure à clé publique (PKI) du VPN est compromise.

2. Déplacer les fichiers de certificats aux emplacements appropriés :

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

3. Créer le fichier de configuration `/opt/relution-shield/etc/strongswan.conf` et y insérer le contenu suivant :

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

> Afficher l'exemple de configuration complet

1. Créer le fichier de configuration `/opt/relution-shield/etc/swanctl/swanctl.conf` :

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

Remplacer les espaces réservés `<%Relution Shield Host%>`, `<%VPN CIDR%>`, `<%Relution Host%>` et `<%DNS Servers%>` :

> Afficher l'exemple de configuration complet

1. Installer Relution Shield avec Docker :

    1. Créer le fichier `/opt/relution-shield/compose.yml` et y insérer le contenu suivant. Les espaces réservés n'ont pas besoin d'être adaptés ici, car ils sont déjà définis dans le fichier `.env`.

Pour la version 26.4.0

```
vi /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"
```

Si Relution Shield 1.x est utilisé, `RELUTION_REST_API_ACCESS_TOKEN` doit être remplacé par `REST_API_ACCESS_TOKEN`.

2. Démarrer Relution Shield :

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

3. Configurer le démarrage automatique de Relution Shield – créer et ouvrir le fichier suivant :

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

Insérer le contenu suivant et enregistrer :

```
[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. Activer le service avec la commande suivante :

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

Variables d’environnement

Les variables d’environnement suivantes peuvent être utilisées pour configurer Relution Shield.

Nom de la variable	Description	Valeurs
`RELUTION_HOSTNAME`	Nom d’hôte du serveur Relution, p. ex. `mdm.mondomaine.fr`	
`RELUTION_REST_API_ACCESS_TOKEN`	Jeton API pour l’accès au serveur Relution (pour Relution Shield 1.x.y : `REST_API_ACCESS_TOKEN`)	
`RELUTION_ACCESS_CHECK_SCOPE`	Scope du contrôle d’accès	`global` / `local`
`RELUTION_SERVER_NOT_REACHABLE_ALLOW_DEVICE`	Autoriser la connexion avec un certificat valide lorsque le serveur Relution n’est pas joignable pour le contrôle de conformité	`true` / `false`
`DEVICE_STATE_CACHE_DURATION_MINUTES`	Durée pendant laquelle l’état de conformité chargé est mis en cache	Valeur numérique

Nom de la variable	Description	Valeurs
	localement avant une nouvelle interrogation du serveur	

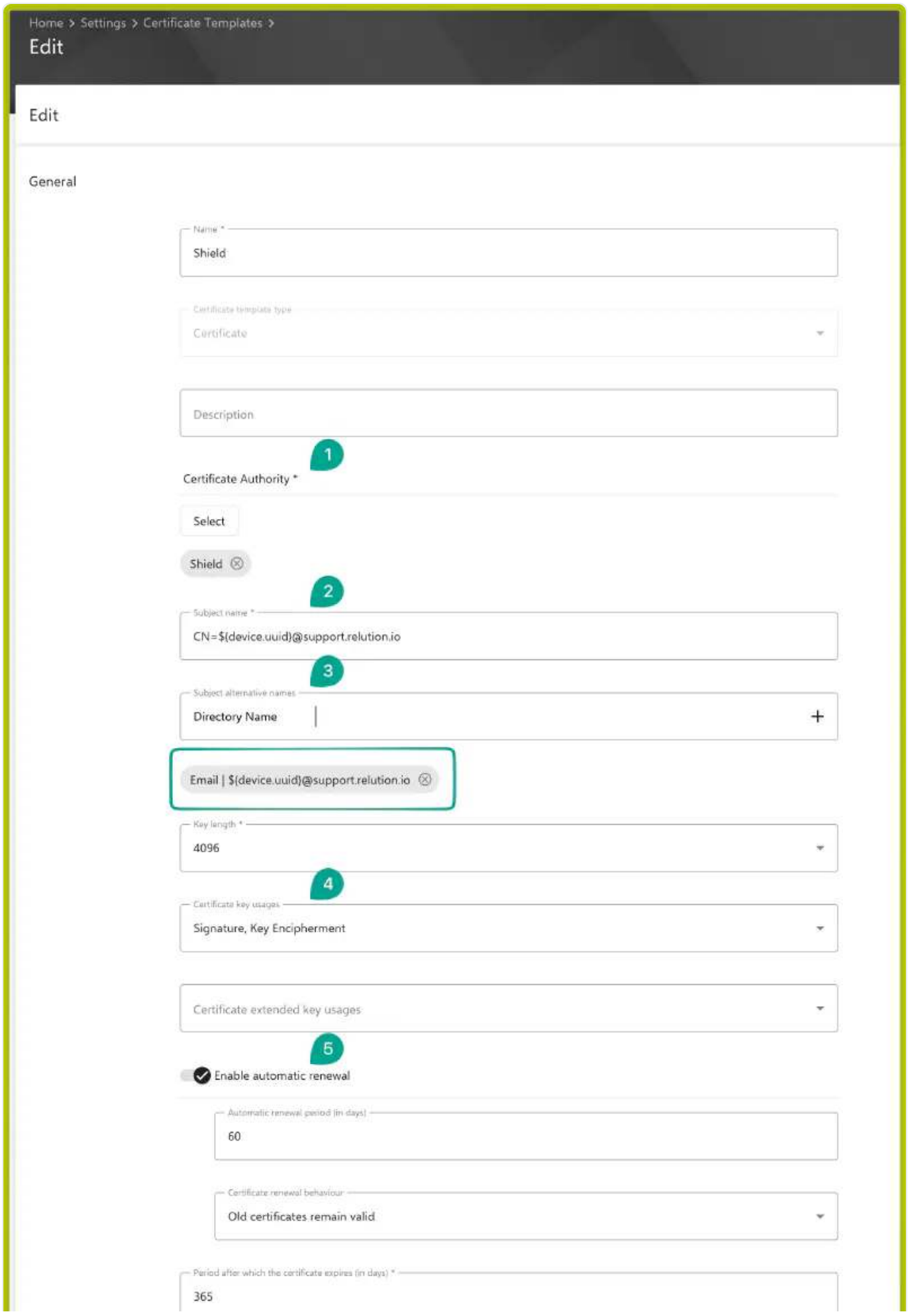
Configuration des certificats

1. Importer les certificats dans l'organisation cible :
    1. Naviguer vers `Paramètres` → `Certificats`
    2. Télécharger le certificat `ca-cert.pem` depuis le serveur Relution Shield `/opt/relution-shield/etc/swanctl/x509ca/ca-cert.pem`, le renommer en `<%Relution Shield Host%> CA Certificate` et l'importer sur le serveur d'application Relution sous `Paramètres` → `Certificats` → `Certificat CA`
    3. Télécharger le certificat `server-cert.pem` depuis le serveur Relution Shield `/opt/relution-shield/etc/swanctl/x509/server-cert.pem`, le renommer en `<%Relution Shield Host%> Server Certificate` et l'importer sur le serveur d'application Relution sous `Paramètres` → `Certificats` → `Certificat serveur`
    4. Télécharger la paire de clés PKCS12 depuis le serveur Relution Shield `/opt/relution-shield/pki/ca.<%Relution Shield Host%>.p12`, la renommer en `<%Relution Shield Host%> CA Key Pair` et l'importer sur le serveur d'application Relution sous `Paramètres` → `Certificats` → `Paire de clés CA`
    5. Sauvegarder le contenu de `/opt/relution-shield/pki/` en externe, puis supprimer le répertoire
2. Créer une autorité de certification et un modèle de certificat :
    1. Naviguer vers `Paramètres` → `Autorités de certification`
    2. Ajouter une nouvelle autorité de certification de type `Built In` et sélectionner le certificat `<%Relution Shield Host%> CA Key Pair` importé précédemment

Pour la version 26.4.0

3. Naviguer vers `Paramètres` → `Modèles de certificats`
4. Ajouter un nouveau modèle de certificat :
    1. Sélectionner l’autorité de certification créée précédemment
    2. Définir le nom du titulaire sur `CN=${device.uuid}@<%Relution Host%>` (noter le `CN=` au début)
    3. Dans le champ Utilisation des clés de certificat, activer Signature et Chiffrement de clé
    4. Ajouter un Subject Alternative Name de type Email avec `${device.uuid}@<%Relution Host%>` (pas de `CN=` au début)
       Confirmer la saisie avec Entrée
    5. Activer le renouvellement automatique et définir des valeurs appropriées, p. ex. 60 ou 180 jours

Pour la 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

Exemple de configuration iOS

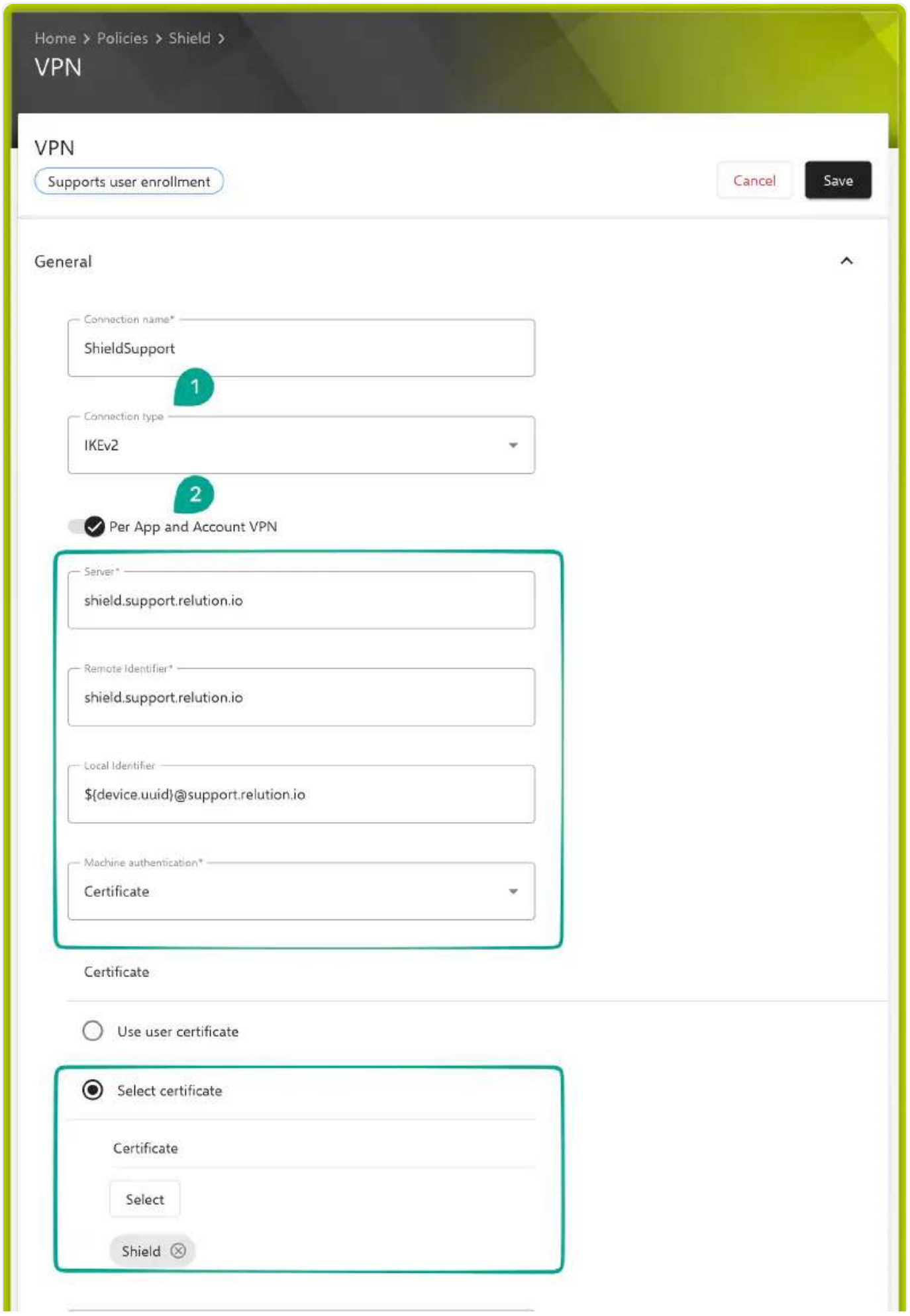
1. Créer une nouvelle politique iOS ou étendre une politique existante
2. Ajouter une configuration VPN :
    1. Sélectionner le type `IKEv2`
    2. Activer `Per App and Account VPN` (voir aussi Relution Hub Docs →)
    3. Définir `Server` et `Remote identifier` sur la valeur de `<%Relution Shield Host%>`
    4. Définir `Local identifier` sur `${device.uuid}@<%Relution Host%>`
    5. Définir la `méthode d'authentification` sur `Certificat` et sélectionner le modèle de certificat créé précédemment
    6. Activer l'`authentification étendue (EAP)`
    7. Définir les paramètres IKE SA et Child SA sur `AES-256`, `SHA2-256`, `DH group 16 : groupe 4096 bits`, `1440` minutes
    8. Facultatif : ajouter un domaine de test sous `Domaines Safari` pour activer automatiquement la connexion VPN lorsque le domaine est ouvert via Safari
3. Ajouter une configuration `Certificat` à la politique et sélectionner le `<%Relution Shield Host%> CA Certificate` importé précédemment
4. Facultatif : ajouter une configuration `App to VPN Mapping`, sélectionner la configuration VPN créée précédemment ainsi qu'une application de navigateur comme Firefox ou Chrome pour tester l'accès VPN. Recommandé : ajouter une conformité d'application afin de garantir que l'application est installée.
5. Publier la politique et l'attribuer à un appareil. La connexion VPN peut ensuite être activée manuellement via `Réglages` → `Général` → `VPN et gestion des appareils` → `VPN`. Relution Shield se connecte également automatiquement lorsque les domaines configurés dans Safari sont ouverts ou lorsque l'application de navigateur est lancée.

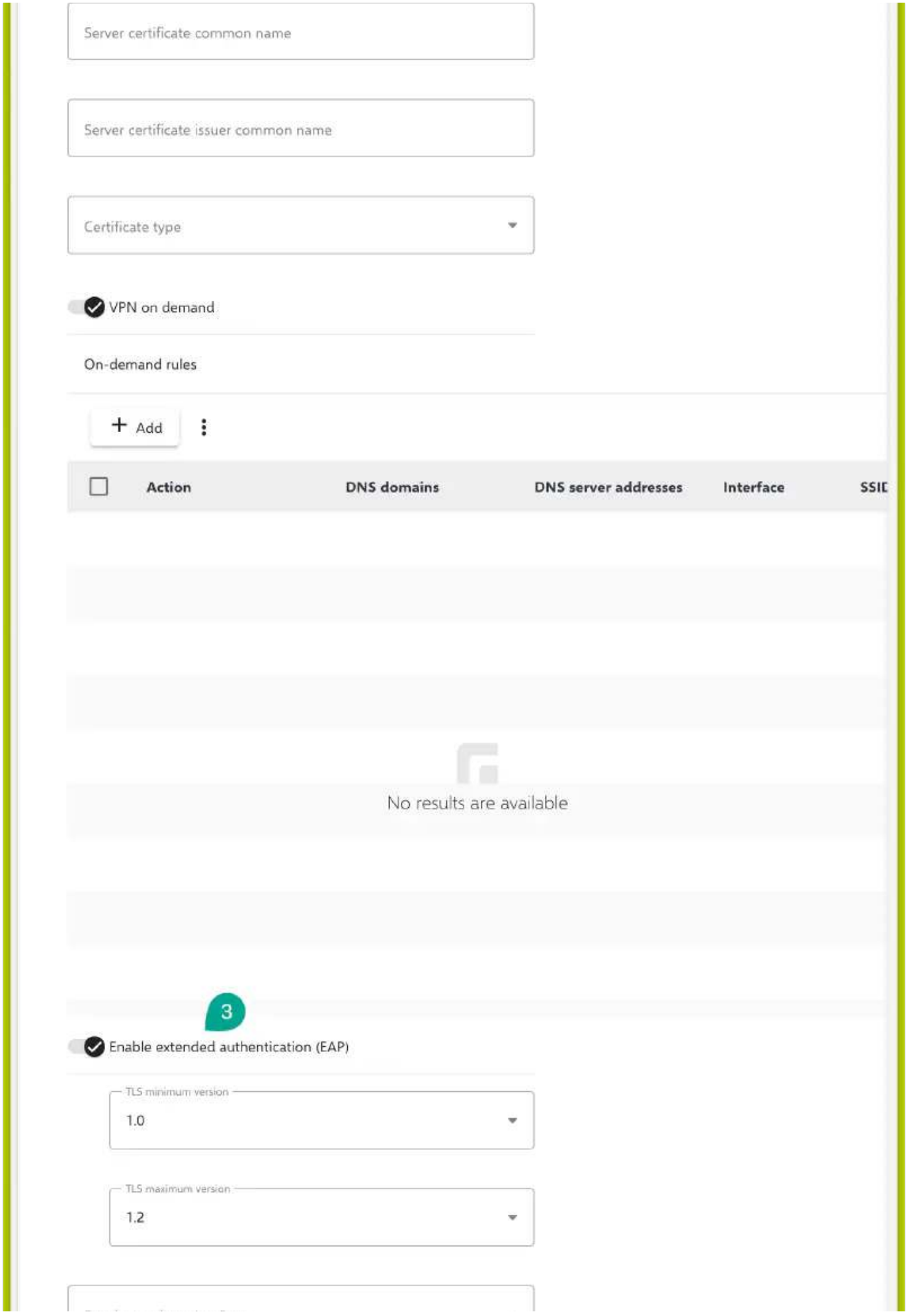
Pour la version 26.4.0

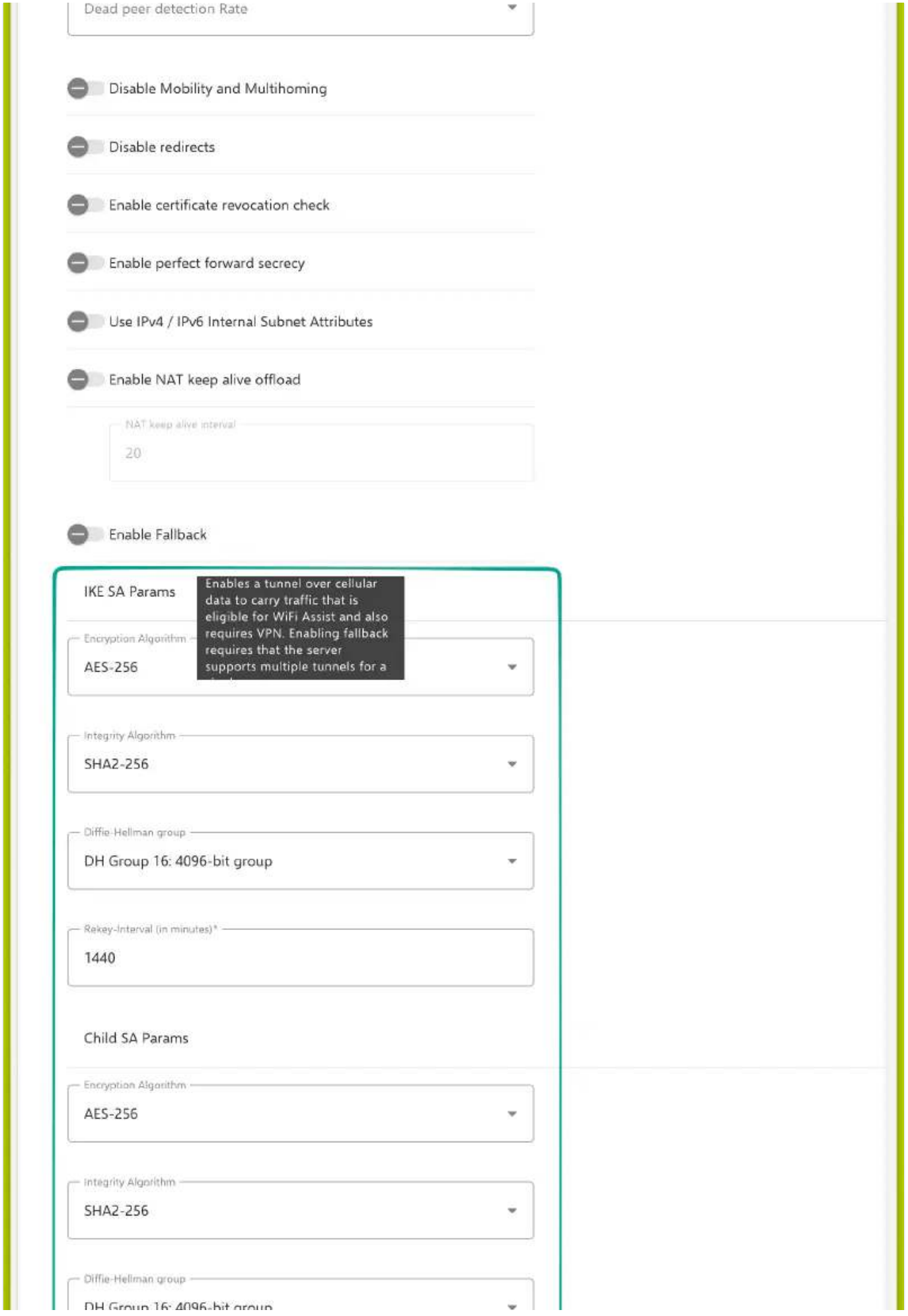
6. Ajuster la configuration pour inclure les comptes, applications et domaines qui ne doivent être accessibles que via Relution Shield.



Pour la 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

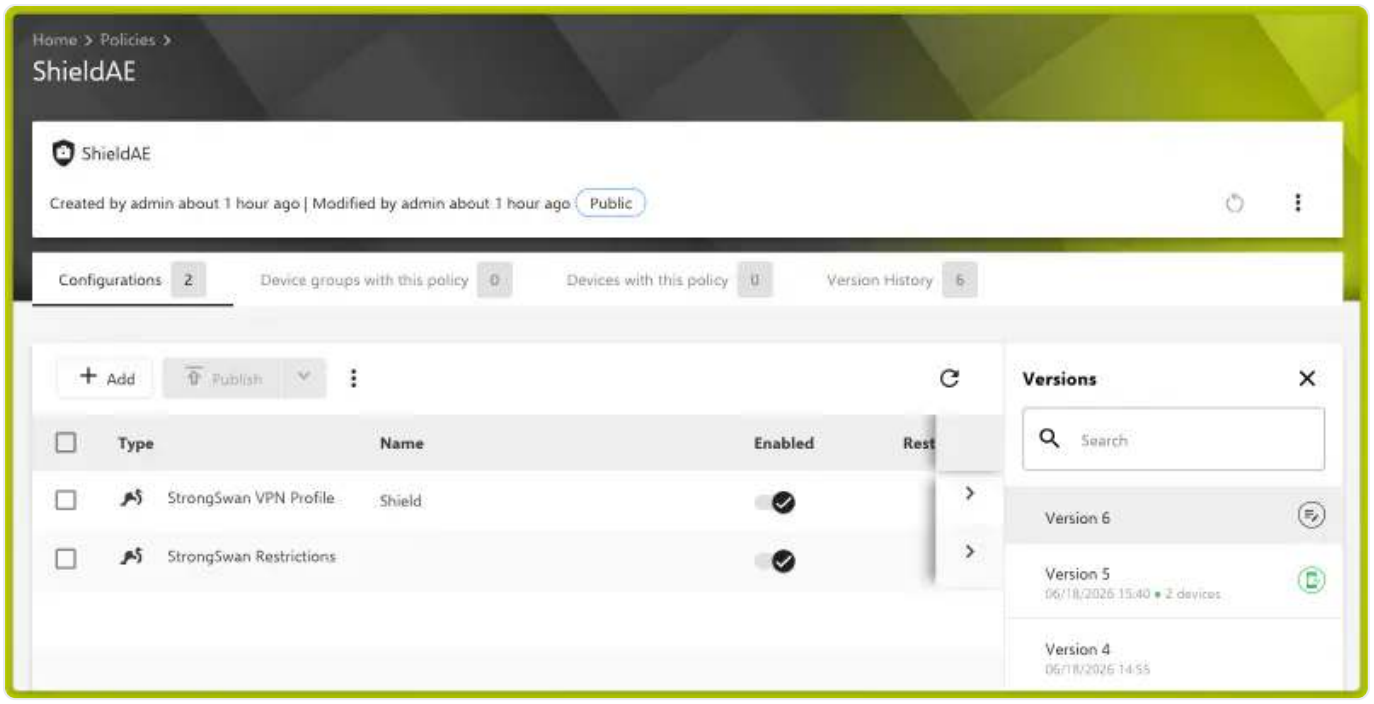

Dead peer detection Rate
Disable Mobility and Multihoming
Disable redirects
Enable certificate revocation check
Enable perfect forward secrecy
Use IPv4 / IPv6 Internal Subnet Attributes
Enable NAT keep alive offload
NAT keep alive interval
20
Enable Fallback
IKE SA Params
Enables a tunnel over cellular 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



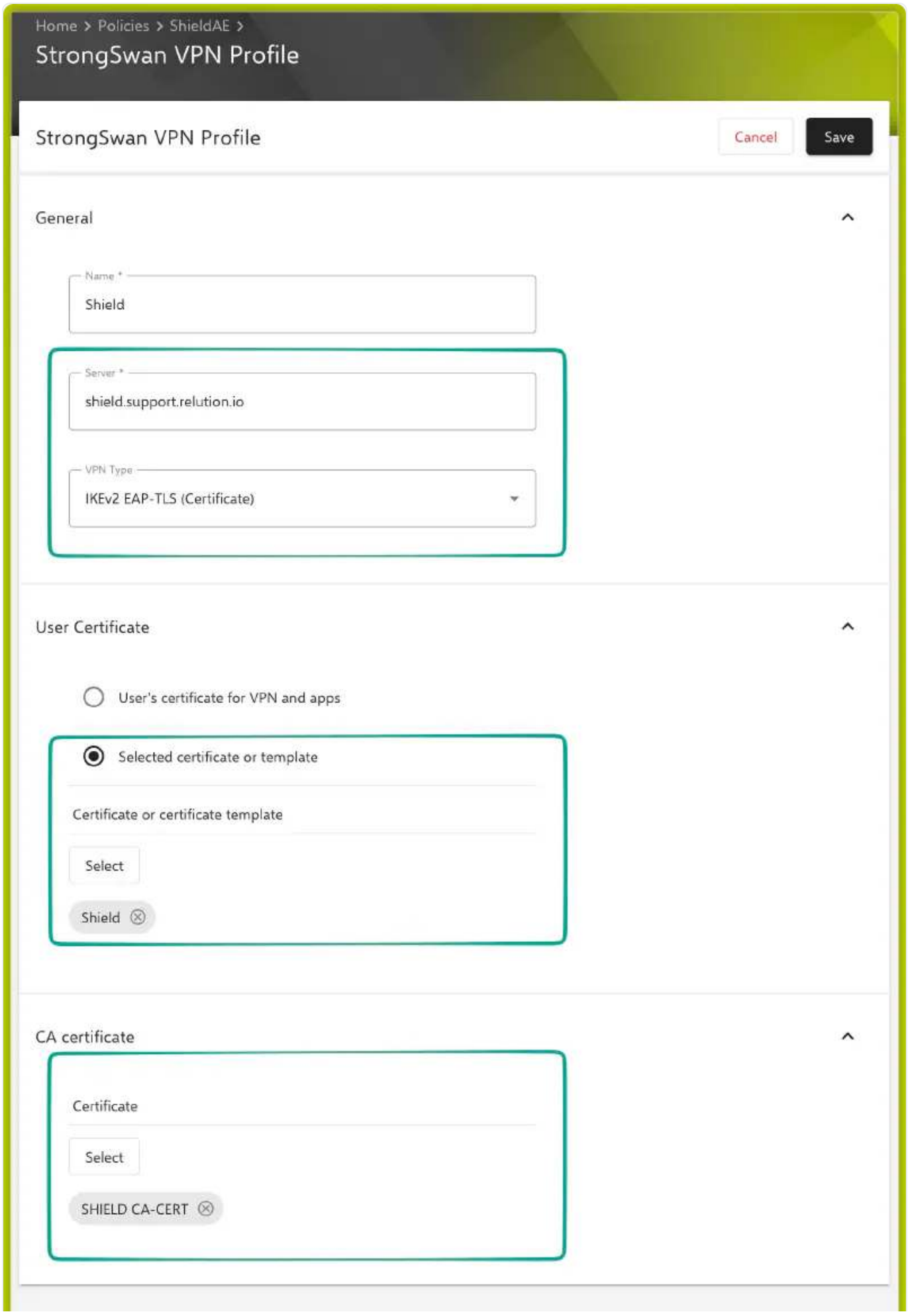
Exemple de configuration Android Enterprise

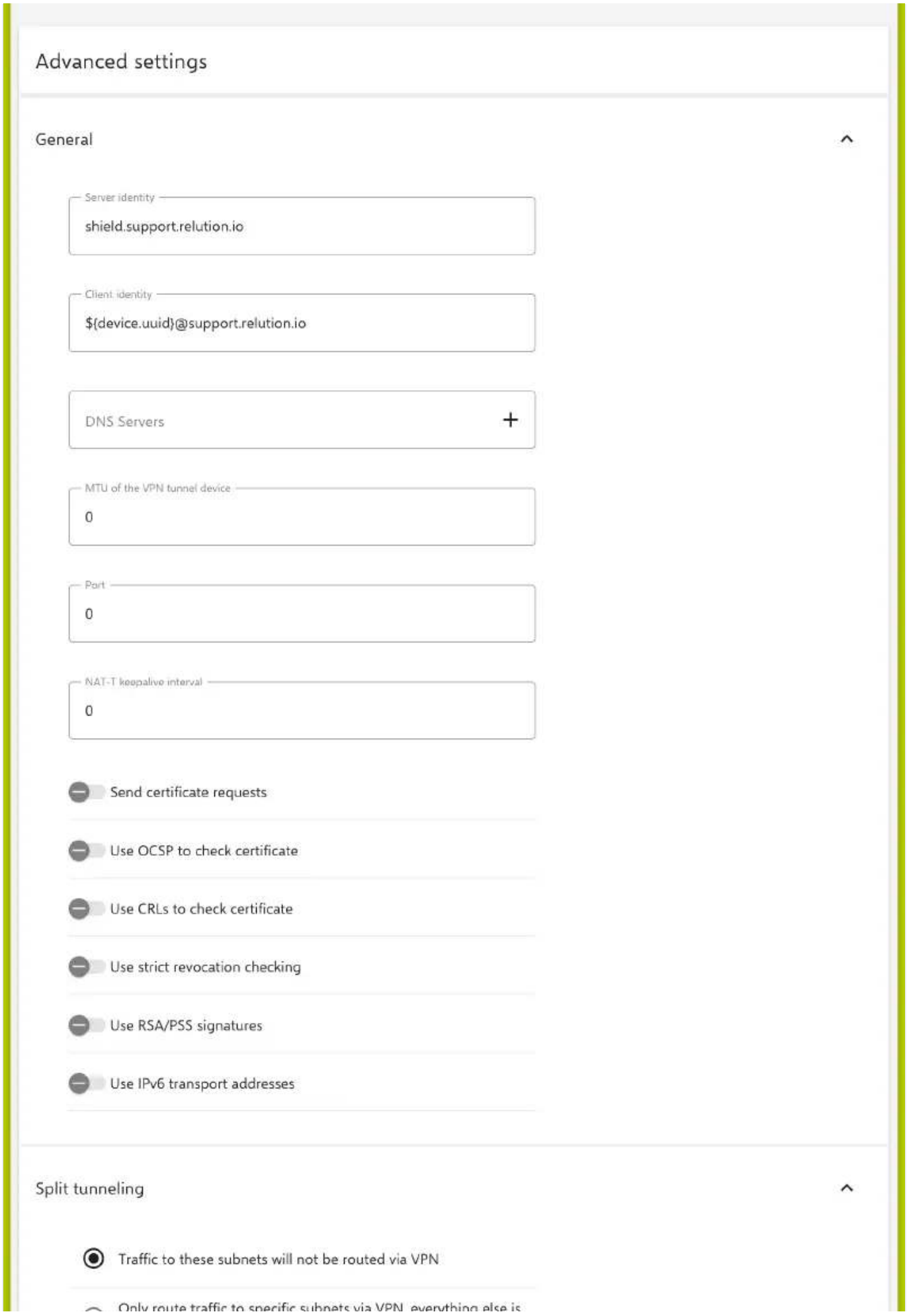
1. Créer une nouvelle politique Android Enterprise ou étendre une politique existante
2. Ajouter une configuration `Profil VPN StrongSwan` :
    1. Sélectionner `IKEv2 EAP-TLS` comme `type de VPN`
    2. Définir `Server` et `Server identity` sur la valeur de `<%Relution Shield Host%>`
    3. Définir le `certificat utilisateur` sur le modèle de certificat créé précédemment
    4. Définir le `certificat CA` sur le `<%Relution Shield Host%> CA Certificate` importé précédemment
    5. Définir `Client identity` sur `${device.uuid}@<%Relution Host%>`
    6. Définir `Seules ces applications utilisent le VPN` sur un navigateur comme Firefox
3. Ajouter une configuration `Restrictions VPN StrongSwan` et sélectionner le profil VPN créé précédemment comme profil par défaut
4. Publier la politique et l'attribuer à un appareil. La connexion VPN peut ensuite être activée manuellement via l'application StrongSwan. Relution Shield se connecte également automatiquement lorsque l'application de navigateur configurée précédemment est lancée.
5. Ajuster la configuration pour inclure les applications qui ne doivent être accessibles que via Relution Shield.

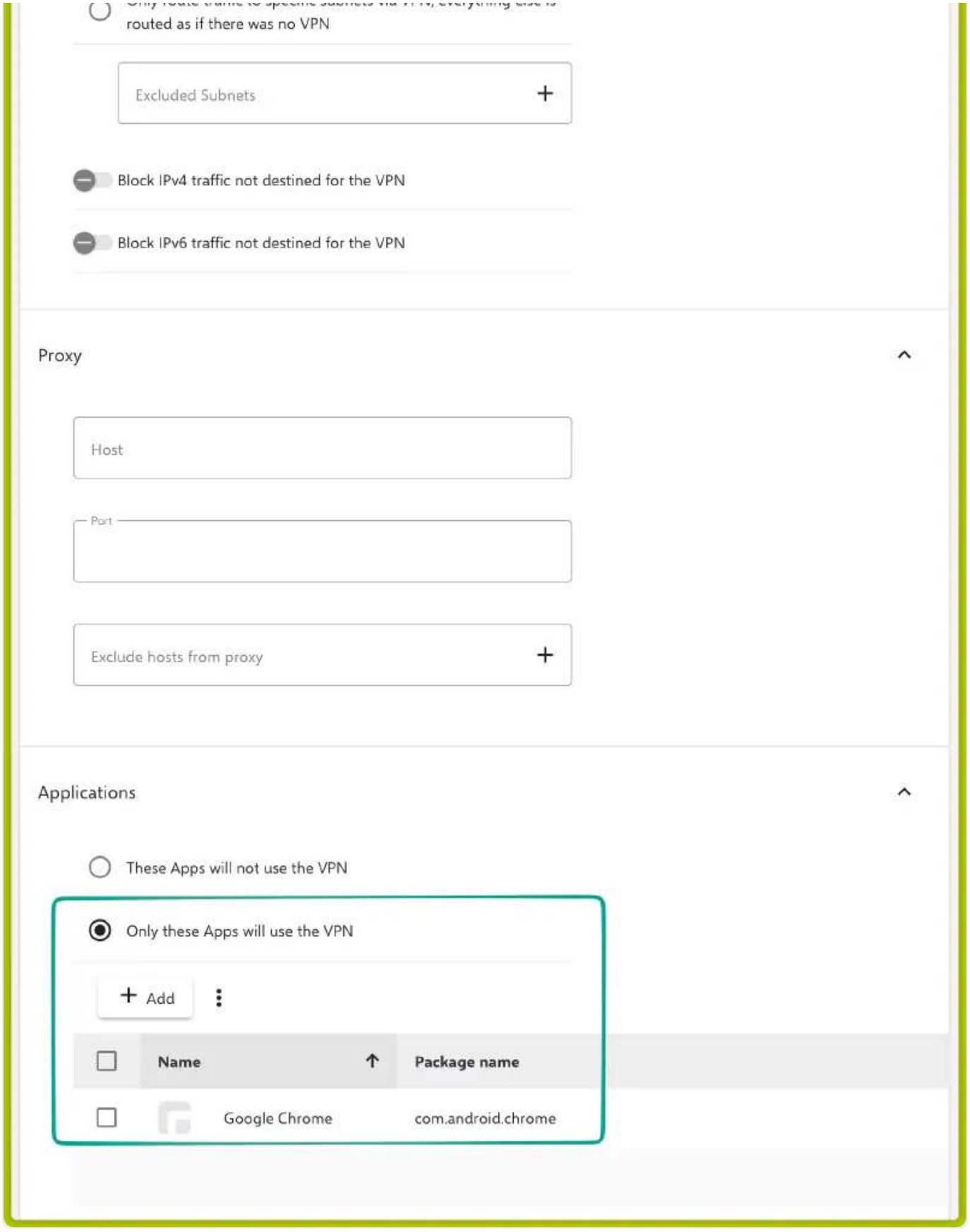
Pour la version 26.4.0



Pour la version 26.4.0


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


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

Pour la version 26.4.0

Mise à niveau de 1.x vers 2.x

> Déposer la clé privée de la CA `/opt/relution-shield/etc/ipsec.d/private/ca-key.pem` en lieu sûr (en dehors du serveur), si ce n'est pas déjà fait.

1. Arrêter Relution Shield :

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

2. Créer ou modifier les fichiers suivants comme décrit dans le guide d'installation :
    1. Créer les nouveaux répertoires pour les fichiers de configuration

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

    2. Créer `etc/swanctl/swanctl.conf`
    3. Adapter `/opt/relution-shield/compose.yml`
    4. Adapter `/opt/relution-shield/.env`
    5. Adapter `/opt/relution-shield/etc/strongswan.conf`
    6. Déplacer les fichiers suivants

pour la version 26.4.0

Ancien chemin	Nouveau chemin
`/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. Supprimer le répertoire `/opt/relution-shield/etc/ipsec.d`
    2. Supprimer `/opt/relution-shield/etc/ipsec.conf`

3. Supprimer `/opt/relution-shield/etc/ipsec.secrets`

4. Démarrer Relution Shield :

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

Pour la version 26.4.0

Secure Mail Gateway

Lorsque la Secure Mail Gateway est utilisée, le service autonome Secure Mail Gateway devient un composant obligatoire à partir de Relution 26.4.0. Cet article décrit la configuration pour les installations on-premise.

Pour la configuration de la Secure Mail Gateway dans Relution : Secure Mail Gateway →

Contexte technique

Lorsque la Secure Mail Gateway est activée sous `Paramètres` → `Gestion des appareils` → `Secure Mail Gateway`, les connexions ActiveSync entrantes sont transmises au serveur Exchange qui y est configuré, à condition que la requête provienne d'un appareil autorisé (inscrit).

Dans la version 26.3.x et antérieures, les requêtes ActiveSync parviennent d'abord au service Relution, qui les transmet au serveur Exchange. Le service Relution vérifie en interne si une requête provient d'un appareil autorisé et peut être transmise. Les requêtes non autorisées sont rejetées.

Pour la version 26.4.0

À partir de la version 26.3.0, le service autonome peut être activé au choix afin de tester à l'avance le passage au conteneur dédié. À partir de la version 26.4.0 et supérieures, la fonctionnalité correspondante a été entièrement retirée de Relution, de sorte que les requêtes ActiveSync doivent toujours transiter par le conteneur Docker dédié.

La configuration nécessaire est décrite ci-dessous.

Migration — Que faut-il faire ?

Installation	Action requise
Relution Cloud – Shared Hosting	Aucune action requise. Relution gère la migration du service SMG.
Relution Cloud – Dedicated Server (clients existants)	Relution hébergera le service SMG. Une prise de contact aura lieu pour coordonner la migration.

Installation	Action requise
Relution Cloud – Dedicated Server (nouveaux clients)	Le service SMG doit être opéré en tant que composant on-premise auto-hébergé. Suivre le guide de configuration plus bas dans cet article.
On-Premise	La procédure complète de configuration est décrite plus bas dans cet article.

Feature toggle pour les installations on-premise (26.3)

Nouveau dans 26.3

Dans Relution 26.3, les installations on-premise peuvent activer le nouveau mode au choix. Pour cela, le fichier `application.yaml` du serveur Relution doit être complété par le feature toggle de préversion suivant :

ersion 26.4.0

application.yaml

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

De plus, un conteneur Docker supplémentaire doit être intégré à l'environnement Docker, comme décrit ci-dessous.

> Tant que le toggle est actif, le nouveau service autonome est utilisé. S'il est supprimé, Relution revient automatiquement au comportement précédent. Relution 26.3 est donc idéale pour tester le nouveau service dans l'environnement concerné avant que la mise à jour vers 26.4.0 ne rende le changement obligatoire.

Composant obligatoire à partir de 26.4.0

Nouveau dans 26.4

Avec Relution 26.4.0, le toggle est supprimé. La Secure Mail Gateway doit obligatoirement être opérée en tant que service distinct. Le composant a été entièrement retiré de Relution.

Configuration initiale

En tant que proxy HTTP, le service autonome Secure Mail Gateway transmet les requêtes ActiveSync des appareils mobiles au serveur Exchange, puis les réponses à l'appareil mobile concerné. Pour cela, il faut d'abord déterminer si une requête peut être transmise ou non. Afin que la Secure Mail Gateway puisse prendre cette décision, elle doit communiquer en interne avec le service Relution pour vérifier si une requête provient d'un appareil autorisé.

Relution

Pour que la Secure Mail Gateway puisse communiquer avec le service Relution, un utilisateur technique disposant des permissions correspondantes doit d'abord être créé dans Relution.

1. Créer un Dynamic Role dans Relution

Télécharger le modèle de rôle prêt à l'emploi et l'importer dans l'organisation Global sous `Paramètres` → `Gestion des utilisateurs` → `Permissions` :

Télécharger le modèle de rôle SMG →

Pour la version 26.4.0

Il est également possible de créer le rôle manuellement :

1. Naviguer vers `Paramètres` → `Gestion des utilisateurs` → `Permissions` dans l'organisation Global
2. Ajouter un nouveau Dynamic Role
3. Activer la permission Secure Mail Gateway (service account)
4. Enregistrer le rôle

2. Créer un utilisateur technique et une clé d'accès API

1. Créer un nouvel utilisateur dans l'organisation Global et lui attribuer le Dynamic Role créé ci-dessus
2. Accéder à la page de détail de l'utilisateur et créer une nouvelle clé d'accès API
3. Copier la clé générée — elle n'est affichée qu'une seule fois

Conteneur Secure Mail Gateway

La Secure Mail Gateway doit maintenant être intégrée à l'environnement en tant que conteneur Docker distinct, puis configurée. Ensuite, le proxy inverse doit être adapté afin que les requêtes

vers le point d'entrée `/Microsoft-Server-ActiveSync` ne soient plus envoyées au conteneur Relution, mais au conteneur Secure Mail Gateway.

1. Déployer le service

Ajouter le service suivant au `compose.yaml` existant. Ceci n'est nécessaire que si la Secure Mail Gateway est utilisée.

> Même si des tags de version plus récents apparaissent sur Docker Hub, nous recommandons vivement de conserver `latest`. Les nouveaux builds passent par plusieurs niveaux de contrôle qualité avant d'être promus en `latest` — épingler un tag de version spécifique peut exposer à un build qui n'a pas encore été validé pour la production.

`compose.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` doit se trouver sur le réseau `reverse-proxy`, comme `relution` et `traefik` — sinon Traefik/nginx ne peut pas router vers ce service.

2. Configurer le service

La clé d'accès API créée précédemment dans Relution doit être reprise dans la configuration de la Secure Mail Gateway afin que le SMG puisse communiquer avec le service Relution.

Si les deux services s'exécutent dans le même `compose.yaml` sur un serveur, ils communiquent en interne via le réseau Docker.

Créer `smg/application.yaml` à côté du `compose.yaml` :

smg/application.yaml

```yaml
relution:
  server:
    url: http://relution:8080    # Ne pas modifier avec un compose.yaml commun
    api-key: votre-cle-api       # Clé d'accès API créée ci-dessus
```

URL du serveur Relution : si la Secure Mail Gateway et Relution s'exécutent dans le même `compose.yaml` sur un serveur, `url: http://relution:8080` reste inchangée. Le nom de service `relution` est alors résolu via le réseau Docker commun.

L'URL n'est à adapter que si le SMG ne s'exécute pas dans le même réseau que Relution, par exemple sur un autre serveur ou dans un `compose.yaml` distinct avec son propre réseau Docker. Il faut alors indiquer l'adresse à laquelle Relution est joignable depuis le SMG, par exemple `https://relution.example.com`.

Pour la version 26.4.0

Configuration du proxy inverse

Le service SMG expose le point d'entrée `/Microsoft-Server-ActiveSync` sur le port `8093`. La configuration du proxy inverse doit être adaptée afin que les requêtes entrantes sur ce chemin soient acheminées vers le service autonome SMG. Les exemples ci-dessous montrent comment procéder pour Traefik et nginx.

En cas d'utilisation d'un autre proxy inverse non officiellement pris en charge par Relution (p. ex. Apache, Sophos, ⋯), sa configuration doit être adaptée en conséquence. La documentation du produit concerné indique comment acheminer des chemins ou des locations individuels vers des points d'entrée distincts.

Remarque : Les exemples ci-dessous utilisent des noms d'hôte résolvables au sein du réseau Docker. Cela n'est possible que tant que Relution, SMG et Traefik/nginx font partie du même réseau Docker. Si le proxy inverse ou les services se trouvent sur des réseaux distincts, il faut utiliser des noms d'hôte que le serveur DNS interne peut résoudre.

Traefik

Ajouter les entrées `smg` supplémentaires suivantes sous `routers` et `services`. Les `routers` et `services` existants, tels que `relution`, doivent être conservés. Voir aussi : configuration Traefik →

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 à Traefik)

Ajouter (ou adapter) le bloc `location ~ /Microsoft-Server-ActiveSync` dans le bloc `server` HTTPS existant afin d'acheminer les requêtes entrantes vers le SMG.

relution-nginx.conf

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

    # (NOUVEAU) Acheminement vers la Secure Mail Gateway
    location ~ /Microsoft-Server-ActiveSync {
        proxy_read_timeout 2100;
        proxy_pass http://smg:8093;
    }
}
```

La position du bloc au sein du bloc `server` n'a pas d'importance, car nginx évalue les locations à expression régulière avant la location de préfixe `/`. Pour des raisons de lisibilité, il reste

néanmoins recommandé de regrouper les différents blocs de localisation.

> Dans une installation Docker, `smg` désigne le nom du service Docker et est accessible au sein du réseau Docker. Pour une installation Linux native, remplacer `smg:8093` par `127.0.0.1:8093`.

Démarrer ou redémarrer les services Docker

Pour que les modifications prennent effet, les conteneurs Docker doivent ensuite être redémarrés.

```
docker compose up -d
```

> En cas de personnalisation préalable de propriétés `relution.smg.*` dans la configuration du serveur Relution, les déplacer dans ce fichier sans modification — les noms des propriétés sont identiques.

Pour la version 26.4.0

Configuration avancée

Les réglages suivants ne sont nécessaires que dans certains environnements — pour les autorités de certification internes et pour les connexions sortantes devant transiter par un proxy d'entreprise.

(Optionnel) Enregistrer un certificat CA de confiance

Si le serveur Exchange présente un certificat serveur émis par une CA interne (« auto-signé »), le certificat racine de cette CA doit être enregistré comme certificat de confiance. Pour cela, un répertoire contenant le fichier de certificat encodé en PEM peut être monté dans le conteneur sous `/opt/app/ca-certs`. Le dossier peut contenir plusieurs certificats si nécessaire.

compose.yaml

```
services:
  …
```

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

Ces certificats sont utilisés lors de la communication avec le serveur Exchange et Relution — aucune propriété de configuration n'est nécessaire. Si rien n'est monté, la fonctionnalité est sans effet et le TLS sortant se comporte comme avant. Ajouter, supprimer ou modifier un certificat nécessite de redémarrer le conteneur ; le répertoire n'est lu qu'une seule fois, au démarrage.

(Optionnel) Proxy pour les connexions sortantes

Les requêtes vers Exchange respectent les propriétés système de proxy de la JVM. Celles-ci sont définies via `JAVA_TOOL_OPTIONS` dans le `compose.yaml` pour le conteneur SMG. De plus, le flag `honor-proxy-settings` doit être défini sur `true` dans l'`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
```

Avec `-Dhttp.nonProxyHosts` (une liste de motifs d'hôtes séparés par `|`, les jokers `*` sont pris en charge), certains hôtes peuvent être exclus du proxy — typiquement Exchange lui-même, s'il est accessible directement sans passer par le proxy de l'entreprise.

Par défaut, les requêtes vers le serveur Relution ne passent pas par le proxy — il est normalement accessible directement. Si l'installation atteint Relution via le même proxy qu'Exchange, définir `honor-proxy-settings: true` dans `smg/application.yaml` :

smg/application.yaml

```
relution:
  server:
    url: https://votre-serveur-relution
    api-key: votre-cle-api
    honor-proxy-settings: true   # false par défaut ; nécessaire uniquement si
```

Dépannage

En cas de problème avec le service SMG — par exemple lors de la connexion à Exchange ou du démarrage du conteneur — augmenter le niveau de journalisation aide à l'analyse. Suivre le guide Niveau de journalisation → pour l'activer.

Le plus simple est d'activer le niveau de journalisation directement dans le conteneur SMG via son `application.yaml`, en ajoutant la section suivante à la fin :

la version 26.4.0

smg/application.yaml

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

Changelog

Version actuellement disponible via `latest` : 26.0.6 (au 06.09.2026)

Version	Catégorie	Modification
26.0.6	Corrections	Les en-têtes HTTP entrants sont désormais correctement traités sans distinction de casse, ce qui évite d'éventuels en-têtes dupliqués dans la requête transmise

Version	Catégorie	Modification
26.0.5	Configuration	La valeur par défaut de `forward-headers-strategy` est désormais `native`
		La valeur par défaut de `max-http-post-size` est désormais `1GB`
	Certificats	Journaux plus utiles concernant les certificats CA personnalisés dans le trust store
		Journaux plus utiles lorsqu'une connexion est refusée en raison d'un certificat non fiable
	Journaux	Une interruption prématurée de connexion est désormais journalisée
		Le code de statut du serveur Exchange est journalisé lorsqu'un message est rejeté
		Les erreurs HTTP sont également visibles dans le journal lors de l'utilisation de HTTP/2
		Les connexions réussies sont journalisées au niveau `INFO`
	Corrections	Les connexions terminées prématurément sont désormais correctement nettoyées
26.0.4	Processus de release	Ajustement du processus de release interne — aucune modification fonctionnelle
26.0.3	Fonctionnalité	Prise en charge des certificats auto-signés et des paramètres de proxy
26.0.2	Corrections	Correction des réponses 404 mal gérées
26.0.1	Métriques	Exposition du point d'entrée health
26.0.0	Processus de release	Code externalisé depuis Relution

Vue d'ensemble

Par défaut, Relution stocke certaines ressources - comme les applications natives - dans sa base de données. Cela peut entraîner une croissance importante de la table `resource`, en particulier lorsqu'un grand nombre d'applications natives est géré.

Pour optimiser les performances, Relution prend en charge le stockage de ces ressources dans des buckets de stockage objet externes compatibles S3.

> Utilisateurs de MinIO : MinIO a cessé son développement en octobre 2025 et ne reçoit plus de mises à jour. Nous recommandons de migrer vers SeaweedFS → à l'aide de notre guide : Migration du stockage objet →

Quand utiliser le stockage objet

L'utilisation d'un stockage objet externe est certes optionnelle, mais elle est particulièrement recommandée dans les cas suivants :

- Installation et gestion d'applications natives sur des appareils Windows
- En cas de nombre élevé d'applications natives, ou d'applications natives de plus de 50 Mo
- Pour des serveurs gérant plus de 5 000 appareils

Pour la version 26.4.0

Options disponibles

Le stockage objet le plus connu est AWS S3, mais il existe de nombreuses solutions compatibles S3 - aussi bien hébergées dans le cloud qu'auto-hébergées.

Auto-hébergé / sur site

Les solutions auto-hébergées permettent d'éviter les coûts liés au cloud et de garder un contrôle total sur les données.

Fournisseur	Description
SeaweedFS →	Recommandé. Simple à déployer, testé avec Relution. Notre guide d'installation →
Garage →	Léger, conçu pour l'auto-hébergement.
Ceph →	Adapté aux entreprises, hautement scalable.
RustFS →	Alternative basée sur Rust.
MinIO →	Non recommandé. Développement arrêté. Notre guide de migration →

Nous avons testé SeaweedFS de manière approfondie avec Relution. D'autres backends peuvent fonctionner, mais n'ont pas été testés.

Fournisseurs cloud

Pour la version 26.4.0

Fournisseur	Remarques
AWS S3 →	L'implémentation S3 d'origine, testée avec Relution.
Hetzner Object Storage →	Fournisseur allemand, économique, testé avec Relution.

Pour un hébergement Relution géré incluant le stockage objet, contacter notre équipe commerciale → – plus d'informations : Relution Cloud →

Prochaines étapes

Les étapes suivantes dépendent de la situation :

Situation	Prochaines étapes
Nouvelle installation avec SeaweedFS (recommandé)	1. Installer SeaweedFS → 2. Connecter le stockage →
Nouvelle installation avec un fournisseur cloud	1. Configuration chez le fournisseur cloud 2. Connecter le stockage →
Migration depuis MinIO ou un autre backend	– Guide de migration →

Pour la version 26.4.0

Installer SeaweedFS

SeaweedFS → est un backend de stockage objet open source sous licence Apache, avec une API compatible S3. Il offre de bonnes performances, une bonne scalabilité et un processus d'installation simple. Il peut être déployé via Kubernetes, Docker, ou directement sur Linux, FreeBSD, macOS ou Windows.

Ce guide explique comment déployer SeaweedFS aux côtés de Relution à l'aide de Docker Compose sous Linux.

Bien que nous l'ayons testé de manière approfondie, SeaweedFS est un logiciel tiers et nous ne pouvons donner aucune garantie de sécurité ou de fiabilité à son sujet.
Pour un hébergement géré, contacter notre équipe commerciale →.
Plus d'informations : Relution Cloud →

Ce guide utilise SeaweedFS en mode `mini`, qui regroupe tous les composants avec des paramètres par défaut adaptés aux déploiements mono-nœud de taille moyenne.
Pour plus d'informations : Wiki SeaweedFS →.

Pour la version 26.4.0

Prérequis

- Une installation Relution fonctionnelle avec Docker Compose
- Un accès pour modifier le fichier `compose.yml`

Préparer le compose.yml

Générer un mot de passe alphanumérique de 24 caractères à l'aide d'un gestionnaire de mots de passe, ou depuis la ligne de commande Linux :

```
pwgen -snc 24 1
```

Dans le `compose.yml` Relution (sur les installations plus anciennes : `docker-compose.yml`), ajouter le service suivant sous `services:` :

```
services:
  seaweedfs:
    image: chrislusf/seaweedfs:4.05 # Vérifiez les versions plus récentes ici
    restart: unless-stopped
    ports:
      - 23646:23646
      - 8333:8333
    command: ["mini", "-dir=/data", "-admin.dataDir=/data/admin", "-admin.pass
    networks:           # Optionnel : pour la segmentation réseau, ajoutez le
      - object-storage  # ici et dans le bloc `networks` du service `relution`
    volumes:
      - seaweedfs-data:/data
```

Ajouter deux volumes dans la section `volumes:` :

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

Pour la ver

> Important : Intégrer les volumes SeaweedFS dans la routine de sauvegarde. Sans ces données, le fonctionnement du serveur et la gestion des appareils ne peuvent pas être garantis.

Démarrer SeaweedFS

Télécharger l’image et démarrer le service :

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

SeaweedFS est prêt en quelques secondes.

Créer l’utilisateur et le bucket

SeaweedFS propose une interface web pour l’administration.

1. Se rendre sur `http://localhost:23646/` dans un navigateur
2. Se connecter avec le mot de passe généré précédemment
3. Dans la barre latérale, aller dans `Object Store` → `Users`
4. Cliquer sur Create User (en haut à droite), saisir `relution` comme nom d’utilisateur et confirmer
5. Noter l’Access Key et la Secret Key affichées (elles peuvent être récupérées plus tard via l’icône 🔑 sous *Actions*)
6. Dans la barre latérale, aller dans `Object Store` → `Buckets`
7. Cliquer sur Create Bucket, saisir `relution` comme nom, sélectionner `relution` comme propriétaire du bucket et confirmer

---

Noter les valeurs de configuration

Ces valeurs seront nécessaires pour configurer Relution :

la version 26.4.0

Paramètre	Valeur
Endpoint	`http://seaweedfs:8333`
Access Key	*(depuis l’étape 3)*
Secret Key	*(depuis l’étape 3)*
Bucket-Name	`relution`

Prochaines étapes

Configurer maintenant Relution pour utiliser le nouveau stockage objet :

Connecter le stockage →

Connecter le stockage

Une fois qu'un backend de stockage objet compatible S3 est disponible - qu'il soit auto-hébergé ou basé sur le cloud - Relution doit être configuré pour l'utiliser.

Prérequis

Les informations suivantes sont nécessaires, à demander auprès du fournisseur de stockage objet :

Paramètre	Description
Endpoint	L'URL de l'API S3
Access Key	L'ID de la clé d'authentification
Secret Key	Le secret d'authentification
Bucket-Name	Le nom du bucket de stockage

Dans les exemples de configuration ci-dessous, nous utilisons des valeurs d'exemple correspondant à notre guide SeaweedFS →. Pour un backend ou un fournisseur différent, adapter ces valeurs en conséquence.

Configuration

Choisir une des deux options suivantes. Les deux permettent d'obtenir le même résultat.

Option A : utilisation de application.yml

Ajouter ce qui suit à l'`application.yml` :

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

Option B : utilisation de variables d'environnement

Ajouter ces variables d'environnement au service `relution` dans le `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"
```

Si le stockage objet doit être chiffré avec une clé fournie par le client, cela doit être fait avant le premier démarrage : Chiffrement côté serveur (SSE-C) →

Démarrer les services

1. Télécharger les images les plus récentes :

   ```
   docker compose pull
   ```

2. Démarrer ou redémarrer les conteneurs :

```
docker compose up -d
```

3. Relution commence automatiquement la migration du contenu de la table de base de données `resource` vers le bucket de stockage objet.

Surveiller la progression

Observer la progression de la migration dans les logs :

```
docker logs -f relution
```

Il est également possible de vérifier que des fichiers sont créés en consultant le backend de stockage objet (par exemple via l'interface web de SeaweedFS ou la console du fournisseur cloud).

pour la version 26.4.0

Remarques importantes

> Processus non réversible : À partir de Relution 26.0.0, la migration vers le stockage objet ne peut pas être annulée.

> Sauvegarde : S'assurer que le bucket de stockage objet est inclus dans la routine de sauvegarde. Sans ces données, le fonctionnement du serveur et la gestion des appareils ne peuvent pas être garantis.

Chiffrement côté serveur (SSE-C)

Relution peut chiffrer les objets qu'il stocke dans un bucket compatible S3 à l'aide du chiffrement côté serveur avec une clé fournie par le client (SSE-C). Avec SSE-C, Relution envoie la clé avec chaque requête, et le backend de stockage l'utilise pour chiffrer les objets à l'écriture et les déchiffrer à la lecture. Le backend ne stocke jamais lui-même la clé : sa conservation en toute sécurité relève de la seule responsabilité de l'exploitant.

> À lire avant l'activation : SSE-C prend effet immédiatement au démarrage, et Relution ne chiffre pas les objets déjà présents dans le bucket. L'activer uniquement sur une instance neuve avec un bucket vide, ou chiffrer d'abord tous les objets existants. En cas de perte de la clé, toutes les données chiffrées sont perdues de manière définitive. Voir Remarques importantes ci-dessous pour plus de détails.

> SSE-C vs. chiffrement KMS : SSE-C n'est pas la même chose que le chiffrement côté client via AWS KMS (introduit dans Relution 26.3.3 →). Avec KMS, une clé gérée par le client (CMK) est détenue et gérée par AWS KMS. Avec SSE-C, la clé est transmise par Relution à chaque requête vers S3 et stockée uniquement par l'exploitant. Ces deux mécanismes s'excluent mutuellement - il est possible d'activer SSE-C ou KMS ou aucun des deux, mais jamais les deux en même temps.

Pour la version 26.4.0

Prérequis

- Une configuration de stockage objet compatible S3 fonctionnelle - voir Connecter le stockage →.
- Un backend de stockage objet prenant en charge SSE-C. Nous avons vérifié la prise en charge avec SeaweedFS et Hetzner Object Storage. D'autres backends compatibles S3 peuvent fonctionner, mais n'ont pas été testés.
- Une clé de 256 bits (voir ci-dessous).

Générer la clé

SSE-C nécessite une clé de 256 bits (32 octets), fournie sous forme de chaîne encodée en Base64. Une clé peut être générée avec `openssl` :

```
openssl rand -base64 32
```

Conserver la valeur obtenue en toute sécurité. En cas de perte de cette clé, tous les objets chiffrés du bucket S3 ne pourront plus être déchiffrés et seront perdus de manière définitive.

Configuration

SSE-C est activé dès qu'une clé est configurée. La clé peut être fournie soit directement via la propriété `relution.storage.s3.serverSideEncryption.key` (options A et B), soit sous forme de fichier via `relution.storage.s3.serverSideEncryption.keyFile` (option C). Si les deux sont définis, le fichier de clé est prioritaire.

Option A : utilisation de application.yml

Ajouter le bloc `serverSideEncryption` à `application.yml` :

ion 26.4.0

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

Option B : utilisation de variables d'environnement

Ajouter la variable d'environnement suivante au service `relution` dans le `compose.yml` :

```
services:
  relution:
```

```
    environment:
      - RELUTION_STORAGE_S3_SERVERSIDEENCRYPTION_KEY=%IHR-BASE64-SCHLÜSSEL%
```

Option C : clé sous forme de fichier

Nouveau dans 26.5

Au lieu d'indiquer la clé directement, il est possible de la lire depuis un fichier. Cela est particulièrement utile lorsque la clé est montée dans le conteneur sous forme de secret Docker ou Kubernetes. Le chemin vers le fichier de clé est configuré via `relution.storage.s3.serverSideEncryption.keyFile` :

```
relution:
  storage:
    s3:
      serverSideEncryption:
        keyFile: /chemin/vers/ssec.key
```

Pour la version

Ou via la variable d'environnement correspondante :

```
services:
  relution:
    environment:
      - RELUTION_STORAGE_S3_SERVERSIDEENCRYPTION_KEYFILE=/chemin/vers/ssec.key
```

Le fichier doit contenir la même clé de 256 bits encodée en Base64 que pour l'indication directe (par exemple, générée avec `openssl rand -base64 32`). Un saut de ligne final est sans conséquence, car la valeur est nettoyée ; les clés binaires ou hexadécimales sont rejetées.

Au démarrage, Relution journalise la lecture avec `Reading SSE-C key from file <chemin>`. Si le fichier est absent ou ne contient pas une clé de 32 octets, le démarrage s'interrompt avec un message d'erreur correspondant.

Remarques importantes

Aucune migration des fichiers existants : SSE-C prend effet immédiatement dès que Relution démarre avec la clé configurée. Relution ne chiffre pas les objets déjà présents dans le bucket. Utiliser SSE-C uniquement sur une instance neuve avec un bucket vide, ou chiffrer tous les objets S3 existants avant de démarrer Relution avec la clé. Sinon, les objets précédemment stockés resteront non chiffrés et pourraient devenir inaccessibles.

La perte de la clé signifie la perte des données : Le backend de stockage ne stocke pas la clé : sa conservation relève de la seule responsabilité de l'exploitant. Si la clé est perdue, tous les objets chiffrés du bucket deviennent définitivement irrécupérables, et Relution ne peut plus livrer d'applications ou de ressources depuis le stockage objet. Conserver la clé dans un endroit sûr et sauvegardé.

La rotation de la clé nécessite un rechiffrement : La rotation de la clé relève de la responsabilité de l'exploitant. Relution ne rechiffre pas les objets lors d'un changement de clé. Pour effectuer la rotation de la clé, il est nécessaire de rechiffrer tous les objets existants du bucket avec la nouvelle clé (par exemple en les copiant avec la nouvelle clé) avant de démarrer Relution avec la configuration mise à jour. Si Relution démarre avec une nouvelle clé alors que des objets sont encore chiffrés avec l'ancienne, ces objets deviendront inaccessibles.

Pour la version 26.4.0

Exclusion mutuelle avec KMS : Le chiffrement côté serveur (SSE-C) et le chiffrement côté client (KMS) ne peuvent pas être actifs simultanément. Configurer au maximum l'un des deux.

Guide de migration

Ce guide explique comment migrer les données Relution d'un backend de stockage objet vers un autre. Les scénarios courants incluent :

- La migration de MinIO vers SeaweedFS (MinIO n'est plus maintenu)
- Le passage d'un fournisseur cloud vers un hébergement auto-géré (ou l'inverse)
- Le changement de fournisseur cloud

Les exemples ci-dessous illustrent une migration de MinIO vers SeaweedFS, mais les étapes peuvent être adaptées à toute source et destination compatibles S3.

Le processus de migration comprend quatre étapes :

1. Mettre en place le nouveau backend de stockage
2. Copier les données de l'ancien vers le nouveau stockage
3. Mettre à jour la configuration de Relution
4. Supprimer l'ancien backend

Pour la version 26.4.0

Prérequis

- Un accès simultané aux deux backends de stockage
- L'outil en ligne de commande `rclone` (guide d'installation →)
- Les identifiants des deux backends de stockage

Mettre en place le nouveau backend

Pour une migration vers SeaweedFS, suivre d'abord notre guide d'installation SeaweedFS →, mais ne pas encore démarrer Relution.

S'assurer que l'ancien et le nouveau backend de stockage sont tous deux en cours d'exécution :

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

Configurer rclone

L'outil `rclone` offre un moyen rapide et fiable de copier des données entre backends compatibles S3.

Installer rclone

Suivre les instructions sur rclone.org/install → selon le système d'exploitation utilisé.

Créer les configurations distantes

Lancer l'assistant de configuration :

```
rclone config
```

Pour la version 26.4.0

Configurer la source (MinIO) :

1. Taper `n` pour un nouveau remote
2. Nom : `source`
3. Type de stockage : sélectionner `s3`
4. Fournisseur : sélectionner `Minio` (ou `Other` pour un S3 générique)
5. Saisir l'Access Key et la Secret Key
6. Endpoint : `http://localhost:9000`
7. Conserver les valeurs par défaut pour les options restantes
8. Confirmer avec `y`

Configurer la destination (SeaweedFS) :

1. Taper `n` pour un nouveau remote
2. Nom : `dest`
3. Type de stockage : sélectionner `s3`
4. Fournisseur : sélectionner `Other`
5. Saisir le nouvel Access Key et le nouveau Secret Key
6. Endpoint : `http://localhost:8333`
7. Conserver les valeurs par défaut pour les options restantes
8. Confirmer avec `y`

Taper `q` pour quitter la configuration.

Vérifier l'accès aux ports

S'assurer que les ports de l'API S3 sont exposés sur l'hôte. Vérifier le `compose.yml` :

```
minio:
  ports:
    - "9000:9000" # API S3 - doit être accessible
    - "9001:9001" # Console web
# ...
seaweedfs:
  ports:
    - "8333:8333" # API S3 - doit être accessible
    - "23646:23646" # Console web
```

Copier les données

our la version 26.4.0

1. Vérifier que Relution est arrêté afin d'éviter toute modification des données pendant la migration :

   ```
   docker compose ps  # Doit afficher les backends de stockage, mais PAS relu
   ```

2. Démarrer le transfert :

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

3. Attendre la fin du transfert. Le temps de transfert dépend de la quantité de données dans le bucket.

4. Vérifier le transfert :

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

Sortie attendue : `0 differences found`

Mettre à jour la configuration de Relution

Mettre à jour la configuration de Relution pour qu'elle pointe vers le nouveau backend. Les éléments suivants doivent être modifiés :

Paramètre	Ancienne valeur	Nouvelle valeur
Endpoint	`http://minio:9000`	`http://seaweedfs:8333`
Access Key	Ancienne clé	Nouvelle clé
Secret Key	Ancien secret	Nouveau secret

Pour une description détaillée de la configuration/modification, consulter Connecter le stockage →

Vérifier et nettoyer

1. Démarrer Relution :

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

2. Vérifier le bon fonctionnement : Se connecter à Relution et confirmer que les applications et ressources se chargent correctement.
3. Supprimer l'ancien backend (uniquement après une vérification approfondie) :

```
docker compose down minio  # Arrêtez l'ancien service
```

4. Nettoyer la configuration : Supprimer l'ancien service du `compose.yml`.
5. Supprimer les anciennes données : Supprimer l'ancien volume ou répertoire de stockage (par exemple `./volumes/minio/data`).
6. Nettoyer rclone : Il est également possible de supprimer la configuration rclone :

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

Connexion refusée / Timeout

S'assurer que les ports de l'API S3 sont exposés et non bloqués par un pare-feu ou une segmentation réseau. Tester la connectivité :

Pour la version 26.4.0

```
curl http://localhost:8333  # Doit retourner une erreur S3
```

Access denied / 401 / 403

Vérifier que les identifiants sont corrects et que l'utilisateur a accès au bucket.

Fichiers manquants après la migration

Relancer la vérification :

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

Si des différences sont détectées, relancer `rclone copy` ; seuls les fichiers manquants seront transférés.

Obsolète : MinIO

Important : MinIO a cessé son développement sans préavis en octobre 2025. Nous déconseillons donc de continuer à utiliser MinIO.

Les nouvelles informations sur le stockage objet sont disponibles ici :
Stockage objet →

Pour migrer depuis MinIO, nous avons créé un guide : Migration du stockage objet →

Pour la version 26.4.0

▸ Instructions d'installation MinIO obsolètes

Liste de contrôle

Une fois l'installation terminée, voici une liste de petites tâches à effectuer pour s'assurer que l'installation fonctionne comme prévu.

Connexion

Pour des raisons de sécurité, la connexion n'est possible que via HTTPS. Toute tentative de connexion via HTTP entraîne une erreur indiquant 'L'accès est interdit'.

Administrateur du système

L'administrateur système peut être utilisé pour créer des organisations supplémentaires.

Il est possible de se connecter à Relution en tant qu'administrateur système en utilisant les définies dans le fichier `application.yml` ou dans les variables d'environnement.

application.yml

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

Variables d'environnement

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

> Pour des raisons de sécurité, il est nécessaire de changer le mot de passe après la première connexion ! Le mot de passe sysadmin est évalué et défini uniquement lors de la création

la version 26.4.0

initiale (généralement au premier démarrage du serveur). Il ne peut pas être modifié par la suite via la configuration.

Administrateur de l’organisation

Il est possible de se connecter à Relution en tant qu’administrateur de l’organisation. En cas d’utilisation de LDAP, s’assurer qu’une connexion est possible avec au moins un compte utilisateur LDAP.

Test
La connexion avec un compte local est possible.
La connexion avec un compte LDAP est possible

Pour des raisons de sécurité, il est vivement recommandé de modifier le mot de passe après la première connexion.

Pour la version 26.4.0

Certificats

S’assurer qu’une connexion à Relution est possible en utilisant le nom d’hôte externe. Les appareils mobiles peuvent être plus stricts lorsqu’il s’agit de vérifier les certificats SSL. Même si le navigateur de bureau affiche une connexion HTTPS valide, les appareils peuvent rejeter la connexion si certains éléments ne sont pas configurés correctement. Il est vivement recommandé d’utiliser SSL Labs → pour vérifier que tout est correctement configuré.

Erreurs courantes.

- Chaîne de certificats incomplète (certificats intermédiaires manquants). Chrome, Firefox, etc. peuvent l’ignorer, mais les appareils mobiles peuvent rejeter la connexion.
- Le proxy inverse utilise l’indication du nom du serveur (SNI). Cette fonctionnalité n’est pas prise en charge par certaines anciennes versions d’Android. Comme solution de contournement, il convient de s’assurer que le certificat du serveur MDM est le premier à être renvoyé.

Les appareils mobiles rejettent le certificat

Cause possible.

- La chaîne de certificats peut être incomplète. Une chaîne incomplète est ignorée par la plupart des navigateurs de bureau, mais peut provoquer des erreurs sur les appareils mobiles.

Solution

- Utiliser SSL Labs → pour vérifier que le certificat SSL est correctement configuré. Le test dure environ 5 minutes. Corriger tous les problèmes signalés.

Les appareils mobiles reçoivent un certificat différent

Cause possible.

- Le serveur utilise peut-être l'indication de nom de serveur (SNI), qui n'est pas prise en charge par tous les appareils mobiles.

Solution

- Reconfigurer le serveur web de manière à ce que le premier certificat renvoyé soit celui requis par les appareils mobiles. Les appareils ne sont pas en mesure de demander un certificat spécifique et utilisent toujours le premier certificat envoyé par le serveur.

Pour la version 26.4.0

Sauvegardes de la base de données

S'assurer de disposer d'une sauvegarde fonctionnelle de la base de données. C'est important au cas où le matériel tomberait en panne ou qu'une mise à jour se passerait mal.

Test
La base de données de Relution est incluse dans les sauvegardes automatiques.
La base de données peut être restaurée (sur un autre ordinateur).

iOS

Nous recommandons toujours d'utiliser la famille d'applications Relution pour iOS à partir de l'App Store public. Celles-ci sont automatiquement importées dans l'App Store de Relution.

Android

Pour utiliser la version native de ces applications directement dans Relution, elles sont disponibles ici : Jusqu'à Relution Server 5.10:

- Android →

À partir de Relution Server 5.11:

- Android Companion →
- Android Agent →

Support

À des fins d'assistance, il peut être utile d'autoriser l'accès à distance au serveur Relution. Envisager d'activer ou d'installer un logiciel d'accès à distance tel que Remote Desktop, SSH ou TeamViewer. Pour une sécurité optimale, nous recommandons d'utiliser SSH avec une authentification par clé.

Envisager d'utiliser un compte utilisateur distinct pour le personnel d'assistance (par exemple, à des fins d'audit). Le personnel d'assistance a généralement besoin d'un accès en lecture et en écriture au répertoire d'installation et de la possibilité de redémarrer le service Relution. Redémarrer le service Relution.

L'assistance Relution est généralement payante.

Pour la version 26.4.0

Mail dispatch

A partir de la version 5.22 de Relution Server, la connexion au serveur SMTP peut être configurée via l'interface web. Cette connexion est nécessaire si Relution doit envoyer activement des courriels. Il peut s'agir, par exemple, de courriels de réinitialisation de mot de passe, d'inscriptions ou de notifications. La connexion à un serveur SMTP est facultative. Jusqu'à la version 5.21, la connexion au serveur SMTP devait être configurée sur le serveur via le fichier `application.yml`.

Configuration

Pour les administrateurs système, la configuration du serveur SMTP est disponible dans l'organisation `Global` sous `Paramètres` → `Configuration du serveur de messagerie`. Elle comprend les champs suivants :

- Hôte et Port
- Sécurité des connexions : Aucun, STARTTLS, STARTTLS (REQUIRETLS) ou SSL/TLS. Avec STARTTLS, Relution passe à une connexion chiffrée si le serveur la prend en charge ; avec STARTTLS (REQUIRETLS), l'envoi échoue si le serveur ne propose pas STARTTLS.
- Utiliser l'option "Extended Hello" (EHLO)
- Nom d'hôte local pour HELO/EHLO : si le champ reste vide, le nom d'hôte externe du serveur est utilisé.
- Nom d'utilisateur et Mot de passe : si le champ du mot de passe reste vide lors de la modification, le mot de passe existant est conservé.
- Adresse de l'expéditeur : champ obligatoire ; cette adresse est utilisée comme expéditeur des e-mails sortants.

Dans la section Configuration de l'e-mail de test, Envoyer envoie un e-mail de test à l'adresse e-mail enregistrée pour l'administrateur système.

Priorité entre l'interface web et application.yml

La configuration enregistrée dans l'interface web est prioritaire. Les valeurs du fichier `application.yml` ou des variables d'environnement ne sont utilisées que tant qu'aucune configuration n'est enregistrée dans l'interface web. Une configuration existante est supprimée dans la catégorie Configuration du serveur de messagerie, section Effacer la configuration, via Clair ; Relution utilise alors le fichier `application.yml`.

Pour la version 26.4.0

Les modifications du fichier `application.yml` ne prennent effet qu'après un redémarrage du serveur Relution.

---

application.yml

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

Pour la version 26.4.0

Les paramètres indiqués ci-dessus sont les valeurs par défaut s'ils ne sont pas configurés. La connectivité SMTP est testée dans le cadre du contrôle de santé du serveur, qui est affiché dans le portail du système.

L'ancienne clé `ttls` à la place de `starttls` est toujours prise en compte. Si `ssl` et `starttls` valent tous deux `true`, Relution utilise SSL/TLS.

> Relution lit la configuration de messagerie exclusivement sous `relution.mail` et `relution.smtp`. Les entrées sous `spring.mail` sont ignorées. Si la configuration s'y trouve, Relution tente d'envoyer les e-mails via `localhost` sur le port `25`.

Les valeurs peuvent également être définies via des variables d'environnement, par exemple dans une installation Docker :

Variable d'environnement	Clé dans application.yml
`SMTP_HOST`	`relution.mail.host`
`SMTP_PORT`	`relution.mail.port`
`SMTP_USERNAME`	`relution.mail.username`

Variable d’environnement	Clé dans application.yml
`SMTP_PASSWORD`	`relution.mail.password`
`SMTP_TTLS`	`relution.smtp.starttls`
`SMTP_SSL`	`relution.smtp.ssl`
`SMTP_EHLO`	`relution.smtp.ehlo`

Une valeur définie explicitement dans le fichier `application.yml` est prioritaire sur la variable d’environnement.

Options supplémentaires pour la session de messagerie

D’autres options peuvent être transmises directement à la bibliothèque de messagerie (Jakarta Mail) via `relution.mail.properties`. Les entrées sont reprises telles quelles et remplacent les valeurs définies par Relution. Elles ne s’appliquent que tant que la configuration provient du fichier `application.yml`, c’est-à-dire qu’aucune configuration n’est enregistrée dans l’interface web.

Pour la version 26.4.0

```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
```

Les clés contiennent des points et sont donc placées entre crochets et guillemets. Options fréquemment utilisées :

Option	Effet
`mail.smtp.from`	Adresse de l'expéditeur. Sans indication, Relution forme une adresse à partir de l'URL externe du serveur (`no-reply+relution@<domaine>`).
`mail.smtp.localhost`	Nom d'hôte annoncé dans la commande `EHLO`. Sans indication, le nom d'hôte de l'URL externe du serveur est utilisé.
`mail.smtp.starttls.required`	Interrompt l'envoi si le serveur ne propose pas STARTTLS.
`mail.smtp.ssl.trust`	Hôtes dont le certificat est accepté sans vérification. Utile pour les serveurs de messagerie dont la chaîne de certificats est incomplète.

`mail.smtp.ssl.trust` doit contenir le nom d'hôte précis du serveur de messagerie. La valeur `*` fait confiance à tout certificat de tout serveur. La meilleure solution reste d'ajouter le certificat de l'autorité de certification émettrice au truststore.

Pour la version 26.4.0

En cas d'échec de l'envoi, Relution journalise l'intégralité de la communication SMTP dès que le niveau de log de `io.relution.setting.system.email.SystemEmailConfigurationService` est réglé sur `DEBUG`. Adapter le niveau de log →

Amazon Simple Email Service (SES) SMTP

Les paramètres recommandés pour la connexion à Amazon SES sont les suivants :

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

```
    ssl: false
    ehlo: true
```

Les paramètres SMTP `username` et `password` sont une clé d'accès AWS et une clé secrète d'un utilisateur IAM avec les permissions `AmazonSesSendingAccess`, qui doivent être des permissions `ses:SendRawEmail`. S'assurer que la bonne région est spécifiée dans `host`. Ces paramètres peuvent être trouvés sur la page `SMTP Settings` du service SES dans la console AWS.

Microsoft Office365 SMTP

Les paramètres recommandés pour pouvoir envoyer du courrier via Office 365 sont les suivants :

L'Adresse de l'expéditeur sous `Paramètres` → `Configuration du serveur de messagerie` doit correspondre au nom d'utilisateur du compte. Si la configuration est effectuée via le fichier `application.yml`, l'adresse de l'expéditeur est définie via `mail.smtp.from` (voir Options supplémentaires pour la session de messagerie →). SMTP AUTH doit être activé pour le compte.

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

Disaster Recovery

Ce guide décrit le concept de sauvegarde et de sécurisation d'un serveur Relution qui utilise une base de données (PostgreSQL ou MariaDB) et intègre éventuellement un système de stockage compatible S3 exploité on-premises (par exemple MinIO).

L'objectif est de garantir l'intégrité des données, de minimiser les temps d'arrêt (RTO) et d'assurer une restaurabilité fiable en cas d'urgence.

> La configuration de l'automatisation des sauvegardes, la surveillance ainsi que la garantie de l'exécution des sauvegardes relèvent de la responsabilité du client.

Vue d'ensemble du système

L'infrastructure Relution se compose généralement des composants suivants, qui doivent être sauvegardés :

- Serveur d'application : héberge l'application et les services Relution.
- Base de données (on-premises) : MariaDB ou PostgreSQL.
- Stockage S3 (on-premises) : système de stockage objet (optionnel) pour le dépôt de fichiers, de sauvegardes et de données persistantes.

Pour la version 26.4.0

> Toutes les applications peuvent également être exploitées ensemble sur une seule machine. L'utilisation du stockage S3 est optionnelle, mais si elle est utilisée, le fonctionnement du serveur Relution est impossible sans le contenu du bucket S3.

Objectifs de sauvegarde

- Minimisation de la perte de données (RPO – Recovery Point Objective)
- Restauration rapide des services (RTO – Recovery Time Objective)
- Protection contre les pannes matérielles, les erreurs logicielles et les erreurs humaines
- Protection contre la manipulation de données ainsi que contre les ransomwares

1. Sauvegarde de la base de données

Stratégie	Détails
Fréquence	Dumps complets quotidiens (par ex. via `mariadb-dump` ou `pg_dump`)
Incrémentiel	Sauvegardes incrémentielles horaires (selon les besoins)
Gestion	Rotation automatisée et règles de conservation
Sécurité	Chiffrement des fichiers de sauvegarde (AES256 ou GPG) selon les besoins
Cohérence	Pendant la sauvegarde, le service Relution devrait être temporairement arrêté afin d'éviter les incohérences !

Pour la version 26.4.0

2. Sauvegarde du stockage S3 (optionnel)

Stratégie	Détails
Méthode	Réplication vers une seconde cible S3 ou synchronisation régulière (`s3cmd sync`, `rclone sync`)
Périmètre	Sauvegarde des buckets critiques à des intervalles définis
Cohérence	Pendant la sauvegarde, le service Relution devrait être temporairement arrêté afin d'éviter les incohérences !

3. Sauvegarde de la configuration du serveur

Tous les fichiers de configuration pertinents doivent être sauvegardés :

- `/opt/relution` (répertoire du serveur Relution)
- `compose.yml` (ou scripts de démarrage comparables)
- `application.yml` (configuration Relution)
- Le cas échéant, le fichier de configuration NginX
- Le certificat SSL et la clé

Emplacements de stockage des sauvegardes

Le respect du principe de sauvegarde 3-2-1 est recommandé :

- 3 copies des données
- 2 systèmes/supports différents
- 1 copie externe/hors site

Planification

sion 26.4.0

Intervalle	Sauvegarde
Quotidien	Sauvegarde complète de la base de données
Horaire	Sauvegarde incrémentielle de la base (selon les besoins)
Quotidien	Synchronisation S3 des buckets critiques
Hebdomadaire	Sauvegarde complète de la configuration du serveur

---

Autres aspects

Domaine	Détails
Automatisation	Cronjobs ou timers systemd ; journalisation de tous les processus ; notifications en cas d’erreur
Chiffrement	Chiffrement de toutes les sauvegardes ; TLS/HTTPS/SSH pour le transport
Contrôle d’intégrité	Restauration test mensuelle

---

1. Restauration de la base de données

1. Sélection du fichier de sauvegarde correct
2. Préparation du système cible (arrêt du service de base de données)
3. Exécution de l’import des données (par ex. via `psql` ou `mysql`)
4. Test fonctionnel de l’application Relution

Pour la version 26.4.0

---

2. Restauration du stockage S3

1. Sélection des objets/buckets
2. Restauration via `rclone`, `s3cmd` ou API
3. Contrôle d’intégrité (vérifier que les fichiers sont présents dans Relution)

---

3. Restauration complète du système

- Restauration des configurations (à partir des sauvegardes de configuration du serveur)
- Redémarrage de tous les services
- Test fonctionnel de l’ensemble de l’application

Surveillance et alerte

- Surveillance de tous les processus de sauvegarde (par ex. avec des outils tels que Grafana + Prometheus)
- Alertes en cas de :
  - Erreurs lors de la sauvegarde
  - Espace de stockage faible
  - Erreurs d'intégrité
  - Échecs de la restauration test

Sécurité

- Restrictions d'accès (principe du moindre privilège)
- Stockage sécurisé des clés et des identifiants
- Mises à jour régulières des logiciels utilisés

Pour la version 26.4.0

Documentation

- Documentation de toutes les modifications de processus (configuration, plannings)
- Responsabilités claires pour la sauvegarde et la restauration
- Conservation des journaux pendant au moins 90 jours

Conclusion

Ce concept de sécurisation garantit que la base de données et le système de stockage S3 on-premises sont tous deux protégés de manière fiable et peuvent être rapidement restaurés en cas d'urgence. Grâce à l'automatisation et à des contrôles réguliers, la sécurité opérationnelle est assurée à long terme.

Update - Relution

Les étapes suivantes permettent de mettre à jour l'installation Relution.

> Avant de commencer, s'assurer qu'une sauvegarde fonctionnelle de la base de données et, le cas échéant, du stockage S3 a été effectuée ! En règle générale, un snapshot du serveur est également suffisant.

Installation Docker

Modifier le fichier `docker-compose.yml` et remplacer `image : relution/relution:xxx` par `image : relution/relution:latest`.

La mise à jour de Relution est alors très simple :

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

Dans les nouvelles versions de Docker, l'orthographe a changé pour docker compose sans trait d'union.

S'assurer de comparer `docker_relution` avec le nom du conteneur Relution `container_name` spécifié dans le `docker-compose.yml`, s'il est différent de celui par défaut.

Cette commande téléchargera la dernière version de l'image Docker et l'installera. Le service Relution sera indisponible pendant quelques minutes pendant le redémarrage du conteneur.

La commande suivante peut être utilisée pour supprimer les anciens conteneurs et caches, ce qui peut libérer beaucoup de mémoire.

```
docker system prune -a
```

```
ATTENTION ! Ceci va supprimer :
  - tous les conteneurs arrêtés
  - tous les réseaux non utilisés par au moins un conteneur
  - toutes les images qui ne sont pas associées à au moins un conteneur
  - tout le cache de construction

Etes-vous sûr de vouloir continuer ? [y/N]
```

Installation native Linux

1. Télécharger le dernier paquetage de Relution : Latest Relution Package →
2. Arrêter le service Relution
3. Sauvegarder la base de données Relution
4. Sauvegarder le répertoire d'installation

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

5. Extraire le paquet zip dans `<INSTALL_DIR>`
6. Définir le propriétaire du répertoire `<INSTALL_DIR>`, par exemple :

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

7. Copier `<INSTALL_DIR>.bak/application.yml` dans `<INSTALL_DIR>/application.yml`
8. Démarrer le service Relution
9. Attendre que le service Relution soit démarré

La base de données sera mise à jour vers la dernière version. La mise à jour de la base de données peut prendre un certain temps

---

Installation native Windows

1. Télécharger le dernier paquet Relution : Latest Relution Package →
2. Arrêter le service Relution via la console Services (`services.msc`)
3. Enregistrer le répertoire d'installation existant sous `relution_bak_`
4. Extraire le paquet zip dans l'ancien répertoire d'installation `<INSTALL_DIR>`
5. Copier le fichier de configuration de la sauvegarde `relution_bak_/application.yml` dans `<INSTALL_DIR>/application.yml`
6. Démarrer le service Relution
7. Attendre que le service Relution ait démarré. dans le répertoire `<INSTALL_DIR>/log/relution.txt`, le journal peut être consulté

   La base de données est en train d'être mise à jour vers la dernière version. La mise à jour de la base de données peut prendre un certain temps."

la version 26.4.0

Messages d'erreur connus

```
Le service "Relution" sur "Ordinateur local" n'a pas pu être démarré
Le service n'a pas renvoyé d'erreur.
Il peut s'agir d'une erreur interne de Windows ou d'une erreur interne du serv
Veuillez contacter votre administrateur système si le problème persiste.
```

Si ce message s'affiche lors du démarrage du service Relution, cela peut indiquer que la version de Java utilisée est trop faible. Pour résoudre ce problème, télécharger et installer la dernière version de Java 17 LTS à partir du lien suivant : Adoptium Java →
. Pendant l'installation, activer l'option `Set Home PATH` ; sinon, le Home PATH devra être entré manuellement dans les variables Windows par la suite.
Après l'installation, redémarrer le service Relution.

Liste de contrôle après la mise à jour.

- Les applications de relution sur les appareils mobiles doivent-elles également être mises à jour ?
- Les fichiers CSS personnalisés doivent-ils être mis à jour ?
- Les appareils inscrits sont-ils toujours accessibles ?
  - Envoyer une action `update device information` à un appareil
- L'inscription fonctionne-t-elle toujours pour les différentes plateformes ?

Remarque : Mise à jour de Relution 5.3x.x vers 26.2.x

Lors d'une mise à jour de `Relution 5.3x.x` vers `Relution 26.2.x`, il est impératif de passer d'abord par la version intermédiaire `Relution 26.0.3`.

Docker

Pour les installations Docker, la version peut être définie directement dans le fichier `compose.yml`.

Pour la version 26.4.0

1. D'abord, mettre à jour vers la dernière version 5.x publiée :

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

2. Ensuite, mettre à jour vers la dernière version 26.0.x publiée :

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

3. Après une mise à jour réussie, la version peut être remise sur `latest` afin d'utiliser automatiquement la version la plus récente disponible :

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

Linux et Windows (natif)

Pour les installations natives sous Linux et Windows, la procédure est identique à celle de Docker :

1. Mise à jour vers `Relution 5.35.4`
2. Mise à jour vers `Relution 26.0.3`
3. Mise à jour vers la version la plus récente (`latest`)

Téléchargements :

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

Pour la version 26.4.0

Certificats de poussée APNS

Pour communiquer avec les appareils Apple via MDM, Relution nécessite un certificat push APNS signé → (Apple Push Notification service). Ce certificat est lié à un identifiant Apple (Apple ID) et doit être renouvelé avant son expiration.
Si un certificat expire, tous les appareils Apple inscrits perdent leur connexion MDM et doivent être réinscrits.

> À partir de Relution 26.3.0, les nouvelles installations sont tenues de fournir leur propre certificat APNS via l'assistant en libre-service décrit sur cette page. Les installations existantes continueront de fonctionner avec leur configuration actuelle et pourront migrer vers la nouvelle méthode à leur propre rythme.

> Toujours renouveler le certificat existant au lieu d'en créer un nouveau. En cas de téléversement d'un certificat avec un sujet push différent, les appareils inscrits continueront d'utiliser l'ancien certificat jusqu'à son expiration — après quoi, ils devront être réinscrits.

Migration depuis le processus précédent

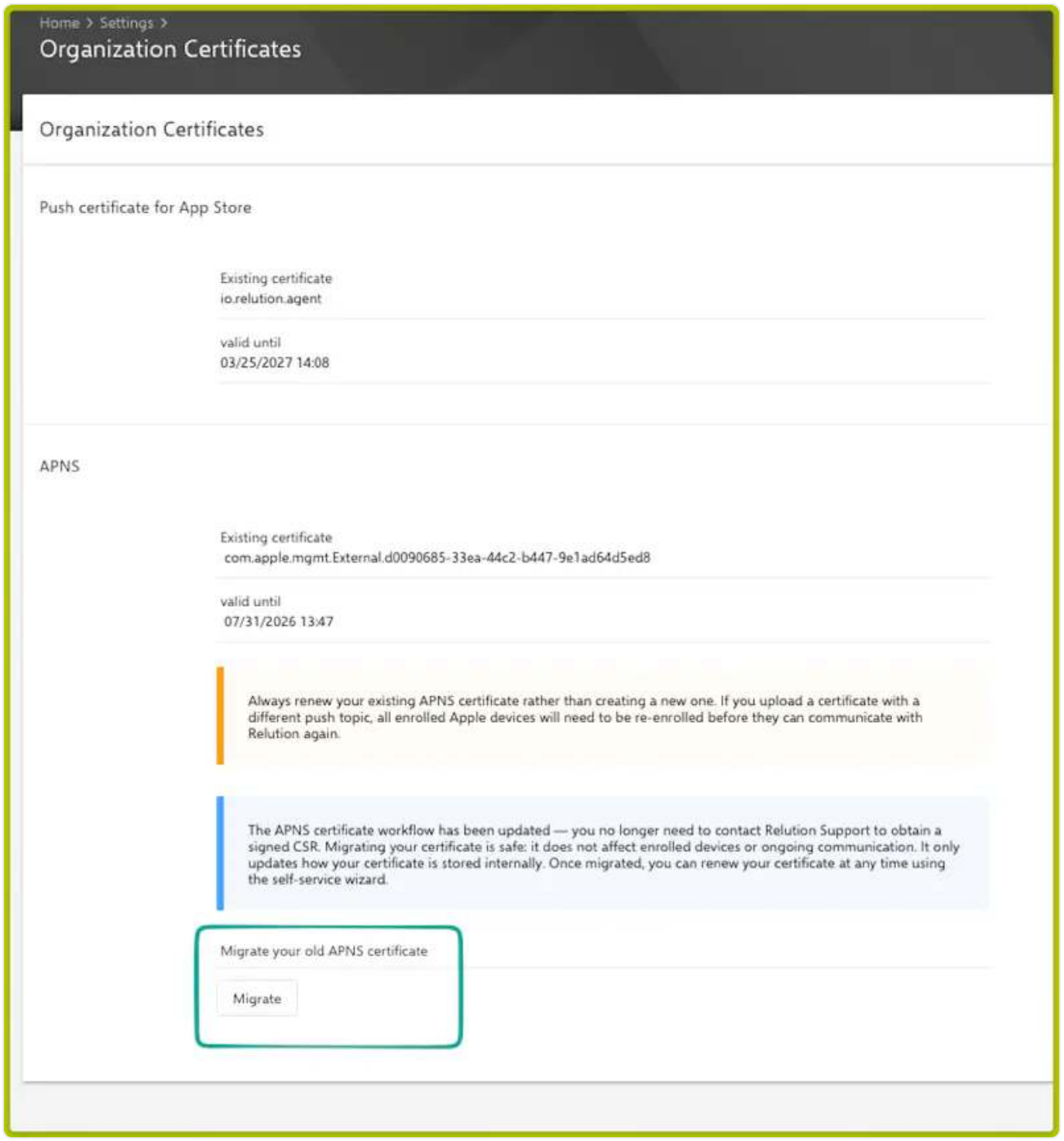
Nouveau dans 26.3

> Cette section s'applique uniquement en cas de certificat APNS personnalisé déjà fourni en envoyant une CSR au support Relution. Pour une nouvelle installation, ou si le certificat par défaut de Relution était utilisé, ignorer cette section.

Si l'installation Relution a été configurée avant la version 26.3.0 et qu'un certificat a été précédemment fourni en envoyant une CSR au support Relution, une migration unique doit être effectuée avant de pouvoir utiliser l'assistant en libre-service.

Accéder à `Paramètres` → `Certificats de l'organisation`. Si une migration est disponible pour l'organisation concernée, une boîte d'information s'affiche avec un bouton intitulé Migrer l'ancien certificat APNS. Cliquer dessus.

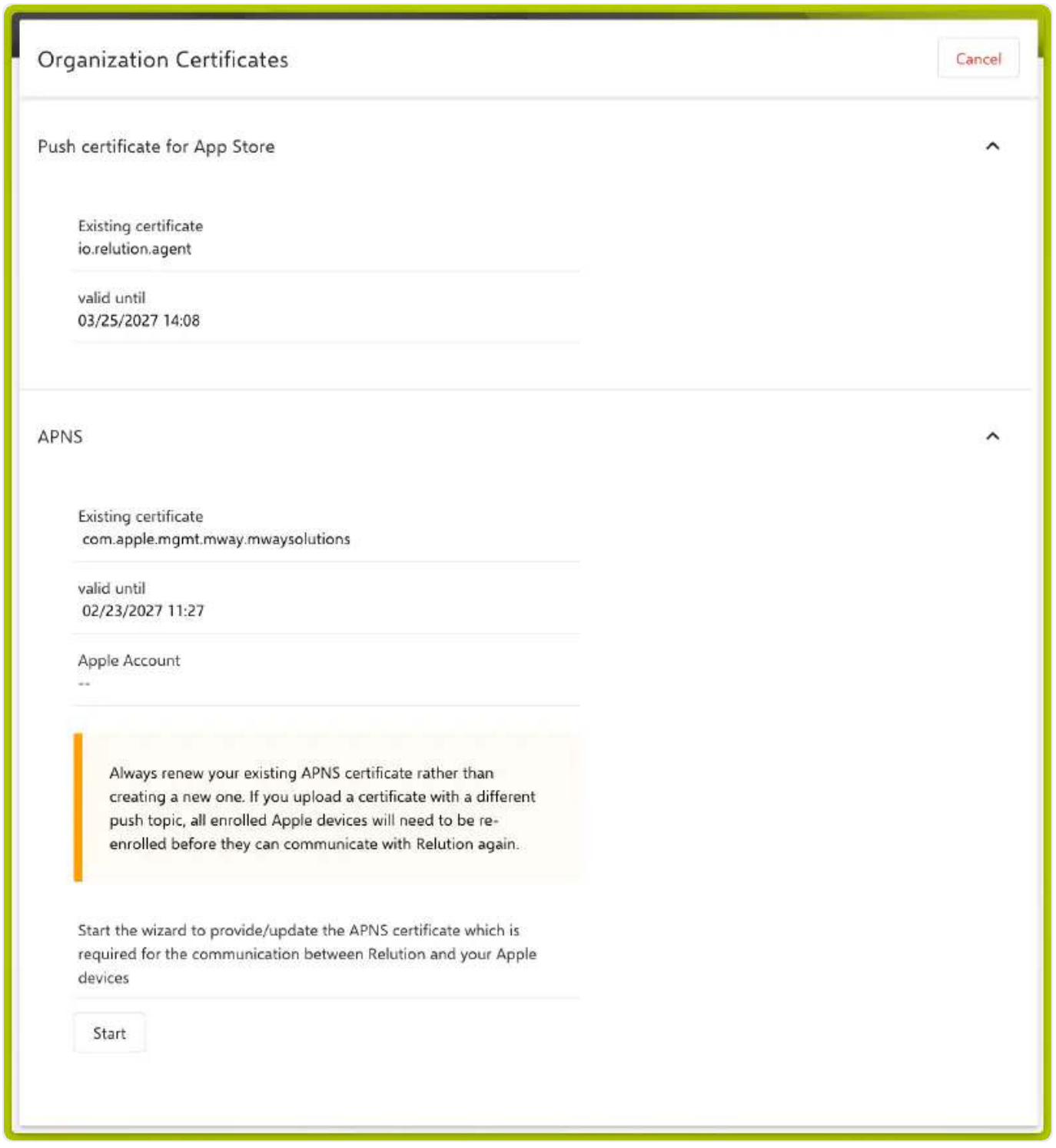
Pour la version 26.4.0



La migration est instantanée et sécurisée : elle n’a aucun impact sur les appareils inscrits ni sur la communication MDM en cours. Elle met simplement à jour la manière dont le certificat est stocké en interne dans Relution. Après la migration, l’assistant en libre-service pourra être utilisé pour tous les futurs renouvellements de certificats.

Configuration ou renouvellement d’un certificat

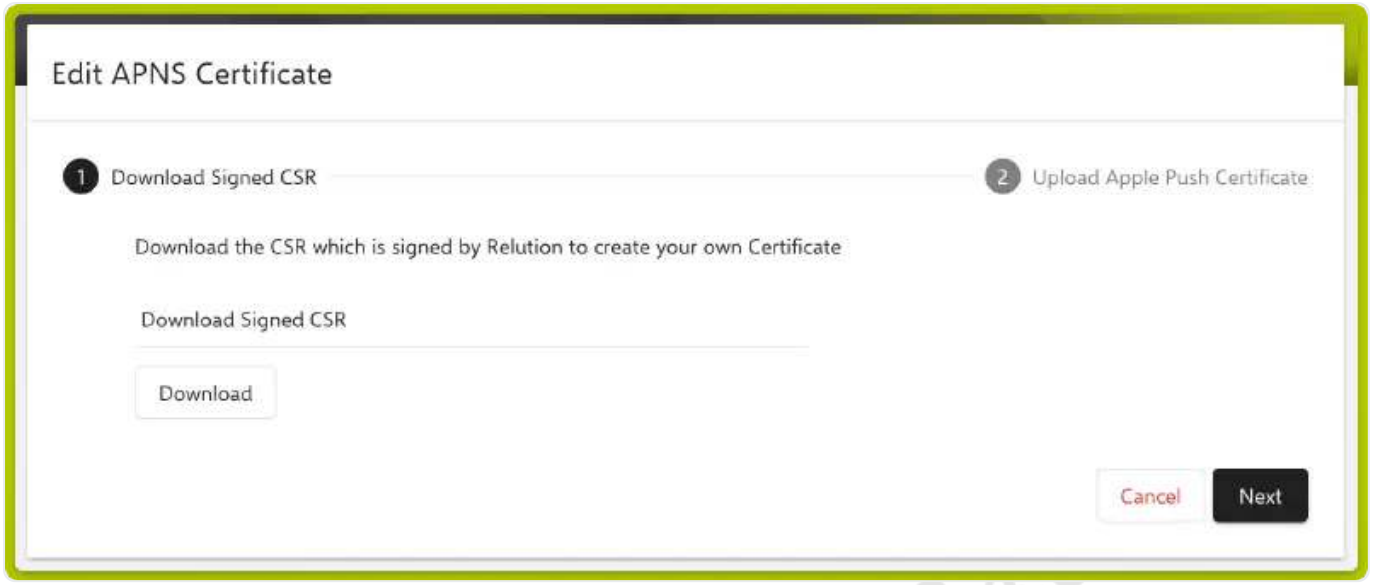
Accéder à `Paramètres` → `Certificats de l'organisation` et cliquer sur Démarrer dans la section APNS.



L’assistant de certificat APNS s’ouvre alors.

1. Télécharger la CSR signée

Relution génère et signe automatiquement une demande de signature de certificat (CSR). Cliquer sur Télécharger pour la sauvegarder. Attendre que le téléchargement soit terminé avant de cliquer sur Suivant.



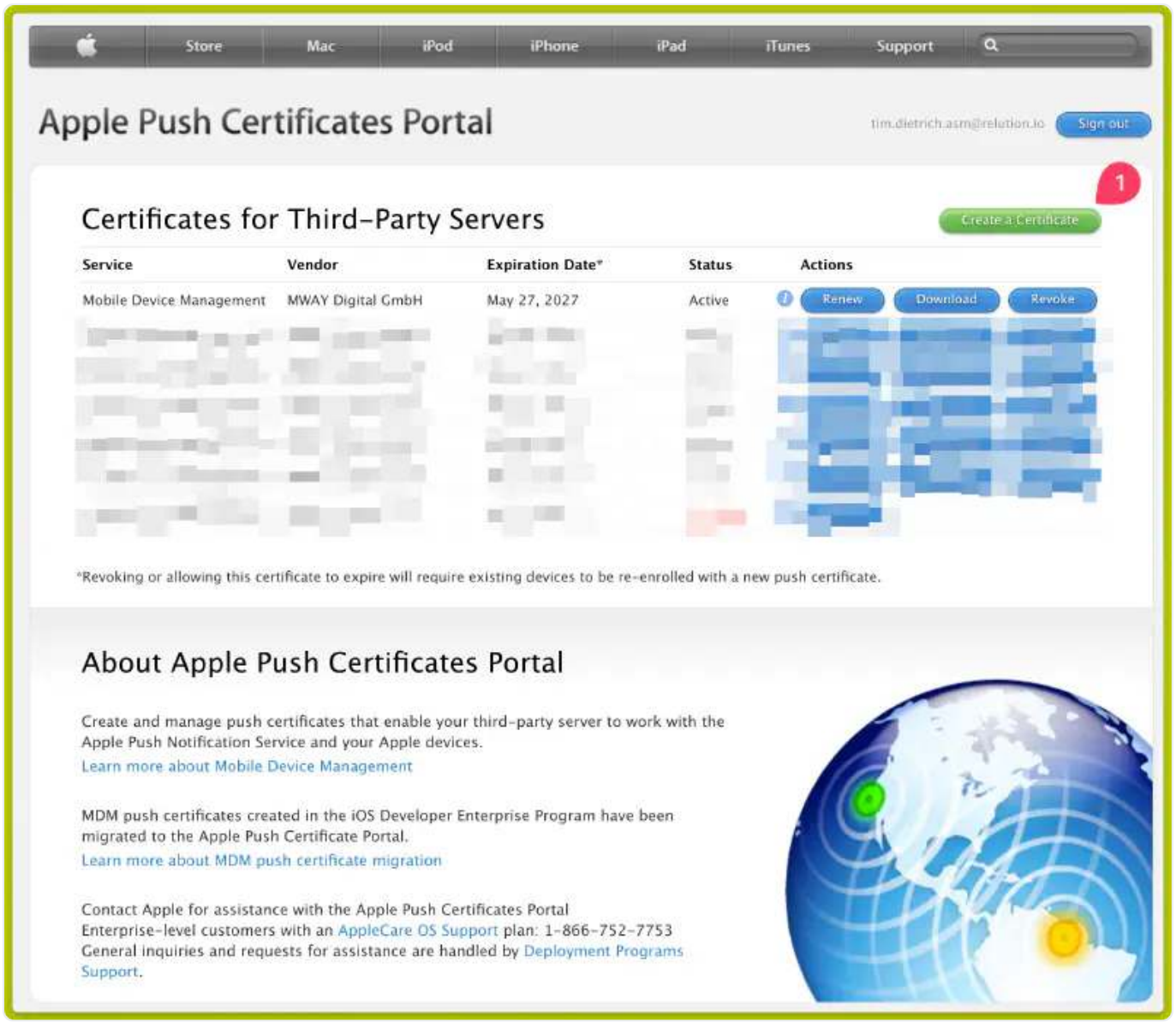
Pour la version 26.4.0

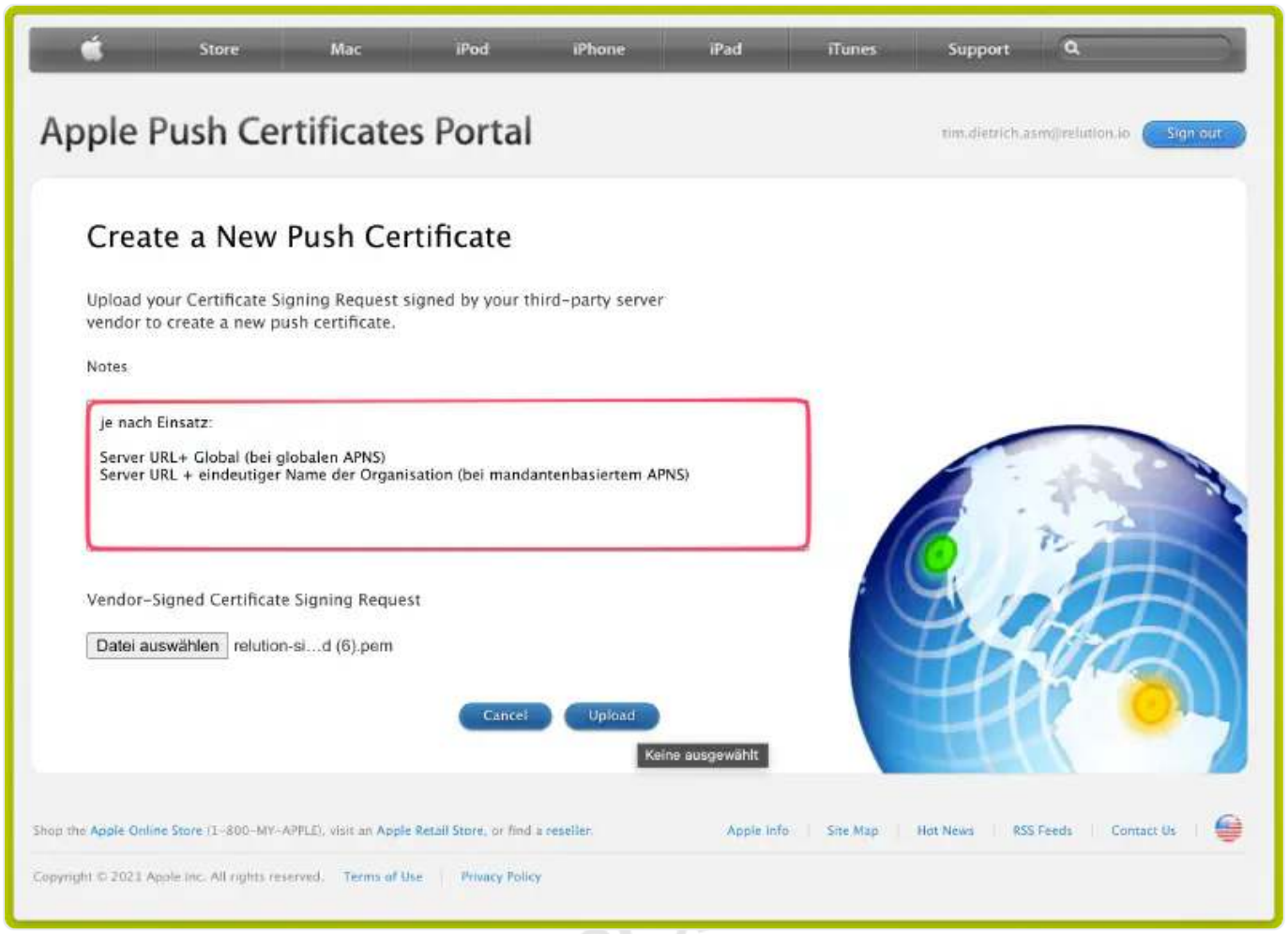
2. Téléverser le certificat Apple Push

Ouvrir le portail des certificats Apple Push (Apple Push Certificates Portal) → et se connecter avec le compte Apple concerné.

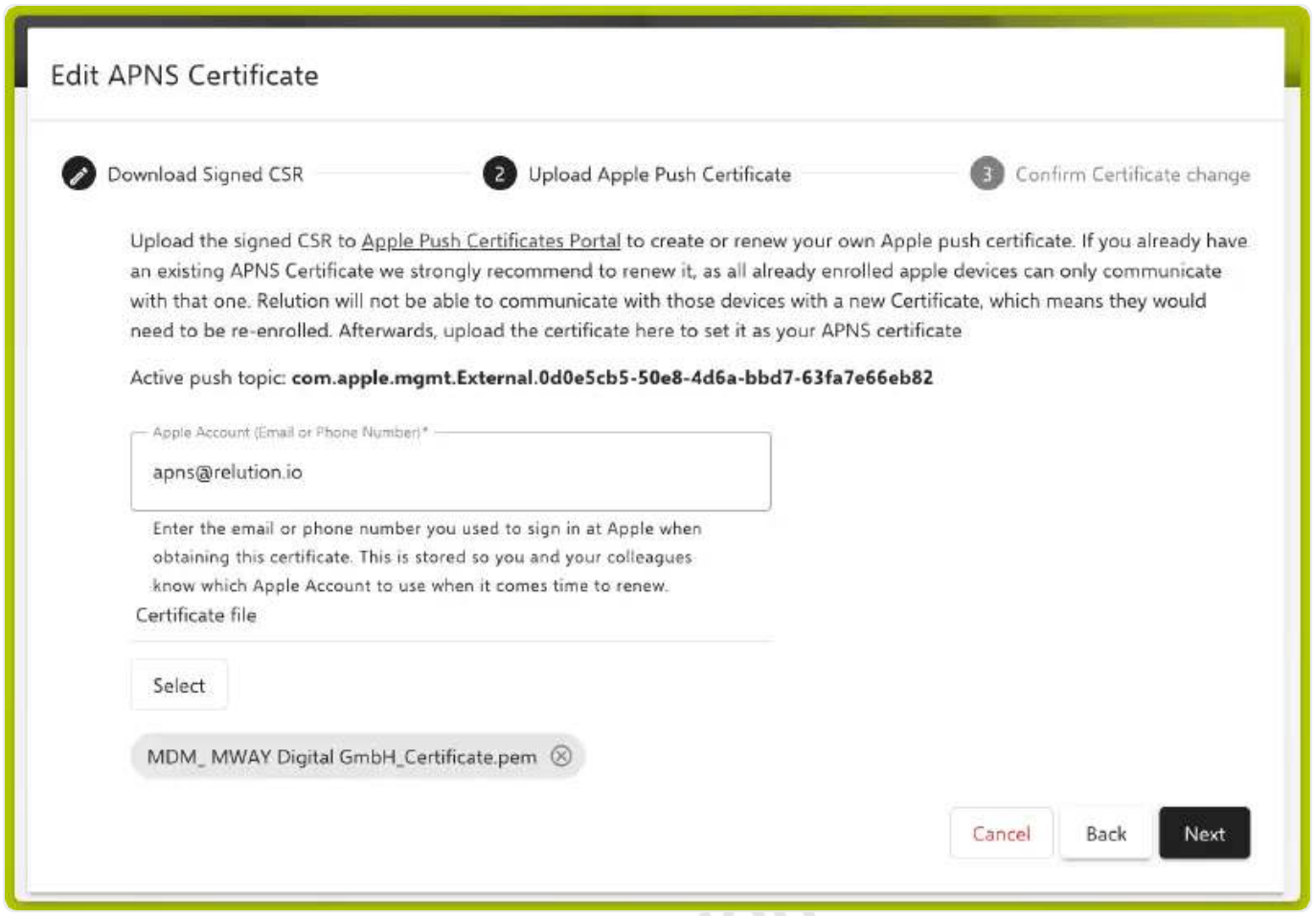
- Renouvellement d'un certificat existant : Rechercher le certificat concerné dans la liste et cliquer sur Renew. Téléverser le fichier CSR obtenu à l'étape 1. Cela permet de conserver le même sujet push (push topic), de sorte que les appareils inscrits n'ont pas besoin d'être réinscrits.
- Nouvelle installation : Cliquer sur Create a Certificate et téléverser le fichier CSR.

Télécharger le fichier de certificat `.pem` depuis le portail Apple.


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



Saisir le compte Apple qui a généré le certificat dans le champ de texte libre.

Téléverser le certificat dans Relution à l'aide de la zone de téléversement de fichiers prévue à cette étape.

Le sujet push actif est affiché au-dessus de la zone de téléversement. S'assurer de renouveler le bon certificat — le sujet push du certificat téléversé doit correspondre à celui affiché.

- Si le sujet push correspond, cliquer sur Enregistrer — l'assistant est terminé.
- Si le sujet push a changé, l'assistant passe à l'étape 3.

3. Confirmer le changement de certificat (uniquement en cas de conflit de sujet push)

Cette étape n'apparaît que si le certificat téléversé présente un sujet push différent de l'actuel. Cela peut se produire si un nouveau certificat a été créé au lieu de renouveler l'existant, ou si un autre identifiant Apple a été utilisé.

> Lors de la première utilisation de l'assistant dans une organisation qui utilisait auparavant le certificat par défaut de Relution, un conflit de sujet push est attendu — le nouveau certificat

aura un sujet push différent. Un certificat configuré sur l'organisation globale s'applique à toutes les organisations ; un certificat sur une méta-organisation s'applique à toutes ses sous-organisations. Les organisations individuelles peuvent le remplacer par leur propre certificat. Avant de confirmer, vérifier quelles organisations héritent de ce paramètre et si des appareils Apple sont inscrits dans ce périmètre.

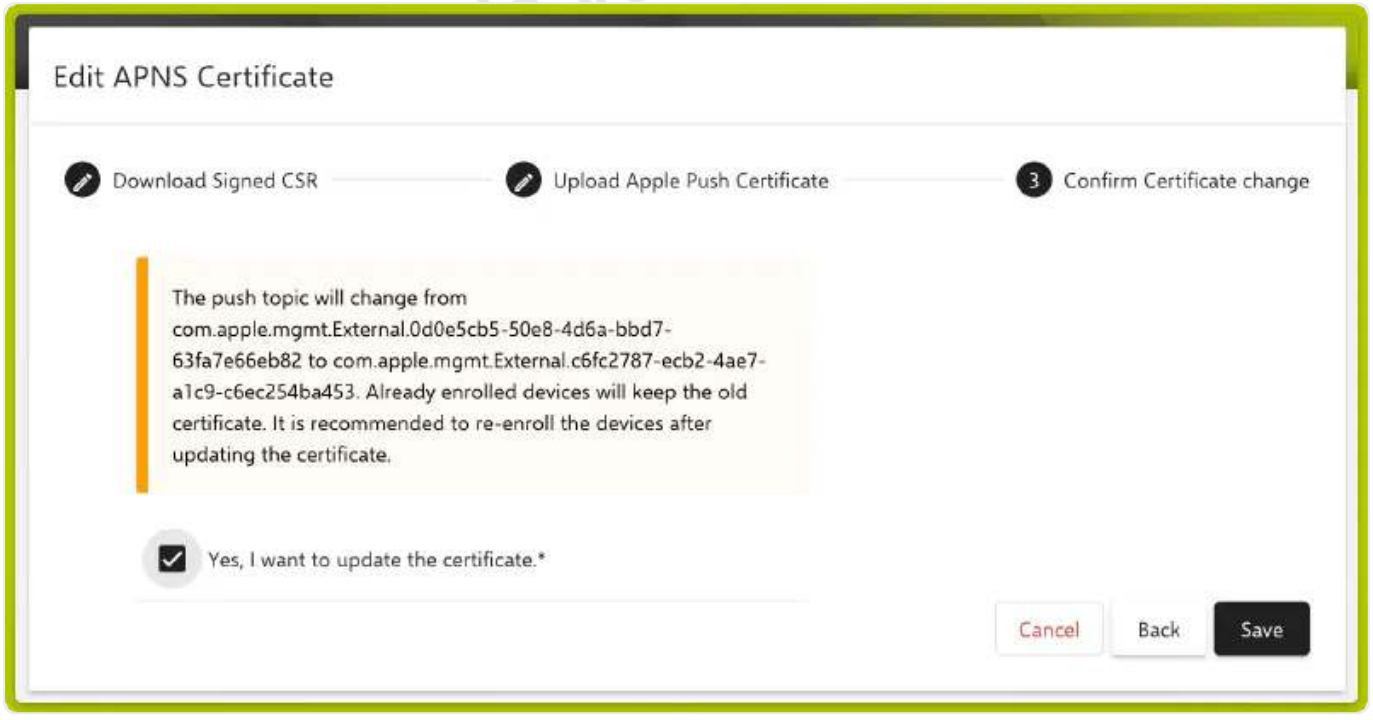
La modification du sujet push affecte les appareils Apple inscrits dans l'organisation concernée :

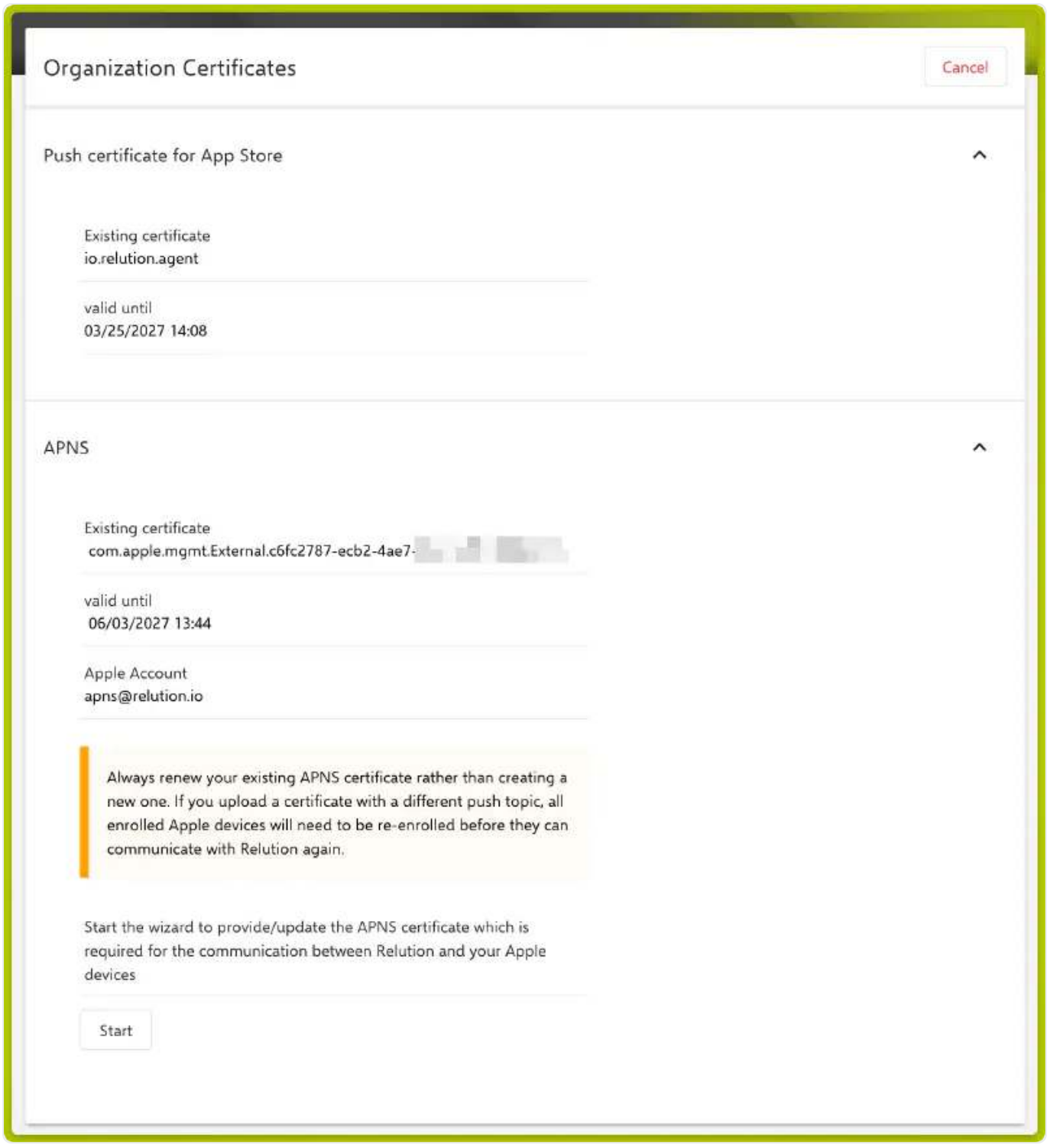
- En cas de passage du certificat Relution à un certificat propre : Les appareils existants continueront d'utiliser le certificat fourni par Relution — aucune réinscription immédiate n'est requise. Relution prévoit de retirer le certificat partagé à l'avenir, mais veillera à fournir un délai de migration suffisant.
- En cas de remplacement du certificat existant par un autre : Les appareils inscrits continueront d'utiliser l'ancien certificat jusqu'à son expiration. Une fois expiré, ils perdront la connexion MDM et devront être réinscrits.

L'assistant affiche l'ancien et le nouveau sujet push. Pour confirmer le changement :

1. Cocher la case Oui, je souhaite mettre à jour le certificat pour confirmer.

Cliquer sur Enregistrer pour appliquer la modification.





Expiration et renouvellement du certificat

La page Certificats de l'organisation affiche la date d'expiration du certificat actif. Relution envoie un avertissement lorsque la date d'expiration approche.

Renouveler le certificat avant son expiration. En cas de dépassement de la date limite :

- Tous les appareils Apple inscrits perdent instantanément leur connexion MDM.
- Les appareils devront être réinscrits une fois le certificat renouvelé téléversé.

Remarques

- Toujours utiliser le même identifiant Apple lors du renouvellement d’un certificat. L’utilisation d’un identifiant Apple différent crée un nouveau sujet push et nécessite une réinscription complète de tous les appareils.
- Toujours renouveler le certificat existant au lieu d’en créer un nouveau. En cas de téléversement d’un certificat avec un sujet push différent, les appareils inscrits continueront d’utiliser l’ancien certificat jusqu’à son expiration — après quoi, ils devront être réinscrits.
- Si un certificat expire, tous les appareils Apple inscrits perdent leur connexion MDM et doivent être réinscrits.

Pour la version 26.4.0

Certificat de signature iOS

> Si un certificat de signature personnalisé n'est pas nécessaire, Relution fournit un certificat de signature valide à partir de la version 5.

Lors de l'enrôlement d'appareils Apple, Relution délivre un certificat de signature dans la configuration de base qui n'est pas fiable et qui a expiré. Il ne s'agit pas d'un problème fonctionnel, mais il peut être résolu en modifiant la configuration. À trouver sur l'appareil sous `Réglages` → `Général` → `VPN et gestion des appareils` → `Profil MDM` → `Certificat de signature`

```
CERTIFICAT DE SIGNATURE
scep-WIN2008SCEP-CA
Délivré par : scep-WIN2008SCEP-CA
Expiré le : 28 octobre 2015
```

Pour la version

Ajuster la configuration

Le certificat peut être modifié. Dans ce cas, la section suivante doit être ajoutée au fichier `application.yml` :

```
relution :
  signer :
    certificatePath : "CHEMIN D'ACCÈS À VOTRE CERTIFICAT"
    keyPath : "CHEMIN D'ACCÈS À VOTRE CLÉ"
```

Relution s'attend à ce que les fichiers se trouvent toujours dans `/opt/relution`. Lors de l'ajout des deux chemins, seul le nom de fichier du certificat doit être indiqué, si celui-ci est stocké dans `/opt/relution`.

Dans cet exemple, le certificat et la clé correspondante doivent être stockés dans le chemin approprié.

Environnement Docker

Si Relution est exploité dans Docker, les certificats doivent toujours être montés dans le conteneur correspondant :

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

Le volume application.yml ne doit être ajouté que s'il n'existe pas encore de fichier de ce type.

Pour la version 26.4.0

Convertir le certificat SSL

Les certificats PFX sont utilisés pour stocker les identités numériques et le cryptage dans un format de fichier. Leur conversion est nécessaire pour assurer la compatibilité entre différents systèmes. La conversion vers d'autres formats tels que PEM permet d'utiliser les certificats dans un plus grand nombre d'applications.

Conversion en fichiers PEM séparés

Extraction de la clé privée d'un fichier PFX vers un fichier PEM

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

Supprimer le mot de passe de la clé privée extraite

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

Exporter le certificat

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

> L'intermédiaire doit être inclus dans server.pem, ceci peut être facilement vérifié et corrigé sur la page suivante WhatsMyChainCert →

SMG

Lors de l'utilisation de SMG, la chaîne de certificats complète doit être exportée en tant que `server.pem`.

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

Pour la version 26.4.0

Renouveler le certificat SSL

Un certificat SSL expiré du serveur affecte la gestion des appareils inscrits. Il est donc important de mettre à jour régulièrement le certificat SSL pour garantir un fonctionnement et un contrôle sans faille des appareils.

Le certificat doit être renouvelé. La procédure diffère selon le système d'exploitation et l'installation.

Docker

Pour une installation Docker, procéder comme suit :

1. Vérifier le fichier `docker-compose.yml` pour voir où le certificat ou la `clé` est stocké. Habituellement, ces fichiers sont nommés `server.pem` et `server.key`. Ils sont généralement situés dans le même répertoire
2. Rechercher la section suivante dans le fichier `docker-compose.yml`

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

3. Dans cet exemple, les fichiers sont dans le même répertoire que `docker-compose.yml`
4. Remplacer le fichier `server.pem` par le nouveau certificat. Il est également possible d'ouvrir le fichier et de remplacer le contenu
5. Redémarrer le conteneur Docker. Pour ce faire, utiliser les commandes `docker compose down` pour arrêter le conteneur et ensuite `docker compose up -d` pour le redémarrer.

Installation native Windows avec nginx

Pour une installation sous Windows, procéder comme suit :

1. Si le fichier `server.pem` n'est pas dans le répertoire `%ProgramFiles%\nginx\conf`, vérifier le fichier `nginx.conf` pour voir où le certificat a été placé. Ce fichier se trouve généralement dans `%ProgramFiles%\nginx\conf\nginx.conf`
2. Dans ce fichier, chercher cette section :

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

Remplacer le fichier `server.pem` par celui du nouveau certificat, ou ouvrir le fichier dans un éditeur (exécuté en tant qu'administrateur) et remplacer le contenu par celui du nouveau certificat. Redémarrer ensuite le service `nginx`.

Installation native CentOS Linux avec nginx

Pour une installation Linux native, procéder comme suit

1. Vérifier si le certificat expiré se trouve dans `/etc/pki/tls/certs/server.pem`
2. Si c'est le cas, faire une copie, ouvrir le fichier, supprimer le contenu et copier le contenu du nouveau certificat dans le fichier `server.pem`.
3. Alternativement, renommer le fichier existant et placer le nouveau certificat sous le nom `server.pem` dans ce chemin.

```
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. Après cela, le service `nginx` doit être redémarré. Pour ce faire, taper `systemctl stop nginx` suivi de `systemctl start nginx`

Pour la version 26.4.0

Certbot

Il peut arriver que Certbot n’ait pas demandé de nouveau certificat pour diverses raisons. Il est alors possible de le faire manuellement. Pour ce faire, taper `certbot renew` dans la console pour demander un nouveau certificat.

Pour la version 26.4.0

Certificat CA dans Docker

Pour connecter des services utilisant un certificat TLS auto-signé ou interne à l'entreprise, l'autorité de certification racine ou intermédiaire correspondante doit être ajoutée au magasin de confiance du conteneur Relution afin que la connexion soit considérée comme fiable. Selon la version de Relution, différentes méthodes s'appliquent.

Ajout de certificats via l'interface utilisateur

Nouveau dans 26.4

À partir de la version 26.4, l'image Docker de Relution est basée sur Ubuntu et non plus sur AlmaLinux. Le chemin `/etc/pki/ca-trust/source/anchors/` n'existe donc plus dans le conteneur, ce qui fait échouer un script de copie basé sur ce chemin. À partir de Relution 26.4, les certificats CA sont donc ajoutés via l'interface utilisateur — ce qui permet également d'ajuster la configuration pendant le fonctionnement du système.

Pour la version 26.4.0

Les étapes nécessaires sont les suivantes :

- Un script de démarrage existant (variable d'environnement `RELUTION_PRERUN_SCRIPT` dans `docker-compose.yml`) est retiré de la configuration, puis le conteneur Relution est redémarré.
- La connexion s'effectue dans l'organisation globale.
- Sous `Paramètres` → `Certificats`, les certificats CA souhaités sont téléchargés (voir Gestion des certificats →).
- Sous `Paramètres` → `Configuration de confiance TLS` → `Certificats de confiance`, les certificats CA téléchargés sont sélectionnés dans la bibliothèque de certificats via Ajouter un certificat.

Intégration par script (avant Relution 26.4)

Afficher les instructions

Certificat CA (keystore Java)

Il peut être nécessaire de charger un certificat dans le keystore Java et de le rendre fiable. Cela peut s'avérer nécessaire si, par exemple, un certificat auto-signé d'un serveur Exchange doit être utilisé avec la passerelle Relution Secure Mail Gateway.

Instructions

1. Ouvrir la ligne de commande Windows avec une autorisation administrative
2. Accéder au répertoire `%JAVA_HOME%\lib\security`. Le chemin d'accès peut varier en fonction de la version de Java et du fournisseur.
3. Exécuter cette commande dans le CMD (dans l'exemple, le certificat se trouve sous `C:\temp\mdeCert.cer`) :

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

4. En cas de demande de mot de passe, entrer `changeit`. Il s'agit du mot de passe par défaut du keystore.
5. En cas de demande de confirmation pour faire confiance au certificat, entrer `oui`. Le certificat sera importé et un message avec le contenu suivant sera affiché : "Certificate has been added to the keystore" (Le certificat a été ajouté à la base de données de clés) devrait s'afficher.

Convertir la base en UTF8MB4

UTF8MB4 est une extension du format de codage de caractères UTF-8. Le format UTF-8 original utilise un nombre variable d'octets pour représenter les caractères Unicode. Cependant, il ne prend en charge que les caractères de la norme Unicode d'origine, qui comptait un maximum de 65 536 caractères.

Conversion de la base de données

S'assurer que :

- Le fichier `my.cnf` / `my.ini` correspond à celui spécifié dans le guide d'installation de Relution pour le système d'exploitation concerné. pour le système d'exploitation concerné.
- Une base de données existe.
- La base de données a les permissions correctes.

Pour mettre à jour :

1. Arrêter le service Relution.
2. Exécuter cette requête sur la base de données.

Pour la version 26.4.0

```
USE information_schema ;
SELECT "SET SESSION innodb_strict_mode=OFF, NAMES 'utf8mb4' COLLATE 'utf8mb4_g
UNION
SELECT concat("SET foreign_key_checks = 0 ;") as _sql
UNION
SELECT concat("ALTER DATABASE `",table_schema,"` CHARACTER SET = utf8mb4 COLLA
UNION
SELECT concat("ALTER TABLE `",table_schema,"`.`",table_name,"` ENGINE=InnoDB R
FROM `TABLES` where table_schema like "relution" group by table_schema, table_
UNION
SELECT concat("ALTER TABLE `",table_schema,"`.`",table_name,"` CONVERT TO CHAR
FROM `TABLES` where table_schema like "relution" group by table_schema, table_
UNION
SELECT concat("ALTER TABLE `",table_schema,"`.`",table_name,"` CHANGE `",colum
FROM `COLUMNS` where table_schema like "relution" and data_type in ('varchar')
UNION
SELECT concat("ALTER TABLE `",table_schema,"`.`",table_name,"` CHANGE `",colum
FROM `COLUMNS` where table_schema like "relution" and data_type in ('text', 't
```

```
UNION
SELECT concat("SET foreign_key_checks = 1 ;") as _sql ;
```

Cette opération génère un script SQL qui peut être utilisé pour migrer la base de données. base de données.
3. Copier le résultat de la requête et l'exécuter en tant que nouvelle requête SQL 4. s'assurer que les tables ont les spécifications modifiées suivantes modifiées suivantes : - Row Format = Compressed - File Format = Barracuda - Table collation = utf8mb4_general_ci.

Pour la version 26.4.0

Illegal mix of collations

Sur les installations utilisant MariaDB, certaines opérations échouent avec l'erreur de base de données `1267`. Cela se remarque souvent d'abord avec l'Inscription automatisée des appareils (ADE, DEP dans le portail) : la synchronisation des appareils échoue pour toutes les organisations, tandis que le reste du fonctionnement se poursuit normalement. À chaque synchronisation, un message tel que le suivant apparaît dans le journal Relution :

```
Internal Exception: java.sql.SQLException: Illegal mix of collations (utf8mb4_
Error Code: 1267
Call: DELETE FROM `mdm_auto_enrllmnt_dflt_plcy` USING `mdm_auto_enrllmnt_dflt_
```

Les collations indiquées peuvent varier selon l'installation, p. ex. `utf8mb4_uca1400_ai_ci` au lieu de `utf8mb4_unicode_ci`. Le signe distinctif est une table avec le préfixe `TL_` dans la requête. L'emplacement des fichiers journaux est décrit sous Relution Logs →.

Pour la version 26.4.0

Cause

Relution attend la collation `utf8mb4_general_ci` pour toutes les colonnes de texte. Les tables de la base de données sont créées en conséquence, et la connexion de Relution à la base de données utilise également cette collation.

Pour les opérations de masse, comme la suppression de plusieurs inscriptions d'appareils lors de la synchronisation ADE, Relution crée brièvement des tables auxiliaires temporaires avec le préfixe `TL_`. Aucune collation n'est spécifiée pour ces tables, elles héritent donc de la collation par défaut de la base de données. Si cette collation par défaut diffère de `utf8mb4_general_ci`, MariaDB ne peut pas comparer les colonnes de la table auxiliaire avec celles des tables réelles et interrompt la requête. Les données enregistrées ne sont pas affectées.

Une collation par défaut divergente apparaît généralement dans les cas suivants :

- La base de données a été créée sur un serveur MariaDB dont le paramètre `collation-server` n'est pas défini sur `utf8mb4_general_ci`. Les versions récentes de MariaDB utilisent une autre collation par défaut en l'absence de configuration explicite.

- La base de données a été transférée vers un nouveau serveur ou un nouveau conteneur au moyen d'un dump. Le dump restaure les tables avec leur collation d'origine, mais la base de données nouvellement créée reçoit la valeur par défaut du nouveau serveur.

Solution

La collation par défaut de la base de données est alignée sur celle des tables Relution. Seule la valeur par défaut pour les tables nouvellement créées est modifiée ; les tables et données existantes restent inchangées.

> Une sauvegarde complète de la base de données est recommandée avant toute intervention sur la base de données.

Étapes nécessaires :

1. Le service Relution est arrêté.
2. Une sauvegarde de la base de données est créée.
3. Le script ci-dessous est enregistré sous `repair_temp_table_collation_mariadb.sql` et exécuté sur la base de données Relution.
4. La sortie du script est vérifiée (voir ci-dessous).
5. Le service Relution est démarré.

Pour la version 26.4.0

Le redémarrage est indispensable. Les tables auxiliaires temporaires existent pendant toute la durée d'une connexion à la base de données. Sinon, les connexions déjà ouvertes continuent d'utiliser la table auxiliaire créée avec la mauvaise collation.

Script

Le script détermine la collation des tables Relution, liste les colonnes divergentes et définit la collation par défaut de la base de données. Il peut être exécuté plusieurs fois sans risque.

repair_temp_table_collation_mariadb.sql

Dans les commandes suivantes, les espaces réservés entre chevrons sont remplacés par les valeurs du fichier `application.yml` ou `docker-compose.yml`. Le nom de la base de données Relution (`<database>`) figure dans le fichier `application.yml` à la fin de l'URL de la base de données, p. ex. `relution` dans `jdbc:mariadb://localhost/relution?useServerPrepStmts=true`.

Docker

Les commandes sont exécutées dans le répertoire `/opt/relution/`, dans lequel le script est également enregistré.

```
docker compose stop relution

docker exec <containername> mariadb-dump -u <username> -p<password> --single-t

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

docker compose start relution
```

Le mot de passe est indiqué ici directement après `-p`, car le script est transmis via l'entrée standard et une saisie interactive du mot de passe n'est alors pas possible.

> Pour éviter que le mot de passe ne soit enregistré en clair dans l'historique du shell, la commande peut être précédée d'un espace, ou l'historique peut être nettoyé ensuite.

Pour la version 26.4.0

Natif

Sous Linux :

```
sudo systemctl stop relution

mariadb-dump -u <username> -p --single-transaction <database> > relution_backu

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

sudo systemctl start relution
```

Le script peut également être exécuté sur la base de données Relution à l'aide d'un outil d'administration tel que `HeidiSQL` ou `DBeaver`.

Vérifier la sortie

La dernière sortie du script indique la nouvelle collation par défaut de la base de données. Elle correspond alors à la collation des tables Relution, généralement `utf8mb4_general_ci`.

Si le message `ERROR: mdm_auto_enrllmnt.uuid not found - wrong schema?` s'affiche à la place, le script n'a pas été exécuté sur la base de données Relution, le plus souvent parce que le nom de la base manque dans l'appel. Dans ce cas, rien n'a été modifié.

La section 2 du script liste toutes les colonnes de texte dont la collation s'écarte de la référence. Normalement, cette liste est vide. Si elle contient des entrées, des tables avec une mauvaise collation ont été créées depuis la mise en place de la base de données, par exemple par des mises à jour de la base lors de mises à jour de Relution. Ces tables peuvent provoquer la même erreur lors d'autres opérations. Elles sont entièrement converties en `utf8mb4_general_ci` à l'aide du guide Convertir la base en UTF8MB4 →.

Prévention

Pour que les bases de données nouvellement créées reçoivent directement la bonne collation, le serveur MariaDB est exploité avec les paramètres suivants dans la section `[mysqld]` :

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

À partir de MariaDB 11.5, la ligne `character-set-collations` est nécessaire. Sans elle, MariaDB utilise la collation `utf8mb4_uca1400_ai_ci` pour les connexions, même si la base de données et les tables sont en `utf8mb4_general_ci`. L'option existe à partir de MariaDB 11.2. Les versions plus anciennes comme MariaDB 10.11 LTS ne la reconnaissent pas et ne démarrent pas avec cette ligne ; elle y est donc omise.

La vérification des paramètres actuels s'effectue dans la console MariaDB. La base de données Relution est d'abord sélectionnée :

```
USE <database>;
```

```
SHOW VARIABLES LIKE '%collation%';
```

Les valeurs de `collation_server` et `collation_database` sont `utf8mb4_general_ci`. Sans `USE`, aucune base de données n'est sélectionnée (reconnaissable à l'invite `MariaDB [(none)]`), et `collation_database` n'indique que la valeur par défaut du serveur au lieu du paramètre de la base de données Relution. Si `collation_connection` est en `utf8mb4_uca1400_ai_ci` à partir de MariaDB 11.5, la ligne `character-set-collations` manque dans la configuration. La configuration complète est décrite dans le guide d'installation pour Linux →.

Pour la version 26.4.0

Base de données verrouillée

Le verrou sur la table changelog n'a pas pu être supprimé. Le service Relution ne démarre plus ou continue à redémarrer (Docker). Le journal affiche les messages suivants :

```
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 : Connecté à relution@... []
iquibase.MariaDBDatabase : Setting auto commit to false from true []
vice.StandardLockService : Waiting for changelog lock.... []
vice.StandardLockService : Attente du verrouillage du journal des modification
```

Le dernier message se répète périodiquement jusqu'à ce que le service se termine avec un `timeout` et redémarre automatiquement si nécessaire (Docker).

Pour la version 26.4.0

Causes

Au démarrage, le service Relution vérifie d'abord si les mises à jour de la base de données doivent être exécutées. Pour éviter que deux noeuds ne modifient le schéma de la base de données en même temps en mode cluster, un verrou est toujours placé dans la table `DATABASECHANGELOGLOCK` à cette fin. Ce verrou est libéré une fois que le contrôle et/ou les mises à jour sont terminés.

Si le service Relution est arrêté dans cet état, ce verrou reste en place. Au prochain démarrage de Relution, il attend que le verrou soit libéré car le service suppose qu'un autre nœud est en train de mettre à jour la base de données. Si ce n'est pas le cas après environ 5 minutes, le service se termine avec un message d'erreur approprié.

Cette situation se produit généralement lorsque Relution se termine prématurément au cours de l'exécution de mises à jour importantes de la base de données, car le processus de démarrage prend un temps anormalement long.

Natif

Pour résoudre le problème, il est possible de supprimer l'unique entrée de la table `DATABASECHANGELOGLOCK`, ou de modifier la valeur de la colonne `LOCKED` de `1` à `0`. Selon la base de données, `1` peut également s'afficher comme `True` et doit alors être changé en `False`.

Pour mettre à jour la base de données, l'outil de gestion de la base de données ou une alternative gratuite (`BeeKeeper`, `DBeaver`, `HeidiSQL`, ⋯) peut être utilisé. Selon la base de données, la mise à jour peut également être effectuée via les outils en ligne de commande correspondants. Par exemple, dans `DBeaver` :

```
TRUNCATE TABLE DATABASECHANGELOGLOCK;
```

Les espaces réservés entre chevrons doivent être remplacés par les valeurs présentes dans le fichier `application.yml` ou `docker-compose.yml` concerné.

Pour la version 26.4.0

Docker

Pour une configuration Docker, la commande permettant de déverrouiller la table peut être exécutée depuis le serveur dans le répertoire `/opt/relution/` comme suit :

Exemple long

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

Exemple long rempli :

```
docker exec -it docker_mariadb \
  mariadb --user=relution \
```

```
        --password=admin123 \
        --database=relution \
        --execute="TRUNCATE TABLE DATABASECHANGELOGLOCK;"
```

Exemple court

```
docker exec -it docker_mariadb mariadb -u <username> -p<password> <database> -
```

Exemple court rempli :

```
docker exec -it docker_mariadb mariadb -u relution -padmin123 relution -e "TRU
```

Pour éviter que le mot de passe ne soit enregistré en clair dans l'historique Bash, il est possible d'omettre l'option `-p` ou `--password` lors de l'exécution de la commande sans saisir le mot de passe. Ainsi, le mot de passe de la base de données sera demandé de manière interactive après l'envoi de la commande.

Pour la version 26.4.0

Migration de MariaDB vers PostgreSQL

Ce guide décrit le processus de migration de base de données pour une instance Relution au sein d'un environnement Docker.

Prérequis

Avant de commencer la migration, s'assurer que les conditions suivantes sont remplies :

- Espace disque : Au moins autant d'espace disque libre que la taille actuelle de la base de données MariaDB (rapport 1:1).
- Stockage S3 : Un stockage compatible S3 doit déjà être configuré.
  Documentation sur S3/SeaweedFS →
- Version : L'instance Relution devrait être mise à jour vers la version 26.0.0, ou au minimum vers la version 5.31.0.

Pour la version 26.4.0

Sauvegarde des données (optionnel)

Si aucun snapshot de la machine virtuelle ni de sauvegarde externe n'est disponible, effectuer un export manuel ainsi qu'une sauvegarde des fichiers.

1. Export de MariaDB dans un fichier SQL

```
docker exec docker_mariadb mariadb-dump -u relution -p --max_allowed_packe
```

2. Sauvegarde des fichiers de configuration

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

Mettre à jour Relution

S’assurer d’être à jour :

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

Arrêter les services

Arrêter le conteneur Relution afin de garantir la cohérence des données pendant la préparation :

```
docker compose down relution
```

Pour la version 26.4.0

Adapter la configuration Docker

Compléter le `docker-compose.yml`. Ajouter les services `pgloader` et la nouvelle `database` (PostgreSQL), et adapter le bloc `relution`.

Ajouter les nouveaux 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
```

Adapter le bloc Relution existant

Modifier les dépendances et ajouter l'argument de migration :

```
  relution:
    image: relution/relution:latest
    restart: on-failure # Geändert von always auf on-failure
    container_name: docker_relution
    networks:
      relution-network:
        aliases:
          - relution-docker
    depends_on:
      - database # Geändert von mariadb
    environment: # remplacer l'ancienne notation en liste (ex. "- TZ=Europe/Be
      TZ: "Europe/Berlin"
      RELUTION_ARGUMENTS: "--database-migration-only" # Neu hinzugefügt

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

Configuration de pgloader

1. Télécharger le fichier pgloader.load → dans le répertoire `/opt/relution/`.

2. Adapter la configuration à l'environnement concerné.

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

Initialiser le schéma de la base de données

Adapter d'abord l'`application.yml` afin que Relution sache qu'il doit désormais utiliser PostgreSQL :

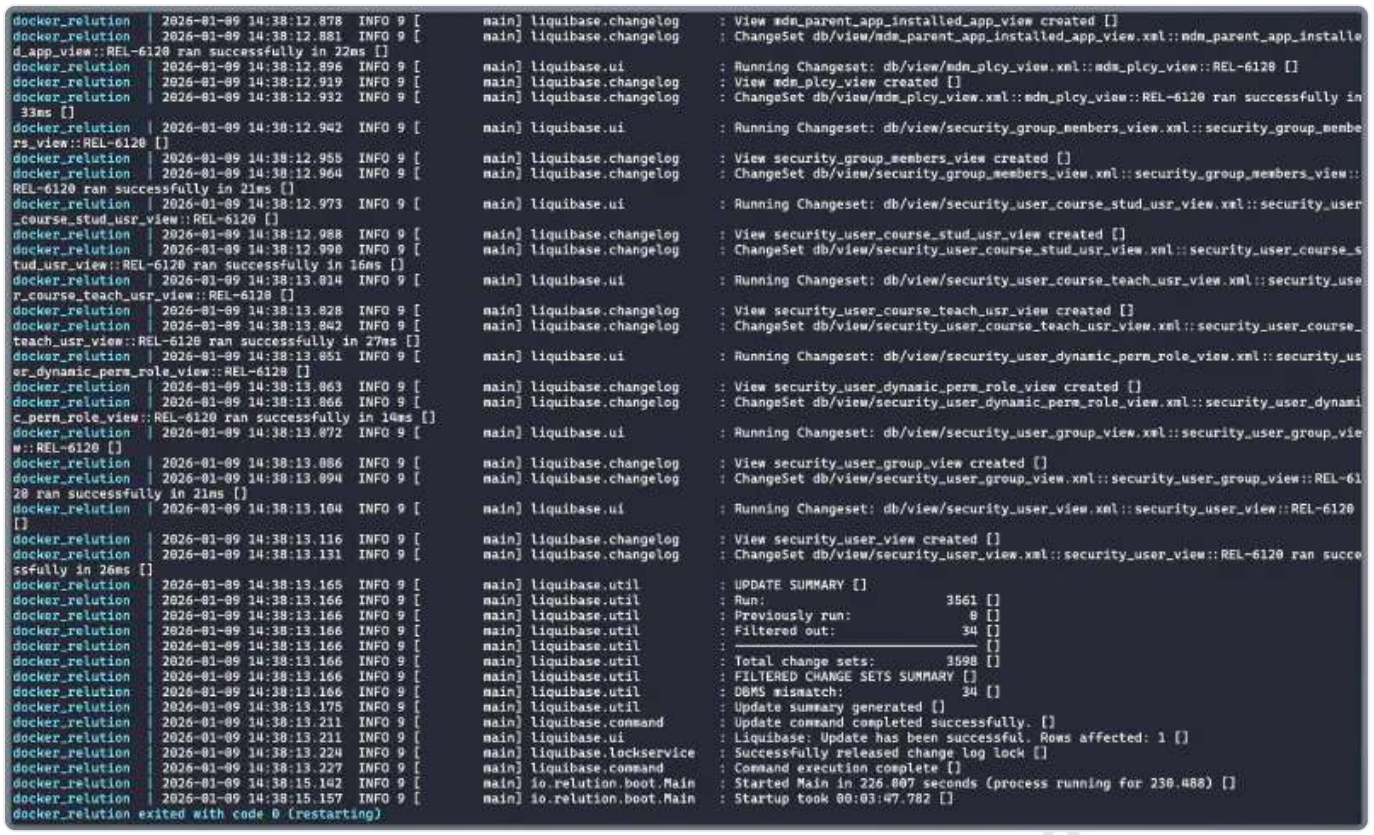
```
relution:
  database:
    type: postgresql
    url: jdbc:postgresql://database/relution?currentSchema=public
    username: relution
    password: $PASSWORD
```

Pour la

Démarrer maintenant PostgreSQL et Relution. En raison du flag `--database-migration-only`, Relution va uniquement créer le schéma dans PostgreSQL, puis s'arrêter.

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

Le processus est terminé lorsque le conteneur s'est arrêté avec le code 0 : `docker_relution exited with code 0`



Pour la version 26.4.0

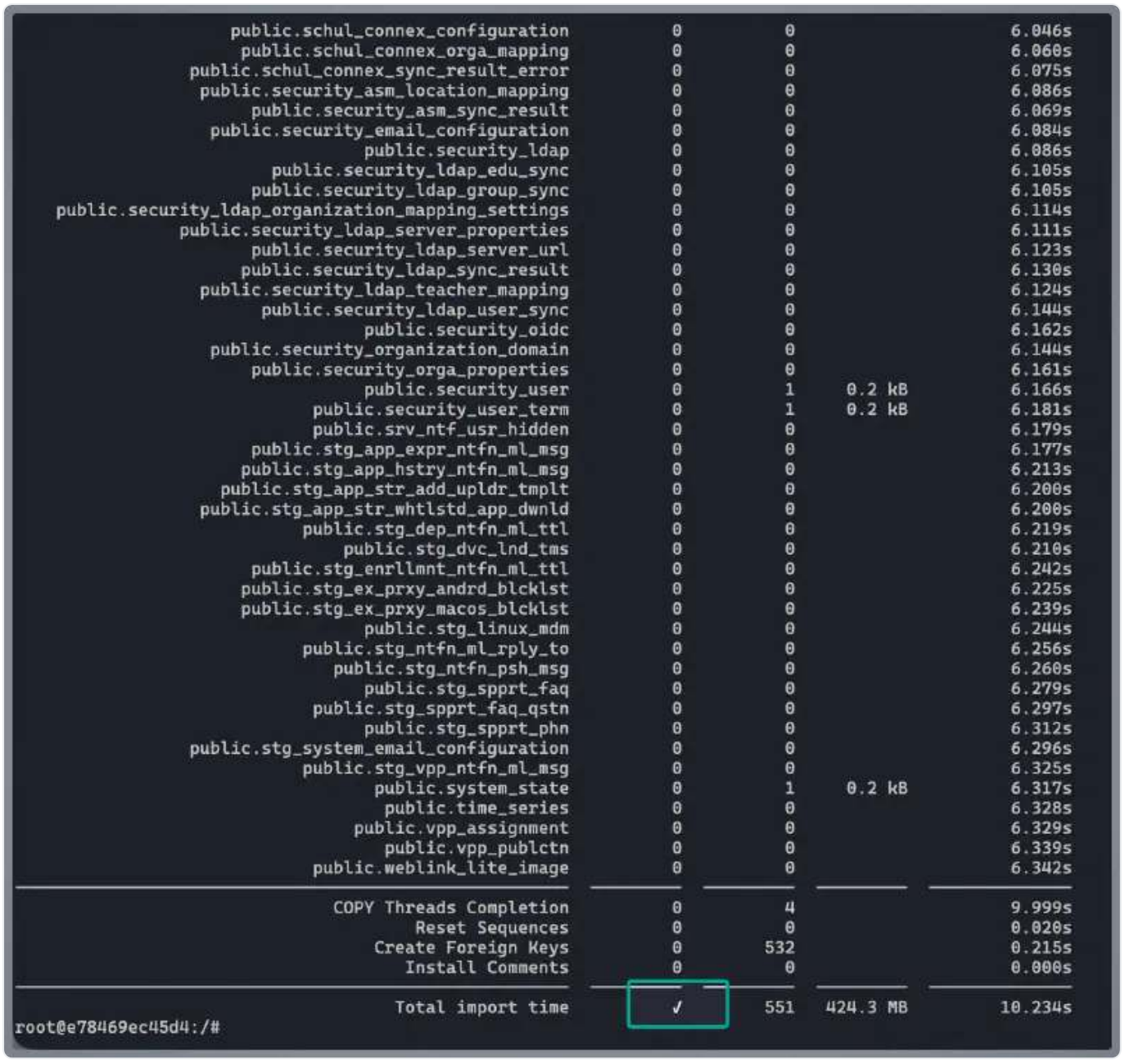
Effectuer la migration des données

Démarrer le conteneur pgloader et exécuter la migration des données de MariaDB vers PostgreSQL :

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

À l’intérieur du conteneur, exécuter la commande de migration :

```
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:/#

Nettoyage et finalisation

Après une migration réussie, les configurations temporaires et l'ancien conteneur MariaDB doivent être supprimés.

1. Supprimer dans le **`docker-compose.yml`** :
    - L'ensemble du bloc `mariadb:` sous `services`.
    - Le bloc `pgloader:` sous `services`.
    - Le volume `mariadb:` sous `volumes`.
2. Adapter le bloc **`relution`** :

- `restart: unless-stopped` (revenir à `always`).
- Supprimer la ligne : `- RELUTION_ARGUMENTS=--database-migration-only`.

3. Nettoyer :

```
rm pgloader.load
```

Redémarrer les services : Arrêter tout pour supprimer les conteneurs orphelins, puis redémarrer le système :

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

La migration est ainsi terminée et Relution fonctionne désormais nativement sur PostgreSQL.

Pour la version 26.4.0

Migrer MSSQL vers MariaDB

Avec Relution 5.25, la prise en charge de Microsoft SQL Server sera finalement abandonnée. Les instructions ci-dessous (valables à partir de la version 5.24.2/ 5.25.0 de Relution) décrivent comment migrer en utilisant l'interface graphique HeidiSQL. En cas de besoin d'aide, contacter l'équipe Relution Helpdesk.

Migration

1. Arrêter Relution 1.1 Créer une nouvelle base de données et configurer my.cnf cnf template → 1.2 Créer une nouvelle base de données avec HeidiSQL
2. Connecter l'ancienne et la nouvelle base de données dans HeidiSQL
3. Créer un schéma dans la nouvelle base de données
4. Dans le fichier application.yml, mettre à jour les valeurs suivantes 4.1 Changer `database type` en `mariadb` 4.2 Personnaliser la chaîne de connexion JDBC

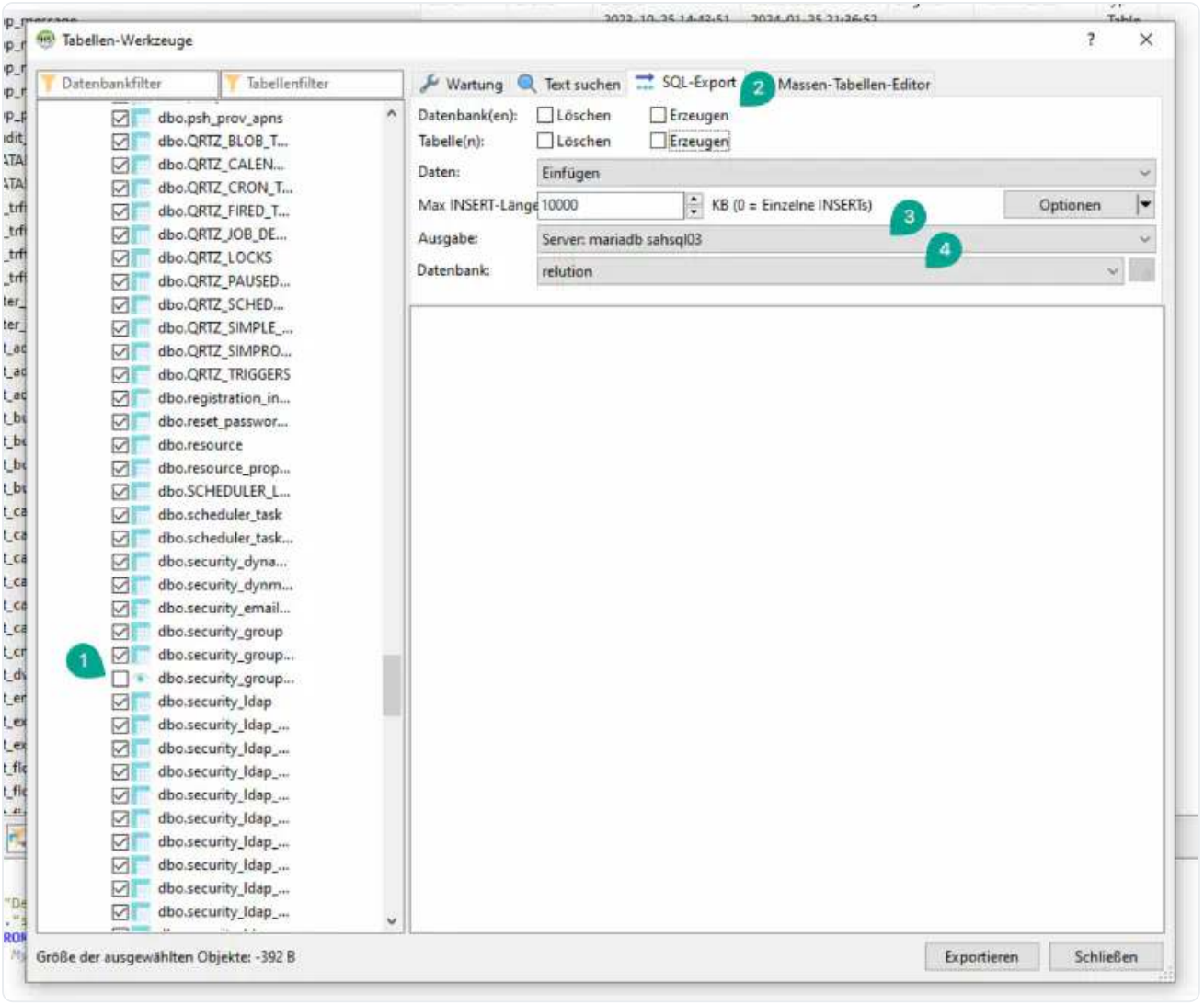
   ```
   - jdbc:mariadb://<db_server>:<db_port>/<db_name>?useServerPrepStmts=true
   ```

   4.3 Mise à jour du nom d'utilisateur et du mot de passe de la base de données
5. Démarrer Relution contre la nouvelle base de données avec foreground.bat avec + paramètre

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

6. Quitter Relution
7. Clic droit sur l'ancienne base de données
8. Exportation de la base de données
9. Databasechangelog + DatabaseChangeLockLock Table + deselect all views + JGROUPSPing

10. Longueur maximale de l’INSERT à 10k
11. Désélectionner toutes les bases de données et tables



12. Résultat : New database Server
13. Base de données : Nouvelle base de données
14. Démarrer la migration

Après la migration

1. Démarrer Relution
2. Vérifier dans le journal de Relution si le démarrage s’est déroulé correctement
3. Se connecter à Relution et vérifier si les ressources peuvent être chargées
4. Ouvrir Device Inventory (vérifier si les vues de la base de données sont ouvertes)

Migration de Windows vers Docker

Ce guide accompagne pas à pas la migration d'une installation Relution existante sur un serveur Windows vers une installation moderne basée sur Docker sur un serveur Linux.

> Lire chaque section dans son intégralité avant d'exécuter une commande.

Que se passe-t-il lors de cette migration ?

L'installation Relution actuelle fonctionne sur un serveur Windows avec une base de données MariaDB. La nouvelle configuration fonctionne sur un serveur Linux dans des « conteneurs » (Docker). La différence qui rend cette migration nécessaire : Windows ne distingue pas les majuscules et les minuscules dans les noms de fichiers et de tables. Linux, en revanche, fait cette distinction. C'est pourquoi certains noms de tables dans la base de données doivent être convertis en majuscules après le déménagement – un script prêt à l'emploi est fourni à cet effet à la fin de ce guide.

Pour la version 26.4.0

La migration se déroule selon les phases suivantes :

1. Créer une sauvegarde (dump) de la base de données sur le serveur Windows
2. Préparer le nouveau serveur Linux avec Docker
3. Importer la sauvegarde dans la nouvelle base de données
4. Renommer les noms de tables en majuscules
5. Démarrer Relution et vérifier

Éléments nécessaires avant de commencer

S'assurer de disposer des éléments suivants :

- Un accès au serveur Windows (directement sur site ou via Bureau à distance / RDP)
- Le nom de la base de données Relution – si celui-ci est inconnu, consulter l'administrateur ou le fichier de configuration Relution existant. Le nom est souvent simplement `relution`.
- Le mot de passe de l'utilisateur de la base de données MariaDB (généralement `root` ou un utilisateur Relution dédié)
- Un serveur Linux (Ubuntu 22.04 ou 24.04 recommandé) sur lequel Docker et Docker Compose sont déjà installés

- Un accès au serveur Linux via SSH (un programme de terminal tel que PuTTY sous Windows ou le terminal intégré sous macOS/Linux)
- Un programme de transfert de fichiers tel que WinSCP → (gratuit), pour copier des fichiers du serveur Windows vers le serveur Linux

---

Phase 1 – Créer une sauvegarde sur le serveur Windows

Cette étape crée une copie de sauvegarde complète de la base de données Relution sous forme de fichier SQL. Ce fichier contient l'ensemble des données et sera importé plus tard dans le nouvel environnement.

1.1 Ouvrir l'invite de commandes en tant qu'administrateur

1. Sur le serveur Windows, appuyer sur la combinaison de touches Windows + R
2. Saisir `cmd` et appuyer sur Ctrl + Maj + Entrée (pas seulement Entrée) – cela ouvre l'invite de commandes avec les droits administrateur
3. Confirmer la demande de sécurité avec Oui

Pour la version 26.4.0

1.2 Créer le dossier de destination pour la sauvegarde

Saisir la commande suivante et appuyer sur Entrée :

```
mkdir C:\backup
```

Cette commande crée le dossier `C:\backup`, dans lequel le fichier de sauvegarde sera déposé. Si le dossier existe déjà, un message sans conséquence apparaît – il suffit de continuer.

1.3 Déterminer le chemin de la base de données

`mysqldump` est le programme qui crée la sauvegarde. Il se trouve dans le répertoire d'installation de MariaDB. Vérifier quel chemin est correct dans l'environnement concerné :

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

Un dossier nommé `MariaDB 10.6` ou `MariaDB 10.11` apparaît alors, par exemple. Noter le numéro de version exact – il sera nécessaire à l'étape suivante.

1.4 Créer le dump de la base de données

Dans la commande suivante, remplacer `10.11` par le numéro de version MariaDB réel et `relution` par le nom de la base de données, si celui-ci diffère :

```
"C:\Program Files\MariaDB\MariaDB 10.11\bin\mysqldump.exe" -u root -p --single
```

Après avoir appuyé sur Entrée, le mot de passe de la base de données est demandé. Le saisir (la saisie est invisible – c'est normal) et appuyer sur Entrée.

Si aucune erreur n'apparaît et que l'invite de commandes normale réapparaît, l'export a réussi.

Brève explication des options utilisées :

rsion 26.4.0

Option	Signification
`-u root`	Connexion en tant qu'utilisateur de base de données `root`
`-p`	Le mot de passe est demandé de manière interactive
`--single-transaction`	Sauvegarde sans verrouillage de la base de données (le fonctionnement en cours reste possible)
`--routines`	Les procédures stockées sont également sauvegardées
`--triggers`	Les triggers sont également sauvegardés
`--default-character-set=utf8mb4`	Jeu de caractères pour les caractères spéciaux et les emojis

1.5 Vérifier la sauvegarde

Vérifier que le fichier a été correctement créé :

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

Le fichier devrait apparaître avec une taille (généralement plusieurs Mo). Si le fichier a une taille de 0 octet, quelque chose s'est mal passé – exécuter alors à nouveau la commande de l'étape 1.4 et surveiller les messages d'erreur.

1.6 Transférer le fichier de sauvegarde vers le serveur Linux

Ouvrir WinSCP, se connecter au serveur Linux (adresse IP, nom d'utilisateur et mot de passe) et copier le fichier :

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

Si le dossier `/opt/relution/` n'existe pas encore sur le serveur Linux, le créer d'abord (voir Phase 2, étape 2.1).

Pour la version 26.4.0

Phase 2 – Préparer le serveur Linux

Toutes les commandes suivantes sont exécutées sur le serveur Linux dans un terminal SSH.

2.1 Créer le répertoire de travail

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

La commande `mkdir -p` crée le dossier et tous les dossiers parents s'ils n'existent pas encore. La commande `cd` permet ensuite de se déplacer dans ce dossier.

2.2 Créer le fichier Docker Compose

Docker Compose est une méthode permettant de démarrer et de gérer conjointement plusieurs programmes liés entre eux (ici : base de données + Relution). La configuration est stockée dans un fichier nommé `docker-compose.yml`.

Créer le fichier :

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

La commande `nano` ouvre un éditeur de texte simple directement dans le terminal. Y copier l'intégralité du contenu suivant :

Show full configuration example

Remplacer les trois espaces réservés par des mots de passe sécurisés au choix :

- `HIER_ROOT_PASSWORT_EINSETZEN` → par ex. `Tr0mmelFeuer!92`
- `HIER_RELUTION_PASSWORT_EINSETZEN` → par ex. `Rel@ution#2024` (les deux occurrences doivent être identiques !)

Enregistrer et fermer le fichier : Ctrl + O (enregistrer), puis Entrée, puis Ctrl + X (quitter).

Pour la version 26.4.0

2.3 Démarrer uniquement la base de données

Seul le conteneur de base de données est démarré pour l'instant – pas encore Relution lui-même. Cela est important pour que Relution, lors de son premier démarrage, ne se trouve pas face à une base de données vide et ne commence à créer ses propres tables (incorrectes).

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

L'option `-d` signifie « detached » – le conteneur s'exécute en arrière-plan et ne bloque pas le terminal.

2.4 Attendre que la base de données soit prête

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

Cette commande affiche les journaux (messages de log) du conteneur de base de données en temps réel. Attendre que le message suivant apparaisse :

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

Dès que ce message est visible, appuyer sur Ctrl + C pour arrêter l'affichage. La base de données continue de s'exécuter en arrière-plan.

Phase 3 – Importer la sauvegarde

Si le fichier dump n'a pas encore été transféré vers le serveur, le faire maintenant (voir Phase 1, étape 1.6).

3.1 Importer le dump dans la base de données

ion 26.4.0

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

> Il n'y a pas d'espace entre `-p` et le mot de passe. Remplacer `HIER_ROOT_PASSWORT_EINSETZEN` par le mot de passe root défini dans le `docker-compose.yml`.

Brève explication de ce qui se passe ici : `docker exec -i relution-db` permet d'exécuter une commande à l'intérieur du conteneur de base de données en cours d'exécution. `mariadb ... < fichier.sql` importe le fichier SQL dans la base de données.

L'import peut prendre plusieurs minutes selon le volume de données. Si aucune erreur n'apparaît et que l'invite normale réapparaît, l'import a réussi.

3.2 Vérifier l’import

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

Cette commande liste les 30 premières tables de la base de données. Des noms de tables familiers devraient apparaître (par ex. `databasechangelog`, `qrtz_triggers`, etc.). Si la liste est vide ou qu’un message d’erreur apparaît, répéter la Phase 3.

Phase 4 — Renommer les noms de tables en majuscules

Comme expliqué au début : Linux distingue les majuscules et les minuscules, Windows non. Sous Linux, Relution attend des noms de tables en majuscules. Cette étape renomme toutes les tables concernées.

Pour la version 26.4.0

Comme il n’est pas possible de renommer directement une table de `beispiel` en `BEISPIEL` (Linux considère cela comme le même nom), le renommage se déroule en deux passes : d’abord vers des noms temporaires (avec `_tmp`), puis vers les noms finaux en majuscules.

4.1 Créer le fichier de script

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

Copier l’intégralité du contenu suivant dans l’éditeur :

> Show full configuration example

Enregistrer et quitter : Ctrl + O, Entrée, Ctrl + X.

4.2 Exécuter le script

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

Si aucun message d’erreur n’apparaît, le renommage a réussi.

4.3 Vérifier le résultat

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

Dans le résultat, des noms de tables en majuscules devraient maintenant apparaître, par exemple :

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

Phase 5 – Démarrer Relution

Maintenant que la base de données est correctement remplie et préparée, la pile complète peut être démarrée, y compris Relution :

```
cd /opt/relution
```

```
docker compose up -d
```

5.1 Observer le démarrage

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

Suivre la sortie. Lors de son premier démarrage, Relution effectue diverses vérifications de la base de données – cela peut prendre 1 à 3 minutes. Le démarrage a réussi lorsqu'un message tel que le suivant apparaît :

```
Started Relution in XX seconds
```

Quitter l'affichage des logs avec Ctrl + C.

Pour la version 26.4.0

5.2 Ouvrir Relution dans le navigateur

Ouvrir un navigateur et accéder à Relution :

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

Remplacer `IP-ADRESSE-DES-SERVERS` par l'adresse IP réelle du serveur Linux.

Problèmes fréquents et solutions

Table doesn't exist lors de l'exécution du script de renommage Cela signifie que l'import du dump n'était pas complet. Vérifier avec `SHOW TABLES;` quelles tables manquent et répéter la Phase 3.

Relution ne démarre pas / reste en boucle Consulter les logs : `docker logs relution-app`. Les causes les plus fréquentes sont un mot de passe de base de données incorrect dans le

`docker-compose.yml` ou des tables qui n'ont pas encore été correctement renommées.

Le fichier dump a une taille de 0 octet La commande d'export n'a pas fonctionné. Vérifier le chemin vers `mysqldump.exe` et le mot de passe de la base de données.

Le port 8080 est déjà utilisé Un autre programme utilise le port 8080. Dans le `docker-compose.yml`, modifier la ligne `"8080:8080"` en, par exemple, `"8181:8080"`, puis accéder à Relution via le port 8181.

WinSCP ne se connecte pas S'assurer que le service SSH est actif sur le serveur Linux (`sudo systemctl status ssh`) et que le pare-feu autorise le port 22.

Récapitulatif des chemins de fichiers importants

Fichier	Chemin sur le serveur Linux
Configuration Docker Compose	`/opt/relution/docker-compose.yml`
Dump de la base de données	`/opt/relution/relution_dump.sql`
Script de renommage	`/opt/relution/rename_tables.sql`

Prochaines étapes après une migration réussie

Une fois que Relution fonctionne et que la connexion réussit :

- Vérifier que tous les appareils, utilisateurs et paramètres ont été correctement repris
- Mettre en place un certificat SSL (HTTPS) si ce n'est pas déjà le cas – guide : Configurer un certificat SSL →
- S'assurer que des sauvegardes régulières des volumes Docker sont en place
- N'éteindre l'ancien serveur Windows qu'une fois que le nouvel environnement a fonctionné de manière stable pendant plusieurs jours

Le service ne démarre pas - Linux

Sous Linux, le service Relution ne peut pas être démarré et via `systemctl status relution` ces erreurs sont affichées

```
Apr 12 12:02:52 Relution systemd[1] : A démarré le serveur Relution.
Apr 12 12:02:52 Relution systemd[1] : relution.service : Main process exited,
Apr 12 12:02:52 Relution systemd[1] : relution.service : Failed with result 'e
Apr 12 12:02:52 Relution systemd[1] : relution.service : Service RestartSec=10
Apr 12 12:02:52 Relution systemd[1] : relution.service : Scheduled restart job
Apr 12 12:02:52 Relution systemd[1] : Arrêt du serveur Relution
```

Relution peut également être démarré normalement via `relution-foreground.sh` et fonctionne comme d'habitude. Le problème peut être dû au fait que `bash` n'est pas le shell par défaut du système d'exploitation.

Pour la version 26.4.0

Ajuster le fichier de service de Relution

Pour cela, un petit ajustement peut être fait dans le fichier `Relution Services` et le service devrait redémarrer par la suite.

Dans la ligne `ExecStart` du fichier `/etc/system/system/relution.service`, il faut ajouter `/bin/bash`.
Le service peut ensuite être redémarré.

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

Relution Logs

Docker n'écrit pas de logs par défaut. Tout ce qui peut être lu dans les logs est contenu dans le `system log` du conteneur. Ceci est suffisant pour la plupart des changements. Il est recommandé de provoquer l'erreur pour qu'elle soit visible juste avant de suivre les étapes.

Trouver l'ID du conteneur

1. Démarrer un terminal et se connecter si nécessaire
2. Trouver le nom et l'ID du Docker. Afficher l'ID et le nom du conteneur

```
sudo docker ps
```

Le terminal devrait maintenant afficher la sortie suivante

la version 26.4.0

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	N
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	d re

Les informations seront différentes de celles de l'exemple. Il est possible d'utiliser le nom ou l'ID du conteneur pour lancer le journal. Dans l'exemple, le nom a été utilisé

Démarrer le journal avec le nom du conteneur

```
docker logs -f docker_relution
```

L'option `-f` assure que le journal est toujours affiché en continu. Par conséquent, beaucoup de texte est affiché rapidement dans le terminal. Il est possible d'arrêter le journal avec `CTRL + C` et de faire défiler vers le haut.

Enregistrer le journal dans un fichier

Pour sauvegarder les journaux dans un fichier dans le chemin d'accès actuel, utiliser cette commande

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

Il est également possible d'utiliser un chemin alternatif

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

Pour transférer le fichier sur un PC, utiliser `Filezilla`, `WinSCP` ou un autre `SCP client`

Absolument ! Hier ist der Text auf Französisch, ebenfalls als Markdown formatiert und zum Kopieren bereit:

Rotation des journaux (Logs)

Les journaux Docker sont intrinsèquement éphémères. Parfois, il peut être utile de les conserver pendant une période plus longue. Un exemple basé sur une installation Rocky Linux 9 + Docker est proposé ci-dessous.

Configurer la rotation des journaux pour les hôtes Docker

Docker stocke ses journaux standards sous `/var/lib/docker/containers/<container-id>/<container-id>-json.log`. Pour que ces journaux restent gérables, la rotation de journaux intégrée de Docker peut être activée via le fichier `/etc/docker/daemon.json` :

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

Ensuite, redémarrer le service Docker :

```
sudo systemctl restart docker
```

Faire pivoter, compresser et déplacer les journaux quotidiennement vers le répertoire Relution

Pour l'archivage quotidien, `logrotate` peut être utilisé. Pour cela, il doit être installé ultérieurement sur le système Linux via :

our la version 26.4.0

```
sudo dnf install logrotate
```

Il faut d'abord créer un dossier pour les journaux :

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

Ensuite, un fichier de configuration doit être créé sous `/etc/logrotate.d/docker` avec le contenu suivant :

> Remplacer les deux mots WILDCARD dans la première ligne par `*`.

```
/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 $(find /var/lib/docker/containers/ -type f -name "*.log.*.gz")
        DIR="/opt/relution/logs"
        FILENAME="relution-${TIMESTAMP}.log.gz"
        mv "$file" "${DIR}/${FILENAME}"
    done
endscript
}
```

Une journalisation peut être immédiatement créée à l'aide de la commande de test suivante :

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

Par la suite, un fichier journal devrait être stocké dans le dossier `/opt/relution/logs` :

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

Linux

Si Relution a été installé dans le répertoire par défaut `/opt/relution`, les journaux peuvent être trouvés dans `/opt/relution/log` Le fichier journal le plus récent est appelé relution.log, tandis que les fichiers journaux archivés sont nommés `relution.log.<date>.gz` Si Relution a été installé à un autre endroit, le répertoire du journal est trouvé par rapport à son répertoire d'installation.

Windows

Si Relution a été installé dans le répertoire par défaut `C:\Program Files\Relution`, les journaux se trouvent dans `C:\Program Files\Relution\log`. Le fichier journal le plus récent est appelé `relution.log`, tandis que les fichiers journaux archivés sont nommés `relution.log.<date>.gz`. Si Relution a été installé à un autre endroit, le répertoire du journal est trouvé par rapport à son répertoire d'installation.

Ajuster le niveau de journalisation pour une analyse approfondie

Si les journaux standard ne suffisent pas pour l'analyse des erreurs, le niveau de journalisation peut être augmenté de manière ciblée à `DEBUG` (par exemple à chaud sans redémarrage via l'API Web ou le portail système). Un guide détaillé est disponible sous Définir le niveau de journalisation →.

Pour la version 26.4.0

Docker ne démarre pas sur EL10

Les images minimales et cloud de RHEL, AlmaLinux et Rocky Linux 10 (EL10) ne contiennent pas un paquet de modules du noyau dont Docker a besoin pour sa configuration réseau — dans ce cas, Docker ne démarre pas et l'installation de Relution ne peut pas se poursuivre. Ce guide décrit comment installer le paquet manquant avant le premier démarrage de Docker.

> Seul EL10 (version 10) est concerné. Sur EL9, cette étape n'est pas nécessaire — le paquet y est déjà préinstallé.

Problème

Les images minimales et cloud de RHEL, AlmaLinux et Rocky Linux 10 ne contiennent pas le paquet `kernel-modules-extra`. Sans ce paquet, iptables ne peut pas charger le module du noyau `xt_addrtype`, dont Docker a besoin pour sa configuration de pont (bridge) et de NAT. Le service Docker ne démarre alors pas et s'interrompt avec le message suivant :

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

La sortie de `systemctl status docker` n'affiche souvent que l'erreur consécutive `Start request repeated too quickly` — la cause réelle apparaît dans `journalctl -xeu docker.service`.

Solution

Les étapes suivantes sont exécutées avant le premier démarrage de Docker :

```
# 1. Installer le paquet de modules correspondant au noyau EN COURS
sudo dnf install -y "kernel-modules-extra-$(uname -r)"

# 2. Charger les modules
sudo modprobe xt_addrtype br_netfilter ip_tables
```

```
# 3. Rendre persistant – chargés automatiquement à chaque démarrage
echo -e "xt_addrtype\nbr_netfilter\nip_tables" | sudo tee /etc/modules-load.d/

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

Pourquoi ces deux points sont importants

- Installer la version correspondante (`kernel-modules-extra-$(uname -r)`) : garantit que les modules correspondent au noyau *actuellement en cours d'exécution*. Un simple `dnf install kernel-modules-extra` peut ne fournir les modules que pour un noyau plus récent, pas encore démarré — dans ce cas, `modprobe` échoue avec `Module xt_addrtype not found` jusqu'au redémarrage du système. Si `dnf` ne trouve à l'inverse aucun paquet correspondant au noyau actuellement en cours d'exécution (par exemple après un `dnf update` préalable sans redémarrage), un redémarrage sur le noyau le plus récemment installé est nécessaire avant de relancer la commande.
- `/etc/modules-load.d/docker.conf` : garantit, via `systemd-modules-load.service`, que les modules sont chargés automatiquement à chaque redémarrage. Sans ce fichier, le correctif serait à nouveau perdu après le prochain redémarrage.

Pour la version 26.4.0

Vérifier que cela a fonctionné

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

Si `modprobe` ne renvoie aucune erreur, que le service indique `active` et que le conteneur de test affiche `Hello from Docker!`, l'étape est terminée.

Niveau de journalisation

Dans certains cas, la cause d'un problème ne peut pas être identifiée dans le niveau de journalisation par défaut. Dans ce cas, le niveau du journal peut être ajusté en conséquence et les informations produites peuvent être augmentées.

Le niveau de journalisation peut être défini via le fichier `application.yml`, l'API Web ou le portail système. La voie de l'API Web prend effet immédiatement, ne nécessite ni redémarrage ni configuration supplémentaire et constitue donc la méthode recommandée en fonctionnement. Depuis Relution 26.4, le portail système requiert l'activation unique du point de terminaison actuator correspondant.

> Le niveau de journalisation DEBUG ne devrait être utilisé qu'à des fins d'analyse, car beaucoup plus d'informations sont écrites dans le journal et le journal s'agrandit en conséquence. Une fois l'analyse terminée, le niveau de journalisation doit être remis sur INFO.

Emplacement du fichier journal

L'emplacement des fichiers journaux pour Docker, Linux et Windows est décrit sous Journaux Relution →.

Pour la version 26.4.0

Activation du portail système

Dans le fichier `application.yml` du répertoire Relution, ajouter cette section :

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

> Veiller à indenter chaque ligne ici (deux espaces par niveau). Il est recommandé de désactiver à nouveau le portail système après avoir terminé le travail.

Activation des points de terminaison actuator

Depuis Relution 26.4, seul le point de terminaison health est exposé par défaut pour des raisons de sécurité. Le portail système n'affiche donc d'abord que la section `Details`. La section `Logger` n'apparaît qu'après l'activation du point de terminaison correspondant dans le fichier `application.yml` du serveur Relution :

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

La liste remplace intégralement la configuration par défaut. `health` doit y rester, faute de quoi le point de terminaison health disparaît, et avec lui l'affichage d'état du portail système ainsi que les contrôles de santé des répartiteurs de charge et des nœuds du cluster.

Un redémarrage du serveur Relution est nécessaire pour que la modification prenne effet.

D'autres sections du portail système peuvent être ajoutées individuellement selon le même modèle :

Pour la version 26.4.0

Section du portail système	Point de terminaison
Logger	`loggers`
Environment	`env`
Metrics	`metrics`
Threads	`threaddump`
Caches	`caches`
Scheduled Tasks	`scheduledtasks`
Mappings	`mappings`

Section du portail système	Point de terminaison
Configuration Properties	`configprops`
Logfile	`logfile`
Quartz	`quartz`

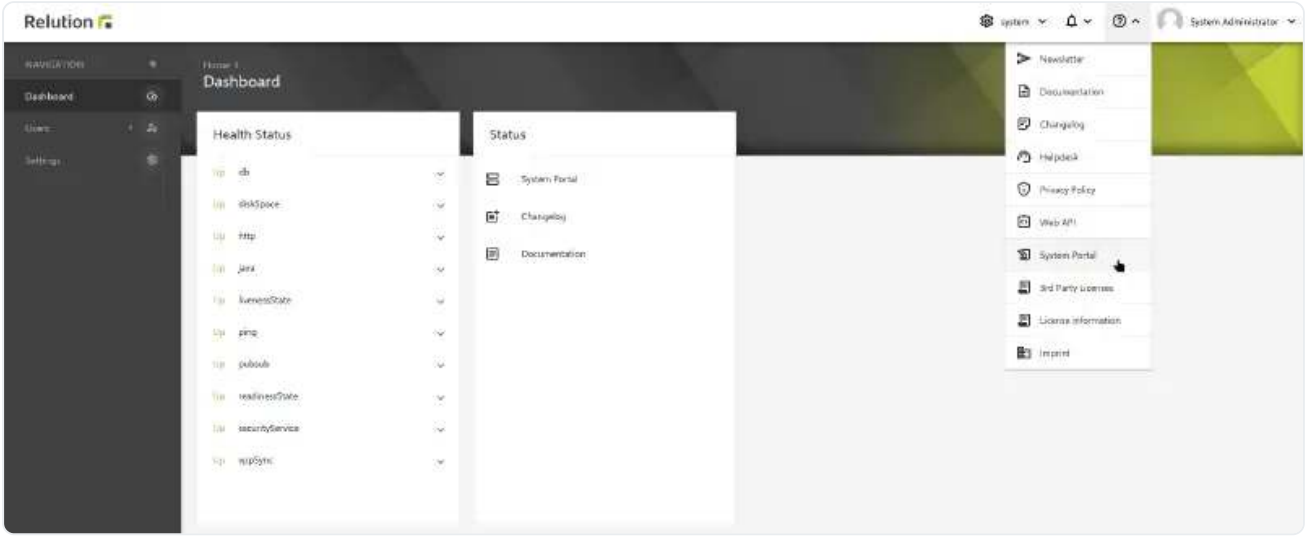
> Les points de terminaison actuator sont exposés sur le port de gestion 8099 sans authentification. Ce port ne doit pas être accessible depuis des réseaux non fiables. Les points de terminaison env, configprops et heapdump exposent en outre des valeurs de configuration et des contenus mémoire, y compris des identifiants. Toute activation doit donc être retirée une fois l'analyse terminée.

Activation du journal DEBUG dans le portail système

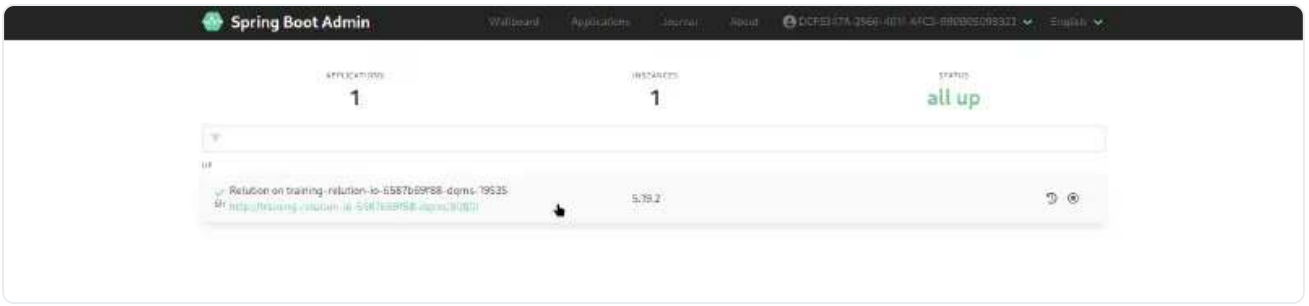
Pour la version 26.4.0

Cela suppose un portail système activé ainsi qu'un point de terminaison `loggers` activé, voir les deux sections précédentes.

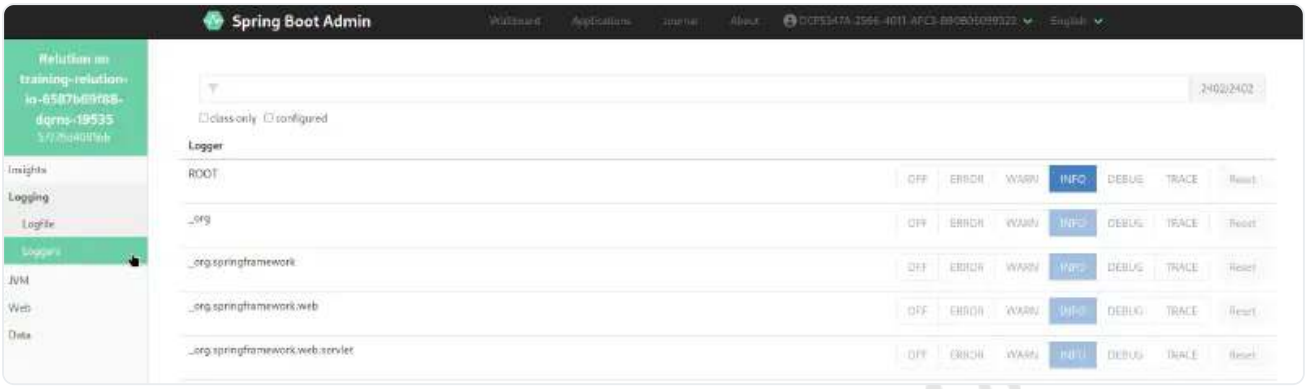
1. Se connecter à Relution en tant qu'administrateur système. Le nom d'utilisateur par défaut est `admin`
2. Aller à `System Portal` dans le menu système.



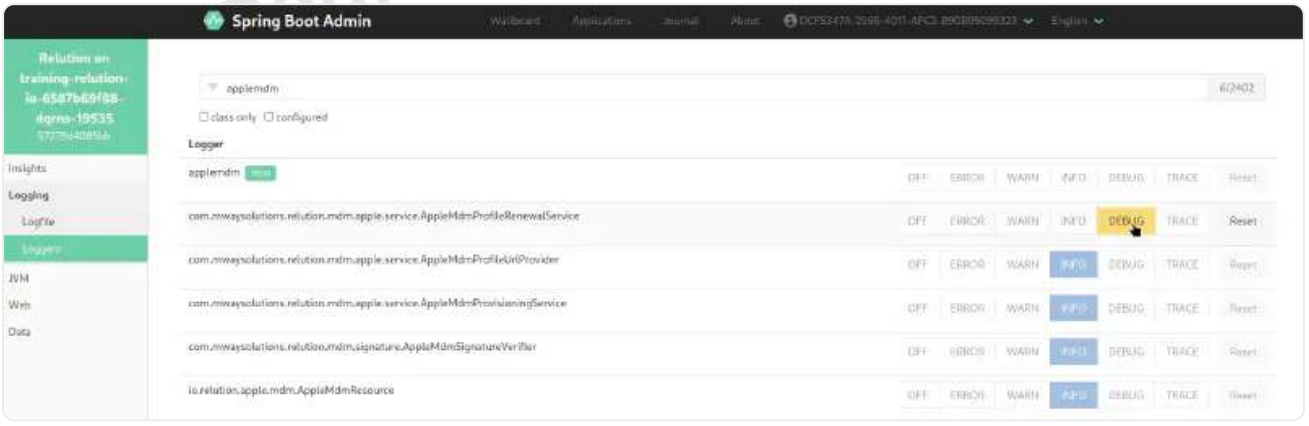
3. Il est ensuite possible d'appeler l'instance associée. Pour cela, cliquer sur la boîte et non pas directement sur le lien vert.



4. Passer à la section `Logger`.



5. Utiliser la recherche pour mettre le `Logger` correspondant à `DEBUG`. `ROOT` active tous les `Loggers` et ne devrait donc être utilisé que dans des cas exceptionnels, car beaucoup de contenu est généré rapidement. Dans l'exemple, le `AppleMDMResource` a été activé.



Le paramètre est directement actif, sans qu'il soit nécessaire de redémarrer les services. Lors du redémarrage du service Relution ou du conteneur Docker, le journal sera réinitialisé à `INFO`.

Garder le journal DEBUG actif après un redémarrage

Puisque le journal `DEBUG` est remis à `INFO` après un redémarrage de l'instance, il n'est pas possible d'enregistrer les erreurs initiales pendant le processus de démarrage, par exemple dans le contexte d'une connexion LDAP, de la manière décrite ci-dessus. Pour cela, il est possible de définir le journal dans le fichier `application.yml`. Celui-ci est chargé directement au démarrage et active ainsi le journal `DEBUG`.

Insérer le contenu suivant directement dans la première ligne à la position 1.

Définir ROOT à DEBUG

> La journalisation au niveau `ROOT` peut générer rapidement beaucoup de contenu. Cette fonctionnalité ne devrait être utilisée que dans des cas tout à fait exceptionnels pour des activités d'analyse courtes. Une dégradation significative des performances peut par ailleurs survenir ici, même avec de petites installations.

Il est recommandé d'activer un ou plusieurs journaux individuellement et de manière ciblée. Pour ce faire, ajouter simplement les `loggers` individuels l'un à la suite de l'autre dans le fichier :

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

Plusieurs journaux individuels

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

Dans l'exemple, la fonctionnalité LDAP et `AppleMdmResource` seraient maintenant activées dans le journal `DEBUG`. Les noms des `loggers` peuvent être consultés dans le portail système si le point de terminaison `loggers` est activé ; sinon, ils correspondent au nom du paquet ou de la classe figurant dans le journal.

Configurer le niveau de log avec un utilisateur de log via l’API Web

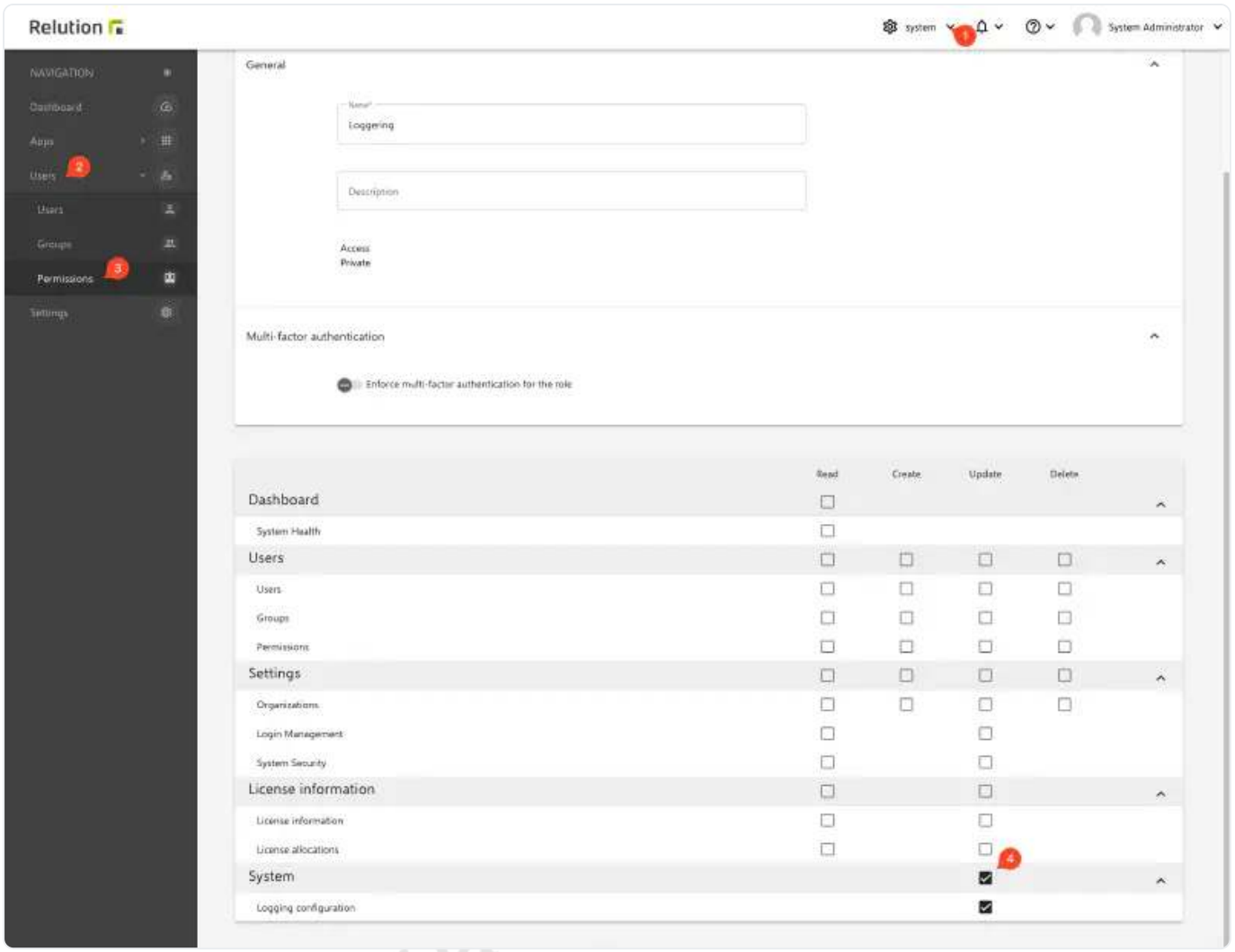
Depuis la version 5.18 de la Relution, il est possible de créer un utilisateur de journalisation spécial sur l’organisation du système, qui peut confortablement changer le niveau de journalisation via l’API Web. Cela permet d’éviter l’édition manuelle du fichier de configuration YAML ainsi qu’un redémarrage du serveur.

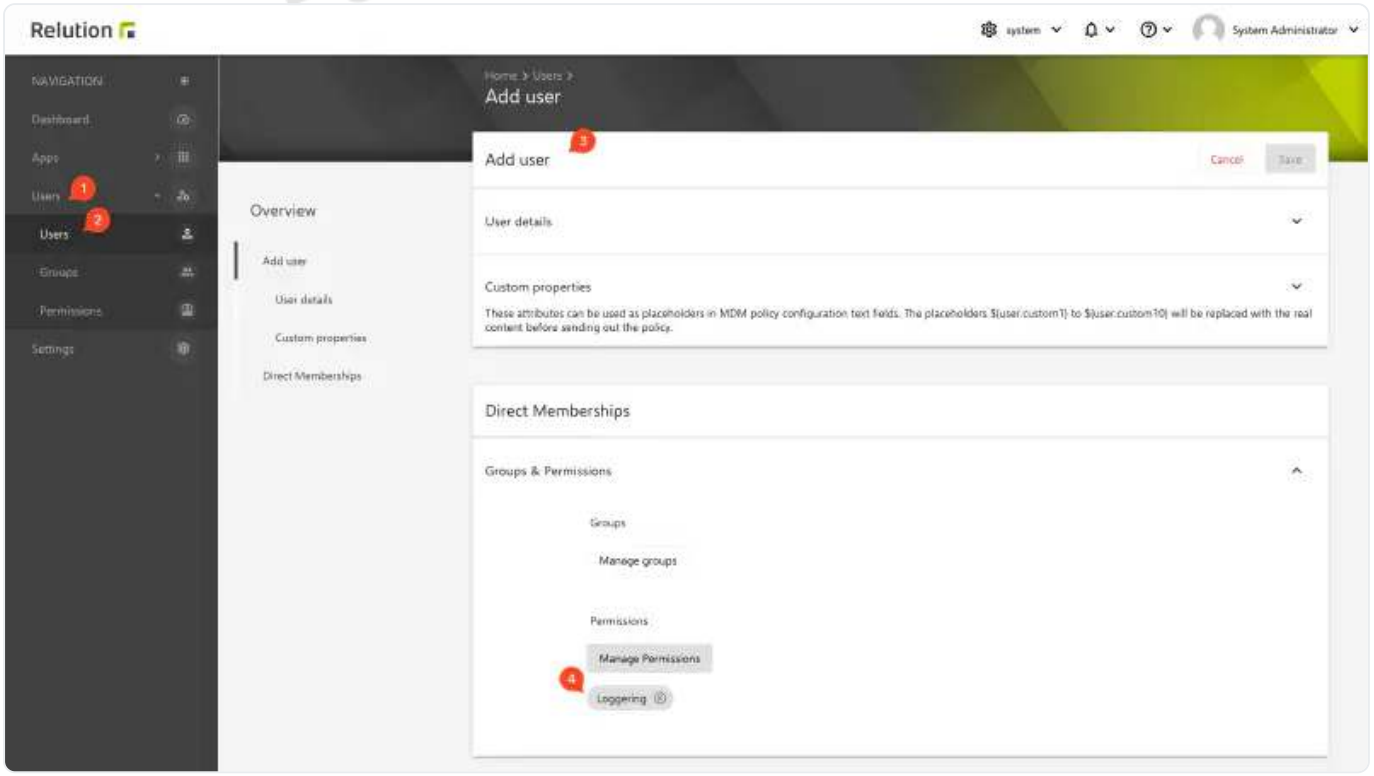
Cette voie ne nécessite ni portail système activé ni activation d’un point de terminaison actuator et constitue donc la méthode recommandée pour modifier les niveaux de journalisation en fonctionnement. Comme dans le portail système, les niveaux définis sont réinitialisés à leur valeur initiale après un redémarrage de l’instance.

1. créer l’autorisation et l’utilisateur

Pour créer l’utilisateur de journalisation, une nouvelle autorisation doit d’abord être créée dans l’organisation du système, où l’option “Système > Configuration de la journalisation” est activée et sauvegardée. Ensuite, un nouvel utilisateur peut être créé exclusivement pour l’accès à la journalisation, auquel l’autorisation précédemment créée est attribuée. Remarque : l’administrateur du système dispose de cette autorisation par défaut.

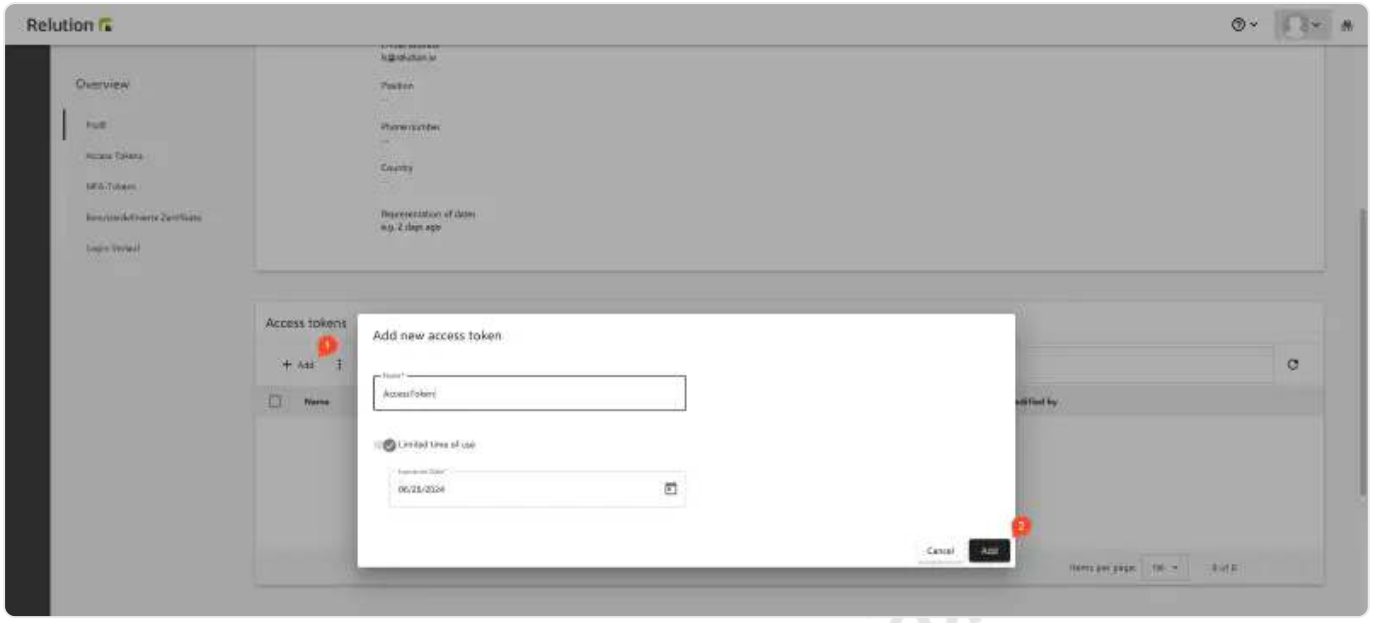
Pour la version 26.4.0

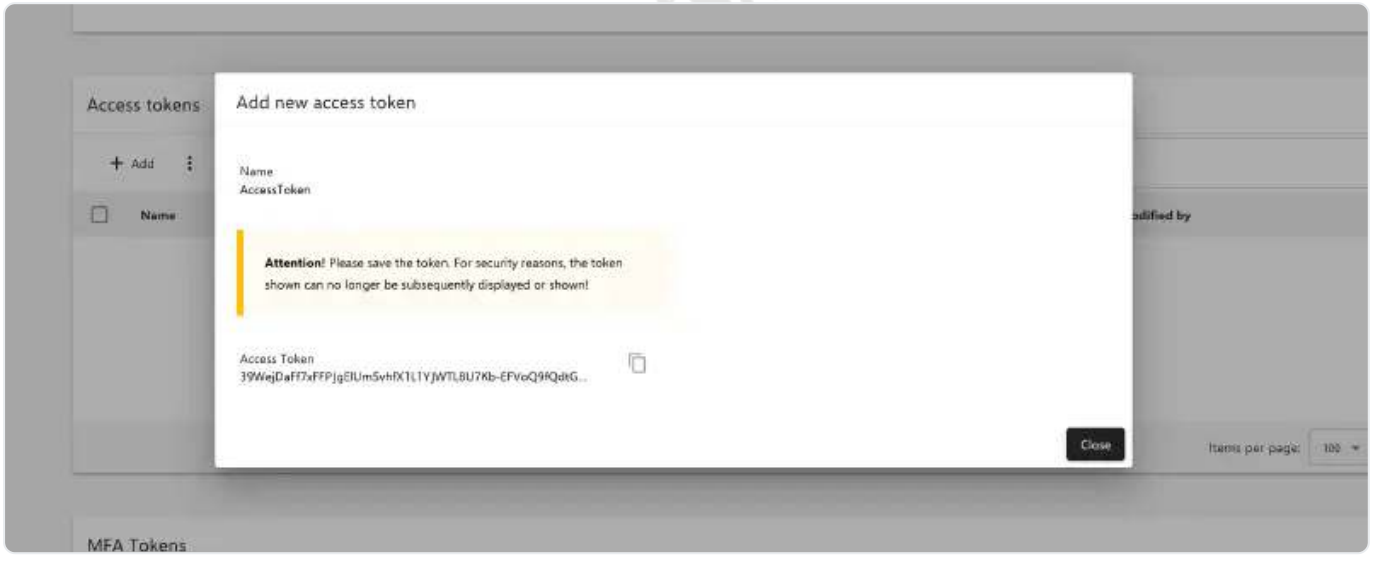

Relution
system
System Administrator
NAVIGATION
Dashboard
Apps
Users
Users
Groups
Permissions
Settings
General
Name*
Loggering
Description
Access
Private
Multi-factor authentication
Enforce multi-factor authentication for the role
Read
Create
Update
Delete
Dashboard
System Health
Users
Users
Groups
Permissions
Settings
Organizations
Login Management
System Security
License information
License information
License allocations
System
Logging configuration
1
2
3
4


Relution
system
System Administrator
NAVIGATION
Dashboard
Apps
Users
Users
Groups
Permissions
Settings
Home > Users >
Add user
Add user
Cancel
Save
Overview
Add user
User details
Custom properties
Direct Memberships
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
1
2
3
4

2. créer un jeton d’accès

Un jeton d’accès peut être créé pour ce nouvel utilisateur afin de faciliter sa manipulation. Pour ce faire, l’utilisateur doit d’abord se connecter et créer le jeton via le profil de l’utilisateur. Le jeton d’accès n’est affiché qu’une seule fois, un autre jeton peut être créé si nécessaire.



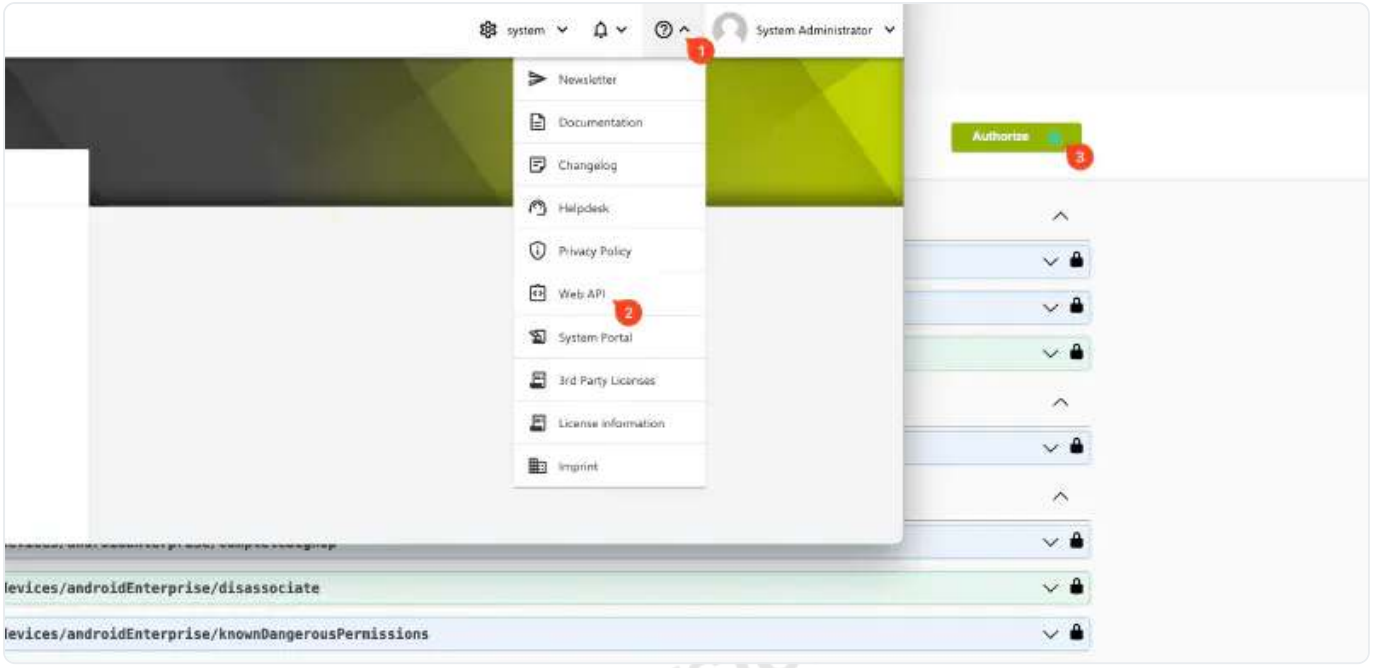


3. contrôler le niveau de journalisation via l’API Web

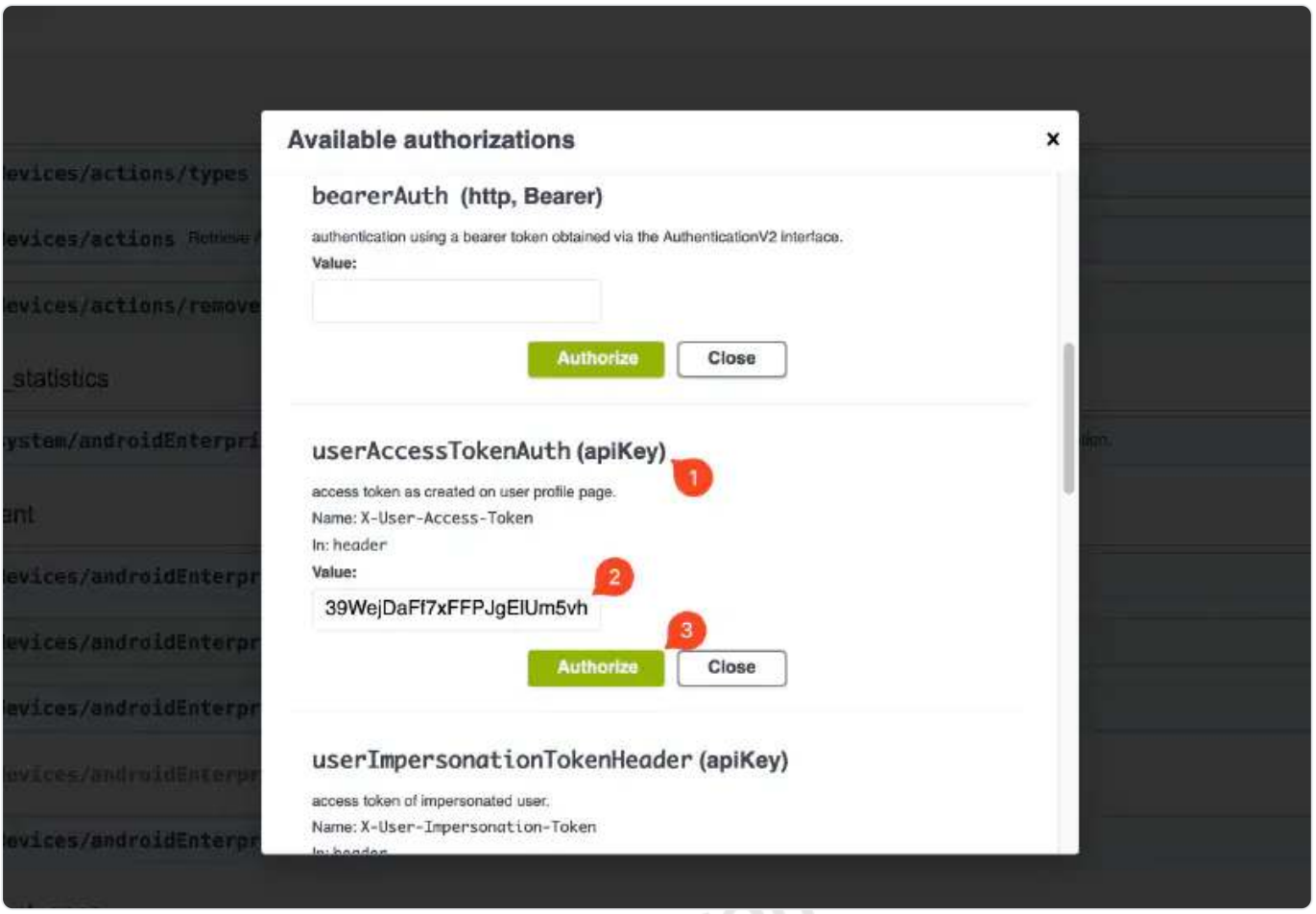
Pour contrôler le niveau de journalisation via l’API Web, il est possible d’accéder à l’utilisateur de journalisation dans l’organisation du système via l’icône ⚙️ > API Web > Autoriser. Le jeton d’accès de l’utilisateur de journalisation peut être utilisé pour faciliter l’accès et ajouter automatiquement l’authentification à curl. Dans l’élément “userAccessTokenAuth”, le jeton doit

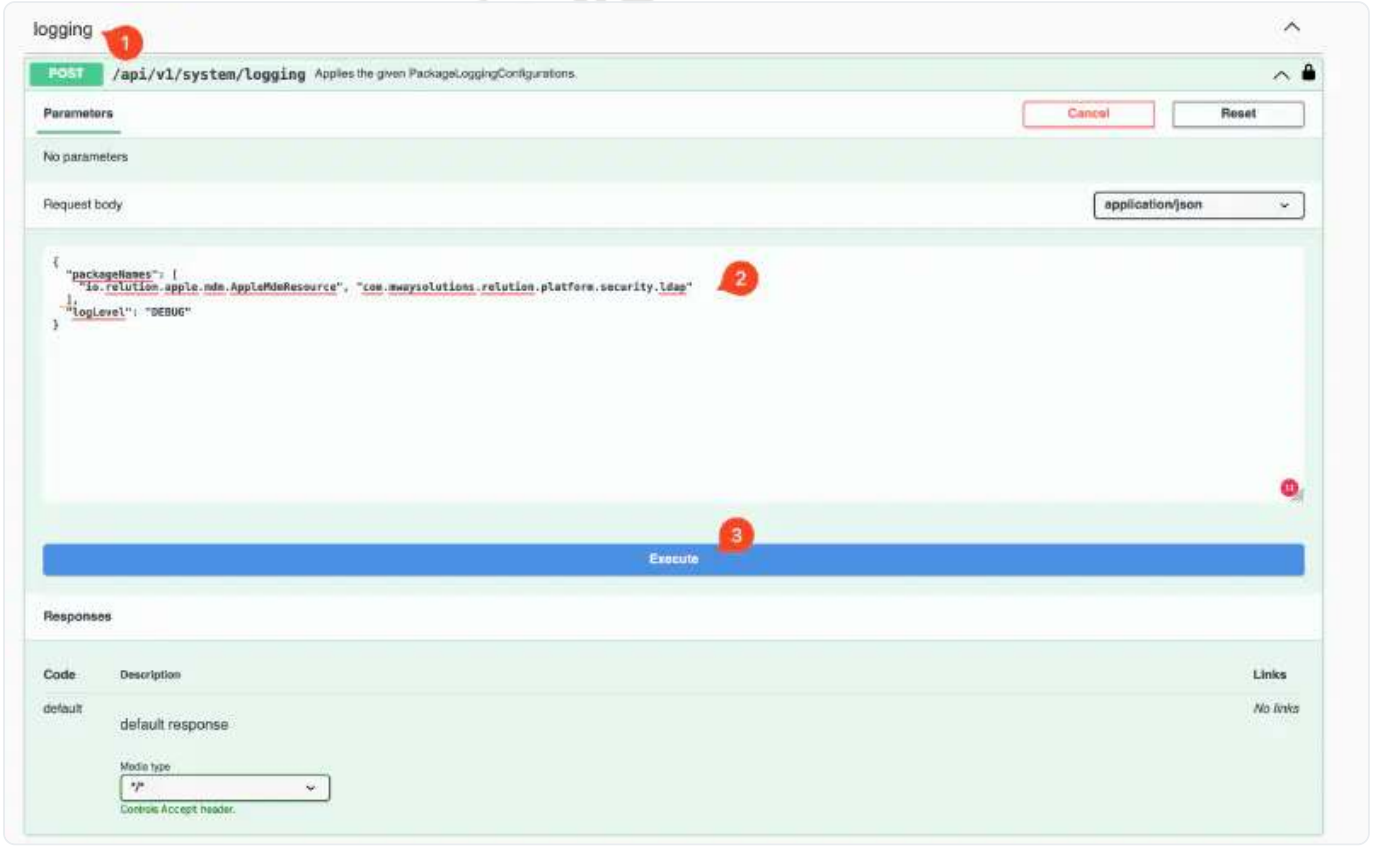
être inséré et autorisé. Note : il est également possible de se connecter avec System System Orga Admin sans saisir le jeton.

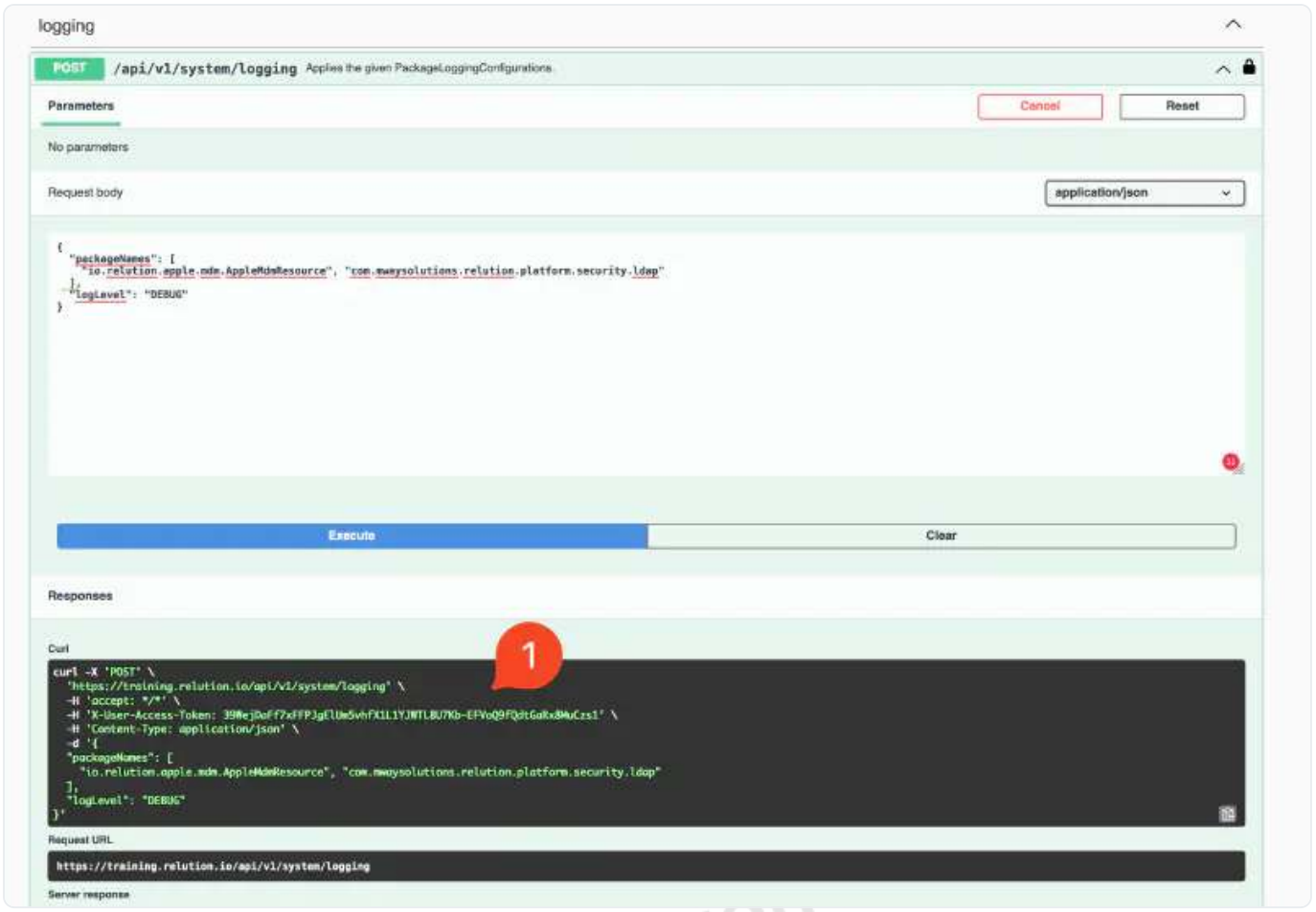
Au point “Logging”, les points d’enregistrement requis ainsi que le niveau d’enregistrement peuvent être définis et exécutés. L’exécution réussie est confirmée par le code 204 et la commande curl exécutée est affichée.



Pour la versi


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.awaysolutions.relution.platform.security.ldap"
],
"logLevel": "DEBUG"
}
2
3
Execute
Responses
Code
Description
Links
default
default response
No links
Media type
/
Controls Accept header.



En outre, il est possible de rétablir les paramètres d'enregistrement par défaut en déclenchant une réinitialisation ou une restauration des points d'enregistrement.



4. contrôler le niveau de journalisation via la commande curl

Il est également possible de contrôler le niveau de journalisation via la commande curl en enregistrant le curl généré via l'API Web en tant qu'alias ou script pour une utilisation ultérieure.



5. utilisation pour le personnel d’assistance ou d’autres employés

Pour accorder l’accès à un utilisateur, par exemple un membre du personnel d’assistance de Relution, il suffit de, transmettre le jeton ou l’adresse électronique de l’utilisateur, qui est liée à une instance valide de Relution, à l’équipe d’assistance de Relution.

Pour la version 26.4.0

Problème lors de la mise à jour vers 26.1

Après une mise à jour vers Relution 26.1, le conteneur Docker ne démarre plus. Le journal du conteneur affiche de manière répétée l'erreur suivante :

```
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

Avec la version 26.1, l'ID de l'utilisateur dans le conteneur a été modifié en raison de bonnes pratiques de sécurité mises à jour. Le répertoire temporaire existant (`/tmp`) dans le volume Docker appartient désormais à un utilisateur incorrect, ce qui empêche le service Relution d'obtenir un accès en écriture au démarrage et provoque son arrêt. Malheureusement, cela ne peut pas être corrigé automatiquement lors de la mise à jour.

Pour la version 26.4.0

Au démarrage, le service vérifie l'accès au répertoire temporaire :

- S'il n'existe pas, il est recréé (avec les bonnes permissions).
- S'il existe déjà, le service tente de le vider – ce qui échoue avec des permissions incorrectes.

Solution

La commande suivante recrée le conteneur Relution, y compris le volume.

```
docker compose up -d --force-recreate --renew-anon-volumes --no-deps relution
```

Remplacer `relution` le cas échéant par le nom de service réel du conteneur concerné.

Après le redémarrage, Relution recrée automatiquement le répertoire `relution.tmp` avec les permissions correctes. L'erreur `Permission denied` ne se produit plus et le service démarre normalement.

Remarques complémentaires

- Cette erreur se produit uniquement lors des mises à jour d'une version antérieure vers 26.1, car le répertoire existe déjà avec les anciennes permissions.
- Pour les nouvelles installations à partir de la version 26.1, ce problème ne se produit pas.
- Si l'erreur persiste après ces étapes, vérifier si d'autres montages de volumes contiennent leurs propres répertoires `tmp`.

Pour la version 26.4.0

Démarrage du serveur avec un certificat S3 auto-signé

Après une mise à jour d'une version antérieure à 26.2 directement vers Relution 26.4 ou une version plus récente, le serveur ne démarre plus si le stockage d'objets S3 connecté est accessible via TLS avec un certificat auto-signé ou interne à l'entreprise. L'erreur suivante apparaît dans le journal :

```
2026-08-18 10:06:09.875 ERROR 12 [ main] s.boot.SpringApplication: Application
AccessDeniedException: software.amazon.awssdk.core.exception.SdkClientExceptio
```

Cause

Au démarrage, Relution lit le certificat de signature JWT depuis le stockage d'objets configuré. Si le certificat de l'autorité de certification émettrice n'est pas enregistré comme étant de confiance, la connexion TLS vers le point de terminaison S3 échoue et le démarrage est interrompu.

Pour la version 26.4.0

Les éléments suivants se combinent ici :

- Lorsqu'un stockage d'objets est configuré, les ressources y sont déportées. Cela concerne également les certificats et donc le certificat de signature JWT.
- Avec Relution 26.2, les certificats sont classés comme sensibles sur le plan de la sécurité et sont conservés durablement dans la base de données. Les certificats déjà déportés sont automatiquement migrés du stockage d'objets vers la base de données.
- Avec Relution 26.4, les certificats CA ne sont plus enregistrés dans le système d'exploitation du conteneur, mais dans la base de données, et sont gérés via l'interface utilisateur (voir Certificat CA dans Docker →). L'ajout du certificat suppose donc un serveur en cours d'exécution, alors que le serveur ne démarre à son tour que lorsque le certificat est déjà considéré comme de confiance.

Si la mise à jour est effectuée par étapes intermédiaires via 26.2 ou 26.3, le certificat de signature se trouve de nouveau dans la base de données après la migration inverse, de sorte que le démarrage sous 26.4 ne nécessite plus d'accès au stockage d'objets. Ce n'est que lors d'une mise à jour directe d'une version antérieure à 26.2 vers 26.4 ou une version plus récente

que cette migration inverse n’a pas lieu, alors que le certificat CA ne peut simultanément plus être ajouté via le système d’exploitation.

Solution

Pour permettre au serveur de démarrer, le certificat de signature concerné est supprimé de la base de données. Au démarrage suivant, Relution génère un nouveau certificat de signature et l’enregistre dans la base de données, de sorte qu’aucun accès au stockage d’objets n’est nécessaire pour le démarrage.

> Une sauvegarde complète de la base de données est recommandée avant toute intervention sur la base de données.

Étapes nécessaires :

1. Le service Relution est arrêté.
2. L’enregistrement du certificat de signature est supprimé de la base de données à l’aide de l’instruction ci-dessous.
3. Le service Relution est démarré.

Pour la version 26.4.0

Pour PostgreSQL, le nom de colonne `usage` est encadré par des guillemets doubles. Dans MariaDB, `usage` est un mot-clé réservé et y est encadré par des accents graves.

PostgreSQL :

```
DELETE FROM mdm_crtfct WHERE "usage" = 'JWT_SIGNER_CERTIFICATE';
```

MariaDB :

```
DELETE FROM mdm_crtfct WHERE `usage` = 'JWT_SIGNER_CERTIFICATE';
```

Conséquences

Un nouveau certificat de signature JWT est généré lors du démarrage suivant. Les cookies de connexion existants deviennent ainsi invalides, ce qui oblige tous les utilisateurs à se reconnecter.

Après le démarrage du serveur

Une fois le serveur démarré, le certificat de l'autorité de certification interne est ajouté afin que la connexion au stockage d'objets soit de nouveau considérée comme de confiance :

- La connexion s'effectue dans l'organisation globale.
- Sous `Paramètres` → `Certificats`, le certificat de l'autorité de certification interne est téléchargé (voir Gestion des certificats →).
- Sous `Paramètres` → `Configuration de confiance TLS` → `Certificats de confiance`, le certificat téléchargé est sélectionné dans la bibliothèque de certificats via Ajouter un certificat.

> Si cette étape est omise, le serveur démarre certes, mais tous les accès au stockage d'objets continuent d'échouer. Par conséquent, les applications natives déjà téléchargées ne peuvent plus être récupérées et les icônes des applications ne s'affichent pas.

Pour la version 26.4.0

La prise en compte s'effectue pendant le fonctionnement du système ; aucun redémarrage supplémentaire du serveur n'est nécessaire. Les autres certificats sensibles sur le plan de la sécurité — par exemple le certificat de signature pour les services externes et le certificat de l'autorité SCEP — sont ensuite également transférés du stockage d'objets vers la base de données.

Remarques complémentaires

- Si le stockage d'objets est connecté sans TLS ou avec un certificat publiquement reconnu, le problème ne se produit pas.
- La migration inverse des certificats vers la base de données est effectuée par une tâche d'arrière-plan exécutée une fois par jour par défaut. En cas de mise à jour par étapes intermédiaires, il convient donc de s'assurer que la migration est terminée sous 26.2 ou 26.3 avant de passer à 26.4.
- La configuration du stockage d'objets est décrite sous Connecter le stockage →.

Connexion : L'accès est interdit

Avec Relution 26.4.0, le serveur d'application interne est passé d'Undertow à Tomcat. Si le reverse proxy (par exemple nginx ou Traefik) s'exécute sur un serveur différent de celui de Relution, cela peut entraîner l'erreur suivante lors de la connexion :



Le journal du serveur Relution affiche alors une entrée `ERROR` correspondante avec l'indication `TLS required`.

Cause

Pour qu'une connexion soit possible, la liaison entre le reverse proxy et Relution doit remplir deux conditions simultanément :

1. Le reverse proxy doit communiquer avec Relution depuis une adresse IP considérée comme interne. Par défaut, seules les plages IPv4 privées `10.x.x.x`, `172.16.x.x`–`172.31.x.x` et `192.168.x.x`, ainsi que `localhost`, sont considérées comme internes.
2. L'en-tête `X-Forwarded-Proto` doit être envoyé par le reverse proxy avec la valeur `https`.

Ce n'est que si les deux conditions sont remplies que Tomcat considère la connexion entrante comme sécurisée par TLS. Si le reverse proxy s'exécute sur un serveur distinct avec sa propre adresse IP (externe), la première condition n'est déjà plus remplie. Si l'en-tête `X-Forwarded-Proto` est en plus, ou à la place, manquant ou incorrect, la connexion n'est pas non plus reconnue comme sécurisée. Dans les deux cas, Relution interrompt la connexion avec `TLS required` dans le journal du serveur, tandis que le navigateur affiche le message `L'accès est interdit`.

Pour la version 26.4.0

Confirmer la cause (optionnel)

Pour confirmer la cause, la journalisation DEBUG du composant Tomcat concerné peut être activée. Pour cela, ajouter l'entrée suivante au niveau supérieur du fichier `application.yml` :

```
logging:
  level:
    org.apache.catalina.valves.RemoteIpValve: DEBUG
```

Une nouvelle tentative de connexion doit ensuite être effectuée. Si une entrée telle que la suivante apparaît alors dans le journal, l'adresse IP du reverse proxy est la cause : la requête n'est pas considérée comme fiable.

```
DEBUG ... ina.valves.RemoteIpValve: Skip RemoteIpValve for request /api/device
```

Si cette entrée n'apparaît pas mais que l'erreur persiste, la cause est plutôt l'en-tête `X-Forwarded-Proto` manquant ou incorrect, voir Solution →.

> Comme alternative à la modification du fichier `application.yml` (qui nécessite un redémarrage), le niveau de journalisation pour `org.apache.catalina.valves.RemoteIpValve` peut également être défini sur `DEBUG` à chaud sans redémarrage via l'API Web ou le portail système. Le niveau de journalisation doit être remis sur `INFO` une fois l'analyse terminée, voir Définir le niveau de journalisation →.

Solution

Selon celle des deux conditions de la section Cause qui n'est pas remplie, l'une des deux adaptations suivantes est nécessaire — les deux si besoin.

Déclarer l'IP du reverse proxy comme fiable

Pour que Relution accepte les requêtes du reverse proxy, son adresse IP doit être explicitement déclarée comme proxy interne fiable. Pour cela, ajouter l'entrée suivante au niveau supérieur du

fichier `application.yml` :

```
server:
  tomcat:
    remoteip:
      internal-proxies: '<IP-du-proxy>|127\.\d{1,3}\.\d{1,3}\.\d{1,3}|0:0:0:0:
```

`<IP-du-proxy>` doit être remplacé par l'adresse IP réelle du reverse proxy, avec les points échappés, par exemple `194\.95\.62\.71`. Pour plusieurs serveurs proxy, d'autres IP peuvent être ajoutées, chacune séparée par `|`.

Le fichier `application.yml` contient généralement déjà d'autres entrées, par exemple pour l'administrateur système, l'URL externe ou la connexion à la base de données. La nouvelle entrée `server` constitue une clé de premier niveau distincte, à côté du bloc `relution` existant, et non un sous-élément de celui-ci — même si une section également nommée `server` existe sous `relution` (avec, par exemple, `externalURL`). L'exemple suivant présente un fichier complet contenant les deux blocs :

```
server:
  tomcat:
    remoteip:
      internal-proxies: '<IP-du-proxy>|127\.\d{1,3}\.\d{1,3}\.\d{1,3}|0:0:0:0:

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%
```

> Il est également possible d'attribuer au serveur Relution une adresse IPv4 locale/privée, par laquelle la communication avec le reverse proxy s'effectue en interne. Dans ce cas, aucune configuration supplémentaire n'est nécessaire, les plages IPv4 privées étant considérées comme internes par défaut.

Définir l'en-tête X-Forwarded-Proto

Le reverse proxy doit en outre transmettre à Relution l'en-tête `X-Forwarded-Proto` avec la valeur `https`. Le bloc `location /` de la configuration nginx doit pour cela contenir la ligne suivante :

```
proxy_set_header X-Forwarded-Proto $scheme;
```

Cette ligne est déjà incluse dans le modèle standard `relution-nginx.conf`. En cas de configuration de reverse proxy personnalisée ou modifiée, ou si un autre proxy se trouve en amont, il convient de vérifier que l'en-tête est correctement défini et n'est pas écrasé par un proxy en amont.

Après avoir adapté le fichier `application.yml` ou la configuration du reverse proxy, le service ou le conteneur Relution (et, le cas échéant, le reverse proxy) doit être redémarré pour que la modification prenne effet.

Pour la version 26.4.0

Remarques complémentaires

- Ce problème concerne en premier lieu les installations dans lesquelles le reverse proxy ne s'exécute pas sur le même hôte que Relution.
- Les installations Relution à partir de la version 26.4.0 sont concernées.
- Le message `L'accès est interdit` est un message d'erreur générique, affiché dans le portail pour de nombreuses requêtes rejetées par le serveur. La solution décrite dans cet article ne s'applique que si le journal du serveur affiche en plus l'entrée `ERROR` `TLS required`.
- Voir aussi : Installation Docker : Nginx comme alternative à Traefik →

Dépannage et assistance

En cas de perte d'accès au compte administrateur système de Relution et d'impossibilité de réinitialiser le mot de passe à l'aide de l'adresse électronique configurée, il est également possible de réinitialiser le mot de passe à partir de la base de données. Cette procédure nécessite un accès en écriture au serveur de base de données et à la base de données de Relution.

Essayer de réinitialiser le mot de passe via le lien "mot de passe oublié" avant d'essayer de le réinitialiser à partir de la base de données. N'utiliser cette option qu'en dernier recours.

Pour réinitialiser le mot de passe, se connecter d'abord à la base de données via la ligne de commande ou un outil d'administration. Exécuter ensuite le script SQL correspondant au serveur de base de données concerné.

MariaDB/MySQL

ion 26.4.0

```
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' ;
```

Remplacer `password123` par le nouveau mot de passe.

Microsoft SQL Server

```
UPDATE security_user SET password = LOWER(CONVERT(VARCHAR(40), HASHBYTES('
    FROM security_organization org
    JOIN security_user usr on usr.organization_uuid = org.uuid
    WHERE usr.name = 'admin' AND org.name = 'system'
    AND org.name = 'system' ;
```

Remplacer `password123` par le nouveau mot de passe.

Le serveur ne démarre pas

Vérifier les fichiers journaux dans le répertoire `log`, qui est situé dans le répertoire d'installation de Relution.
Si le problème ne peut pas être identifié, ouvrir un ticket d'assistance et nous fournir les fichiers journaux.

Fichiers journaux

L'emplacement des fichiers journaux pour Docker, Linux et Windows est décrit sous Journaux Relution →.

Analyse des performances avec Glowroot

Nouveau dans 26.5

> Ce guide s'applique à partir de Relution 26.5.

Pour la version 26.4.0

En cas de problèmes de performances, l'assistance Relution peut demander une analyse avec Glowroot →. Glowroot enregistre la durée de chaque requête et présente le résultat dans sa propre interface web.

Dans un environnement Docker, Glowroot ne fait pas partie de l'image, il est téléchargé automatiquement au démarrage dès que `RELUTION_ENABLE_GLOWROOT` est défini :

```
relution:
  image: relution/relution:latest
  environment:
    - RELUTION_ENABLE_GLOWROOT=true
    - RELUTION_GLOWROOT_ADMIN_JSON_BASE64=ewogICJ3ZWIiOiB7CiAgICAiYmluZEFkZH
  ports:
    - '4000:4000'
```

La seconde variable contient simplement la configuration Glowroot encodée en base64 `{"web": {"bindAddress": "0.0.0.0"}}`. Sans elle, l'interface n'est accessible que depuis l'intérieur du conteneur. Après un redémarrage du conteneur, elle est disponible sur le port 4000.

Les enregistrements se trouvent dans le conteneur et sont perdus dès que celui-ci est recréé. Pour la durée d'une analyse, cela suffit généralement. Pour les conserver, définir `RELUTION_GLOWROOT_DIR` sur un répertoire accessible en écriture pour l'UID `20001`.

> N'activer Glowroot que pendant la durée de l'analyse. L'interface sur le port 4000 n'est pas protégée par un mot de passe et expose les requêtes de base de données, les temps de réponse et les traces d'exécution. Elle ne doit en aucun cas être accessible depuis Internet.

Pour la désactiver, supprimer `RELUTION_ENABLE_GLOWROOT` et redémarrer le conteneur.

Notes de sécurité

- Installer les dernières mises à jour du système d'exploitation et du logiciel, ainsi que les correctifs de sécurité.
- Utiliser des mots de passe forts pour les comptes administrateurs
- Utiliser des mots de passe longs pour les communications entre services. Les mots de passe ne doivent pas être utilisés ou mémorisés par des humains.
- S'assurer que le compte d'utilisateur utilisé pour accéder au LDAP dispose d'un accès en lecture seule.
- Ne pas créer de comptes avec des mots de passe faibles tels que `password` ou `test`.
- Ne pas stocker les mots de passe dans des fichiers qui sont globalement lisibles.

Pour la version 26.4.0

Marché local sans SMG

La configuration d'un serveur Exchange local sans SMG (Secure Mail Gateway) peut facilement échouer. C'est pourquoi nous avons identifié les causes les plus courantes et enregistré les solutions appropriées. Pour vérifier la connectivité de base, il y a quatre étapes à suivre.

Analyse du fichier journal

Le journal du proxy inverse (par exemple nginx) est nécessaire pour une analyse plus approfondie.

- Sous Linux, le journal est situé dans le répertoire suivant `/var/log/nginx/relution_access.log`
- Pour Windows, par exemple dans le chemin d'installation de nGinx `/nGinx/logs/relution_access.log`.

Si les courriers sont récupérés sur l'appareil final, le journal doit contenir une référence à l'URL suivante `/Microsoft-Server-ActiveSync`

Si l'entrée /Microsoft-Server-ActiveSync est laissée derrière, la connexion fonctionne.

Pour la version 26.4.0

Dépannage

Si rien n'est saisi dans le journal, l'URL doit être saisie dans le navigateur si elle est généralement accessible. `https://myexchange.com/Microsoft-Server-ActiveSync` Si l'URL est appelée, une entrée doit être laissée dans le journal nginx.

- Si aucune entrée n'est générée, l'infrastructure doit être vérifiée.
- Si l'entrée peut être trouvée, il est probable que les paramètres de la configuration Exchange dans la politique de Relution ne sont pas définis correctement ou sont invalides.

Vérification de la connexion

Une commande curl peut être utilisée pour vérifier la connexion de Relution au serveur Exchange :

```
curl https://outlook.XXX.de/Microsoft-Server-ActiveSync --user Our-Exchange-ho
```

Il se peut qu'une sortie avec une erreur de certificat s'affiche, comme indiqué :

```
Essai sur 172.16.105.109:443....
Connecté à outlook.XXX.de (172.000.000.000) port 443 (#0)
schannel : a désactivé l'utilisation automatique du certificat client
ALPN : offre http/1.1
schannel : SEC_E_UNTRUSTED_ROOT (0x80090325) - *La chaîne de certificats a été
Fermeture de la connexion 0
curl : (60) schannel : SEC_E_UNTRUSTED_ROOT (0x80090325) - *La chaîne de certi
Plus de détails ici : https://curl.se/docs/sslcerts.html
```

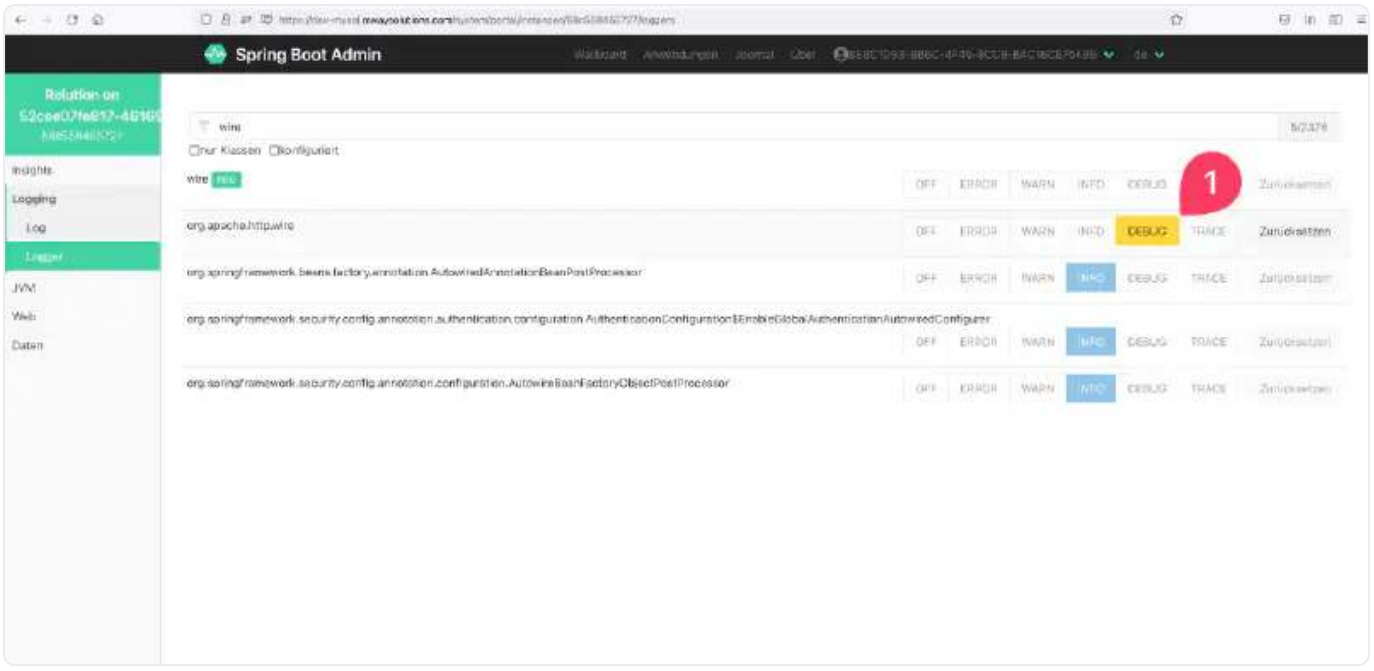
Si le message d'erreur s'affiche comme ci-dessus, le certificat de l'autorité de certification n'est pas stocké dans le système d'exploitation du serveur ; en fonction du système d'exploitation, le certificat doit donc être installé en conséquence.

Exemple de solution dans Docker →

Pour la version 26.4.0

Lire la communication HTTPS

En réglant le niveau de journalisation du logger `org.apache.http.wire` sur `DEBUG`, la communication HTTPS entre Relution et Exchange devient lisible dans le fichier journal. Les différentes voies pour définir le niveau de journalisation — API Web, `application.yml` ou portail système — sont décrites sous Niveau de journalisation →. La voie du portail système présentée dans la capture d'écran ci-dessous requiert depuis Relution 26.4 l'activation du point de terminaison actuator correspondant →.



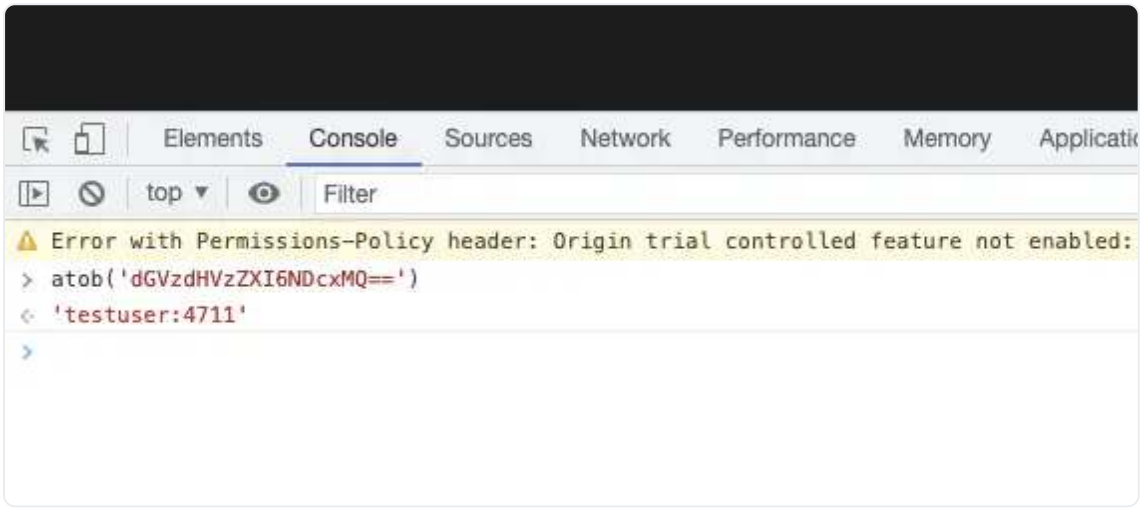
Une communication doit être déclenchée par le dispositif pour remplir le journal avec des indices sur la cause. Le niveau du journal doit être remis à `INFO` après l'analyse.

Évaluer le journal

Pour la version 26.4.0

Par la suite, il est possible de rechercher des indices évidents dans le niveau de journalisation accru. Par exemple, si l'utilisateur et les informations d'identification de l'utilisateur ne sont pas corrects, la connexion échoue et un message 401 Unauthorized est affiché, qui peut ressembler à ceci dans l'authentification de base : `dGVzdHVzZXI6NDcxMQ==`

Ce message peut être décodé dans la console du navigateur pour comparer le mot de passe transmis et l'utilisateur `atob('dGVzdHVzZXI6NDcxMQ==')`



SMG n’est pas fonctionnel avec Outlook365, Microsoft a désactivé Basic Auth pour cela et utilise OAuth2

Désactivation de Basic Auth →

Pour la version 26.4.0

Annonces et conseils

Logiciels en fin de vie (EOL)

Pour des raisons de sécurité, Relution ne prend généralement pas en charge les logiciels ayant déjà atteint leur fin de vie (End-Of-Life, EOL), car plus aucun correctif de sécurité n'y est fourni.

Annonces et dépréciations

- Mise à jour vers 26.4.0+ : Avec Relution 26.4.0, le serveur d'application interne est passé d'Undertow à Tomcat. Si le reverse proxy est exécuté sur un serveur différent de celui de Relution, la connexion peut ensuite échouer avec le message `L'accès est interdit` (`TLS required` dans le journal du serveur). Dans ce cas, la configuration doit être adaptée selon les étapes décrites dans Connexion : L'accès est interdit →.
- Nouvelle image de base : Ubuntu au lieu d'AlmaLinux : à partir de la version 26.4.0, l'image de conteneur Relution est basée sur Ubuntu et non plus sur AlmaLinux.
- Secure Mail Gateway : À partir de Relution 26.4.0, l'utilisation de la fonctionnalité Secure Mail Gateway nécessite un service autonome dédié — sans ce service, la fonctionnalité ne sera plus disponible. Dans la version 26.3, le nouveau mode peut déjà être activé en option via un feature toggle. Pour les instructions de migration, consultez Secure Mail Gateway →.
- Mise à jour vers 26.1+ : avant une mise à niveau vers la version 26.1 ou supérieure, une version 26.0.x doit avoir été installée et démarrée au moins une fois. Si une version 26.0.x est déjà utilisée, la mise à jour vers 26.0.3 en particulier n'est pas nécessaire. Contexte : Relution 26.1 ne prend en charge les mises à niveau de base de données qu'à partir de la version 26.0, une version 26.0.x est donc requise comme étape intermédiaire. Lors de la mise à jour vers 26.1, il peut en outre arriver que le conteneur Docker ne démarre plus en raison d'un problème de droits sur le répertoire temporaire. La solution est décrite dans Problème lors de la mise à jour vers 26.1 →.
- Object Storage : en cas d'utilisation de MinIO comme stockage local compatible S3, une migration vers SeaweedFS est recommandée, MinIO ayant arrêté son développement. Un guide est disponible dans Migration du stockage d'objets →.
- Groupes d'appareils : comme annoncé précédemment, Relution 26.0 bascule automatiquement les organisations non encore migrées vers les groupes d'appareils ; la prise en charge de l'ancienne fonctionnalité est supprimée. Les jeux de règles remplacés par les actions de groupes d'appareils disparaissent également définitivement.

Pour la version 26.4.0

- Java : à partir de la version 5.35, Relution nécessite *Java 21*. Avec 26.0, le démarrage de Relution avec des versions antérieures de Java n'est plus possible.
- MariaDB : Relution 5.30 nécessite *MariaDB 10.11 ou supérieur*. La *prise en charge de MariaDB ne sera globalement assurée que jusqu'à fin 2027.*
- PostgreSQL : Relution 5.29 nécessite *PostgreSQL 14 ou supérieur*. Il est recommandé d'utiliser directement *PostgreSQL 18*.

Nouveaux articles du manuel

Un aperçu des nouvelles fonctionnalités des trois dernières versions, avec des liens vers les articles du manuel correspondants.

Version 26.5

On Premises Installation

- Dépannage et assistance → Analyse des performances avec Glowroot
- Chiffrement côté serveur (SSE-C) → Option C : clé sous forme de fichier
- Relution Shield (Add-on) → Création d'un utilisateur technique et d'un jeton d'accès API{#create-technical-user}

Pour la version 26.4.0

Général

- Tableau de bord
- Teacher → Liens web et restrictions de navigation
- Espaces réservés avancés → Certificats utilisateur
- Profil pour l'ADE → Version minimale du système d'exploitation
- Groupes d'appareils → Groupes Éducation

Apple macOS

- Verrouillage de récupération → Vérifier le verrouillage de récupération
- Relution Decon (filtre)

Éducation

- Groupes Éducation

Android Enterprise

- Lier l'organisation → Réparer l'inscription

Paramètres

- Pool de certificats
- Configuration de confiance TLS → Épinglage de certificats (inscription Apple)

- Organisations Meta
- OIDC avec Entra → URI de redirection pour l’enrôlement des appareils
- Relution en tant que fournisseur d'identité
- OIDC avec Workspace → URI de redirection pour l’enrôlement des appareils

---

Version 26.4

On Premises Installation

- Certificat CA dans Docker → Ajout de certificats via l’interface utilisateur
- Connexion : L'accès est interdit
- Secure Mail Gateway → Composant obligatoire à partir de 26.4.0

Général

- Portail libre-service → Afficher la position sur une carte
- Profil pour l'ADE → Authentification de l’utilisateur lors de l’inscription

Apple iOS

- Mise à jour logicielle → Mises à jour logicielles gérées

Apple macOS

- Verrouillage de récupération → Définir le verrouillage de récupération
- Mises à jour logicielles → Mises à jour logicielles gérées

Android Enterprise

- Localiser un appareil Android → Afficher la position dans le portail libre-service

Windows

- Configurer le Companion

Paramètres

- Organisation globale → Sélecteur d’organisation
- Configuration de confiance TLS
- OIDC avec Entra → Ajouter l’URI de redirection
- OIDC avec Workspace → URI de redirection scopées
- Secure Mail Gateway → Configuration de Secure Mail Gateway

Version 26.3

On Premises Installation

- Certificats de poussée APNS → Migration depuis le processus précédent
- Chiffrement côté serveur (SSE-C)
- Secure Mail Gateway → Feature toggle pour les installations on-premise (26.3)

Pour la version 26.4.0

Commencer

- Gérer les appareils Apple → Certificats

Apple iOS

- Paramètres Intelligence
- Paramètres d'intelligence externe
- Paramètres du clavier
- Paramètres Siri

Apple macOS

- Paramètres Intelligence
- Paramètres d'intelligence externe
- Paramètres du clavier
- Paramètres de Siri
- Assistant Migration → Déclaration de paramètres

Apple visionOS

- Paramètres Intelligence

Paramètres

- Certificats d'organisation

Pour la version 26.4.0

Technical Changelog

This page contains the technical changelog and is intended for an experienced audience. You can find the release notes containing a lot more explanation 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)

Avant la mise à jour vers Relution 26.1

Une version 26.0.x (par exemple la dernière version 26.0.3 →) doit être installée et démarrée au moins une fois avant de procéder à une mise à niveau vers la version 26.1 ou supérieure. Si une version 26.0.x est déjà utilisée, il n'est pas nécessaire de mettre à jour vers la 26.0.3 en particulier.

Pour la version 26.4.0

Contexte : Relution 26.1 ne prend en charge que les mises à niveau de la base de données à partir de la version 26.0. Une mise à niveau directe vers la version 26.1 ou supérieure sans installation et démarrage préalables d'une version 26.0.x n'est donc pas prise en charge.

De plus, la mise à jour vers la version 26.1 peut entraîner l'échec du démarrage du conteneur Docker en raison d'un problème de permissions sur le répertoire temporaire. Consulter Problem with update to 26.1 → pour la solution.

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

Pour la version 26.4.0

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]

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]

Pour la version 26.4.0

- 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]

Pour la version 26.4.0

Updates

- 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

Pour la 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]

Pour la version 26.4.0

- 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]
- 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]

Pour la version 26.4.0

- 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

Pour la version 26.4.0

- Ensure that apps from a global VPP token are also preserved when the “Preserve all existing apps” option is active in the DEP profile [REL-13320]

Version 26.4.5

2026-08-19

Fixes

- Fix persisting the push token of Android Classic devices [REL-13243]

Version 26.4.4

2026-08-18

Updates

- Augment “preserve all apps” functionality for Apple device migration [REL-13167]

Fixes

- Prevent loss of ON-Demand App Installation for Apps iOS 26 device migration [REL-12442]
- Improve caching of Image Render Service [REL-13159]

Pour la 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]

Pour la version 26.4.0

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

2026-07-16

With Relution 26.4.0, the internal application server was switched from Undertow to Tomcat. If the reverse proxy runs on a different server than Relution itself, logging in may subsequently fail with the message `Access is forbidden` (`TLS required` in the server log). In this

case, the configuration must be adjusted according to the steps described in Login: Access is forbidden →

New

- Improve self-service portal device locate flow so authorised users can access location feedback [REL-11014]
- Add shutdown action support for Newline smartboards [REL-10615]
- Add time zone information to Apple device details [REL-12447]
- Add enhanced retry and backoff handling for object storage operations [REL-11912]
- Improve foundation of object storage and general resource storage handling with better resilience and observability [REL-11910]
- Improve object storage client connection handling and timeout configuration [REL-11911]
- Improve device history localization by storing translation keys and translating entries when read [REL-12067]
- Add support for DEP enrollment using username and enrollment code authentication [REL-11841]
- Add support for managing additional CA certificates in global settings for outbound SSL/TLS connections [REL-11453]
- Add server version to audit log start and stop entries [REL-12423]
- Improve organization switcher to pin specific items [REL-11748]
- Introduce scoped OIDC redirect URIs for reverse-proxy path gating. Legacy URI stays valid but is deprecated, register the new URIs at your Identity Provider, check Relution Hub for more information [REL-10832]
- Add support for automatically updating the assigned device user when a user logs into a managed Windows device, with organization-level and device-level controls [REL-8313]
- Extend agent-scope API support by mirroring relevant server endpoints and migrating Relution Assets to use only endpoints from its dedicated API scope [REL-10523]
- Add search bar to Apple and Android app compliance lists to make apps easier to find [REL-12023]

Updates

- Exclude obsolete Relution client certificates from key store checks and cleaned up leftover database entries [REL-11535]
- Update Spring Boot to Version 4 [REL-10462]
- Disable audit logs for get actions management endpoint by default [REL-12475]
- Support pinning the TLS certificate for Apple Software Update lookup service (GDMF) requests [REL-11344]
- Adjust handling of VPP apps being reported with zero licenses [REL-10792]

Pour la version 26.4.0

- 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]

Pour la version 26.4.0

Fixes

- 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]

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]

Pour la version 26.4.0

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

Pour la version 26.4.0

- Fix an issue where providing an own APNS Certificate via global did not get propagated properly to other orgas [REL-12370]
- Fix problems with license handshake in cluster setup [REL-12200]
- Fix an issue where Android Enterprise SIM card details did not get updated properly [REL-12315]

Version 26.3.0

2026-06-08

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]

Pour la version 26.4.0

- 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]

Pour la version 26.4.0

- 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]

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]

Pour la version 26.4.0

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]

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]

Pour la version 26.4.0

- 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]

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]

Pour la version 26.4.0

- 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]

Pour la 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

Pour la version 26.4.0

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 (published & 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

- 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]

Pour la version 26.4.0

- 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]

Pour la version 26.4.0

Version 26.0.3

2026-02-11

Fixes

- Fix Secure Mail Gateway returning HTTP 403 instead of 401 when unauthenticated leading to reduced number of password prompts [REL-10973]

Version 26.0.2

2026-02-05

New

- Add support for disabling Safari history retention in Apple Web Content Filter configurations [REL-10181]

Fixes

- Fix Windows Push token update failing for unexpected device response causing communication errors in special cases [REL-10778]
- Prevent license handshake request creation failing due to license claim retrieval for lifetime licenses [REL-10866]
- Fix Local Windows Account action failure when creating non-admin accounts only [REL-10831]
- Fix saving Web Content Filter configurations with plugin filter type [REL-10883]

Pour la 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

- Improve performance impact of nested dynamic device group filters with user group recursion [REL-10205]

Pour la version 26.4.0

- 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

- Remove unintended data from logging [REL-10445]

Pour la version 26.4.0

- 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]

Pour la version 26.4.0

- 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]

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]

Pour la version 26.4.0

Version 5.35.2

2025-11-14

Fixes

- Avoid issues with unexpectedly missing organization meta data during license handshake [REL-10163]

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]

Pour la version 26.4.0

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]

Pour la 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

Pour la version 26.4.0

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]

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]

Pour la version 26.4.0

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]

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]

Pour la version 26.4.0

- 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]

Pour la 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]

Pour la version 26.4.0

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]

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]

Pour la version 26.4.0

Fixes

- Fix compliance violation behaviour for Windows devices between policy version changes [REL-8428]
- Fix blocking of Android apps via Android Enterprise [REL-9239]
- Fix handling of connection failures when receiving VPP notifications for new apps [REL-9173]
- Update of CORS header to enable Zero Touch in Android Enterprise settings [REL-9158]
- Fix lending system, so that duplicate active lendings are no longer possible [REL-8943]
- On enrollment of an Android legacy device Relution no longer sents an unsupported device name action [REL-7732]
- Fix Wi-Fi SSID as required for Android Enterprise connectivity configuration [REL-8857]
- Fix autopilot enrollments [REL-8885]
- Resolve action details permanently storing device credential data intended for single-usage only [REL-5529]
- Add sorting by name and description in category list [REL-9291]
- Update app detail screen on multi tenant switch [REL-9287]
- Fix minimum permissions needed to show the dashboard [REL-9255]
- Fix resetting of filters in lists [REL-9246]
- Fix navigation sometimes switching you back to previous tenant when navigating between views in different organizations [REL-9242]
- Add translation to all setup modes in macOS global ethernet settings configuration [REL-6605]
- Fix wrong last connection date for Android Enterprise devices [REL-7907]
- Update view for Windows “Add Accounts” action [REL-7622]
- Fix checking activation state of Android Enterprise at several places in web portal [REL-8856]
- Ensure that only the latest Relution File Shares configuration can be edited [REL-7412]
- Fix layout of MFA setup dialog [REL-8733]
- Fix opening links in new tabs when navigating in a tenant organisation at various places [REL-9216]
- Fix radio button alignment in MFA token modal [REL-2116]

Pour la version 26.4.0

Version 5.32.2

2025-08-12

Fixes

- Fix database migration issue for MariaDB — Resolved a migration failure on some instances containing DEP host certificates, likely related to internal InnoDB index prefix length handling [REL-9002]

- Ensure license models ‘Public’, ‘NGO’, and ‘MAM’ display correct license limitations by default [REL-9012]

Version 5.32.1

2025-07-17

Fixes

- Fix Android Enterprise connection warning notifications in cluster setups [REL-8852]
- Fix handling of configuration templates in LDAP still defined via YML configuration file [REL-8919]
- Fix creation of new ASM SFTP sync settings in Portal [REL-8925]
- Fix autopilot enrollments [REL-8885]

Version 5.32.0

2025-07-03

New

Pour la version 26.4.0

- 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

- 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]

Pour la version 26.4.0

Fixes

- 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]

Pour la version 26.4.0

- 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]

Version 5.31.0

2025-05-27

Pour la version 26.4.0

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]

Pour la version 26.4.0

Updates

- Remove unused “Interface” setting from iOS WiFi configuration [REL-8490]
- Show automated enrollments via Autopilot in audit log [REL-8238]
- Extend clean up of duplicate open actions [REL-6822]
- Execute Windows Deploy app actions with sub actions [REL-5364]
- Optimize Android Enterprise communication [REL-8494] [REL-7462]
- Optimize Android Enterprise subscription polling in clustered installations [REL-8186]
- Extend lesson template with Decon options [REL-7902]
- Improve reliability of access to Relution Google Play, WinGet, Google Places and SMS services [REL-8037]
- Avoid redundant error log for push messages [REL-8150]
- Show package name in open app action details [REL-7895]
- Make device logs include `DEBUG` level logs by default [REL-8142]
- Allow extensible matches and nested structures in LDAP filters [REL-7234]

- Fix criteria for showing hint that Entra ID has been configured in global organization in settings [REL-8160]
- Do not send query action after device reboot for Apple devices [REL-7945]
- Adjust handling of already deleted scripts in script history [REL-2466]
- Add single app mode configuration for tvOS [REL-7702]
- Use default template and language handling for reset password notification mails [REL-7881]
- Replace all HTML email templates with an updated, much more appealing, template [REL-6951]
- Decrease default push queue delays and reduce number of multiple pushes to the same device in a very short amount of time [REL-444]
- Use user preferred language to send notifications via email or push [REL-7230]
- Make dynamic device group filter “security patch level does not contain…” accept Android Enterprise devices only [REL-7809]
- Optimize database model of action table [REL-2640]
- Update iOS SCEP configuration with additional configuration options [REL-7452]
- Optimize page handling during LDAP synchronization [REL-7446]
- Ensure buttons in modals are shown without scrolling in Portal [REL-7122]
- Optimize display of OpenID Connect URLs in settings [REL-8390]
- Show address in device location [REL-8328]
- Allow clearing of fields in the managed app configuration of a managed app in a Android Enterprise policy [REL-7782]
- Remove option to select a custom client for organizations which do not use this feature already [REL-8034]
- Avoid showing notification messages in Portal when location of a device is not available [REL-7890]
- Update icons of several macOS configurations [REL-7626]
- Fix validation of certificate templates in Portal if expiration in days is less than automatic renewal [REL-7724]
- Configure agreements for Apple enrolments [REL-7706]
- Restore teacher device provisioning and always make sure Relution Teacher is available if the device has an app allow list [REL-8374]

Pour la version 26.4.0

Fixes

- Allow toggling optional parts of macOS energy saver configuration [REL-7548]
- Fix automated disassociation of VPP licenses on app removal for global apps [REL-8460]
- Fix error message when trying to request an app that already exists as a global app [REL-8489]
- Fix possible issue when handling “Not Now” responses for remove profile requests [REL-8446]

- Fix issues with some international number formats when sending enrollment SMS [REL-8383]
- Prevent users from changing their profile when they are synced via external providers [REL-8377]
- Fix possible values for deadline updates in Windows Update Configuration [REL-8262]
- Optimize Decon license query [REL-7523]
- Fix handling possible performance issue when handling device authorization [REL-8307]
- Fix issue when moving an Apple device enrolled via a multi enrollment [REL-7936]
- Fix location handling for Android Enterprise companion [REL-7840]
- Optimize display and validation of device availability check settings [REL-7516]
- Fix selection of device groups in enrollments [REL-7623]
- Fix S3 health indicator when using AWS S3 [REL-7415]
- Fix issue preventing the windows app store search from functioning properly when receiving empty results [REL-7605]
- Fix installing WinGet apps manually via Portal [REL-8447]
- Fix language of manual link in user CSV import modal [REL-8452]
- Fix caching issue of the web portal during a Relution Update by performing a reload of the browser [REL-8365]
- Allow selecting public scripts in local script configurations [REL-8309]
- Fix handling of invalid filter query URLs in Portal [REL-8161]
- Adjust validation of Android Enterprise internal name for managed apps [REL-8204]
- Fix floating of auto complete selection dialogs in device group filter selection [REL-7741]
- Fix deselecting items in single selection lists via the radio button in Portal [REL-7549]
- Fix refresh of policy version selection in Portal [REL-7987]
- Fix issue that the count of the affected devices in the device group preview and the shown devices in the preview can diverge [REL-7896]
- Hide managed app store option if Andoid Enterprise setup is not completed [REL-7692]
- Show full details of compliance violations as tooltip [REL-6553]
- Fix ICCID column behaviour in new device details view [REL-7837]

Pour la 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]

Pour la version 26.4.0

- 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]

Pour la version 26.4.0

Updates

- 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]

Pour la version 26.4.0

Fixes

- Fix applying of edu configuration if the same teacher user is removed and then added again to the same device [REL-7835]
- Fix possibly missing update of tenant switch after creating new orgas when running Relution as a cluster [REL-7733]
- Add a toggle to bypass internal name mismatches when a new DMG app version gets uploaded [REL-7750]
- Fix S3 health indicator when using AWS S3 [REL-7415]
- Fix race condition when saving compliance violations [REL-7707]
- Fixed an internal server error when adding an unreleased app to the managed app configuration of an Android Enterprise policy. [REL-7694]
- Fix DEP enrollment without user authentication which now also requires a login since 5.29.2 [REL-7631]
- Adjust validation for install priority values in Android Enterprise configuration [REL-6998]

- When importing users from CSV with creation of classes enabled, the import of classes stopped on first encounter of a class without students or teachers. The fix applied merely records the issue to the log, continuing creation of further classes. [REL-7524]
- Adjust behaviour of several filter types in dynamic device groups with platform specific filter criteria like security patch level [REL-7376]
- Fix policy not being imediately removed from all devices when being deleted [REL-7365]
- Adjust error handling when public app store service is not available [REL-5832]
- Fix ICCID column behaviour in new device details view [REL-7837]
- Fix wording in macOS dock configuration [REL-7781]
- Adjust error hint for unique name of organizations [REL-7731]
- Fix an issue where refreshing the app details page lead to an “App does not exist” error when multiple tenants are available. [REL-7796]
- Fix supervision filter in device inventory [REL-7783]
- Add missing translations for action channel filter in action list [REL-7739]
- Show “manage app assignments” in installed app list only for Android Enterprise devices [REL-7693]
- Improve description of macOS firewall confiuration [REL-7674]
- Fix displaying the Relution login page on iOS 15 devices during DEP enrollment and Relution Shared Device [REL-7614]
- Fix validators in Android Enterprise managed app configuration [REL-7633]
- Fix bug reporter popping up in manual macOS user enrollment creation [REL-7630]
- Tweak display of device details after design update [REL-7540]
- Fix on leave device group notification actions being sent to devices which were not part of the group before [REL-7635]

Pour la 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]

Pour la version 26.4.0

Version 5.29.1

2025-01-28

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]

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]

Pour la version 26.4.0

- 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

Pour la 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]

Pour la version 26.4.0

- 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

- 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]

Pour la version 26.4.0

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]

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]

Pour la version 26.4.0

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]

Pour la version 26.4.0

Updates

- Add workaround for iOS/iPadOS not showing AirDrop UI by automatically adding the OS-internal identifier for it to the allowed apps if AirDrop is allowed in restrictions and an allow list is configured [REL-6222]
- Improve performance of loading current user information, speeding up actions like login, switching tenants and reload of web portal [REL-6513]
- Reduce log level for Android Enterprise status reports [REL-6493]
- Extend restrictions with new Apple AI settings [REL-6453]
- Add workaround for iOS/iPadOS showing the same web link multiple times until device or spring board is restarted [REL-5797]
- Drop `DISABLE_RESOURCE_HASH` feature flag [REL-6406]

- Add support for devices providing multiple Bitlocker recovery keys [REL-3993]
- Adjust periodic push for devices with open actions to rotate the devices it pushes to [REL-3907]
- Show type of native apps for macOS (`.dmg` or `.pkg`) at additional places [REL-6236]
- Adjust handling of script file updates [REL-6277]
- Make withdraw of Android Classic devices on missing device administrator compliance violation configurable [REL-4241]
- Remove deprecated `/enumerables/pairs` endpoints [REL-5331]
- Add missing unique constraints to a few database tables [REL-4420]
- Adjust default external app store refresh interval and batch size [REL-6245]
- Add support for sending files to Android Enterprise devices [REL-6099]
- Optimise creation of audit log entries [REL-5851]
- Add explicit option to allow login on iOS/iPadOS devices if an allowlist is configured [REL-5873]
- Support mapping of IPv4-Mapped IPv6 addresses → [REL-6087]
- Adjust handling of user logouts [REL-1706]
- Automatically refresh map with device location display in portal [REL-6246]
- Add Samsung KSP widget [REL-6355]

Fixes

Pour la 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]

Pour la 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]

Pour la version 26.4.0

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]

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

Pour la version 26.4.0

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]

Pour la 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]

Pour la version 26.4.0

- 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]

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]

Pour la version 26.4.0

- 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

Pour la version 26.4.0

- Resolve issue with updating installed apps of devices which report the same app multiple times [REL-5662]
- Fix display of selected scheduled days of week in scheduled policies [REL-5798]
- Fix selection of separator of CSV upload in device inventory [REL-5808]
- Resolve a possible issue during database migration if lesson or lesson templates contain unexpected data [REL-5848]

Version 5.26.3

2024-09-02

Fixes

- Fix database query for lent devices which has an issue since 5.26.0 [REL-5761]

Version 5.26.2

2024-08-30

Updates

- Decrease default push queue delays and reduce number of multi-push to the same device [REL-444]

Fixes

- Fix sporadic connection issues of Relution apps on Android Enterprise devices when delivery of devices policies gets delayed by communication infrastructure [REL-5620]
- Improve dashboard performance by only listing the first 50 organisations [REL-5677]

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]

Pour la version 26.4.0

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]

Pour la version 26.4.0

Updates

- 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 hehaviour, 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]

Pour la version 26.4.0

Fixes

- Fix deleting users by clearing audit log references on deletion [REL-5419]
- Extend error details shown for several failures in Apple MDM payload generation [REL-1174]
- Fix display of provider names for OIDC configurations which are misconfigured [REL-2503]
- Fix serialization behaviour of some enrollment events [REL-5127]
- Avoid sending expiration notifications for APNS push certificate of the legacy Relution client [REL-4888]
- Fix context information missing from logs [REL-5002]
- Avoid possible deadlocks when adding a device to a large number of static groups with a single operation [REL-4388]
- Adjust cleaning up of finished push jobs [REL-4175]
- Adjust payload properties of generated configurations for macOS [REL-4862]
- Fix responsive behaviour of device group header box [REL-5261]
- Make device group column and filter labels more consistent [REL-5194]
- Improve error handling and display in app uploader [REL-4519]

- Adjust translation in the device group action deletion dialog [REL-5275]
- Fix saving strongSwan Profile configurations that contain a user certificate template [REL-5032]
- Limit filter values in device inventory and trash to values actually occurring in the set of devices shown in the respective list [REL-4572]
- Fix Android Classic passcode configuration, when selecting complex as type [REL-3509]
- Ignore selected permissions when hitting cancel in the permission selection modal in user and group details [REL-5023]
- Show correct last modified date in compliance violation view [REL-4565]
- Disable “add new version” button for public apps since they are retrieved from external app stores [REL-4194]
- Fix possible issue during enrollment of Degen ADVANTouch interactive boards keeping them in ’enrollment pending’ state [REL-5518]

Version 5.25.3

2024-07-26

Updates

- Prepare additional permissions for Relution Shield [REL-4996]

Pour la version 26.4.0

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]

Pour la 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

Pour la version 26.4.0

- 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

- 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]

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]

Pour la version 26.4.0

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

- 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]

Pour la version 26.4.0

- 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

Pour la 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]

Pour la version 26.4.0

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

- 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]

Pour la version 26.4.0

- 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]

Pour la 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]

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]

Pour la version 26.4.0

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

Pour la version 26.4.0

New

- Extend device group filter to also evaluate group membership of the assigned device user. When saving device groups or performing a login on a shared device, this will be evaluated immediately, otherwise updates will be performed periodically in background [REL-2711] [REL-2849]
- Add device group actions allowing to schedule actions or notifications via device groups. They will fully replace the now deprecated rule sets in a future release, which are no longer shown in organizations not using them already. Please migrate your rule set configurations to device group actions [REL-859] [REL-2919] [REL-2612] [REL-3101]
- Allow notifying users and groups in device group actions via push or email [REL-2613]
- Add extensible SSO policy configuration for Apple devices [REL-2802] [REL-3667]
- Add support making PowerShell scripts public, so they can be used in all organisations of a Relution server [REL-2801]
- Add self-service portal which allows users to view their devices and trigger actions on them if enabled by assigning the necessary permissions [REL-2816]

- Add interactive board configuration for SMART boards [REL-1233]
- Allow configuring outgoing mail server configuration via system organization settings in web portal [REL-2822] [REL-3134] [REL-3177]
- Show if Apple are denied communication due to expired identity certificates and support selectively allowing them anyway to renew their profile. Also add corresponding columns to device inventory and details and add filters to device groups [REL-3282]
- Allow customising compliance enforcement rules for Android Enterprise devices [REL-2877]

Updates

- 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]

Pour la version 26.4.0

- 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]

Pour la version 26.4.0

Fixes

- 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]

Pour la 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]

Pour la version 26.4.0

- 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

- 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]

Pour la version 26.4.0

- 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

Pour la 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]

Pour la version 26.4.0

Version 5.20.8

2023-11-21

Updates

- Clean up actions in terminal state only by default, since the cleanup now happens earlier than before [REL-3030]
- Use clean up with default expiration instead of short expiration for action types where only one pending, successful and failed action is kept anyway [REL-3030]

Version 5.20.7

2023-11-15

Updates

- Clean up device actions more often and earlier by default. By default, actions are removed after 90d, 30d for short-lived types. The clean up by default runs every 15 minutes between 18:00 and 7:00, and deletes up to two times 1000 actions [REL-2832] [REL-2895]
- Run the clean up of device actions described above also per device when ever an action is put into a terminal state [REL-2894]
- Keep only the latest pending, successful and failed action of several types per device to reduce size of action history [REL-2603]

Fixes

- Fix HTTP method for (not yet used) `POST` endpoint erroneously being marked as `GET` [REL-2843]

Version 5.20.6

2023-11-08

Pour la version 26.4.0

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

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]

Pour la version 26.4.0

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

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]

Pour la version 26.4.0

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]

Pour la version 26.4.0

Updates

- 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

Pour la 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]

Pour la version 26.4.0

- 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]

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]

Pour la version 26.4.0

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]

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]

Pour la version 26.4.0

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]

Pour la 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]

Pour la 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

Pour la version 26.4.0

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

- 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]

Pour la version 26.4.0

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]

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]

Pour la version 26.4.0

- 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]

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

Pour la version 26.4.0

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]

Pour la 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]

Pour la version 26.4.0

- 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]

Pour la 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]

Pour la 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]

Pour la version 26.4.0

Version 5.16.4

2023-03-02

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]

Pour la version 26.4.0

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]

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

Pour la version 26.4.0

- 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

- 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]

Pour la 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]

Pour la version 26.4.0

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]

Pour la 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]

Pour la version 26.4.0

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

- 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]

Pour la version 26.4.0

- 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]

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]

Pour la version 26.4.0

Version 5.13.4

2022-11-03

Fixes

- Fix DEP profile lookup for auto-enrollments in store organization using authorization and default profile device name and distributing to other organizations [MDM-25128] [REL#223539]
- Speed up home screen layout editor for Android Enterprise devices by querying installed apps by platform of specific organization only [MDM-25173]
- Avoid periodically logging failures when repeatedly trying to reach Android devices having outstanding ping actions [MDM-25177]
- Fix visibility of location tab for iOS devices which are in the new lost mode states [MDM-25178] [REL#223665]

Version 5.13.3

2022-10-26

Fixes

- Ensure a value is set for lost mode in auto-enrollments, to avoid entries not to be shown in Portal due to filtering [MDM-25105] [REL#223539]
- Fix downloading supervision certificates with tenant users belonging to a different organization [MDM-25118] [REL#223594]
- Fix display of device details when OS update information is not up-to-date [MDM-25129] [REL#223611]

Version 5.13.2

2022-10-20

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]

Pour la version 26.4.0

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]

Pour la version 26.4.0

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

- 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]

Pour la version 26.4.0

Version 5.12.2

2022-09-14

Updates

- Support compression when setting application.yml via environment variables in cloud scenarios [MDM-24705]

Fixes

- Fix display of license views when using system organization based licensing [MDM-24706]
- Fix database migration failing when encountering unexpected invalid references in database [MDM-24704]

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

Pour la version 26.4.0

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

- 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]

Pour la version 26.4.0

- 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

Pour la 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]

Pour la version 26.4.0

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]

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

Pour la version 26.4.0

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]

Pour la version 26.4.0

Fixes

- Synchronization errors no longer trigger post-sync actions, which could incorrectly delete users [MDM-22991][REL#221066]
- Fix manual LDAP sync in cluster environments not running when connected to a secondary node [MDM-23125]
- Fix applying a policy in a tenant organization, when the policy contains a Relution Shared Device configuration [MDM-23249] [REL#221342]
- Fix being stuck on login page because of missing permissions after page redirect [MDM-22783]
- Fix organization icon in the portal header not refreshing after switching the organization [MDM-23530] [REL#221485]
- Fix background transparency of information box in the DEP settings [MDM-23551]
- Fix device custom fields only being displayed when the settings were loaded before [MDM-23130] [MDM-23721] [REL#221759]
- Fix print view in Portal [MDM-23247]

Version 5.10.1

2022-05-13

New

- Use new Microsoft Store endpoints to fetch meta data of Windows public apps [MDM-23642]

Version 5.10

2022-03-31

New

- Use Apple VPP v2 API including real-time notifications for updated data [MDM-22114]
- Execute high priority actions (e.g. enable lost mode, reset passcode, locate device) before regular actions for Apple Devices [MDM-22708]
- Add support for Windows Autopilot enrollment [MDM-21897]
- Add properties to Windows Antivirus configuration to improve scheduling defender scans [MDM-22563]
- Make helpdesk link configurable via `relution.legal.helpdeskUrl` [MDM-22915]
- Make imprint link configurable via `relution.legal.imprintUrl` [MDM-22917]
- Add configurable privacy policy and EULA links which will be used instead of the previous privacy policy setting [MDM-22586] [MDM-23126]
- Support user-defined custom device properties names as column header names in the CSV import for auto-enrollments and devices [MDM-22916]
- Add full S/MIME support for iOS Mail configuration [MDM-22602]
- Add custom JSON code for Android Enterprise to enroll a device via a Zero Touch profile. [MDM-23040] [REL#22979]

Updates

- 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]

Pour la version 26.4.0

- 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]

Pour la version 26.4.0

Fixes

- 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]

Version 5.9.2

2022-03-16

Fixes

Pour la version 26.4.0

- 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

- 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]

Pour la version 26.4.0

- 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]

Pour la version 26.4.0

Fixes

- 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]

Pour la version 26.4.0

- 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]

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]

Pour la version 26.4.0

- 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

Pour la 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]

Pour la version 26.4.0

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

- 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]

Pour la version 26.4.0

- 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

- 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]

Pour la version 26.4.0

- 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]

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]

Pour la version 26.4.0

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]

Pour la 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]

Pour la version 26.4.0

Fixes

- 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

Pour la version 26.4.0

- 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]

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]

Pour la version 26.4.0

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]

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]

Pour la version 26.4.0

- 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

- 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]

Pour la version 26.4.0

- 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]

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]

Pour la version 26.4.0

- 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]

Pour la version 26.4.0

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]

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]

Pour la version 26.4.0

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]

Pour la version 26.4.0

Fixes

- 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]

Pour la 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

New

Pour la version 26.4.0

- 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]

Pour la version 26.4.0

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

- 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]

Pour la version 26.4.0

Version 5.1.2

2022-05-25

Updates

- Optimize pub/sub poll for large instances with support for parallel poll requests [MDM-21078]

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

Pour la version 26.4.0

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]

Pour la version 26.4.0

- 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

- 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]

Pour la 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]

Pour la version 26.4.0

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

- 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]

Pour la version 26.4.0

- 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]

Pour la version 26.4.0

Known Issues

Politique Exchange : aucun certificat utilisateur du sous-type Exchange

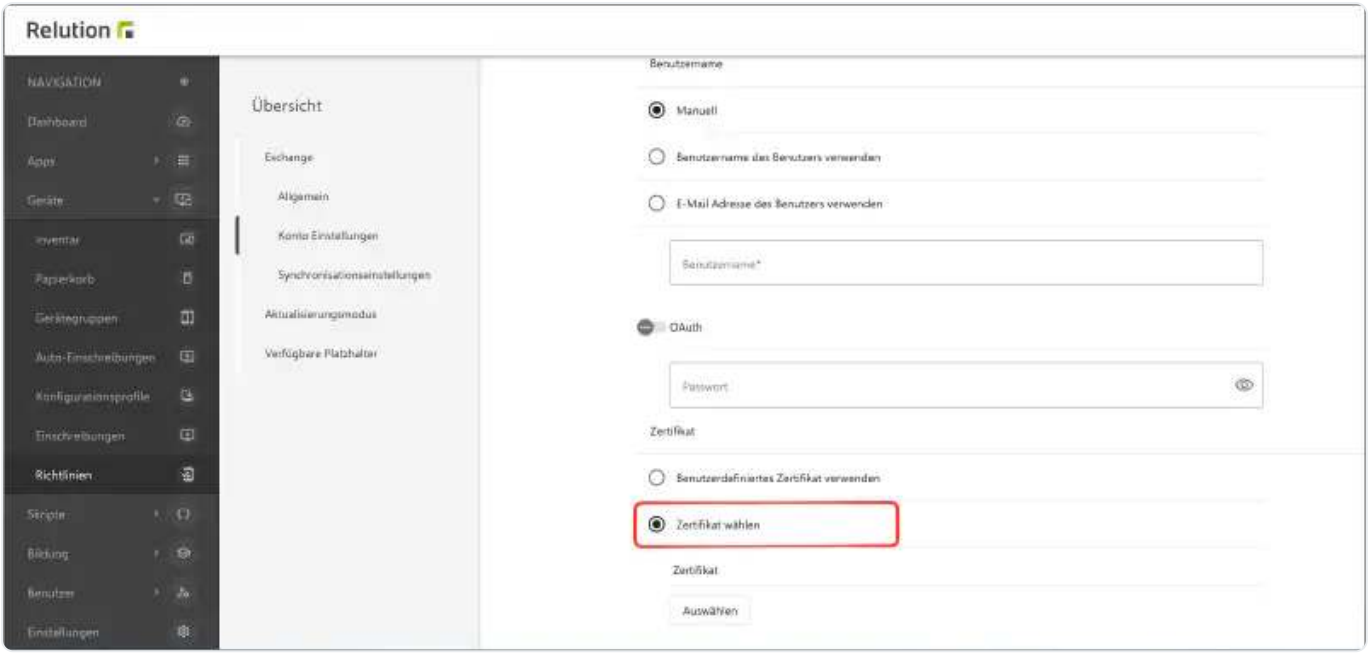
Lors de l'application d'une politique comportant une configuration Exchange, l'action Politique de changement échoue dans les actions de l'appareil. Le message suivant s'affiche :

```
Au moins une sous-action a échoué : ErrorCode: -, Message: Aucun certificat ut
```

La cause est le paramètre Utiliser un certificat utilisateur dans la section Certificat de la configuration Exchange. Avec cette option, Relution recherche un certificat utilisateur du sous-type Exchange pour l'utilisateur de l'appareil. Si aucun certificat de ce type n'existe pour l'utilisateur, le compte ne peut pas être déployé.

Solution : Dans la configuration Exchange appliquée, l'option Sélectionnez un certificat est activée dans la section Certificat. Aucun certificat ne doit être sélectionné ; la configuration peut être enregistrée directement.

Pour la version 26.4.0



Il en va de même pour les certificats S/MIME situés plus bas dans la configuration Exchange. Lorsque la signature ou le chiffrement S/MIME est activé, les sections Certificat de signature S/MIME et Certificat de cryptage S/MIME y apparaissent avec le même choix. Si l'une de ces sections est réglée sur Utiliser un certificat utilisateur, Relution recherche en plus un certificat utilisateur du sous-type Signature S/MIME ou Cryptage S/MIME, et l'action échoue avec le message correspondant si aucun n'existe. Dans ce cas, l'option Sélectionnez un certificat est également activée dans ces sections.

Plus d'informations : Configuration Exchange →

Raccourcis en tant qu'application obligatoire

Apple a modifié l'ID de bundle de l'application `Raccourcis`. L'ancienne fiche VPP avec l'ID de bundle `is.workflow.my.app` ne peut plus être installée sur les appareils équipés d'iOS 26 ou d'une version ultérieure, car iOS refuse activement l'installation avec l'erreur `AppBlacklisted`. Si cette ancienne fiche est renseignée dans la liste `Applications requises`, le déploiement est relancé en continu sans que l'installation n'aboutisse jamais.

Pour la version 26.4.0

Signes caractéristiques :

- Les appareils iOS concernés sont affichés comme `non conforme` dans l'inventaire des appareils.
- `Raccourcis` figure pourtant correctement dans `Apps installées`.
- Le déploiement de l'application est relancé à répétition, sans jamais aboutir.
- Le journal de l'appareil affiche le message `Cette app ne peut plus être installée sur cette version du système d'exploitation.` accompagné du code d'erreur `AppBlacklisted`.

Solution de contournement : L'ancienne app VPP avec l'ID de bundle `is.workflow.my.app` est retirée de la liste `Applications requises`, et l'attribution VPP correspondante est supprimée.

> L'application actuelle `Raccourcis` avec l'ID de bundle `com.apple.shortcuts` ne devrait pas être ajoutée en remplacement dans la liste `Applications requises` pour le moment, car Relution la considère encore comme une application système non installable. Si `Raccourcis` est réellement absente sur certains appareils, elle peut à la place être installée séparément via la distribution d'une application de l'App Store Apple (Gérer les apps de l'App Store →).

OIDC + Entra ID

- L’authentification OIDC avec l’identifiant Entra Microsoft a été reconfigurée conformément à notre documentation.
  La configuration est correcte, mais la connexion ne fonctionne pas immédiatement après l’installation.
  Les utilisateurs reçoivent un message d’erreur après s’être connectés avec leurs identifiants Microsoft :



Solution / Contournement

La connexion OIDC fonctionne correctement uniquement après le redémarrage du serveur Resolution.

Le démarrage du serveur échoue avec un certificat S3 auto-signé

Après une mise à jour d'une version antérieure à 26.2 directement vers Relution 26.4 ou une version plus récente, le serveur ne démarre plus si le stockage d'objets S3 connecté est accessible via TLS avec un certificat auto-signé ou interne à l'entreprise. L'erreur suivante apparaît dans le journal :

```
AccessDeniedException: software.amazon.awssdk.core.exception.SdkClientExceptio
```

Cause et solution — y compris la reconnexion nécessaire de tous les utilisateurs : Démarrage du serveur avec un certificat S3 auto-signé →

Les métriques Prometheus ne sont pas exposées

Depuis Relution 26.4, seul le point de terminaison health est exposé par défaut pour des raisons de sécurité ; le point de terminaison Prometheus (`/actuator/prometheus`) est désactivé. La surveillance Prometheus ne reçoit donc aucune métrique tant que le point de terminaison n'a pas été activé une fois dans le fichier `application.yml`.

Cause et solution : Activer les métriques Prometheus dans Relution →

Les niveaux de journalisation ne peuvent pas être modifiés via le portail système

Depuis Relution 26.4, seul le point de terminaison health est exposé par défaut pour des raisons de sécurité. Le portail système n'affiche donc que la section `Details` ; les sections `Logger`, `Environment`, `Metrics` et `Threads` n'apparaissent qu'après l'activation des points de terminaison correspondants dans le fichier `application.yml`. Indépendamment de cela, les niveaux de journalisation restent modifiables via l'API Web.

Cause et solution : Activation des points de terminaison actuator →

Pour la version 26.4.0

Sauvegardes avec iOS 26.4

- Lors de la restauration de sauvegardes provenant d'iOS 26.3 ou d'une version antérieure sur un appareil équipé d'iOS 26.4, l'état de la gestion des appareils (Device Management) est perdu.

AppleID

- Connexion à l'application Wallet (`com.apple.Passbook`) avec un identifiant Apple possible, même si la restriction *Autoriser la modification du compte* est désactivée.
  - Solution de contournement : Ajouter l'application `com.apple.Passbook` à la liste de blocage dans la configuration *Gérer les applications*. Sur les appareils concernés, il faut :
    1. autoriser temporairement la modification du compte,
    2. se déconnecter de l'identifiant Apple,
    3. puis désactiver à nouveau la modification du compte.

Pour la version 26.4.0

Nouvelles applications

- Nouvelles applications et les identifiants de bundle à bloquer
  - Preview → `com.apple.Preview`
  - Games → `com.apple.games`
  - Tipps → `com.apple.tips`

Relution Agent 5.19.0

Le problème (1) est résolu avec Relution Agent 5.19.2. La version a été approuvée par Apple !

Actuellement, il y a deux problèmes avec la version 5.19.0 de Relution Agent.

1. lors de la connexion au Relution Shared Device, une erreur peut se produire dans certains cas. Celle-ci s'affiche après la connexion. Le message d'erreur est le suivant : `Bad state : Stream has already been listened to`. Comme solution de contournement, il suffit d'appuyer sur la touche Home de l'iPad. L'utilisateur devrait être connecté et l'appareil devrait être utilisable normalement.

2. dans l’App Store, toutes les applications avec une mise à jour disponible sont affichées. Il s’agit d’une erreur d’affichage.

---

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.

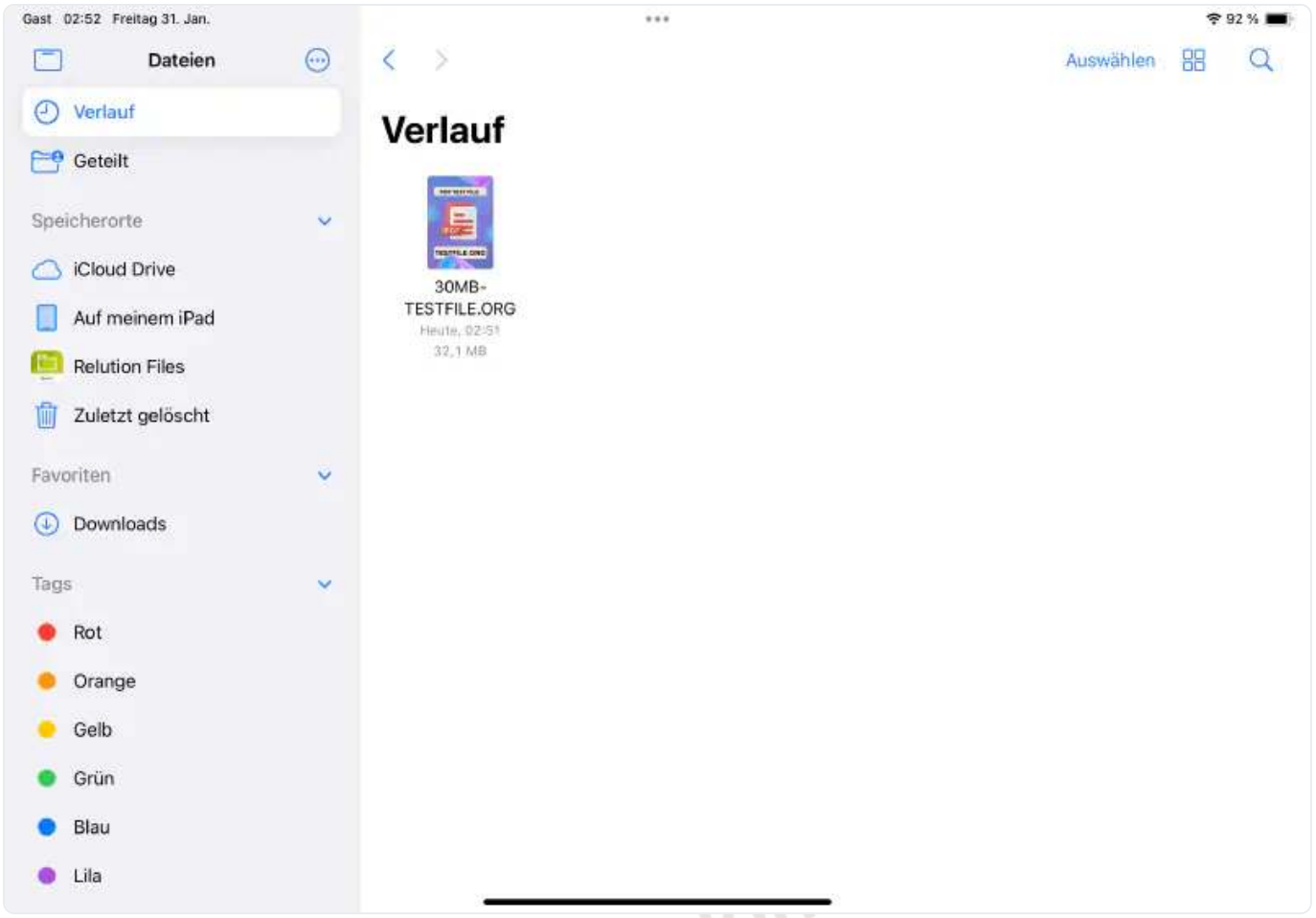
Apple Files App

Pour la version 26.4.0

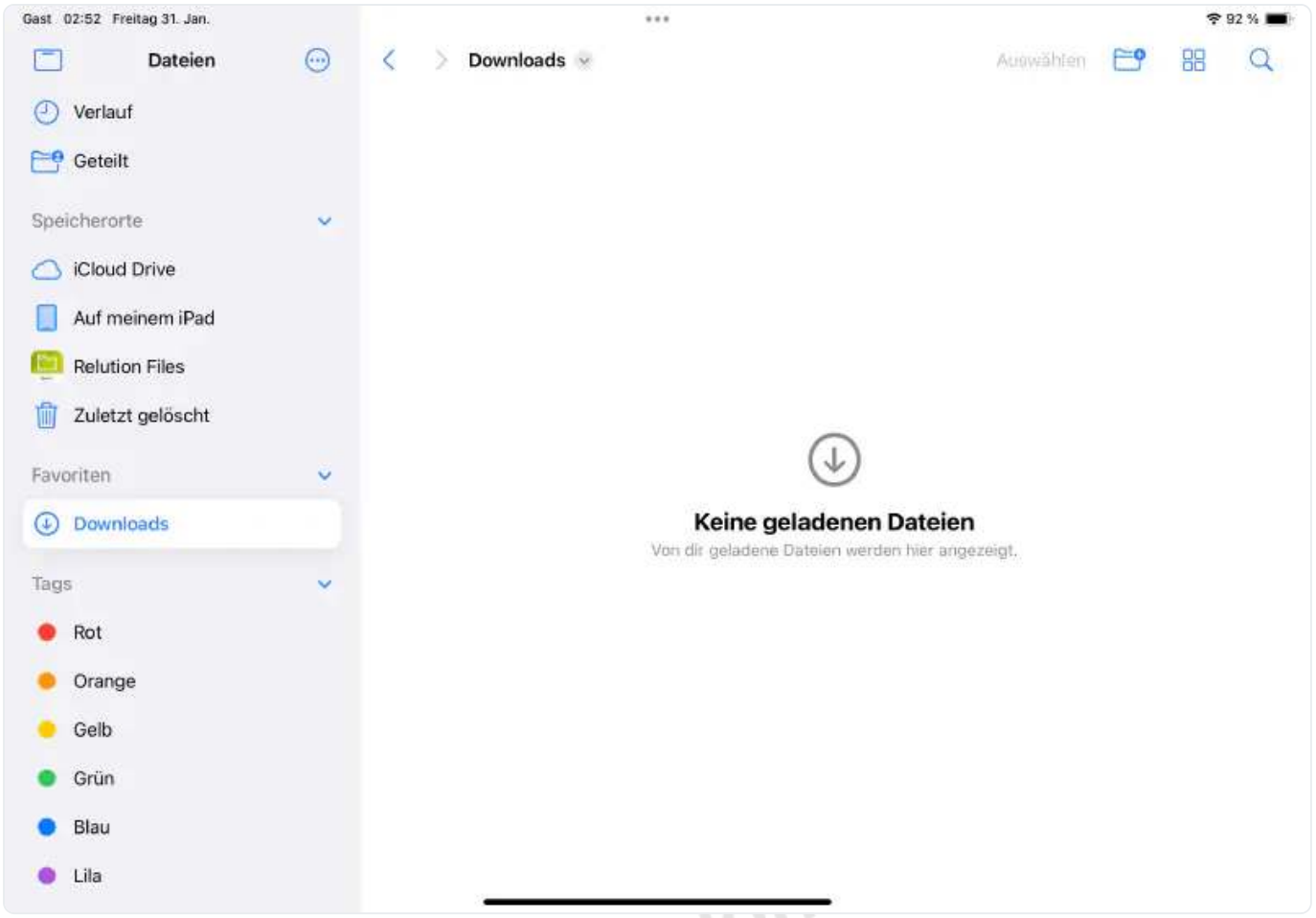
There is currently an error in the Files app on Apple shared iPads (tested with iOS 18.2 and 18.3).

> 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.



Pour la version



Pour la version

Le problème est résolu avec Relution Server 5.32. Ici, un nouveau paramètre peut être configuré dans la configuration pour les partages de fichiers. Pour cela, réglez le Type d'extension de Modern sur Classique.

Issues with SMB Access in iOS 18

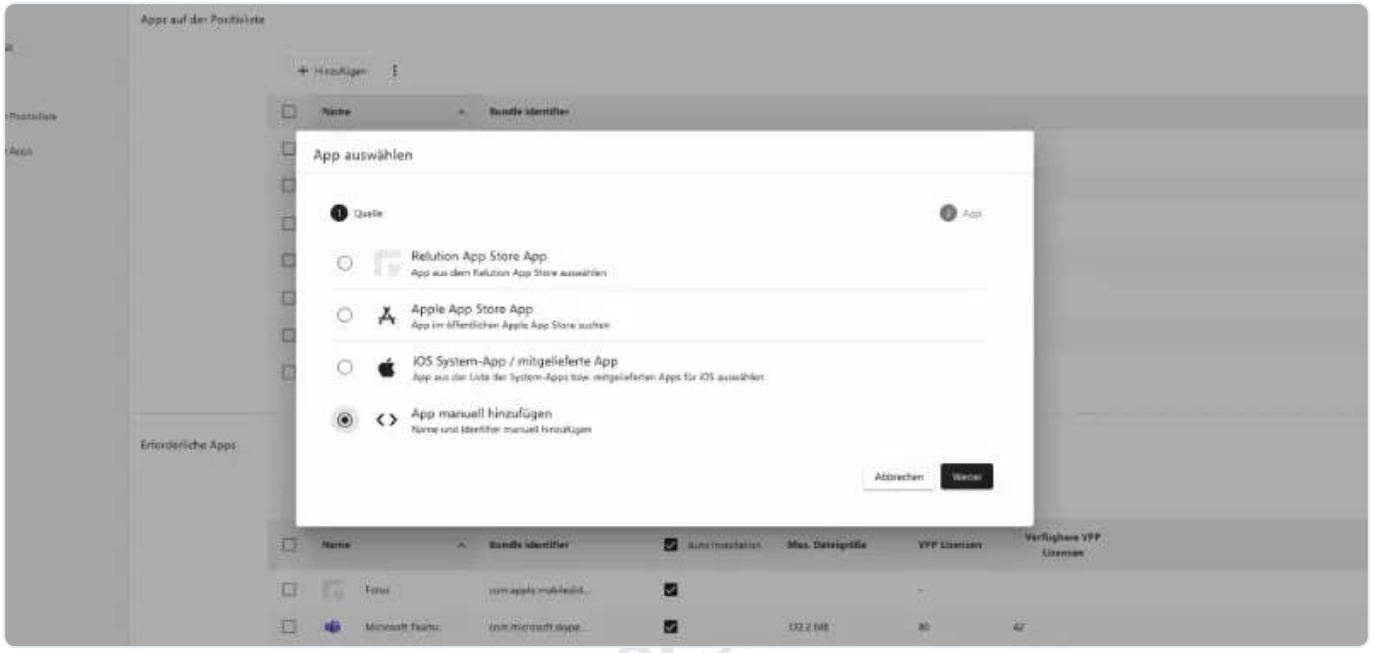
There is a known issue in iOS 18 that can cause problems when writing to SMB shares. This is a bug that occurs independently of Relution and is related to a problem within iOS 18 itself. Apple is aware of the issue, and we recommend keeping an eye on upcoming updates from Apple, as a solution may be included in a future iOS release.

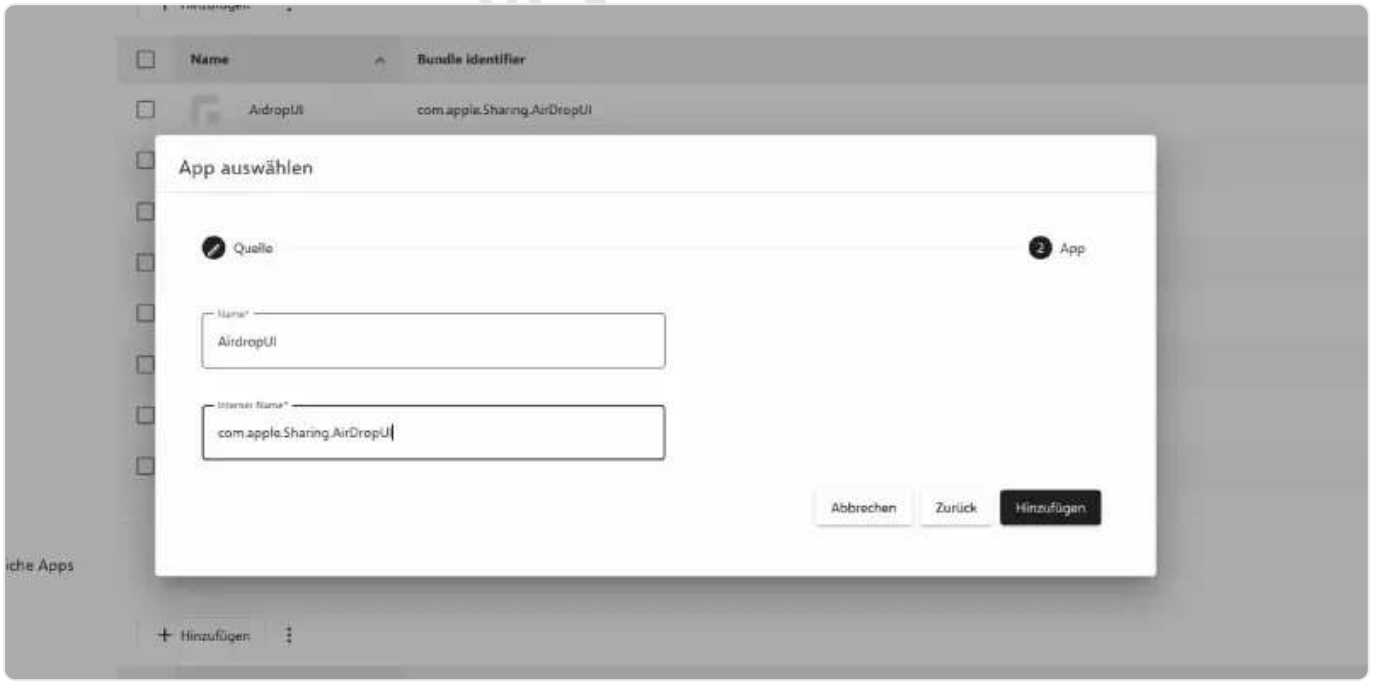
Airdrop

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
```

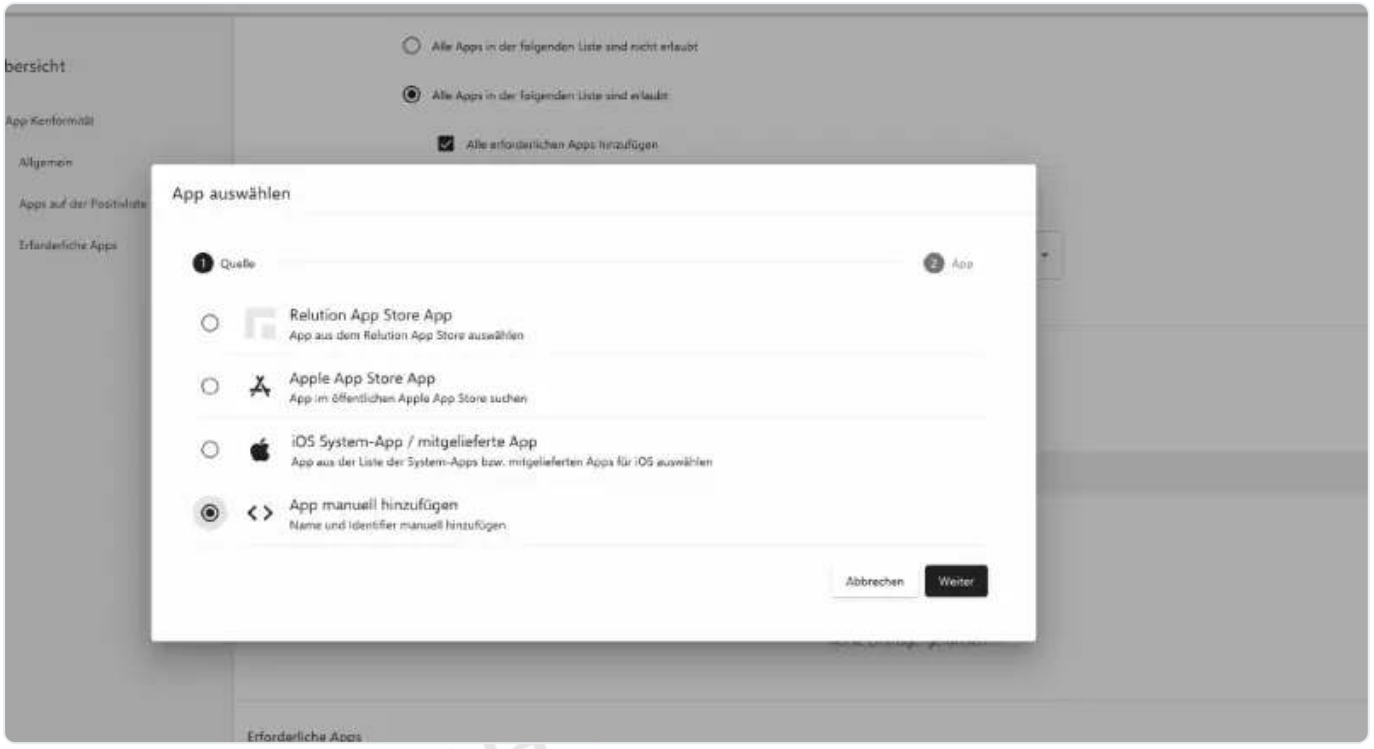
Please note that the bundle identifier is case-sensitive.

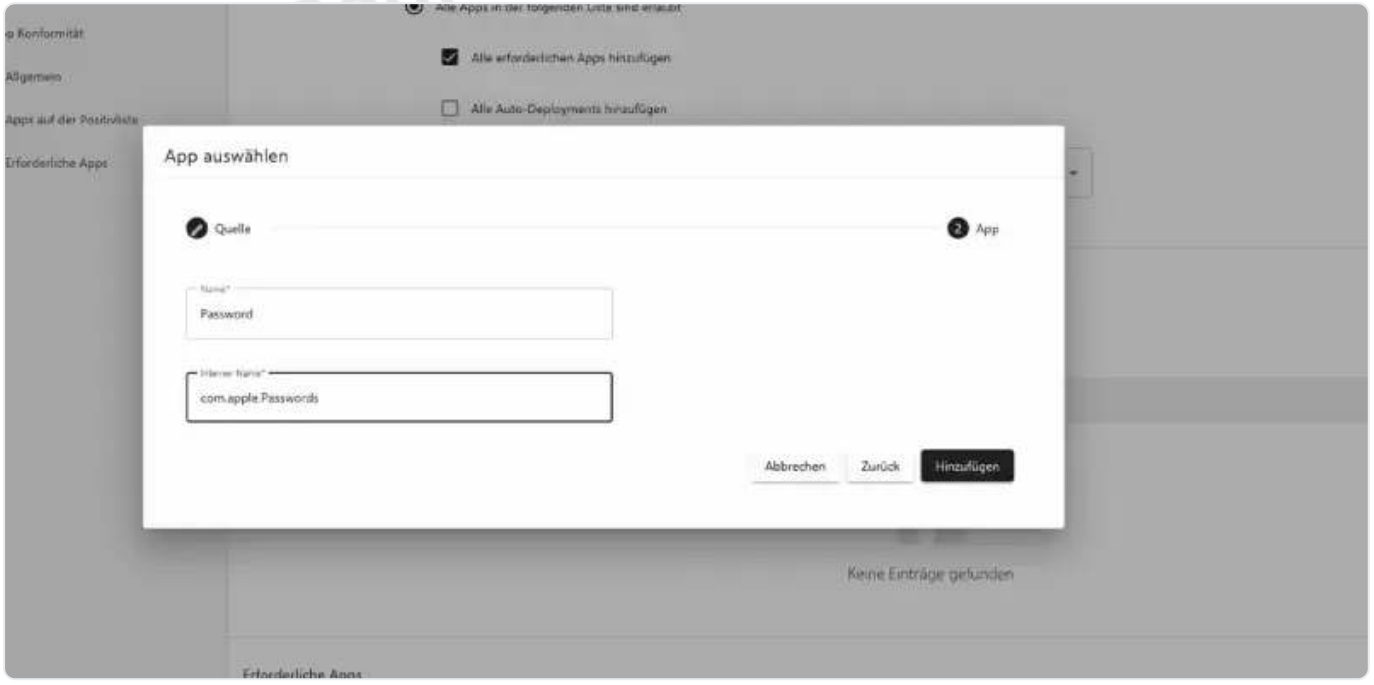




Password app

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.





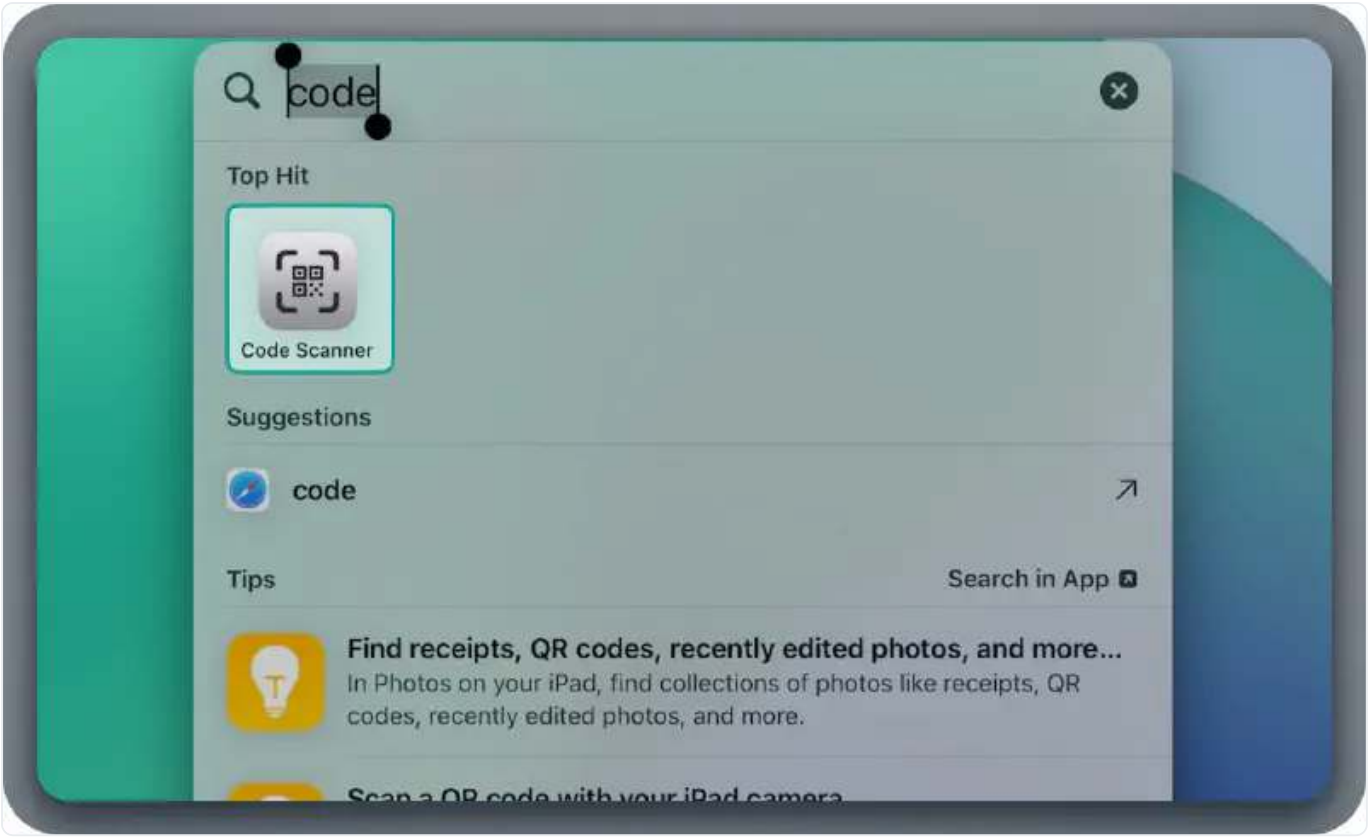
QR code scanner

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.

Pour la version 26.4.0

Avis de sécurité

Cette page présente une vue d'ensemble des vulnérabilités de sécurité identifiées dans nos produits, y compris leur identifiant REL interne et les identifiants CVE associés (si disponibles), ainsi que des informations détaillées sur leur divulgation. Nous suivons un processus de divulgation coordonnée des vulnérabilités (en anglais) → et publions les avis complets une fois que les correctifs sont disponibles et que la fenêtre de divulgation convenue est arrivée à échéance. Notre objectif est d'assurer la transparence, de soutenir des déploiements sécurisés et d'aider nos clients à protéger leurs systèmes grâce à des mises à jour régulières.

Ce processus sera mis en place à partir de 2026 ; les avis créés dans ce cadre seront publiés sur cette page.

Abonnez-vous à notre newsletter → pour être informé des vulnérabilités et d'autres informations importantes.

RVD-2026-6: Accès non authentifié dans Relution Server

la version 26.4.0

Information	Valeur
Identifiant	`RVD-2026-6`
CVE	non attribué
Composant concerné	Relution Server
Versions concernées	jusqu'à `26.5.3`
Corrigé dans	`26.5.4`
Publié le	20 octobre 2026
Statut	Mise à jour disponible

Relution Server 26.5.4 corrige une vulnérabilité pouvant permettre un accès sans authentification préalable.

Nous recommandons à tous les clients disposant d'une installation on-premises de mettre à jour vers la version `26.5.4` ou ultérieure dans les meilleurs délais.

Toutes les instances cloud exploitées par Relution ont déjà été mises à jour ; aucune action n'est requise pour les clients cloud.

De plus amples détails techniques seront publiés ici dès que la mise à jour aura été largement déployée.

RVD-2026-5: Vulnérabilité de force brute dans Relution Server

Information	Valeur
Identifiant	`RVD-2026-5`
CVE	non attribué
Composant concerné	Relution Server
Versions concernées	jusqu'à `26.5.1`
Corrigé dans	`26.5.2`
Publié le	19 octobre 2026
Statut	Mise à jour disponible

Relution Server 26.5.2 corrige une vulnérabilité pouvant permettre un accès non autorisé par essais automatisés (force brute).

Nous recommandons à tous les clients disposant d'une installation on-premises de mettre à jour vers la version `26.5.2` ou ultérieure dans les meilleurs délais.

Toutes les instances cloud exploitées par Relution ont déjà été mises à jour ; aucune action n'est requise pour les clients cloud.

De plus amples détails techniques seront publiés ici dès que la mise à jour aura été largement déployée.

RVD-2026-4: Vulnérabilité d’accès à la base de données dans Relution Server

Information	Valeur
Identifiant	`RVD-2026-4`
CVE	non attribué
Composant concerné	Relution Server
Versions concernées	jusqu’à `26.5.2`
Corrigé dans	`26.5.3`
Publié le	16 octobre 2026
Statut	Mise à jour disponible

Pour la ver

Relution Server 26.5.3 corrige une vulnérabilité pouvant permettre à des utilisateurs authentifiés d’accéder sans autorisation au contenu de la base de données.

Nous recommandons à tous les clients disposant d’une installation on-premises de mettre à jour vers la version **`26.5.3`** ou ultérieure dans les meilleurs délais.

Toutes les instances cloud exploitées par Relution ont déjà été mises à jour ; aucune action n’est requise pour les clients cloud.

De plus amples détails techniques seront publiés ici dès que la mise à jour aura été largement déployée.

RVD-2026-3: Exécution de code dans Relution Server

Information	Valeur
Identifiant	`RVD-2026-3`
CVE	non attribué
Composant concerné	Relution Server
Versions concernées	jusqu'à `26.5.2`
Corrigé dans	`26.5.3`
Publié le	16 octobre 2026
Statut	Mise à jour disponible

Pour la version 26.4

Relution Server 26.5.3 corrige une vulnérabilité pouvant permettre, dans certaines circonstances, à des utilisateurs authentifiés d'exécuter du code.

Nous recommandons à tous les clients disposant d'une installation on-premises de mettre à jour vers la version **`26.5.3`** ou ultérieure dans les meilleurs délais.

Toutes les instances cloud exploitées par Relution ont déjà été mises à jour ; aucune action n'est requise pour les clients cloud.

De plus amples détails techniques seront publiés ici dès que la mise à jour aura été largement déployée.

RVD-2026-2: Problème de permissions dans Relution Server

Information	Valeur
Identifiant	`RVD-2026-2`
CVE	non attribué
Composant concerné	Relution Server
Versions concernées	jusqu'à `26.5.2`
Corrigé dans	`26.5.3`
Publié le	16 octobre 2026
Statut	Mise à jour disponible

Pour la version

Relution Server 26.5.3 corrige une vulnérabilité pouvant permettre à des utilisateurs authentifiés un accès non autorisé.

Nous recommandons à tous les clients disposant d'une installation on-premises de mettre à jour vers la version **`26.5.3`** ou ultérieure dans les meilleurs délais.

Toutes les instances cloud exploitées par Relution ont déjà été mises à jour ; aucune action n'est requise pour les clients cloud.

De plus amples détails techniques seront publiés ici dès que la mise à jour aura été largement déployée.

RVD-2026-1: Problème de permissions dans Relution Server [REL-13078]

Information	Valeur
Identifiant	`RVD-2026-1`
CVE	non attribué
Composant concerné	Relution Server
Versions concernées	`5.32` - `26.4.1`
Corrigé dans	`26.4.2`
Publié le	13 août 2026
Statut	Mise à jour disponible

Pour la version

Relution Server 26.4.2 corrige un problème de permissions pouvant affecter les utilisateurs authentifiés.

Nous recommandons à tous les clients disposant d’une installation on-premises de mettre à jour vers la version **`26.4.2`** ou ultérieure dans les meilleurs délais.

Toutes les instances cloud exploitées par Relution ont déjà été mises à jour ; aucune action n’est requise pour les clients cloud.

De plus amples détails techniques seront publiés ici dès que la mise à jour aura été largement déployée.

Optimisation de la sécurité

Relution est un outil puissant avec lequel les utilisateurs disposent parfois d'autorisations étendues sur les appareils gérés. Le système doit donc être protégé de manière optimale contre les accès non autorisés. Le portail Relution peut être optimisé en termes de sécurité à différents endroits grâce à des fonctions intégrées. A cela s'ajoute la distribution ciblée des autorisations nécessaires.

Utiliser un mot de passe sûr

Lorsqu'un nouveau compte utilisateur est créé dans Relution, un mot de passe complexe est proposé. Celui-ci peut être accepté ou modifié. Dans tous les cas, respecter la [recommandation de complexité du BSI]. recommandation de complexité du BSI →

Ajouter un deuxième facteur d'authentification

Pour la version 26.4.0

Relution prend en charge la connexion avec un deuxième facteur. Les utilisateurs doivent le configurer eux-mêmes pour leur propre compte. Pour ce faire, cliquer sur le nom de l'utilisateur > Profil en haut à droite. Un jeton MFA pour une application d'authentification ou une vérification par email peut être stocké à cet endroit. L'utilisation de cette fonction est fortement recommandée !

Utiliser le jeton d'accès

Dans Relution, un jeton d'accès pour l'utilisation de l'API peut également être stocké dans le profil du compte utilisateur. Ce jeton offre l'avantage qu'aucune combinaison nom d'utilisateur/mot de passe ne doit être stockée en texte clair dans les scripts. En outre, une date d'expiration peut être attribuée au jeton afin de s'assurer qu'il n'est pas actif plus longtemps que nécessaire.

Configuration des règles d'accès IP & Fail2Ban

Dans la Global Organisation, il est possible de configurer à la fois les règles d'accès IP et Fail2Ban sous

`Paramètres` → `Sécurité du système`.

Cela permet par exemple de définir qu'une adresse IP sera bloquée pendant une certaine durée après un nombre défini de tentatives de connexion échouées (par ex. 10).

Les règles d'accès IP contrôlent de manière générale depuis quelles adresses IP ou quels réseaux une connexion est autorisée ou bloquée. Il est possible de définir à la fois des IP individuelles et des plages complètes.

> Avant toute configuration, il convient de vérifier quelle adresse IP est utilisée pour se connecter au serveur afin d'éviter tout blocage involontaire.

Signification des statuts

Autorisé

- La connexion est actuellement possible
- Est défini automatiquement dès qu'une tentative de connexion a lieu (même en cas d'échec)
- Sert principalement à la visibilité et à la journalisation

Autorisé de manière permanente

- L'adresse IP est explicitement autorisée
- A priorité sur les autres règles
- Reste active de manière permanente
- Recommandé pour les emplacements de confiance (par ex. bureau ou VPN)

Bloqué

- L'adresse IP est bloquée temporairement
- Peut être débloquée à tout moment

Bloqué de manière permanente

- L'adresse IP est bloquée définitivement
- Plus aucune connexion possible
- Utile pour les accès clairement indésirables

Pour la version 26.4.0

Utilisation des plages IP

Le préfixe CIDR permet de définir la taille de la plage d’adresses IP concernée par une règle.

Préfixe	Signification
`/32`	Une seule adresse IP
`/24`	Un réseau typique (par ex. réseau interne)

Règle de base :
Plus le nombre est petit, plus la plage d’adresses IP est grande.

Exemples CIDR

Pour la version 26.4.0

- `192.168.1.10/32`
  → Concerne un seul appareil
- `192.168.1.0/24`
  → Concerne tous les appareils de `192.168.1.1` à `192.168.1.254`

Exemple : bloquer tout sauf les IP autorisées

Définir les IP de confiance

- Définir les réseaux connus ou internes
- Les configurer comme Autorisé de manière permanente
- Exemples :
  - Réseau de bureau
  - Accès VPN

Créer une règle de blocage globale

- Créer une règle couvrant toutes les autres adresses IP
- Exemple : `0.0.0.0/0` (couvre toutes les IP dans le monde)
- Statut : Bloqué de manière permanente

> Avant d'activer la règle de blocage globale, s'assurer que l'adresse IP utilisée pour la connexion est correctement définie comme autorisée de manière permanente.

Optimisations de sécurité pour les inscriptions

Le lien et le code QR d'une inscription agissent comme une clé d'accès : tant que l'inscription est valable, ils permettent d'inscrire un appareil dans Relution. L'appareil reçoit ensuite les politiques et les ensembles de règles associés à l'inscription – y compris, le cas échéant, des identifiants Wi-Fi, des certificats ou des accès à des services de l'entreprise. Il convient donc de limiter au strict nécessaire le nombre d'inscriptions ouvertes.

Pour la version 26.4.0

- Limiter la durée de validité : lors de la création d'une inscription, Valable jusqu'au est fixé par défaut à sept jours. La durée ne devrait pas dépasser ce qui est réellement nécessaire pour l'inscription prévue. Si le délai ne suffit pas, les inscriptions qui n'ont pas encore été utilisées peuvent être prolongées ultérieurement via Prolonger les inscriptions – de longues durées de validité par précaution ne sont donc pas nécessaires.
- Privilégier les inscriptions à usage unique : par défaut, chaque inscription ne peut être utilisée que pour un seul appareil. Une Inscription à usages multiples permet en revanche d'inscrire un nombre illimité d'appareils jusqu'à la date d'expiration, dans la seule limite des licences disponibles. Elle ne devrait donc être utilisée que de manière ciblée pour des déploiements importants et associée à une durée de validité particulièrement courte.
- Supprimer les inscriptions devenues inutiles : les inscriptions ouvertes qui ne sont plus nécessaires – par exemple après la fin d'un déploiement ou si un appareil n'est finalement pas inscrit – devraient être supprimées sous `Appareils` → `Inscriptions`. Les appareils déjà inscrits via une inscription à usages multiples restent inscrits. Pour Android Enterprise, le jeton d'inscription correspondant est en outre supprimé chez Google, de sorte que le code QR ne fonctionne plus.
- Ne pas partager publiquement les liens et codes QR : les liens d'inscription ne sont envoyés qu'aux personnes concernées et ne sont pas publiés sur l'intranet, dans des wikis ou via de grandes listes de diffusion. Les codes QR imprimés sont détruits après le déploiement.
- Contrôler régulièrement les inscriptions : la liste sous `Appareils` → `Inscriptions` permet d'identifier, grâce au statut et à Valable jusqu'au, les inscriptions encore ouvertes. Il

est également utile de vérifier dans l’inventaire des appareils si des appareils inattendus y sont apparus.
- macOS : mot de passe de suppression du profil : pour les inscriptions macOS, l’option Utiliser le mot de passe de suppression de profil peut être activée. Le profil MDM ne peut alors être supprimé de l’appareil qu’à l’aide d’un mot de passe généré automatiquement.

Gérer les autorisations

Relution propose douze préconfigurations d’autorisation en standard. Vérifier quelles fonctions sont actives dans chaque préconfiguration d’autorisation. Pour ce faire, cliquer sur `Utilisateurs` → `Autorisations` et prêter attention aux entrées qui ont été créées par le système. Ces rôles ne peuvent pas être modifiés. Il est toutefois possible de créer de nouvelles autorisations à tout moment et d’activer les fonctions nécessaires pour les utilisateurs individuels de manière très précise. Les autorisations correspondent aux groupes d’utilisateurs créés par Relution.

Pour la version 26.4.0

Créer des organisations

Relution est multi-tenant, ce qui permet une représentation réaliste des structures scolaires ou d'entreprise. Après l'installation, la première connexion se fait au niveau de l'organisation globale. À partir de là, d'autres mandants peuvent être créés.

Cet article explique pas à pas les actions à entreprendre et les points auxquels il faut prêter une attention particulière.

Création d'une organisation

1. Se connecter avec l'administrateur créé `admin` et le mot de passe du système.
    - Lors de la première connexion d'un utilisateur, le CLUF (EULA) doit être accepté.
2. Dans l'organisation Global, naviguer dans la barre latérale vers `Organisations` → `Ajouter`.

Pour la version 26.4.0

Informations générales

- Données de l'organisation
    - Si l'organisation, l'entreprise ou l'établissement n'est pas répertorié, sélectionner l'adresse disponible la plus proche.

Organisation

- Nom
    - Sert à l'affichage général dans Relution et peut être modifié ultérieurement.
- Identifiant unique de l'organisation
    - Ne peut pas être modifié ultérieurement (important pour la base de données).
- Type d'organisation
    - Détermine si l'organisation est créée en tant qu'organisation autonome (Autonome), en tant qu'organisation Meta (Meta) ou en tant que sous-organisation d'une organisation Meta existante (Sous-organisation). Pour Sous-organisation, l'organisation Meta parente est également sélectionnée. Détails sous Organisations Meta →.
- Adresse de l'expéditeur

    - L’adresse e-mail que le serveur utilisera comme expéditeur lors de l’envoi d’e-mails (par ex. lors de la création de nouveaux enrollments ou lorsque des certificats expirent).
- Adresse de réponse
    - Adresse optionnelle qui sera insérée dans le champ Reply-To. Si un utilisateur répond à un e-mail d’inscription, cette adresse sera utilisée comme destinataire à la place de l’expéditeur original (selon le client de messagerie).

Gestion

- Gérer les membres
    - Ajouter les membres existants à l’organisation.
- Créer un administrateur
    - Créer un nouvel administrateur pour cette organisation.

Résumé

Un résumé de tous les éléments saisis ou sélectionnés est affiché.

Licences

Pour la version 26.4.0

- Sans limite, l’organisation créée peut utiliser toutes les licences de l’instance globale jusqu’à épuisement.
- La limite peut être définie, supprimée ou ajustée ultérieurement. → Menu `?` → `Informations sur les licences` (en haut à droite à côté du nom d’utilisateur).

Gérer les appareils Apple

Les systèmes d'exploitation iOS, macOS et tvOS ont été développés exclusivement pour les appareils Apple. Relution fournit un ensemble de fonctionnalités permettant de configurer et de contrôler les appareils Apple. Ici, on peut en savoir plus sur la façon de commencer à gérer les appareils Apple.

Certificats

Nouveau dans 26.3

Avant d'inscrire des appareils Apple, s'assurer qu'un certificat APNS (Apple Push Notification Service) est configuré sur le serveur.

À partir de Relution 26.3.0, les nouvelles installations doivent fournir leur propre certificat APNS avant que les appareils puissent être enrôlés. L'assistant en libre-service dans `Paramètres` → `Certificats d'organisation` accompagne toute la configuration. Les instances déjà en place avant cette version continuent de fonctionner pour l'instant avec un certificat fourni par Relution.

Pour la version 26.4.0

Configurer les certificats APNS Push →

Enrôlement

Pour pouvoir gérer un appareil Apple, celui-ci doit être enrôlé dans Relution. Pour ce faire, un profil MDM est installé sur l'appareil. Trois types d'inscription sont disponibles pour les appareils Apple.

Inscriptions iOS →
inscriptions macOS →
inscriptions tvOS →

Mode supervisé

Le mode supervisé permet de distinguer les appareils Apple appartenant à l'employeur des appareils personnels. Nous recommandons de placer les appareils en mode supervisé pour une

gestion et une utilisation sans restriction de toutes les fonctions MDM. Les restrictions permettent de désactiver de nombreuses fonctions qui ne sont pas nécessaires pour une utilisation dans un environnement scolaire ou professionnel. Pour en savoir plus sur la mise en mode supervisé des appareils Apple, cliquer sur le lien ci-dessous.

Les appareils DEP sont toujours supervisés.

Ajouter des appareils à DEP à l'aide d'Apple Configurator →

Relution Agent

Relution Agent est toujours installé automatiquement sur les appareils Apple lors de l'inscription. Il n'est pas nécessaire pour la gestion des appareils, mais il offre une série de fonctions supplémentaires utiles aux utilisateurs.

Il est recommandé de disposer d'un nombre suffisant de licences VPP basées sur les appareils pour l'application, auquel cas l'installation peut s'effectuer sans aucune interaction de l'utilisateur. Dans le cas contraire, les utilisateurs doivent se connecter à l'App Store avec leur compte Apple ; aucune licence VPP n'est donc nécessaire pour l'installation de l'application.

Séparer les données professionnelles des données personnelles

Pour la version 26.4.0

Les applications qui sont déployées sur les appareils Apple par l'intermédiaire de Relution sont appelées des applications gérées. On peut garder le contrôle sur ces apps et les supprimer, ainsi que les données qui leur sont associées, si nécessaire. Pour les appareils iOS et macOS, on peut configurer les apps gérées par le biais de la configuration de la politique des apps gérées.

`Comptes gérés` Pour les appareils iOS et macOS, Relution permet de configurer des comptes de messagerie et d'autres comptes et de les gérer indépendamment des comptes personnels. Avec Relution, les comptes suivants peuvent être configurés :

- Courriel
- Exchange
- CardDAV
- CalDAV
- Calendriers abonnés
- Comptes Google (appareils iOS uniquement).

La séparation des données a lieu dans le système d'exploitation d'Apple.

Gérer les applications

Les applications que l'on souhaite utiliser sur les appareils Apple doivent être sélectionnées et celles qui ne sont pas pertinentes doivent être bloquées ou supprimées. Un grand nombre d'appareils Apple peuvent être gérés, distribués et supprimés efficacement sur un grand nombre d'appareils Apple en même temps.

Gestion des applications →

Licences d'application

Chaque application installée sur les appareils Apple via l'App Store public doit faire l'objet d'une licence. Peu importe que l'application soit gratuite ou non. La licence peut être obtenue soit par l'intermédiaire de l'utilisateur actuellement connecté via l'Apple ID, soit, si l'on travaille sans Apple ID, via le Programme d'achat en volume d'Apple (VPP). Pour le VPP, l'accès à un Apple School/Business Manager est nécessaire. Pour les applications natives, cela n'est pas nécessaire.

Pour la version 26.4.0

Il est possible d'installer les applications sur les appareils Apple sans que les utilisateurs ne déclenchent manuellement l'installation, à condition que les appareils Apple soient surveillés, c'est-à-dire en mode supervisé.

Installation d'applications sans intervention de l'utilisateur →

Les applications VPP (Volume Purchase Program) peuvent être installées sur des appareils Apple supervisés sans intervention de l'utilisateur. En savoir plus sur le VPP :

Configuration du VPP dans Relution →
Déployer des applications VPP →

Liste de blocage ou positive pour iOS et tvOS.

La fonctionnalité de liste bloquée ou positive de Relution permet aux administrateurs de bloquer certaines apps sur les iPhones, les iPads et les Apple TV et d'autoriser l'installation d'apps importantes. Cette fonction empêche l'installation d'applications indésirables et masque aux utilisateurs les applications installées qui se trouvent déjà sur les appareils, si nécessaire. Cliquer sur le lien ci-dessous pour en savoir plus sur le blocage ou l'autorisation des applications.

Conformité des applications pour iOS →
Conformité des applications pour tvOS →

Mode d’application unique pour iOS

Le mode d’application unique peut être activé sur les iPhones et les iPads, limitant les appareils à une seule application et bloquant toutes les autres. Il convient de noter que les appareils doivent être surveillés (supervisés) pour activer le mode “application unique”.

Mode application unique pour iOS →

Lien web

Le webclip ressemble à une icône d’application qui renvoie à un site web lorsqu’on clique dessus. Il suffit de spécifier un libellé et une URL.

Ajouter des liens web via la politique →
Ajouter des liens web et les placer via la disposition de l’écran d’accueil pour iOS →

Protéger le profil MDM contre la suppression

Empêcher la suppression du profil MDM des paramètres de l’appareil en enregistrant les appareils via le programme d’enregistrement des appareils Apple (DEP).

Profil pour l’ADE →
Inscription automatique →

Configuration du réseau et sécurité

Assurer une sécurité maximale du réseau en mettant en place des configurations appropriées. Avec Relution, les paramètres WiFi peuvent être configurés pour tous les systèmes d’exploitation Apple. En outre, les paramètres VPN (réseau privé virtuel) et VPN par application peuvent être configurés pour les appareils iOS et macOS. Les paramètres cellulaires (réseau de points d’accès) peuvent être configurés pour les appareils iOS.

Pour la version 26.4.0

Restrictions

La configuration des restrictions limite les fonctionnalités des appareils Apple. Il est important de noter le type d'inscription, car de nombreuses restrictions ne prennent effet que sur les appareils supervisés (supervisés).

Aller aux restrictions →

Mises à jour du système

Il est possible de mettre à jour les appareils Apple avec la dernière version du système d'exploitation si les appareils sont supervisés.

Les administrateurs peuvent également différer les mises à jour pour les appareils supervisés jusqu'à 90 jours. Pendant cette période, les utilisateurs ne seront pas invités à mettre à jour les appareils avec la dernière version du système d'exploitation. Cela permet aux organisations de rechercher des erreurs/problèmes ou de vérifier la compatibilité des applications déployées avec les dernières versions du système d'exploitation.

Restrictions →

Pour la version 26.4.0

Filtrage du contenu

La fonction de filtrage du contenu web peut être utilisée pour empêcher l'accès à des pages web spécifiques dans l'organisation.

Filtre de contenu →

Disposition de l'écran d'accueil pour iOS

Les applications peuvent être disposées sur l'écran d'accueil de l'iPhone ou de l'iPad ainsi que dans le Dock, et être placées dans des dossiers qui peuvent être créés manuellement ou automatiquement.

Disposition de l'écran d'accueil pour iOS →

Gérer Android Enterprise

Android Enterprise est une initiative de Google visant à améliorer la gestion et la sécurité des appareils Android dans les entreprises. Il s'agit d'un ensemble d'outils, d'API et de services qui permettent aux entreprises de gérer plus efficacement les appareils Android et de garantir la sécurité des données d'entreprise sur ces appareils.

Prérequis

Avant de pouvoir inscrire des appareils Android via Android Enterprise, l'organisation Relution doit d'abord être liée à une organisation Google. La liaison s'effectue sous `Paramètres` → `Spécifique à la plate-forme de l'appareil` → `Android pour les entreprises`.

Lier l'organisation →

Pour la version 26.4.0

Inscription

Plusieurs options d'inscription sont disponibles pour Android Enterprise. Les appareils peuvent être inscrits manuellement, via un code QR, ou automatiquement via Android Zero Touch ou, pour Samsung, via Knox Mobile Enrollment (KME).

KME → et Zero Touch →
Types d'inscription →
Appareil géré par l'employeur →
Profil de travail →
Appareil entièrement géré avec profil personnel →

Relution Agent et Relution Companion

Relution Agent et Relution Companion sont toujours automatiquement installés sur les appareils Android Enterprise lors de l'inscription. Ces deux logiciels ne sont pas obligatoires pour la gestion des appareils, mais ils offrent une variété de fonctions supplémentaires utiles pour les utilisateurs. Avec Relution Companion pour Android Enterprise, il est possible d'installer des certificats sur les appareils et de les localiser.

Séparer les données professionnelles et personnelles

Android Enterprise offre d'excellentes options pour séparer les données professionnelles et privées. Ici, l'utilisateur peut travailler avec un "profil professionnel", qui peut être installé sur des appareils privés. Les utilisateurs peuvent alors se connecter à l'aide d'un compte Google privé et utiliser l'appareil en privé sans pratiquement aucune restriction, sans que le contenu privé et le contenu professionnel ne soient mélangés.

Gérer les applications

Android Enterprise ne permet pas l'installation d'applications natives sur les appareils. Toutes les applications doivent provenir du Google Play Store géré. Les APK personnalisés peuvent y être téléchargés et mis à disposition au sein de sa propre organisation, à condition que le nom du paquet de l'application soit propre à Google.

Gérer les applications →

> Il n'y a actuellement aucun moyen de distribuer des applications payantes avec Android Enterprise.

La configuration peut également être stockée via la gestion des applications. Elles permettent de préconfigurer des applications individuelles pour déployer des profils de messagerie ou d'autres paramètres, par exemple. Les configurations possibles ont été intégrées par le fabricant de l'application. Nous ne pouvons pas fournir d'assistance en cas de dysfonctionnement.

Pour la version 26.4.0

Disposition de l'écran d'accueil et mode kiosque

Avec la politique de disposition de l'écran d'accueil, Relution offre l'activation du mode kiosque avec un lanceur spécialement développé par Relution. Cela permet l'installation d'un fond d'écran ainsi que la disposition des applications sur l'écran d'accueil ou dans des dossiers.

Mode kiosque →

Restrictions

Sur les appareils Android Enterprise, de nombreuses restrictions peuvent être activées avec Relution.

Il est possible de rendre les appareils définitivement inutilisables avec des restrictions. Par exemple, une interdiction de réinitialisation d'usine ne peut pas être outrepassée.

Restrictions →

Permissions d’exécution

Les autorisations d’exécution peuvent être utilisées pour permettre aux utilisateurs de répondre aux questions d’autorisation. Des permissions standard mais définies par l’utilisateur peuvent être configurées ici.

Gestion des autorisations d’exécution →

Pour la version 26.4.0

Manage Windows devices

Relution permet de gérer les appareils équipés de Windows 10/11. Selon la variante, différentes fonctions sont disponibles. La gamme la plus large de fonctions est disponible avec les licences Pro, Education ou Enterprise. Contrairement aux stratégies de domaine, Relution peut effectuer des actions et appliquer des stratégies sur les périphériques Windows même s'ils ne se trouvent pas dans le réseau local. Dans ce cas, une connexion Internet suffit.

Inscription

Les périphériques Windows peuvent être enrôlés de trois manières différentes.

Inscription manuelle →
Inscription en bloc →
Inscription pilote automatique →

Auto Pilot nécessite une licence P2 Premium dans Microsoft Azure.

> Pour l'inscription manuelle et l'inscription en masse, l'utilisateur doit disposer de privilèges administratifs.

Pour la version 26.4.0

Relution Companion

Relution Companion est toujours installé automatiquement sur les appareils Windows lors de l'inscription. Cependant, cela ne fonctionne pas sur cette variante en raison des fonctionnalités limitées de Windows Home. Relution Companion permet d'exécuter des scripts Powershell et d'installer des fichiers MSI et EXE.

Windows Companion →
Limitations de Windows Home →

Gérer les applications

Relution permet d'installer des applications du Windows Store et des applications natives du Relution App Store sur les appareils Windows. Les applications natives doivent être téléchargées

vers Relution et configurées, en fonction du format. Les fichiers MSIX doivent être créés par l'utilisateur et signés par un certificat pour permettre l'installation. Les fichiers EXE et MSI nécessitent des paramètres d'installation et de désinstallation. Ceux-ci peuvent être trouvés sur le site web du fournisseur ou sur des blogs techniques.

Créer des fichiers MSIX→
Utiliser les fichiers EXE et MSI dans Relution →
SilentinstallHQ →

La détermination des paramètres de configuration corrects est souvent une procédure qui prend du temps. L'assistance Relution ne peut fournir qu'une aide très limitée dans ce domaine.

Certificats

Les certificats peuvent être chargés directement sur l'appareil Windows via la configuration de la politique correspondante. Il est également possible de sélectionner le magasin de certificats approprié.

Certificats →

Pour la version 26.4.0

Restrictions

Sur les appareils Windows, de nombreuses restrictions peuvent être activées avec Relution. Ici, il est possible de définir si le profil MDM peut être supprimé par l'utilisateur ou si l'ordinateur peut être réinitialisé.

Restrictions →
Protéger le profil MDM →

Autres configurations

D'autres configurations sont disponibles, par exemple les profils WLAN et VPN, le mode kiosque et la configuration pour le PC partagé Windows.

Gérer les tableaux blancs

L'utilisation des tableaux blancs basés sur Android gagne en popularité dans les écoles, les entreprises et d'autres organisations. Pour gérer ces appareils de manière efficace, Relution offre une solution complète spécialement conçue pour la gestion centralisée des tableaux blancs Android de différents fabricants.

Fonctionnalités selon le fabricant

Les fonctionnalités de gestion des tableaux blancs dépendent des points de terminaison fournis par chaque fabricant. Ces points de terminaison déterminent les options de contrôle et de configuration disponibles via Relution.

Exemples :

- Paramètres spécifiques
- Mises à jour du firmware
- Politiques de sécurité

Les fonctionnalités disponibles dépendent des options prises en charge par chaque fabricant.

Pour la version 26.4.0

Intégration facile via Android Classic

Les tableaux blancs peuvent être enregistrés manuellement sur la plateforme Relution. Cela se fait à l'aide du Relution Companion, qui guide les appareils étape par étape.

Une fois enregistrés avec succès, toutes les fonctionnalités de Relution sont disponibles. Les configurations et politiques peuvent être configurées et appliquées aux appareils de manière flexible via la plateforme.

Large prise en charge de nombreux fabricants

De nombreux fabricants sont déjà pris en charge par Relution. Une liste complète des fabricants actuellement compatibles est disponible ici→.

La liste est mise à jour en continu à mesure que de nouveaux fabricants sont intégrés.

Fonctions avancées via Android Enterprise

En plus des tableaux blancs Android Classic, Relution propose des options avancées via Android Enterprise.

Cette plateforme offre des fonctionnalités supplémentaires et standardisées pour la gestion complète des appareils. Relution étend les capacités d'Android Enterprise spécifiquement pour les tableaux blancs interactifs, en combinant les fonctionnalités standard avec des fonctions spécifiques au fabricant.

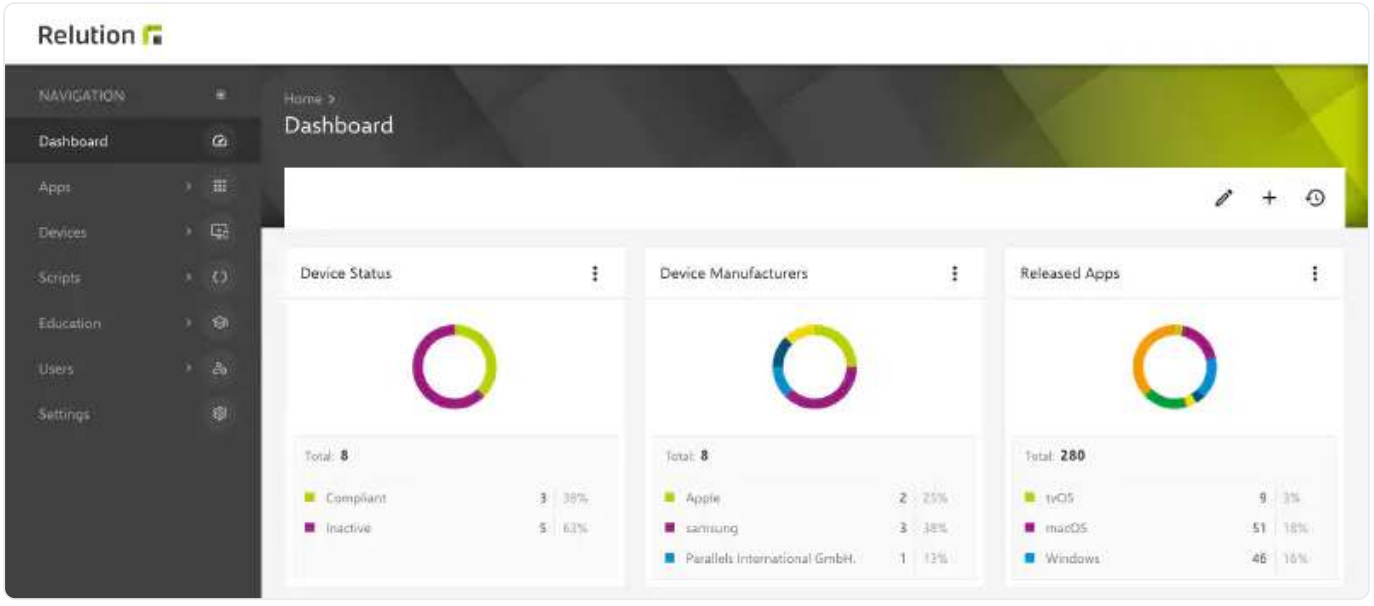
Un aperçu complet des extensions Android Enterprise disponibles est disponible ici→.

Pour la version 26.4.0

Tableau de bord

Le tableau de bord est la page d'accueil du portail Relution et résume l'état actuel d'une organisation : les appareils, les apps, les politiques, les inscriptions, les certificats et l'état du système y sont présentés sous forme de tuiles. La page est accessible via Tableau de bord dans la navigation latérale.

Les différentes tuiles sont appelées widgets. Chaque widget présente une évaluation sous forme de graphique, de tableau ou d'aperçu d'état. Le contenu du tableau de bord n'est pas figé : les widgets peuvent être ajoutés, adaptés, déplacés et supprimés.



Un tableau de bord commun par organisation

Un tableau de bord appartient à l'organisation et non à un compte utilisateur individuel. Les modifications de la disposition ainsi que les widgets ajoutés ou supprimés sont donc visibles par tous les utilisateurs de cette organisation. Un tableau de bord personnel, visible par un seul compte, n'est pas prévu.

Lors d'un changement de mandant, le tableau de bord de l'organisation active est chargé. Les valeurs affichées se rapportent toujours à l'organisation dans laquelle la session est actuellement ouverte.

> Le tableau de bord s'appliquant à toute l'organisation, la suppression d'un widget et le rétablissement du tableau de bord par défaut concernent également tous les utilisateurs de

l'organisation.

Tableau de bord par défaut

Sans personnalisation, un tableau de bord par défaut préconfiguré est fourni. Les widgets qu'il contient dépendent du type d'organisation.

Chaque organisation contient État de l'appareil, Fabricants d'appareils, Modèles d'appareils, Systèmes d'exploitation, Appareils, Propriété de l'appareil, Appareils en mode itinérant par pays, Politiques, Apps publiées, Certificats, Certificats système et Commentaires sur le plugin Knox Service.

Selon l'organisation, d'autres widgets s'y ajoutent :

- Inscriptions ouvertes — dans toutes les organisations, à l'exception de l'organisation globale.
- Organisations — dans les organisations comportant des sous-organisations ainsi que dans l'organisation globale.
- État de santé — uniquement dans l'organisation globale.

Tant que le tableau de bord par défaut n'est pas modifié, l'action de rétablissement est désactivée ; un texte d'aide indique que le tableau de bord par défaut est déjà actif. Dès que la disposition a été enregistrée ou qu'un widget a été modifié, le résultat devient le tableau de bord propre à l'organisation.

Pour la version 26.4.0

Adapter la disposition

L'icône Réorganiser les widgets (crayon) active le mode d'édition. Dans ce mode, les widgets peuvent être déplacés et redimensionnés à la souris ; la grille réorganise automatiquement les autres tuiles.

Les modifications sont appliquées via Sauvegarder les modifications du tableau de bord et annulées via Refuser les modifications du tableau de bord. Les deux actions sont confirmées par une boîte de dialogue, car le résultat s'applique à tous les utilisateurs de l'organisation. En l'absence de modification, une indication sur l'icône d'enregistrement signale qu'il n'y a aucune modification à enregistrer.

Ajouter des widgets

Ajouter un nouveau widget ouvre la boîte de dialogue Créer un widget. Elle se divise en deux zones : Sélectionner un type de graphique pour les évaluations personnalisées et Widgets prédéfinis pour les tuiles fixes.

Widgets personnalisés à partir de métriques

Le point de départ est la forme de présentation. La zone Sélectionner un type de graphique propose Graphique en barres, Graphique en barres empilées, Graphique en secteurs et Graphique en tableau.

Après la sélection, le formulaire du widget s'ouvre avec la section Configuration des widgets. Tous les champs qui y sont affichés sont obligatoires :

- Nom — le libellé de la tuile.
- Entité — la source de données : Dispositifs, Applications, Groupes d'appareils, Inscriptions ou Politiques. Seules les entités pour lesquelles le compte utilisateur actuel dispose d'une permission de lecture sont proposées ; les autres n'apparaissent pas dans la liste.
- Champ — la caractéristique servant au regroupement, par exemple le système d'exploitation ou le fabricant. Ce champ n'existe pas pour les graphiques en tableau.
- Afficher les entités par — uniquement pour le graphique en barres empilées : la seconde caractéristique dont découlent les séries. Elle doit être différente de Champ.
- Colonnes — uniquement pour les graphiques en tableau : la sélection des colonnes affichées.

La section Filtre métrique permet de restreindre davantage la base de données, par exemple à une plateforme ou à un état d'appareil.

Le bouton Prévisualisation affiche le résultat de la configuration à côté des champs avant l'enregistrement ; le nom n'a pas encore besoin d'être renseigné. Si la combinaison choisie ne renvoie aucune valeur, une indication au-dessus des champs signale qu'aucune donnée appropriée n'a été trouvée.

Widgets prédéfinis

La zone Widgets prédéfinis propose des évaluations qui ne peuvent pas être réalisées via la configuration des métriques :

- État de santé — disponibilité des composants du système Relution, affichée sous la forme Up ou Down.

Pour la version 26.4.0

- Organisations — aperçu des organisations accessibles, à partir duquel il est possible de changer de mandant.
- Commentaires sur le plugin Knox Service — retours du Knox Service Plugin.
- Certificats système — date d'expiration du certificat push APNs de l'organisation pour la gestion des appareils Apple et du certificat push intégré du Relution Agent (voir Certificats de poussée APNS →).

Seuls les widgets prédéfinis pour lesquels les permissions de lecture requises sont disponibles sont proposés (voir Permissions). Leur évaluation est fixe et ne peut pas être adaptée via le formulaire du widget. Chaque type ne peut figurer qu'une seule fois sur le tableau de bord ; une tuile déjà utilisée est désactivée dans la boîte de dialogue et signalée par Déjà ajouté.

Modifier, actualiser et supprimer des widgets

Chaque tuile dispose du menu Options des widgets. Il comprend Supprimer, Éditer et Rafraîchir : Rafraîchir recharge les données du widget, Éditer ouvre la configuration dans le formulaire du widget, Supprimer retire la tuile du tableau de bord. Pour les widgets prédéfinis et le widget Certificats, Éditer n'est pas proposé, car leur évaluation n'est pas configurable. Supprimer et Éditer ne s'affichent qu'avec la permission de mettre à jour les tableaux de bord ; sur le tableau de bord par défaut, la permission de créer un tableau de bord est également requise. Le menu n'est pas disponible en mode d'édition, ni pour les widgets dont les données ne sont couvertes par aucune permission de lecture.

Pour la version 26.4.0

La suppression est confirmée par une boîte de dialogue. Le widget et sa configuration sont alors supprimés définitivement et pour tous les utilisateurs de l'organisation ; il n'est pas possible de restaurer un widget individuel. Le widget Certificats n'est pas proposé dans la boîte de dialogue Créer un widget ; une fois supprimé, il ne peut être récupéré qu'en rétablissant le tableau de bord par défaut.

Rétablir le tableau de bord par défaut

Rétablir le tableau de bord par défaut restaure la configuration initiale. Tous les widgets personnalisés sont supprimés définitivement. Cette action ne peut pas non plus être annulée et concerne tous les utilisateurs de l'organisation.

Naviguer des widgets vers les listes

Les widgets sont reliés aux aperçus correspondants. Un clic sur un segment de graphique ouvre la liste correspondante — par exemple l'Aperçu de l'inventaire → — et y applique la sélection cliquée comme filtre ou comme terme de recherche. Pour un graphique en barres empilées, les deux caractéristiques du segment cliqué sont reprises. Dans les widgets de type tableau, un clic sur une ligne ouvre la page de détail de l'objet concerné, à condition qu'une vue détaillée existe pour ce type de données. Dans le widget Certificats, un clic sur une ligne ouvre la liste des certificats avec le nom du certificat comme terme de recherche.

En mode d'édition, cette navigation est désactivée afin que le déplacement d'une tuile ne déclenche pas involontairement un changement de page.

Si un widget ne renvoie aucune donnée, la tuile propose à côté de l'indication un bouton adapté, par exemple Créer une inscription, Créer un groupe de dispositifs, Créer une politique, App Store ou, dans le widget Certificats, Ajouter un certificat. Le bouton ne s'affiche qu'avec la permission requise pour l'action concernée.

Permissions

Pour la version 26.4.0

L'accès au tableau de bord et sa personnalisation sont régis par les permissions de la section Tableau de bord :

- L'affichage du tableau de bord nécessite la permission Lire.
- La modification de la disposition, l'enregistrement des modifications, l'ajout de widgets ainsi que la modification et la suppression de widgets individuels nécessitent la permission Actualisation.
- Tant que le tableau de bord par défaut est actif, la première personnalisation crée le tableau de bord propre à l'organisation. La permission Créer est alors également requise.
- Le rétablissement du tableau de bord par défaut nécessite la permission Supprimer.

S'il manque l'une de ces permissions, l'icône correspondante dans l'en-tête du tableau de bord est désactivée ; une indication sur l'icône nomme la permission manquante. Sans aucune des permissions Créer, Actualisation et Supprimer, l'en-tête n'est pas affiché du tout. L'attribution des permissions est décrite dans l'article Permissions →.

Indépendamment de cela, les widgets n'affichent que les données couvertes par une permission de lecture. Si ce n'est pas le cas, une indication s'affiche à la place de l'évaluation et recommande de demander les permissions nécessaires à l'administration ; pour les widgets personnalisés, elle nomme l'entité concernée.

Chaque widget prédéfini nécessite sa propre permission de lecture. Elle détermine si le widget est proposé dans la boîte de dialogue Créer un widget et s'il affiche des données sur le tableau de bord :

Widget	Permission requise
État de santé	Lire dans la section Santé du système (organisation globale uniquement)
Organisations	Lire dans la section Organisations (organisation globale) ou Sous-organisations (méta-organisation)
Commentaires sur le plugin Knox Service	Lire dans la section Politiques
Certificats système	Lire dans la section Certificats d'organisation

Pour la version 26.4.0

Limites

Les limites suivantes s'appliquent lors de la conception d'un tableau de bord personnalisé :

- Un tableau de bord par organisation. Des tableaux de bord spécifiques à un utilisateur au sein d'une même organisation ne sont pas possibles.
- Nombre limité de widgets. Par défaut, 30 widgets sont autorisés par tableau de bord. Lorsque la limite est atteinte, une indication sur l'icône d'ajout mentionne le nombre actuel et le nombre maximal.
- Nombre limité de filtres par widget. Par défaut, 20 filtres sont autorisés par widget. Si la configuration des filtres dépasse cette valeur, le widget ne peut pas être enregistré tant que des filtres n'ont pas été supprimés.
- Les widgets prédéfinis ne sont pas modifiables et ne peuvent être ajoutés qu'une seule fois chacun.
- Commentaires sur le plugin Knox Service nécessite une connexion Android Enterprise configurée ; à défaut, le widget reste sans données.
- Données rattachées à l'organisation. Ce sont les données de l'organisation active qui sont évaluées.

- Les suppressions sont définitives. Ni un widget supprimé ni un tableau de bord remplacé par un rétablissement ne peuvent être récupérés.

Les deux limites chiffrées sont des valeurs par défaut et peuvent être adaptées côté serveur. Dans une installation configurée différemment, les indications du portail mentionnent les valeurs qui y sont applicables.

Pour la version 26.4.0

Agent

Le Relution Agent surveille le statut de conformité de chaque appareil, fournit des applications via le Relution Store et prend en charge le mode multi-utilisateurs (iOS) sur différents appareils. Ces fonctionnalités complètes permettent une gestion centralisée et fluide de tous les appareils, que ce soit dans les écoles ou dans des environnements d'entreprise exigeants.

Grâce à l'intégration transparente de ces fonctionnalités, le Relution Agent crée une plateforme efficace qui optimise à la fois la sécurité et la productivité dans la gestion des appareils mobiles.

Relution Agent pour iOS

Le Relution Agent est automatiquement installé sur tous les appareils gérés et sert d'application centrale pour les fonctionnalités de Mobile Device Management (MDM). Une mesure de sécurité importante est que le Relution Agent ne peut pas être supprimé de l'appareil par l'utilisateur tant que le profil MDM y est installé. Cela garantit une présence constante et la fiabilité des fonctions MDM.

> L'application Relution Agent fait partie de la plateforme Relution et n'est utilisable qu'avec le composant backend Relution et les identifiants appropriés. L'installation doit être réalisée en coordination avec les administrateurs informatiques de l'organisation.

Pour la version 26.4.0

Fonctionnalités de l'application

- Affichage du statut de conformité de l'appareil
- Installer et mettre à jour les applications pertinentes
- Désinstaller les applications non nécessaires
- Afficher, demander et ajouter des applications et des liens web
- Relution Shared Device (pour les appareils multi-utilisateurs)
- Détection iBeacon, GeoFence et zones
- Afficher les messages du système MDM sur l'appareil
- Connexion à l'appareil via QR code / token MFA
- Afficher les informations de l'appareil
- Activer les notifications push
- Activer l'authentification biométrique pour la connexion à l'appareil

Notifications dans le portail

Pour les appareils iOS, deux messages liés à l'agent peuvent apparaître dans le portail, visibles dans la vue des politiques de l'appareil, sur la ligne des valeurs par défaut de l'appareil (libellée Valeur par défaut de dans le portail) :

1. Connexion de l'application client Relution (dans le portail : `Délimitation de l'application client Relution`) — `Relution Agent n'est pas installé`
2. `Service Push` — `Push doit être activé pour l'application Relution`

Le message relatif à la connexion de l'application client est résolu dès que le Relution Agent est installé et figure dans la liste des applications installées de l'appareil. Si l'application manque, Relution relance automatiquement son installation lors de la prochaine mise à jour de l'appareil. Le message `Service Push` est résolu en ouvrant l'application Relution Agent et en autorisant les notifications. Relution retire de la vue les messages résolus.

Relution Agent pour Android Enterprise

Pour la version 26.4.0

Le Relution Agent fait partie intégrante de la plateforme Relution et n'est utilisable qu'avec le composant backend Relution. Il est installé automatiquement sur tous les appareils gérés et sert d'application centrale pour les fonctionnalités MDM. Il est protégé contre la désinstallation, et Relution le préconfigure automatiquement avec les données de connexion de l'appareil.

Fonctionnalités de l'application

- Affichage du statut de conformité de l'appareil
- Installer et mettre à jour les applications pertinentes
- Désinstaller les applications non nécessaires
- Affichage des applications disponibles depuis le Google Managed Play Store
- Afficher les messages du système MDM sur l'appareil
- Connexion à l'appareil via QR code / token MFA
- Afficher les informations de l'appareil
- Activer les notifications push
- Activer l'authentification biométrique pour la connexion à l'appareil

---

Relution Agent pour Windows

Le Relution Agent pour Microsoft Windows fournit des fonctionnalités de base et est disponible dans le Windows Store. Les utilisateurs disposant des permissions nécessaires (au moins `Appstore User`) peuvent consulter les applications Windows fournies par l'administrateur via le portail Relution. Les administrateurs peuvent gérer les demandes d'application. Si l'agent est distribué depuis le Store via Relution, Relution écrit automatiquement la configuration de connexion dans le registre de l'appareil (`HKLM\SOFTWARE\Relution\Relution Agent`).

Relution Agent pour macOS

Avec Relution 5.25.0 →, le Relution Agent a été publié pour macOS. Cela permet de fournir des informations directement aux utilisateurs des appareils gérés.

Comme pour iOS, le Relution Agent peut être installé depuis l'App Store. Sur les appareils macOS gérés, Relution installe automatiquement le Relution Agent dès que des licences de l'application sont disponibles via Apps et livres (VPP dans le portail). Si l'agent manque ensuite sur l'appareil, Relution l'installe à nouveau. Sans licences, Relution n'installe pas automatiquement le Relution Agent sur macOS.

Pour la version 26.4.0

Fonctionnalités de l'application

- Affichage du statut de conformité de l'appareil
- Installer et mettre à jour les applications pertinentes (appareils gérés)
- Afficher les messages du système MDM sur l'appareil
- Afficher les informations de l'appareil
- Activer les notifications push

Installation d'applications via le Relution Agent

Pour installer et afficher des applications via le Relution Agent, un utilisateur doit être assigné à l'appareil. Cet utilisateur peut être un utilisateur fictif si seule la fonctionnalité de l'application est requise.

L'utilisateur doit être membre du groupe système `[ORGA] Appstore User` ou `[ORGA] Device Manager`, directement ou via un groupe qui en est lui-même membre (p. ex. Teacher, Developer, App Reviewer, Content Manager, Administrator). Sinon, une permission appropriée peut être créée et assignée.

Les applications affichées dans l'agent sont déterminées par les permissions de chaque application ; l'appartenance à un groupe ne suffit pas à elle seule. Par défaut, les nouvelles applications contiennent les groupes Appstore User et Device Manager dans le rôle Utilisateurs. Si un modèle personnalisé est actif sous `Paramètres` → `App Store`, ses groupes s'appliquent (Autorisations par défaut de l'App Store →). Les membres du groupe `[ORGA] Student` ne voient des applications dans l'agent que s'ils sont également membres d'Appstore User ou inscrits dans les permissions de l'application.

Nouveaux utilisateurs

Gestion des utilisateurs → Lors de la création, l'utilisateur peut être directement assigné à un groupe ou à une permission.

Utilisateurs existants via groupe système

L'assignation des membres au groupe `Appstore User` s'effectue sous : `Utilisateurs` → `Groupes` → `[ORGA] Appstore User` ([ORGA] = Nom unique de l'organisation en majuscules)

Utilisateurs existants via permission

Permissions →

Pour la version 26.4.0

Compagnon & Daemon

L'application Relution Companion est disponible sur plusieurs plateformes. Elle permet non seulement d'étendre les fonctionnalités, mais facilite également la mise en service rapide des appareils. En tant qu'élément de liaison, l'application crée un pont fonctionnel entre les systèmes d'exploitation et la plateforme Relution.

Sur les appareils macOS, ce rôle est assuré par le compagnon macOS. Sur le Mac, il s'exécute en tant que service Relution Daemon.

Les versions des applications compagnon installées sur les appareils sont consultables sous `Paramètres` → `Applications client Relution`. C'est également là que le compagnon macOS (interrupteur Activer le compagnon macOS) et le changement d'utilisateur de l'appareil du Windows Companion (interrupteur Activer le changement d'utilisateur de l'appareil) sont activés ou désactivés.

Compagnon pour Android (Legacy)

Pour la version 26.4.0

Android Legacy est une méthode plus ancienne pour gérer les appareils Android, auparavant connue sous le nom d'`administrateur de l'appareil` (Device Administrator). Pour l'inscription et la configuration des appareils Android Legacy, le Relution Companion est indispensable : il est installé depuis Google Play ou sous forme d'APK avant l'inscription, et l'inscription s'effectue ensuite via cette application, voir Inscription manuelle →.

L'application étend non seulement les fonctionnalités, mais fournit également les fonctions essentielles de Mobile Device Management (MDM). Cette intégration permet une gestion fluide des appareils Android plus anciens, améliorant ainsi l'ergonomie et l'efficacité.

Si l'option Retirer les anciens appareils Android si l'autorisation de l'administrateur de l'appareil n'est pas accordée est activée sous `Paramètres` → `Gestion des appareils`, Relution supprime le Companion et donc la gestion lorsque l'autorisation d'administrateur de l'appareil n'est pas accordée ou est révoquée ultérieurement. L'option n'a aucun effet sur les tableaux blancs basés sur Android.

> Avec l'introduction de méthodes plus avancées telles que Android Enterprise, le modèle Legacy n'est plus considéré comme la méthode privilégiée pour la gestion des appareils Android.

Compagnon pour Android Enterprise

Le Relution Companion pour Android Enterprise est installé automatiquement lors de l'inscription et est obligatoire pour la procédure d'inscription. Son type d'installation ne peut pas être remplacé dans la politique.

Le Companion étend les fonctionnalités des appareils avec des options supplémentaires, comme le suivi de localisation des appareils perdus.

De plus, il permet la distribution de certificats aux appareils via le portail Relution (voir Certificat →). Relution utilise également le Companion pour définir le Fond d'écran → et pour fournir le certificat racine de Relution Decon (filtre) →.

Compagnon pour Windows

Le Relution Companion pour Windows est un service Windows exclusif, installé automatiquement sur tous les appareils Windows gérés par Relution, à l'exception des appareils sous Windows Home et des appareils dont l'édition n'est pas reconnue (voir Compagnon Windows →).

Pour la version 26.4.0

Contrairement aux applications classiques, il n'est pas disponible dans le Windows App Store ni dans le Relution App Store. Équipé de droits administrateur, le Relution Companion est destiné uniquement aux administrateurs et fonctionne en arrière-plan de manière invisible, sans interaction directe avec les utilisateurs finaux.

Lors de la configuration des appareils Windows, des Configuration Service Providers (CSP) sont généralement utilisés pour accéder à des paramètres spécifiques du système Windows. Bien qu'utiles, ces CSP présentent certaines limitations dans les options de configuration.

Le Relution Companion pour Windows surmonte ces limitations en étendant considérablement les options de configuration, permettant ainsi une personnalisation plus complète.

Le comportement du Companion (notamment le niveau de journalisation, les délais pour les actions et les installations d'applications, la communication avec le serveur et le changement d'utilisateur à la connexion) est contrôlé via la configuration de politique Windows Companion, voir Configurer le Companion →.

Compagnon pour tableaux blancs

Selon le type de gestion, Relution fournit des applications compagnon ou des extensions dédiées aux tableaux blancs.

Android Classic

Grâce au Relution Companion, il est possible de gérer efficacement les tableaux blancs Android de différents fabricants. Cela se fait via l'enregistrement manuel des appareils avec le Relution Companion.

Une fois enregistrés, les tableaux blancs peuvent être gérés centralement via des règles et des actions dans Relution.

Les fonctionnalités disponibles dépendent des points de terminaison fournis par chaque fabricant.

Une vue d'ensemble de toutes les intégrations Android Classic est disponible sous Fabricants →.

Android Enterprise

Relution offre également la possibilité de gérer les tableaux blancs interactifs via Android Enterprise. Pour utiliser les fonctionnalités supplémentaires des tableaux blancs, l'une des extensions EDLA est nécessaire.

Pour la version 26.4.0

Un aperçu des extensions EDLA est disponible sous Extensions EDLA →.

Compagnon macOS (Relution Daemon)

Le compagnon macOS (installé sur l'appareil en tant que Relution Daemon) a été spécialement conçu pour les appareils macOS afin de permettre l'exécution de scripts et l'installation de fichiers .dmg.

Le démon est installé automatiquement dès qu'un appareil est enrôlé. Conditions :

- L'option Activer le compagnon macOS est activée sous `Paramètres` → `Applications client Relution` (activée par défaut).
- Le Mac exécute macOS 12 ou une version ultérieure.
- Le Mac n'est pas inscrit par l'utilisateur (User Enrollment).

Sur les autres Mac, les scripts ne peuvent pas être exécutés et les fichiers .dmg ne peuvent pas être installés. Si l'option est désactivée, le démon est désinstallé de tous les Mac enrôlés.

Si le compagnon macOS manque sur un Mac qui remplit ces conditions, Relution enregistre pour l'appareil une violation de conformité avec le message `Le Companion macOS n'est pas installé !`.

La configuration de politique Script et l'action Exécuter un script shell ne sont disponibles que si le compagnon macOS est activé, voir Vue d'ensemble → et Installer des applications macOS natives →.

Pour la version 26.4.0

Assets

L’application Relution Assets permet de reprendre facilement les appareils prêtés en scannant simplement un code QR. Pour cela, l’application Relution Assets doit être installée sur un appareil gestionnaire (p. ex. le smartphone ou la tablette de l’administrateur) et l’application Relution Agent sur l’appareil prêté.

La connexion à l’application Assets s’effectue avec un compte utilisateur Relution de l’organisation ; si une authentification multifacteur est configurée pour ce compte, elle est demandée lors de la connexion. Le compte nécessite le droit de lecture des appareils ainsi que les droits de lecture et de modification des prêts. Déconnexion partagée + reprise nécessite en outre le droit de modifier les appareils, et la réinitialisation aux paramètres d’usine le droit d’exécuter cette action sur l’appareil.

Instructions pour la reprise

Pour la version 26.4.0

Pour reprendre un appareil prêté, les étapes suivantes doivent être effectuées :

Appareil prêté

1. Ouvrir l’application Agent
2. Ouvrir le menu hamburger / latéral
3. Ouvrir les informations sur l’appareil
4. Le code QR doit être visible

Appareil gestionnaire

1. Ouvrir l’application Assets
2. Scanner le code QR de l’appareil prêté
3. Après le scan, jusqu’à 3 options sont disponibles selon qu’il s’agit d’un appareil 1:1 ou d’un appareil avec Appareil partagé Relution :

- Reprendre l’appareil : termine le prêt sans autre modification
- Réinitialiser aux paramètres d’usine + reprendre l’appareil : réinitialise complètement l’appareil et termine le prêt
- Déconnexion partagée + reprise : disponible uniquement pour les appareils dotés de la politique Appareil partagé Relution → sur lesquels un utilisateur est actuellement connecté.

Déconnecte cet utilisateur, supprime ainsi l’attribution de l’utilisateur à l’appareil et termine le prêt.

Après le retour

Une fois l’action exécutée avec succès, le portail Relution affiche le prêt comme n’étant plus actif (colonne Actif) ; la date de retour figure dans la colonne Revenus (date de retour).

Plus d’informations sur le système de prêt de Relution : Prêt →

Pour la version 26.4.0

Files

L’application Relution Files est une application mobile pour appareils iOS et Android qui permet d’intégrer des partages de fichiers locaux. Ces partages peuvent être fournis via les protocoles SMB ou WebDAV.

L’application est particulièrement utile pour les entreprises et les écoles qui souhaitent gérer leurs données de manière sécurisée et centralisée. En intégrant des partages de fichiers locaux, les utilisateurs peuvent accéder aux documents et contenus pertinents.

Avec l’application Relution Files, il est possible d’accéder aux partages configurés via le portail Relution. Alternativement, des partages supplémentaires peuvent également être configurés directement dans l’application. L’explorateur de fichiers intégré permet d’accéder aux répertoires et d’ouvrir divers fichiers dans les applications système.

De plus, la caméra intégrée peut être utilisée dans l’application Relution Files pour enregistrer des images directement sur le partage réseau, plutôt que dans l’application Photos d’Apple. Cela contribue à renforcer la protection des données.

Pour la version 26.4.0

Configuration manuelle

La configuration manuelle du partage de fichiers dans l’application Relution Files est intuitive et facile à réaliser. Seuls quelques champs obligatoires doivent être remplis ; après saisie, la connexion peut être testée et établie via le bouton Tester.

Champ	Description
Nom affiché	Nom au choix pour le partage
URL	URL WebDAV ou SMB pour le partage de fichiers
Nom d’utilisateur	Nom d’utilisateur pour le partage de fichiers
Mot de passe	Mot de passe de l’utilisateur pour le partage de fichiers
Type d’extension	Type d’intégration dans l’application Apple Files (iOS uniquement)

Uniquement pour iOS : le Type d'extension doit être défini sur `Modern` ou `Classic`. Selon la version d'iOS et l'utilisation de l'appareil (partagé), le partage peut ne pas s'afficher correctement dans l'application Apple Files. Files Bug →

Configuration gérée

La documentation pour la configuration gérée est disponible sous Relution Files pour iOS → et Relution Files pour Android →.

Pour la configuration gérée via la configuration de politique Partages de fichiers Relution (dans le portail : Partages de fichiers de résolution), le Type d'extension (iOS uniquement) est réglé par défaut sur Moderne. Sous Android, Relution installe automatiquement l'application en tant qu'application obligatoire dès qu'une politique Android Enterprise contient cette configuration.

Utilisation par l'utilisateur

Pour la version 26.4.0

Après une configuration réussie, le navigateur de fichiers de l'application peut être utilisé pour naviguer dans le partage. Les utilisateurs peuvent également ajouter ou modifier des dossiers dans le partage.

La caméra intégrée peut être utilisée pour enregistrer les images conformément à la protection des données directement sur le partage.

Une fois le partage de fichiers configuré, il peut être utilisé directement via l'application Fichiers intégrée, aussi bien sur les appareils iOS que sur les appareils Android.

Parent

L'application Relution Parent permet aux parents de gérer les appareils de leurs enfants, tout en laissant à l'école un contrôle total sur les appareils des élèves. L'administration scolaire conserve en permanence la possibilité de définir le processus de configuration de l'application Parent et de rompre à tout moment la connexion entre celle-ci et l'appareil de l'élève.

Les parents peuvent utiliser l'application Relution Parent pour bloquer ou autoriser l'utilisation d'applications installées sur l'appareil de leur enfant.

Compatibilité

L'application Relution Parent est compatible avec les appareils iOS et Android Enterprise pour les parents. Les appareils des élèves à gérer peuvent également être des appareils iOS ou Android Enterprise.

Une fonctionnalité clé de Relution Parent est sa compatibilité multiplateforme :

Un appareil parent Android Enterprise peut gérer un appareil élève iOS — et inversement.

Cela garantit une flexibilité maximale dans les environnements mixtes.

Pour la version 26.4.0

Conditions de configuration

L'application Relution Parent nécessite un serveur Relution en version 5.23.0 ou supérieure. Pour connecter l'appareil d'un élève à l'application Parent, l'appareil de l'enfant doit :

- Être un appareil iOS ou Android Enterprise
- Disposer au minimum de la version 5.15.0 du Relution Agent →
- Être supervisé
- Posséder les autorisations nécessaires accordées à l'utilisateur de l'appareil de l'élève

Cette autorisation peut être ajoutée à un rôle existant ou à un nouveau rôle créé à cet effet. L'autorisation requise se trouve dans : `L'application Relution pour les parents` → `Permettre l'appariement` → `Créer`

Pour gérer les demandes de liaison, l'administrateur a besoin, dans la section Paramètres, de l'autorisation Liens vers l'application pour les parents : Lire pour afficher les entrées, Actualisation (mise à jour) pour les approuver et les modifier, Supprimer pour les supprimer.

Association des appareils élèves avec l’application Parent

Pour garantir qu’aucune personne non autorisée ne puisse restreindre les appareils des élèves, chaque liaison doit être approuvée par un administrateur. Un champ de texte libre est disponible pour permettre aux écoles d’adapter le processus de liaison à leurs besoins.

Appareil de l’élève

Sur l’appareil de l’élève, la section `Informations sur l’appareil` → `Application Parent` est ouverte dans l’application Relution Agent. Un code QR y est généré et doit être scanné par l’application Relution Parent pour initier la liaison.

Pour la version 26.4.0



Si la section *Application Parent* n'apparaît pas :

- La version du Relution Agent est inférieure à 5.15.0,
- L’appareil n’est pas un appareil iOS ou Android Enterprise, ou
- L’utilisateur de l’appareil de l’élève ne dispose pas de l’autorisation `L'application Relution pour les parents` → `Permettre l'appariement`. (Voir Conditions de configuration ci-dessus.)

Le code QR et l’invitation sont valables 24 heures à compter de la création du code QR.

Un maximum de cinq entrées sous `Liens vers l'application pour les parents` est possible par appareil d’élève. Toutes les entrées sont comptées, sauf celles à l’état Expiré, donc également Ouvert, Sur invitation, E-mail confirmé, Établi et Supprimé par le parent. Un code QR dont la validité de 24 heures est écoulée conserve l’état Ouvert et continue d’être compté. Une fois la limite atteinte, l’administrateur doit d’abord supprimer une entrée sous `Liens vers l'application pour les parents`.

Parents

Les parents peuvent télécharger l’application Relution Parent depuis l’App Store ou le Google Play Store. Après avoir accepté la politique de confidentialité, l’application est prête à être utilisée.

Le code QR généré sur l’appareil de l’enfant est scanné avec le lecteur de code QR intégré dans l’application ou avec n’importe quel lecteur de code QR (par exemple l’application appareil photo).

Pour la version 26.4.0

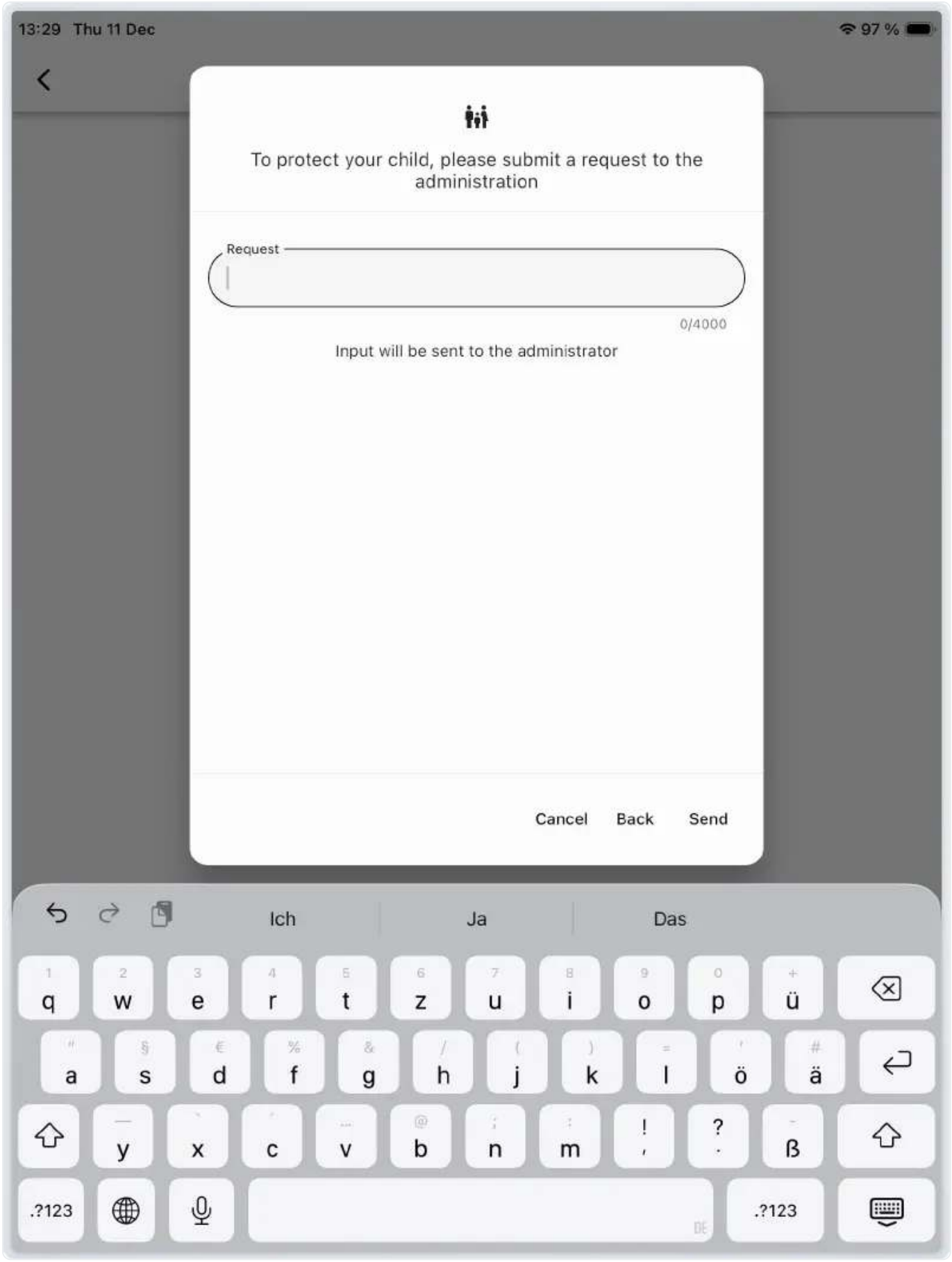


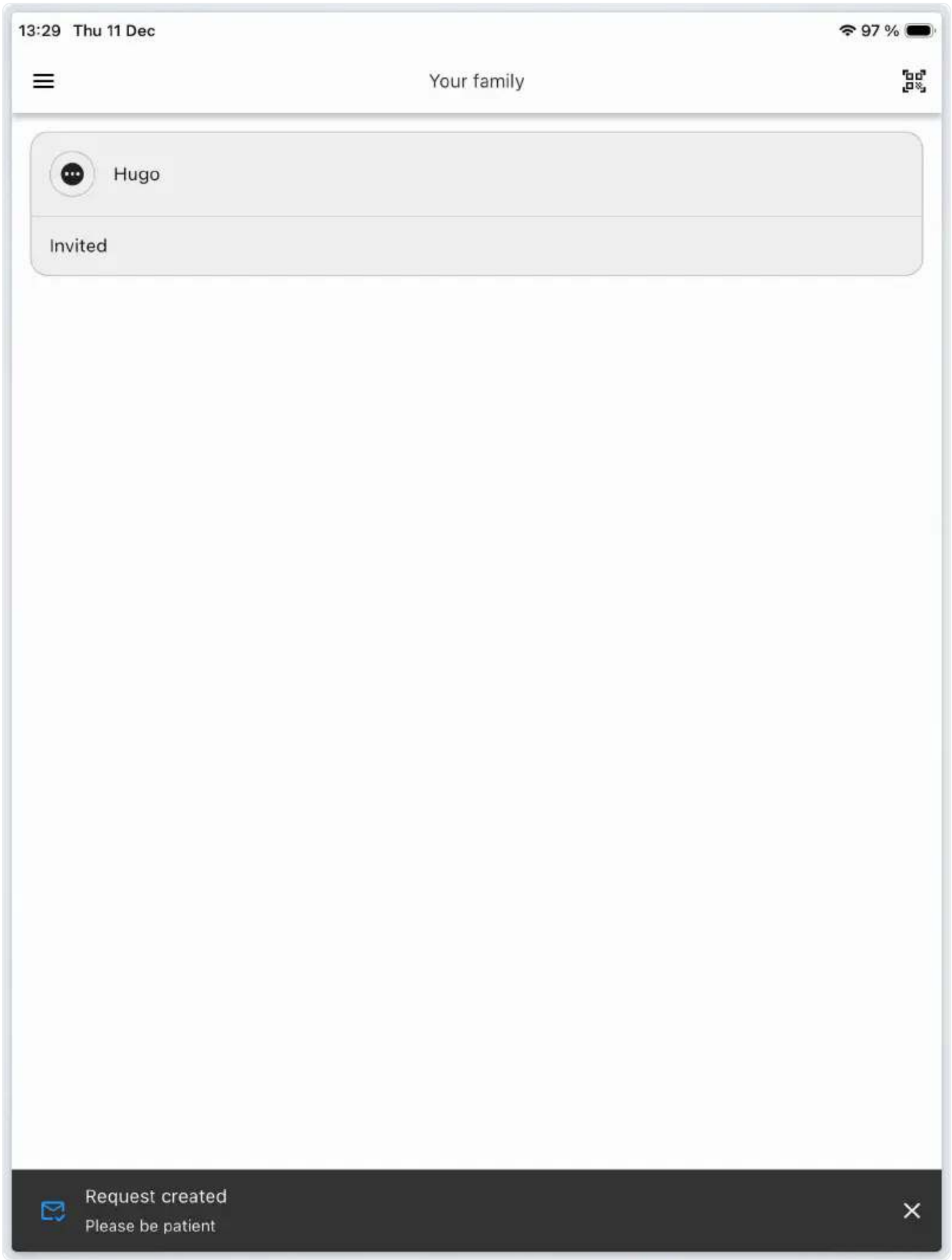
Après avoir scanné un code QR valide, les parents doivent :

- Attribuer un nom à l’appareil de l’enfant
- Fournir une adresse e-mail valide (qui devra ensuite être confirmée)
- Optionnellement, renseigner un champ de texte libre pour des informations supplémentaires

Pour la version 26.4.0

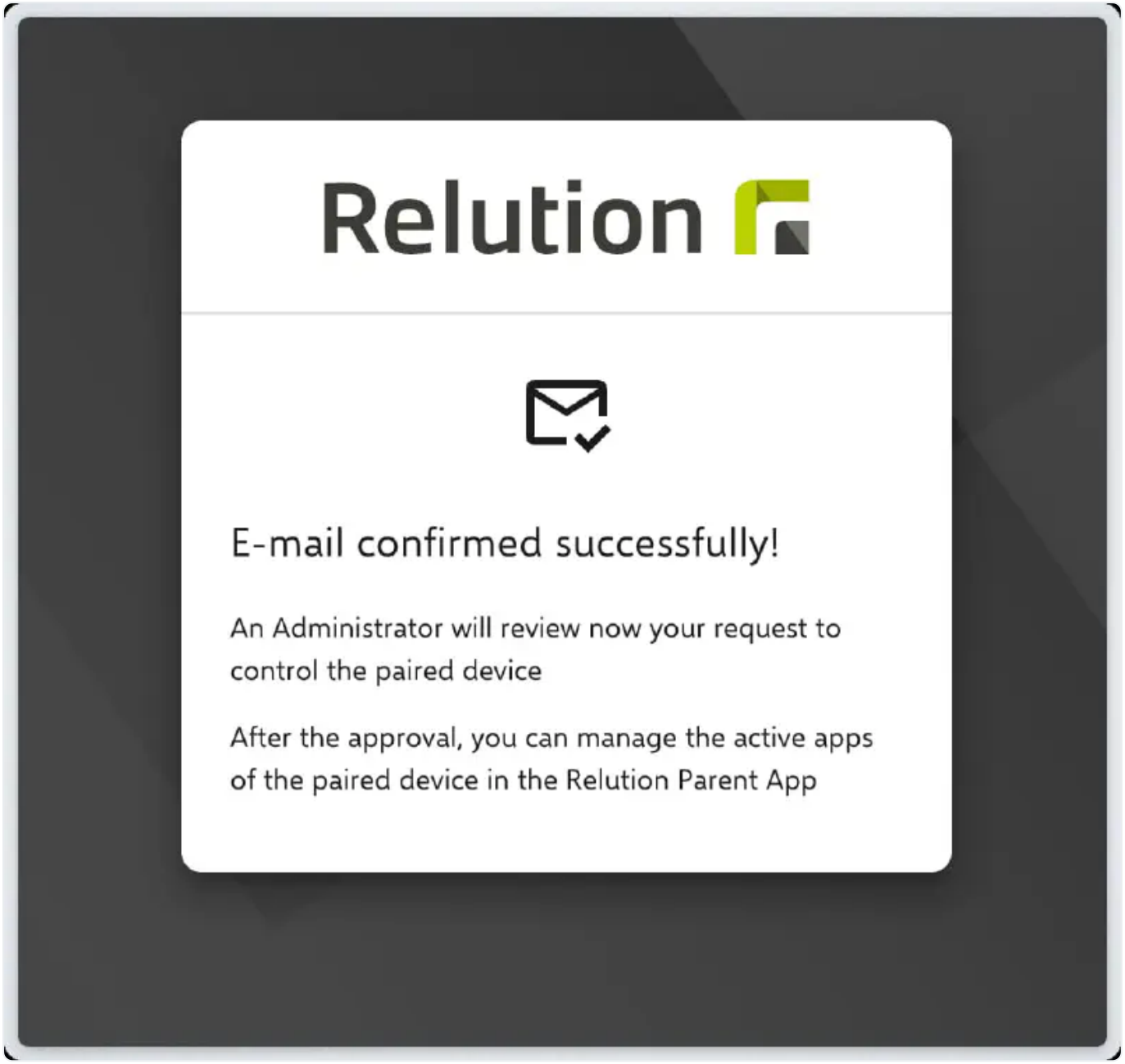

13:29 Thu 11 Dec
97 %
Add child
Give your child's scanned device a name and e-mail address
Name of child's device
For identification of the device in the app
E-Mail address used for confirmation
Enter an E-Mail address for access
Cancel
Next


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

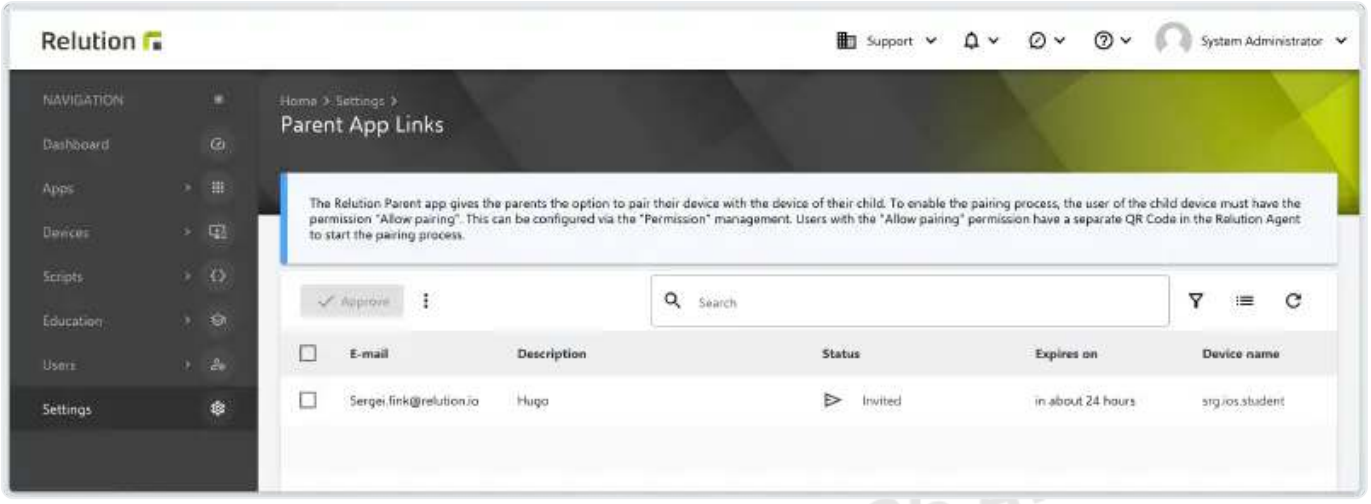
Si le code QR est reconnu mais qu'une erreur survient lors de l'envoi de la demande, il se peut qu'il ait expiré ou qu'il ait déjà été utilisé. Dans ce cas, la section *Application Parent* doit être actualisée dans l'application Relution Agent de l'enfant.

Après l'envoi, les parents reçoivent un e-mail contenant un code de confirmation à huit chiffres et un lien de confirmation. Une fois la confirmation réussie, l'état passe à E-mail confirmé. Si le code de confirmation est saisi de manière incorrecte dix fois, l'entrée passe à l'état Expiré et ne peut plus être confirmée.



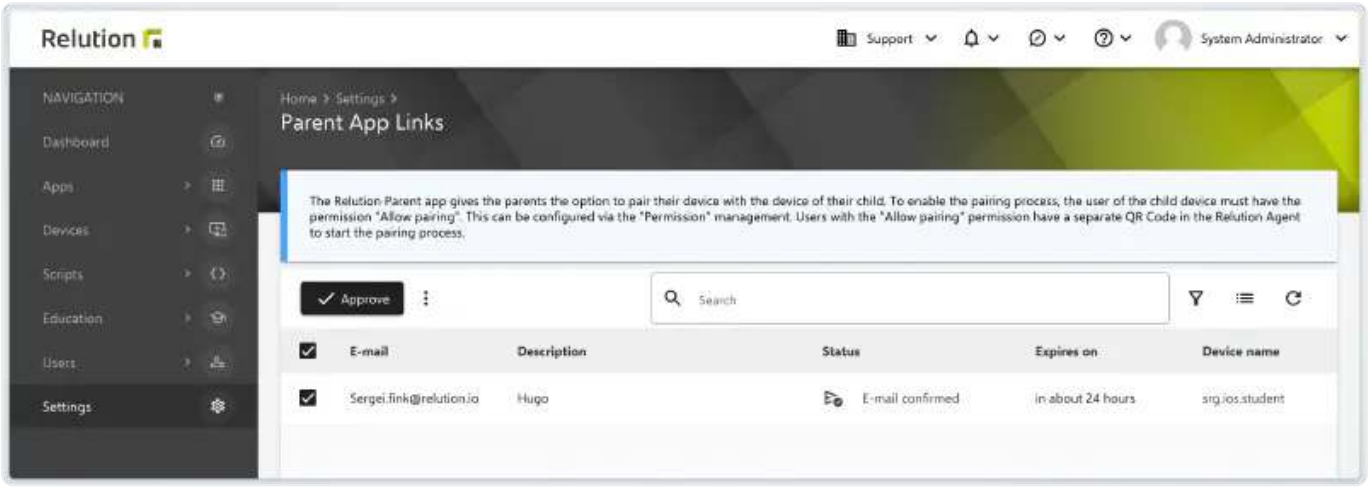
Administration

Toutes les demandes de liaison issues de l'application Parent apparaissent sous : `Paramètres` → `Gestion des appareils` → `Liens vers l'application pour les parents` Les liaisons d'un appareil donné sont également visibles dans le détail de l'appareil, sous `Appareils` → `Inventaire`, dans l'onglet Liens vers l'application pour les parents (iOS et Android Enterprise uniquement).



La colonne Expire le affiche l'heure d'expiration des entrées à l'état Ouvert et Sur invitation. Après expiration, l'entrée conserve l'état Ouvert ou Sur invitation, mais ne peut plus être poursuivie. Le filtre par défaut de la liste masque les entrées à l'état Expiré.

Une fois l'adresse e-mail du parent confirmée (état E-mail confirmé), l'administrateur peut approuver la demande de liaison via Approuver. Plusieurs entrées sélectionnées peuvent être approuvées en une seule fois, à condition qu'elles soient toutes à l'état E-mail confirmé. La description d'une entrée peut être modifiée via Éditer dans son menu contextuel.



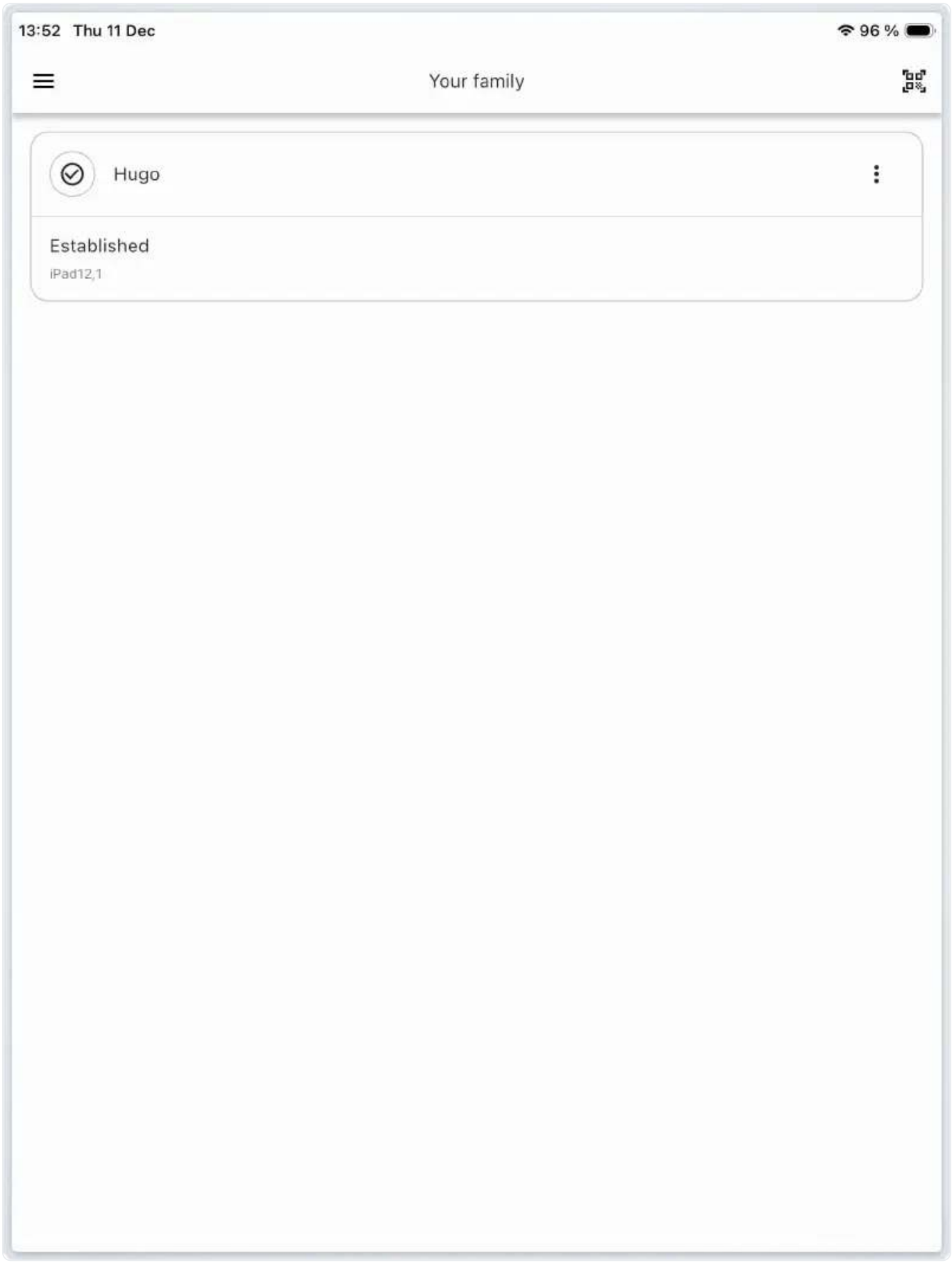
Il n’existe pas d’action de refus distincte : une demande est refusée en supprimant l’entrée via Supprimer. Une liaison existante peut également être supprimée à tout moment de cette manière. Le parent perd alors l’autorisation de contrôler l’appareil de l’enfant. S’il ne reste plus aucune liaison à l’état Établi pour l’appareil, toutes les restrictions définies par les parents sont levées. Il en va de même lorsque les parents suppriment la liaison dans l’application Parent.

Les états possibles d’une liaison sont :

État	Description
Ouvert	Le code QR a été généré sur l’appareil de l’élève mais pas encore scanné
Sur invitation	Le code QR a été scanné, demande envoyée, e-mail non confirmé
E-mail confirmé	Les parents ont confirmé leur adresse e-mail, l’approbation par l’administrateur est en attente
Établi	La liaison a été approuvée par l’administrateur
Expiré	La confirmation de l’e-mail a échoué trop souvent en raison d’un code de confirmation erroné (10 tentatives) ; la liaison ne peut plus être confirmée
Supprimé par le parent	La liaison a été supprimée par le parent

Utilisation de l’application Parent

Une fois la demande de liaison envoyée, son état est affiché sur la page d’accueil de l’application Parent. Cette page liste tous les appareils d’enfants associés ainsi que leur état actuel.


13:52 Thu 11 Dec
96 %
Your family
Hugo
Established
iPad12,1

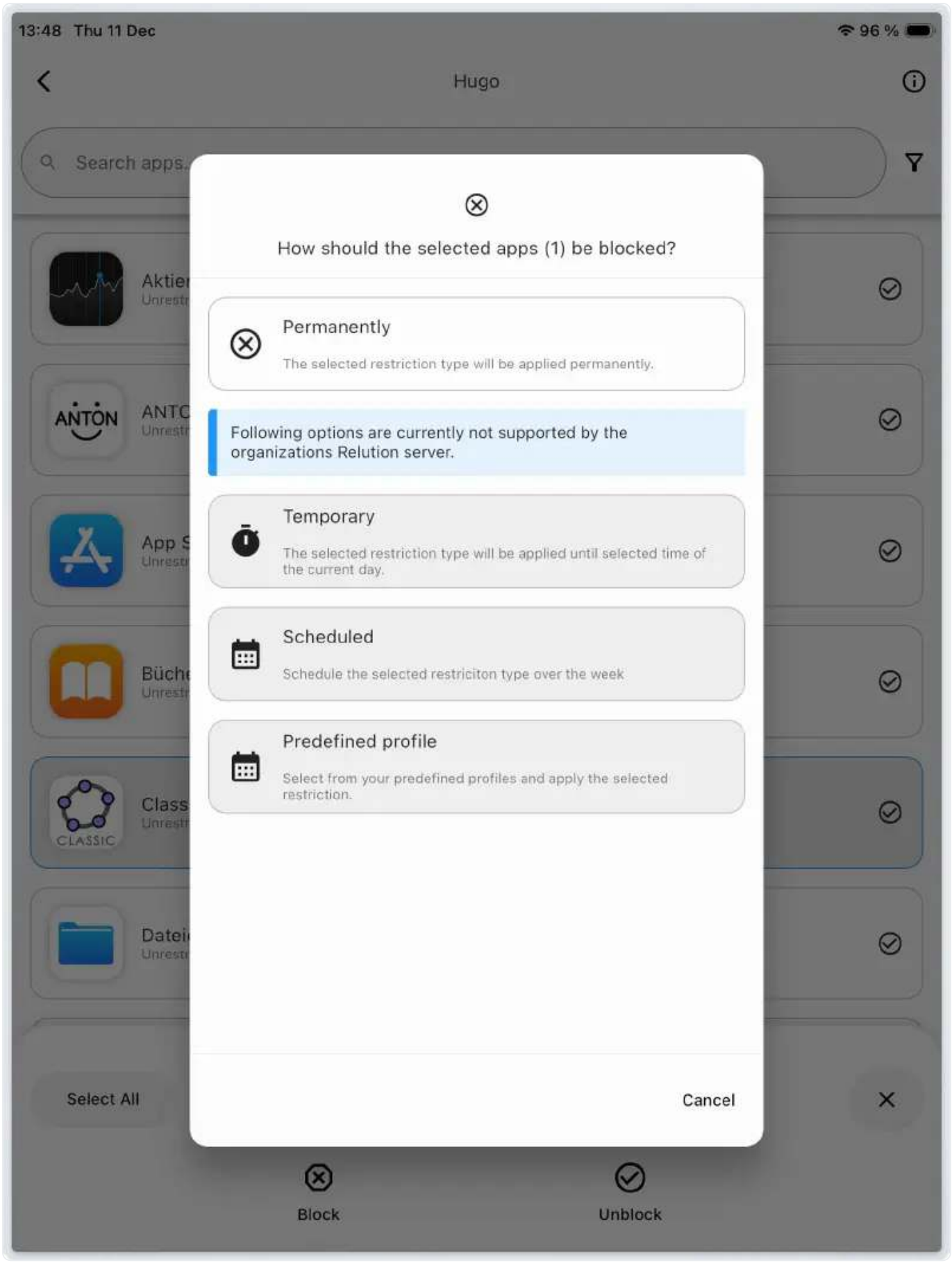
Après approbation par l'administrateur scolaire, les parents peuvent gérer l'appareil directement. L'écran d'accueil affiche alors toutes les applications détectées par Relution.

Les parents peuvent :

- Sélectionner les applications installées sur l'appareil
- Les bloquer ou les autoriser selon leurs besoins
- Les bloquer ou les autoriser de façon temporaire ou planifiée
  À partir de Relution 26.0.0

Une fois la modification validée, une restriction est appliquée sur l'appareil de l'enfant.

Pour la 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

> En cas de conflit entre une restriction parentale et une restriction de cours, le cours est toujours prioritaire.

Application des restrictions

À partir de Relution Server 26.0.0 combiné avec Relution Parent 26.0.0, les parents peuvent désormais contrôler les restrictions de manière flexible dans le temps. Trois types de limitations temporelles sont disponibles :

1. Permanente
    - La restriction s'applique indéfiniment, sans limite de temps, et remplace entièrement la restriction précédente – y compris son type.
    - Idéal pour des règles fixes à long terme de contrôle des appareils.
2. Temporaire
    - Cette restriction est active jusqu'à l'heure spécifiée du jour en cours. Si l'heure est déjà passée, elle s'appliquera le jour suivant.
    - Les restrictions temporaires écrasent uniquement d'autres restrictions temporaires, puis rétablissent automatiquement les paramètres d'origine.
    - Parfait pour des limitations ponctuelles (ex. périodes d'étude ou de repos).
3. Planifiée
    - La restriction s'applique selon l'emploi du temps défini ; en dehors de cette plage, la restriction inverse est activée.
    - Les emplois du temps peuvent être enregistrés comme profils dans Relution Parent et réutilisés pour appliquer rapidement des modèles récurrents.
    - Les modifications d'un profil n'affectent pas les restrictions déjà appliquées : elles doivent être réassignées aux applications cibles.

La restriction temporelle active est affichée sous forme d'icône et de texte pour chaque application.

Notes importantes

- Si une liste d'autorisation (Allowlist) est active sur un appareil iOS d'élève, elle prime sur l'application Parent. Elle peut provenir de la configuration Conformité App (Type de liste Liste d'autorisation : les applications ci-dessous sont autorisées) ou de la configuration Restrictions (ID de bundle d'applications autorisés).
- Un cours actif (Leçons dans le portail) est également prioritaire sur les restrictions définies par les parents.

Pour la version 26.4.0

- Les applications Relution de l’appareil de l’élève (par ex. Relution Agent, Relution Companion, Relution Teacher) ne peuvent pas être bloquées par les parents.
- À partir d’iPadOS 26 sur l’appareil enfant, les applications système (ex. Safari, Books) sont accessibles via l’application Parent.
  Cette fonctionnalité n’est pas disponible sur les versions antérieures d’iPadOS.

Messages d’erreur

- Erreur 500
  L’envoi d’e-mails n’est pas possible depuis le serveur Relution. L’envoi d’e-mails est configuré dans l’organisation `Global` sous `Paramètres` → `Configuration du courrier électronique` et vérifié dans la section de test (Configuration de l’e-mail de test) (voir Envoi d’e-mails →).

Pour la version 26.4.0

Teacher

L'application Relution Teacher (iOS, Android & Windows, et depuis Relution 5.24 également en tant qu'application web) permet aux enseignants de créer des profils spécifiques aux cours, avec lesquels les applications, fonctions des appareils et liens web peuvent être préparés et gérés pour les cours.

Elle permet également de définir des groupes de participants et de contrôler le déroulement des cours.

Grâce à l'intégration avec Apple Classroom et Samsung Classroom Management → (licence séparée requise), un contrôle complet est également possible pendant les cours – sans compte Apple sur les appareils des élèves.

Prérequis

Pour utiliser l'application Relution Teacher, une licence Relution Education est requise.

De plus, des classes avec les élèves et enseignants correspondants doivent être créées (`Éducation` → `Classes`).

Pour la version 26.4.0

L'enseignant doit disposer au minimum de l'autorisation `Éducation` → `Utiliser l'application pour enseignants`. Elle est incluse dans le groupe système [Nom unique de l'organisation] Teacher (par ex. `UIT Teacher`), attribué dans le compte utilisateur sous Groupes et autorisations dans le champ Groupes ; elle peut également être accordée via un rôle dans le champ Permissions.

Les appareils iOS, Android Enterprise et ChromeOS sont pris en charge comme appareils des élèves.

Structure

Le contenu de l'appareil élève est défini par un profil. Les participants sont ensuite définis et la durée est configurée. Le cours peut alors être démarré.

Profils

Les profils définissent l'équipement de l'appareil pour le cours.

L'enseignant peut choisir entre des profils privés et publics. Ces derniers peuvent être utilisés par tous les enseignants de l'organisation. La modification et la suppression restent réservées au créateur.

Pour le profil d'examen (iOS, ChromeOS), le fond d'écran est également défini.

Les applications, liens web, applications système et certaines restrictions peuvent être définis dans le profil.

Les applications ne doivent pas être installées uniquement lors de l'application du profil afin de réduire le temps de préparation du cours.
Lors de l'utilisation du mode examen, un fond d'écran par défaut doit être défini dans une politique séparée.
Pour maintenir les élèves en permanence dans le Wi-Fi ou empêcher la désactivation du Bluetooth, une politique séparée est également recommandée.

Pour la version 26.4.0

Gestion des participants

Pour le cours, une classe existante peut être sélectionnée. Les élèves absents peuvent être retirés directement du cours. Ainsi, le profil est distribué uniquement aux appareils des participants présents.

Il est également possible de créer une classe ad hoc. Dans ce cas, tous les élèves de l'organisation sont disponibles.

Pour des groupes ad hoc récurrents, il est recommandé de définir des classes propres via le portail ou d'assigner les élèves à plusieurs classes.

Définir la durée du cours

Un profil est limité dans le temps – par exemple jusqu'à la fin de la période de cours actuelle.

Sous Paramètres des leçons →, les durées des cours peuvent être définies.

Démarrer et contrôler un cours

Un seul cours peut se dérouler à la fois par enseignant. Au démarrage d'un cours, les autres cours non terminés du même enseignant sont terminés ou supprimés. Si des élèves participent déjà à un autre cours actif, un avertissement s'affiche ; si le cours est malgré tout démarré, ils sont retirés de l'autre cours.

Si l'option Limiter la leçon au calendrier est activée dans les Paramètres des leçons →, aucun cours ne peut être démarré en dehors de l'emploi du temps.

Pendant un cours en cours, les enseignants peuvent ajuster les participants, modifier le temps restant et terminer le cours manuellement. À la fin du cours, les iPad partagés (Shared iPad) peuvent être déconnectés ; pendant le cours, cela est également possible pour des appareils partagés individuels.

Le profil est supprimé des appareils des élèves après la durée définie ou après la fin du cours.

En cas de fin manuelle, Relution envoie immédiatement les modifications aux appareils des élèves ; après expiration de la durée définie, dans un délai d'environ une minute. Les sites web bloqués et les restrictions du cours sont levés dès que la modification atteint l'appareil. Si un appareil n'est pas joignable à ce moment-là, il reçoit la modification dès qu'il redevient joignable. Les applications installées pour le cours ne sont pas désinstallées.

> L'organisation des applications et des dossiers ne peut pas être enregistrée, car la suppression des profils modifie la structure de l'écran d'accueil et la resynchronise.

Pour la version 26.4.0

Créer un modèle de cours

Les unités de cours peuvent être enregistrées comme modèles personnels ou partagés afin de les réutiliser rapidement.

Un modèle de cours comprend les paramètres suivants :

Type de modèle de cours

- Modèle personnel (privé)
- Utilisation uniquement pour le créateur du modèle
- Modèle partagé (partagé)

- Utilisation du modèle pour tous les enseignants

Les modèles privés sans propriétaire (par ex. après la suppression de l'enseignant) sont supprimés automatiquement chaque jour à 01:00.

Mode examen (iOS, ChromeOS)

- Mode examen
- Définit sur les appareils iOS et ChromeOS des élèves un fond d'écran violet portant l'inscription « Klausur » (« Exam » si la langue par défaut du serveur est l'anglais), afin de voir d'un coup d'œil si l'appareil est dans l'état souhaité.
- Sur iOS, le fond d'écran ne peut pas être modifié pendant l'examen et la recherche Spotlight n'affiche pas de résultats Internet.
- À la fin de l'examen, Relution définit un fond d'écran par défaut. Sur iOS, ce n'est pas le cas si une politique définit déjà un fond d'écran pour l'écran verrouillé et l'écran d'accueil.

Mode application unique

Pour la version 26.4.0

- Met l'appareil (Android ou iOS) en mode application unique.
- Pour cela, exactement une application doit être sélectionnée dans le cours.
- En outre, des fonctions de l'appareil peuvent être restreintes en mode application unique, par ex. l'écran tactile, la rotation, les boutons de volume, le commutateur de sonnerie, le bouton de veille et le verrouillage automatique sous iOS, et par ex. le bouton marche/arrêt, la navigation système, la barre d'état, les paramètres de l'appareil et le maintien de l'écran allumé pendant la charge sous Android.

Applications autorisées pendant le cours

- Permet de sélectionner les applications accessibles aux élèves pendant la durée du cours.

Fonctions de l'appareil pendant le cours

- Autoriser la caméra (Android + iOS)
- Autoriser les captures d'écran (Android + iOS)
- Afficher Safari et les liens web (iOS)
- Utiliser des liens web pour filtrer le contenu web (iOS)

- Afficher l’application Messages (iOS)
- Autoriser les aides orthographiques (iOS)
- Autoriser AirDrop (iOS)
- Forcer Bluetooth (iOS)

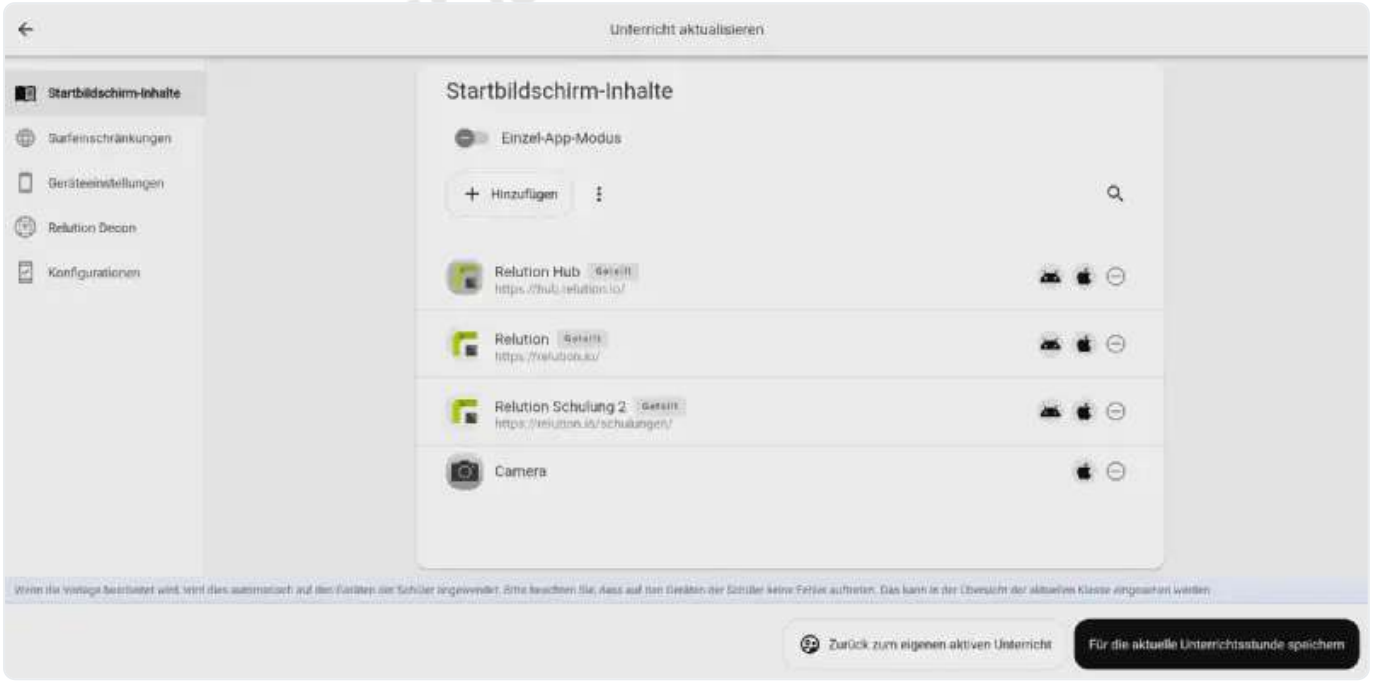
Il est également possible de définir qu’aucune restriction spécifique au cours n’est appliquée.

Liens web et restrictions de navigation

Nouveau dans 26.5

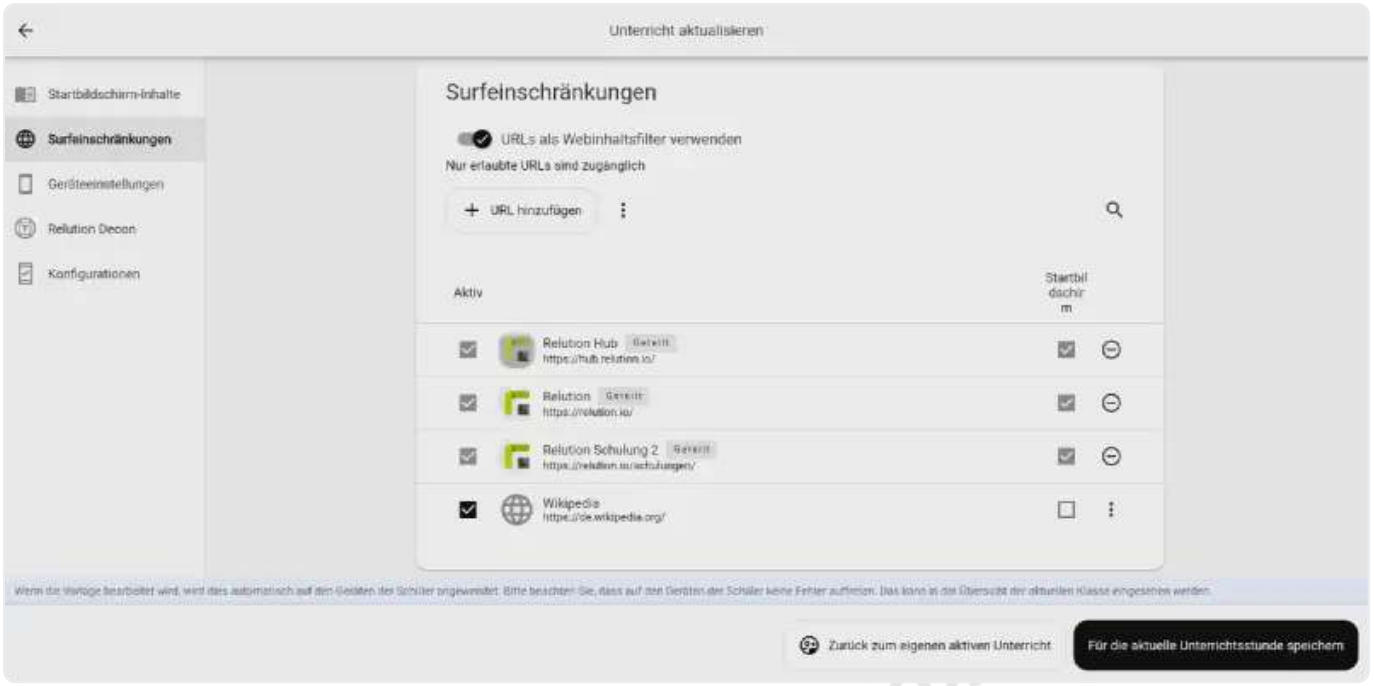
Les liens web peuvent être utilisés dans un modèle de cours de deux manières configurables indépendamment :

- Sous Contenu de l’écran d’accueil, les liens web sont placés comme raccourcis sur l’écran d’accueil des appareils des élèves pour la durée du cours. Via Ajouter, d’autres liens web peuvent être inclus.
- Sous Restrictions de navigation, les URLs servent de liste d’autorisation pour le filtre de contenu web (iOS). Le commutateur Utiliser les URLs comme filtre de contenu web active le filtrage. Lorsqu’il est désactivé, la navigation est libre et les URLs répertoriées n’ont aucun effet.



Dans la liste des restrictions de navigation, la colonne Actif détermine pour chaque URL si elle est autorisée dans le filtre de contenu web, et la colonne Écran d’accueil si elle apparaît également comme raccourci sur l’écran d’accueil. Une entrée peut ainsi servir uniquement d’URL

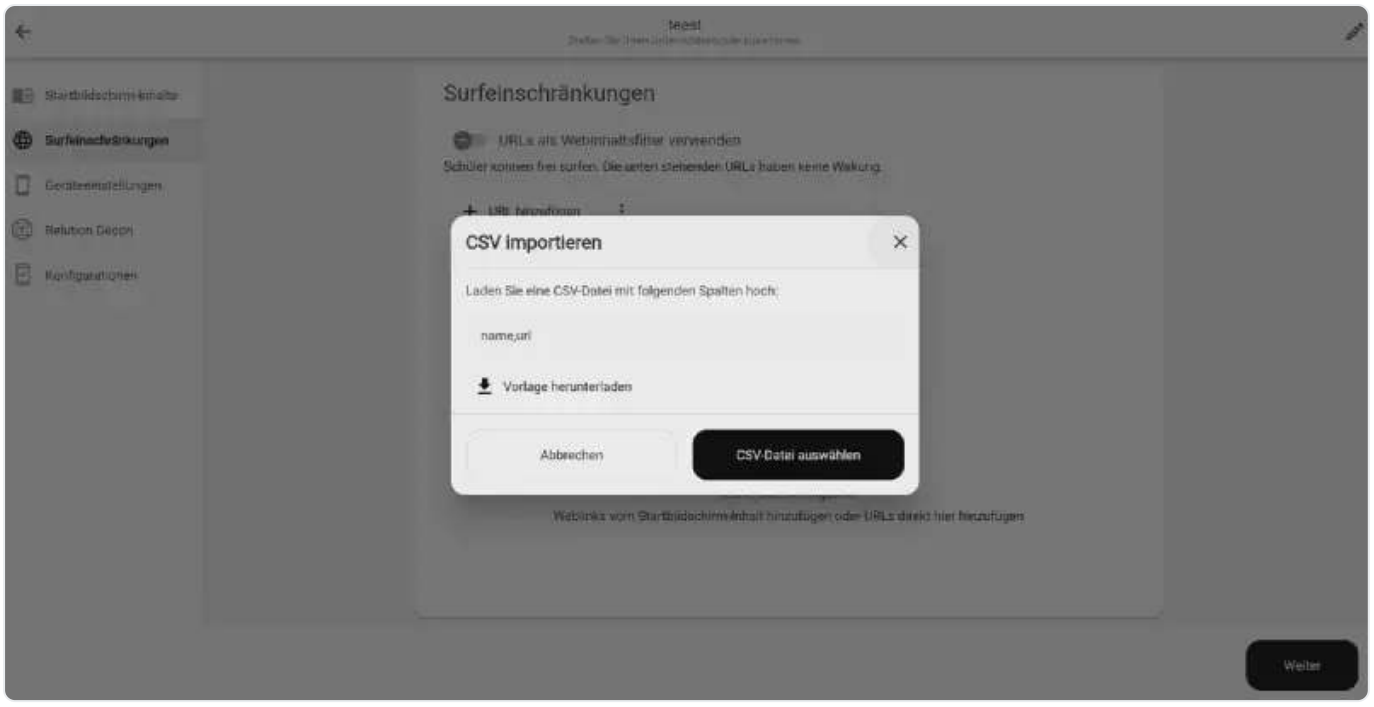
autorisée sans apparaître sur l'écran d'accueil. Lorsque le filtre de contenu web est activé, une URL inactive n'apparaît pas non plus sur l'écran d'accueil. Via Ajouter URL, des URLs peuvent être ajoutées directement ; les liens web déjà créés sous Contenu de l'écran d'accueil peuvent également être repris.



Importer des liens web via CSV

Via le menu à trois points → Importer un CSV, une liste de liens web peut être téléchargée sous forme de fichier CSV. Le fichier contient les colonnes `name` et `url` ; un modèle correspondant est disponible via Télécharger le modèle.

Pour la version 26.4.0




```
name,url
Wikipedia,https://wikipedia.org
```

Pour la ver

Paramètres de l’App Store

- Autoriser Google Play Store (Android)
- Afficher l’App Store (iOS)
- Afficher iTunes Store (iOS)

Relution Decon

- Activer Relution Decon (licence requise. Une politique Decon doit également être attribuée aux appareils élèves dans Relution)
- Liste BPjM
- Recherche sécurisée
- Type de filtre
  - Désactivé
  - Restriction d’âge
    - 0+

        - 6+
        - 12+
        - 16+
    - Catégories
        - Contenu pour adultes
        - Publicité
        - Communication
        - Réseaux sociaux
        - Divertissement
        - Musique
        - Actualités
        - Achats
        - Travail
        - Éducation
        - IA générative
        - Hameçonnage
        - Divers

En savoir plus sur Relution Decon →

En outre, des listes distinctes de sites web autorisés et bloqués peuvent être définies pour le cours. Les liens web actifs du cours sont automatiquement repris comme sites web autorisés. Le type de filtre Catégories et la tranche d'âge 12+ sont présélectionnés.

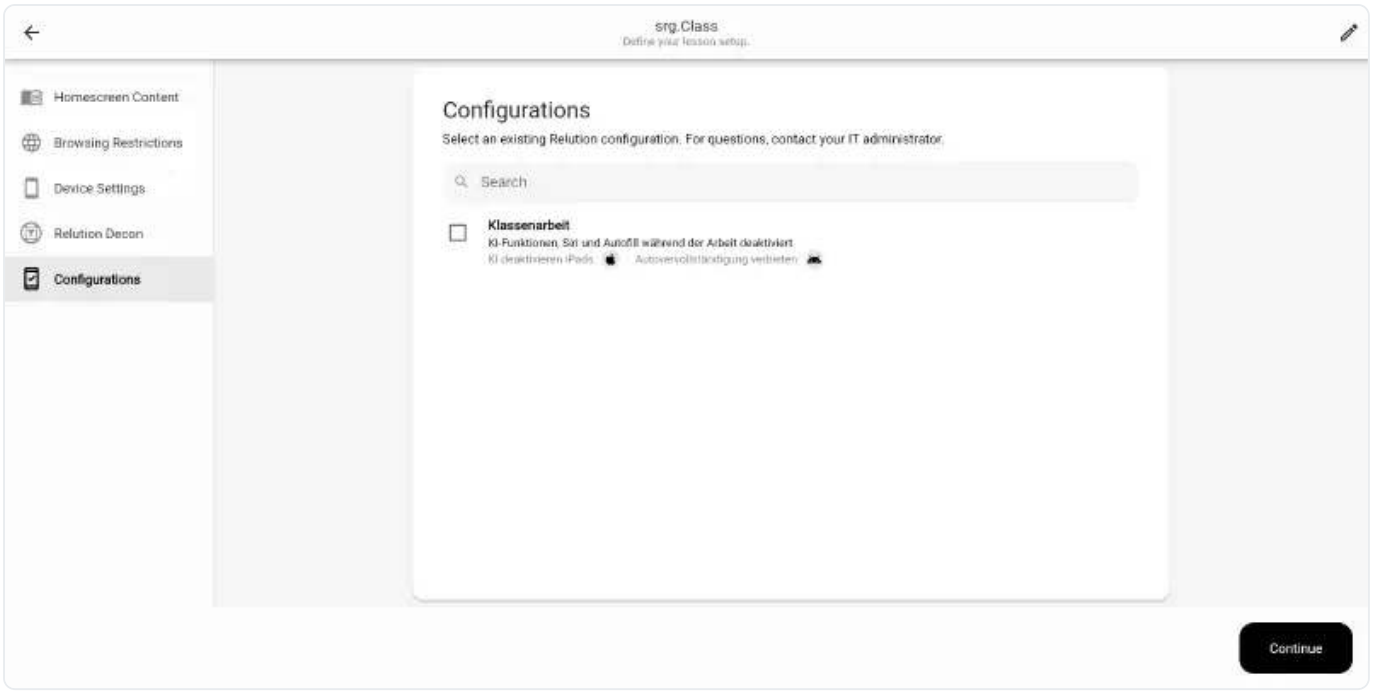
Remarque : Pendant la durée du cours, la configuration Decon normalement active est remplacée.

Pour la version 26.4.0

Configurations

Dans Relution Teacher, les Configurations désignent les groupes Éducation créés et dotés de stratégies dans le portail : Groupes Éducation →.

Dans le modèle de cours, une ou plusieurs configurations peuvent être sélectionnées dans la zone Configurations ; le nom, la description et les stratégies liées sont affichés pour chacune. Au démarrage du cours, les stratégies liées sont appliquées aux appareils des élèves, puis retirées à la fin.



La sélection requiert l'autorisation de lecture `Éducation` → `Groupes d'appareils de cours`. Sans cette autorisation, aucune configuration n'est affichée.

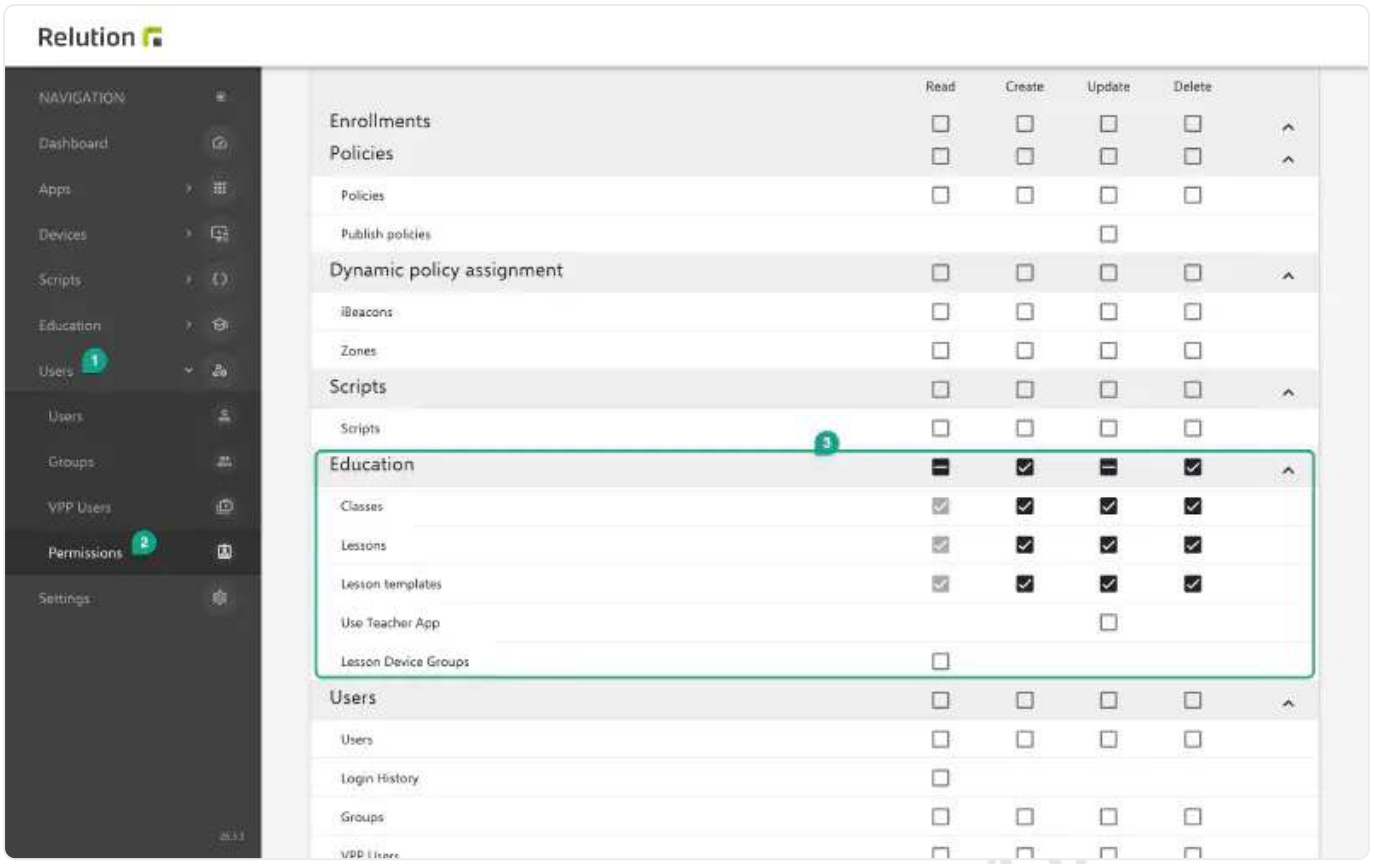
Mode admin pour la consultation des cours

Pour la version 26.4.0

Pour la vue admin dans l'application, la permission en lecture `Éducation` → `Leçons` est requise.

L'administrateur a accès à tous les cours de son organisation. Ceux-ci peuvent être consultés et des informations supplémentaires peuvent être obtenues en cas de problème.

Avec l'autorisation Actualisation (mise à jour) pour `Éducation` → `Leçons`, il est possible de modifier le cours (ajouter/supprimer des élèves) et de le terminer prématurément.



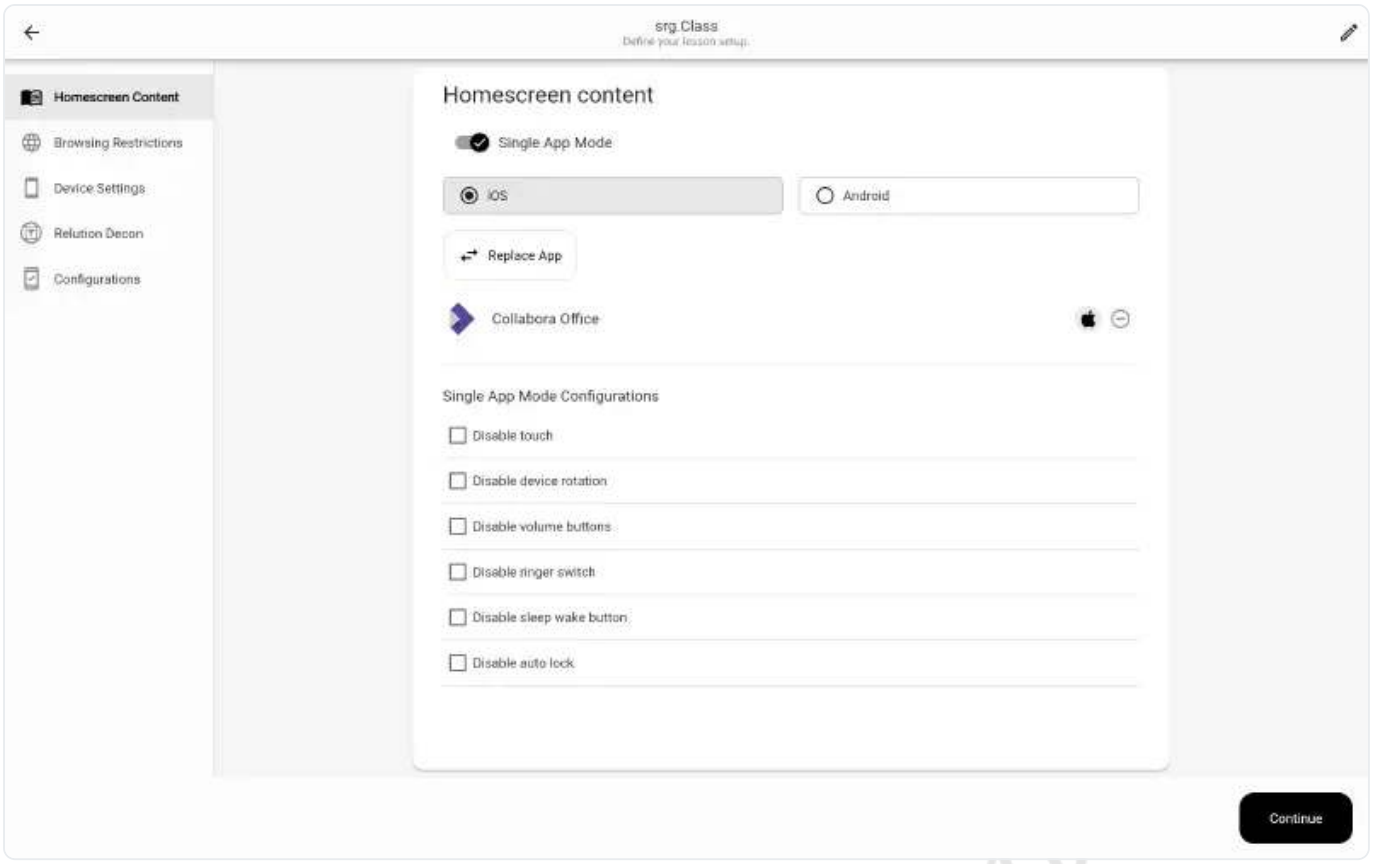
Pour la version 26.4.0

Relution Teacher en tant qu’application web

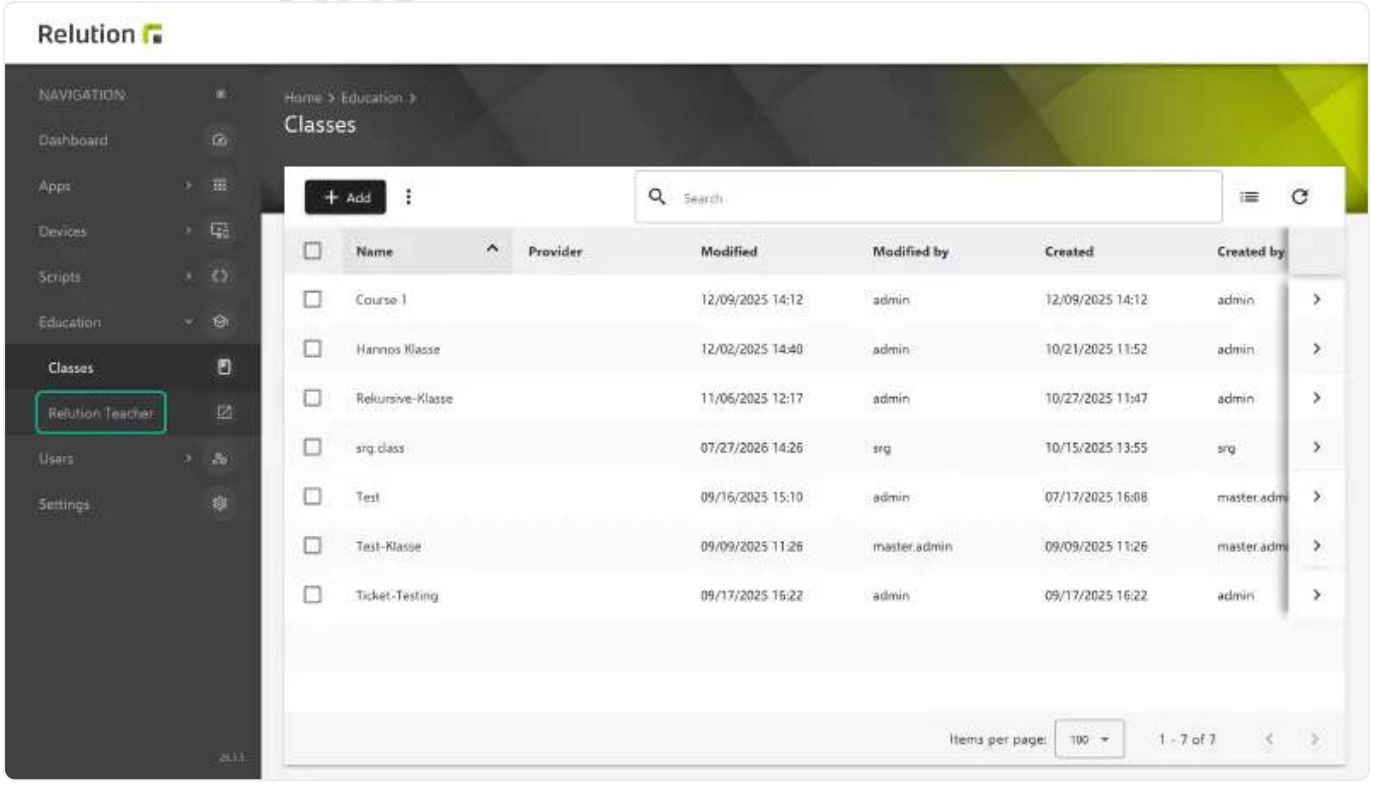
Depuis Relution Server 5.24, l’application web Relution Teacher est disponible.

Les enseignants peuvent désormais créer, démarrer et gérer des cours directement depuis un navigateur, de la même manière que sur iOS et Android.

Cette intégration fluide permet une organisation des cours efficace et adaptée aux environnements éducatifs modernes.



L’application web est accessible dans le menu de navigation sous `Éducation` → `Relution Teacher` et s’ouvre dans un nouvel onglet du navigateur. L’entrée de menu n’apparaît qu’avec l’autorisation `Éducation` → `Utiliser l'application pour enseignants`.



Fonction multitenant pour les enseignants de plusieurs écoles

La fonctionnalité multi-tenant de Relution Teacher permet aux enseignants d'étendre l'utilisation de Relution Teacher à plusieurs organisations.

Cela est particulièrement utile lorsque les enseignants travaillent dans plusieurs écoles qui gèrent leurs appareils élèves via la même instance Relution.

Configuration

Pour permettre l'accès à plusieurs organisations Relution, les étapes suivantes sont nécessaires :

- La connexion s'effectue dans l'organisation `Global`.
- Dans le portail Relution, l'utilisateur concerné (enseignant) est recherché et modifié dans la section `Utilisateurs`.
- L'utilisateur est ajouté aux groupes système des organisations supplémentaires, par ex. au groupe [Nom unique de l'organisation] Teacher.

Pour la version 26.4.0

Après configuration, l'organisation souhaitée peut être sélectionnée dans l'application Relution Teacher ainsi que dans l'interface web via le menu latéral. Seules les organisations dans lesquelles l'enseignant dispose de l'autorisation `Éducation` → `Utiliser l'application pour enseignants` sont proposées.

De plus, dans l'organisation `Global` sous `Éducation` → `Classes`, la colonne Organisation est affichée par défaut et indique l'organisation Relution de chaque classe.

Remarque

Lors de l'application d'un cours via Relution Teacher, la disposition de l'écran d'accueil de l'utilisateur est supprimée.

Techniquement, il n'est actuellement pas possible de sauvegarder la disposition des applications de l'utilisateur et de la restaurer après la fin du cours.

Il est possible de définir une configuration centrale de l'écran d'accueil afin d'imposer une disposition uniforme sur tous les appareils.

Disposition écran d’accueil →

Pour la version 26.4.0

Paramètres des leçons

Sous `Paramètres` → `Éducation` → `Paramètres des leçons` se définit la plage horaire dans laquelle les enseignants peuvent démarrer un cours via l'application Teacher →. Cette page n'est visible qu'avec une licence Education ou Free.

L'autorisation Paramètres des leçons de la section Paramètres est requise : Lire pour afficher la page, Actualisation (mise à jour) pour la modifier. Sans Actualisation, la page est en lecture seule. Les périodes de cours ajoutées, modifiées ou supprimées ne sont appliquées qu'après l'enregistrement de la page via Enregistrer.

Périodes de cours

Les périodes de cours sont gérées sous forme de liste avec Nom, Description, Heure de début et Heure de fin. Le Nom est obligatoire, la Description est facultative. Les périodes de cours ne doivent pas se chevaucher, y compris lors de la modification. Une heure de début qui coïncide exactement avec la fin d'une autre période de cours est également considérée comme un chevauchement ; un écart d'au moins une minute est donc nécessaire. L'heure de fin doit être postérieure à l'heure de début.

Pour la version 26.4.0

Par défaut, la liste contient 14 périodes de cours (1. Stunde à 14. Stunde, de 07:45 à 21:05), les jours de cours sont du lundi au vendredi, le fuseau horaire est UTC et la limitation à l'emploi du temps est désactivée.

Paramètres généraux

- Ignorer les paramètres du système : visible uniquement pour les organisations locataires. Permet de s'écarter des paramètres de cours définis au niveau du système. Si l'option est désactivée, tous les champs sont verrouillés et les périodes de cours ne peuvent être ni ajoutées ni modifiées ; les modifications apportées dans l'organisation système sont reprises automatiquement. En revenant aux paramètres du système, les valeurs de l'organisation système s'appliquent à nouveau.
- Fuseau horaire : fuseau horaire auquel se réfèrent les périodes de cours configurées.
- Limiter la leçon au calendrier : si cette option est activée, un cours ne peut être démarré dans l'application Teacher que les Journées de cours sélectionnées, au plus tôt au début de la première période de cours et avec une heure de fin prévue au plus tard à la fin de la

dernière période de cours. Les pauses entre les différentes périodes de cours ne sont pas bloquées.

- Journées de cours : devient obligatoire lorsque la limitation ci-dessus est activée. Définit les jours de la semaine où les cours peuvent avoir lieu.

Accès aux images de profil pour les configurations Apple Education

Contrôle si Relution est autorisé à accéder aux images de profil des utilisateurs afin d'alimenter la connexion partagée sur iPad et Apple Classroom avec les images de profil enregistrées. Activé par défaut. Avec Désactivé, Relution ne fournit pas les images de profil à l'iPad partagé ni à Apple Classroom.

Les images de profil ne sont fournies qu'aux appareils disposant d'une configuration Apple Education, et uniquement pour les utilisateurs membres d'une classe de cette configuration.

Pour la version 26.4.0

Homescreen

L'application Relution Homescreen est un lanceur qui permet aux administrateurs de personnaliser à distance l'écran d'accueil des appareils Android Enterprise entièrement gérés. L'application remplace le lanceur préinstallé et est configurée de manière centralisée via la configuration Disposition de l'écran d'accueil de Relution dans une politique Android Enterprise. Elle est automatiquement installée sur les appareils dès l'application de la politique.

L'application ne remplace le lanceur préinstallé que sur les appareils entièrement gérés (Device Owner). Avec les autres inscriptions Android Enterprise, l'application reçoit la disposition configurée, mais n'est pas définie comme lanceur. Cette configuration n'existe pas pour Android Legacy.

L'application offre plusieurs fonctionnalités pour personnaliser l'écran d'accueil :

- Personnalisation du thème
- Sélection du fond d'écran
- Choix et disposition des applications affichées

Pour la version 26.4.0

Configuration

La configuration Disposition de l'écran d'accueil de Relution comprend les paramètres suivants :

- Mise en page : Thème (Léger, c'est-à-dire clair, par défaut, ou Dark), Taille de la grille (Auto, 4x4, 5x4 (défaut), 6x4) et Orientation de l'écran (Automatique par défaut, Paysages pour paysage, Portrait).
- Papier peint : fichier image et, en option, un Texte sur papier peint avec Couleur du texte (valeur hexadécimale, par défaut `#ffffff`).
- Les contraintes → Apps autorisées : Afficher uniquement les applications de la mise en page (par défaut) ou Afficher toutes les applications. Avec Afficher uniquement les applications de la mise en page, seules les applications de la disposition sont disponibles sur l'appareil.
- Dans l'éditeur de disposition, les applications, dossiers et liens web sont disposés par glisser-déposer sur les pages et dans le dock ; les dossiers ne sont pas possibles dans le dock. Les applications peuvent aussi être ajoutées manuellement via leur nom de package ; le nouvel élément apparaît alors sur la première page. Sur l'appareil, la disposition est verrouillée et ne peut pas être modifiée par l'utilisateur.

Plus de détails sur la configuration figurent dans l'article Mode kiosque →.

> La configuration Disposition de l’écran d’accueil de Relution n’est disponible que si aucune configuration Mode kiosque n’est appliquée. Il n’est pas possible d’utiliser les deux configurations simultanément. Une seule des deux peut être ajoutée dans une politique ; en cas de plusieurs politiques, la priorité des politiques est déterminante.

Avec Relution Education, le serveur utilise automatiquement l’application Homescreen avec les applications du cours sur les appareils Android Enterprise des élèves pendant un cours, même sans configuration propre. Les cours en mode application unique sont exclus.

Appareils non gérés

L’application Relution Homescreen Layout est également disponible gratuitement pour les appareils non gérés sur le Google Play Store.

Lien Google Play Store →

Pour la version 26.4.0

Relution Decon

À partir de la version 5.27, Relution pour iOS permet la configuration d'un filtre de contenu basé sur DNS. Cette fonctionnalité assure un accès Internet sécurisé et ciblé en restreignant l'accès à certains sites web et applications. Grâce à la catégorisation des contenus basée sur l'IA, Relution Decon fournit également un contrôle parental complet avec des options avancées de configuration.

Qu'est-ce que Relution Decon ?

Relution Decon est un module complémentaire basé sur l'IA pour iOS, iPadOS, macOS et Android Enterprise qui filtre le contenu en temps réel, créant un environnement numérique sécurisé. Grâce au contrôle de contenu basé sur DNS, Decon bloque les sites web et applications indésirables, permettant aux utilisateurs de travailler et d'apprendre dans un espace protégé et sans distraction.

Relution Decon utilise un proxy DNS pour transmettre toutes les requêtes au serveur Decon. Les sites web sont classés et soit autorisés, soit bloqués selon les règles définies par les politiques. Toutes les communications sont chiffrées SSL, garantissant la sécurité des activités des utilisateurs.

Pour la version 26.4.0

Application Decon

L'application Decon est automatiquement déployée sur les appareils iOS, iPadOS, macOS et Android Enterprise lors de l'installation de la politique. Elle surveille les requêtes DNS de l'appareil et garantit que seuls les contenus autorisés sont accessibles.

Fonctionnalités de l'application :

- Active un proxy DNS global, qui ne peut pas être désactivé par l'utilisateur
- Affiche le statut actuel de Relution Decon
- Fournit des informations sur les sites bloqués et les catégories de filtrage appliquées

> Recommandation : pour les appareils Apple, s'assurer de disposer d'un nombre suffisant de licences Apps et livres (VPP dans le portail) avant le déploiement.

Configurer le VPP →
Relution Decon sur l'Apple App Store →

Politique Decon

Dans la politique des appareils, la configuration est créée via `Ajouter` → `Relution Decon`. Cette politique installe automatiquement l'application Decon sur les appareils associés et agit comme proxy pour toutes les requêtes DNS.

La configuration est complétée lors de la publication de la politique. Sans licence Relution Decon valide, le formulaire affiche un avertissement et la configuration ne peut pas être enregistrée. Sous macOS, la configuration n'est disponible qu'avec l'inscription de l'appareil.

Si une politique iOS ou macOS contient déjà une configuration Proxy DNS, Relution Decon ne met pas en place son propre proxy DNS ; l'appareil reçoit alors un avis de conformité.

Les paramètres sont décrits en détail dans les articles par plateforme Relution Decon pour iOS →, Relution Decon pour macOS → et Relution Decon pour Android Enterprise →.

Pour la version 26.4.0

Hiérarchie de configuration des politiques (de la plus haute à la plus basse priorité)

1. Apps autorisées (iOS/iPadOS et macOS uniquement)
2. Apps bloquées (iOS/iPadOS et macOS uniquement)
3. Domaines autorisés
4. Domaines bloqués
5. Type de filtre (catégories bloquées ou niveau d'âge)

Les applications Relution (Relution Agent, Relution Teacher, Relution Files, Relution Assets, Relution Decon) ainsi que les adresses du serveur Relution et du serveur Decon sont toujours autorisées.

Decon dans Relution Teacher

Decon peut être sélectionné et géré dans les profils de classe avec Relution Server 5.32.0 et Relution Agent 5.19.0. Les appareils des élèves doivent avoir une politique Decon assignée.

Teacher →

Remarque : La configuration Decon par ailleurs valide sera écrasée pour la durée de la leçon.

Filtrage

Dans la section Filtrage, le champ obligatoire Type de filtre détermine le mode de filtrage des sites web :

- Arrêt : aucun filtrage par catégories ni par niveau d'âge.
- Catégories (par défaut) : les catégories à bloquer sont sélectionnées individuellement (voir tableau).
- Niveau d'âge : le filtrage s'effectue selon un niveau d'âge (0+, 6+, 12+ ou 16+, par défaut 12+).

Les commutateurs Liste BPJM et Recherche sécurisée sont également disponibles. Les entrées sous Domaines autorisés peuvent permettre l'accès à des contenus classés comme inadmissibles par la BPjM.

Si plusieurs configurations Decon sont utilisées sur un même appareil, le filtrage le plus fort prend automatiquement effet : les filtres par niveau d'âge priment sur les filtres par catégories, et les configurations sans filtrage sont ignorées. Les catégories bloquées sont fusionnées (une catégorie est bloquée dès qu'une configuration la bloque) ; en cas de plusieurs niveaux d'âge, le plus strict s'applique. Les listes de domaines et d'applications sont également fusionnées.

Pour la version 26.4.0

Classification par catégorie

Relution Decon attribue automatiquement chaque site web à une catégorie. Avec le type de filtre Catégories, les administrateurs définissent sous Catégories bloquées quelles catégories doivent être bloquées. Par défaut, seule la catégorie Adulte est bloquée.

Catégorie	Description	Exemples
Adulte	Sites inappropriés pour les jeunes	Pornographie, Violence, Armes, Drogues, Jeux d'argent, Divertissement adulte, Shopping adulte, Rencontres, Google Safe Search
Publicité	Sites publicitaires	Fournisseurs de publicité
Communication	Services de communication	Email, Messenger, Appels (vidéo)

Catégorie	Description	Exemples
Médias sociaux	Contenus de réseaux sociaux	Facebook, Instagram, TikTok, etc.
Divertissement	Sites de divertissement comme streaming ou jeux	Films, Jeux, Vidéos
Musique	Services de streaming musical	Spotify, Tidal, etc.
Nouvelles	Sites d’information et magazines	News, Météo
Achats	Boutiques en ligne (hors contenus adultes)	Amazon, eBay, etc.
Travail	Sites liés au travail	Office, Partage de fichiers, Intranet
Éducation	Sites éducatifs pour l’apprentissage	Wikipedia, Google Scholar
IA générative	Sites liés à l’intelligence artificielle	ChatGPT, Perplexity.ai, etc.
Hameçonnage	Sites potentiellement frauduleux	Escroqueries potentielles, Vol de données
Divers	Tous les autres sites	Restants

Listes d’autorisation et de blocage

- Domaines autorisés / Domaines bloqués : Permet de spécifier des domaines autorisés ou bloqués indépendamment des catégories. Seul le domaine doit être indiqué, pas le chemin. Les domaines avec caractères génériques ainsi que les adresses IPv4 et IPv6 sont possibles. Le nombre de domaines bloqués devrait être limité à environ 500.
- Apps autorisées / Apps bloquées : Permet de contrôler l’accès Internet des applications ; les fonctions de base restent accessibles si aucune connexion Internet n’est nécessaire. Les listes d’applications ne sont disponibles que dans les politiques iOS/iPadOS et macOS, pas pour Android Enterprise.

En outre, Relution ajoute à chaque configuration Decon les domaines autorisés et bloqués à l'échelle de l'organisation sous `Paramètres` → `Demandes de Relution Decon`. Ces domaines ne s'appliquent pas pendant un cours avec Decon.

Configuration DNS avancée

La configuration DNS avancée n'est pas disponible dans les politiques Android Enterprise.

Serveurs DNS sur l'appareil : Des serveurs DNS alternatifs peuvent être configurés si le DNS Relution Decon n'est pas disponible. Fallback : Cloudflare Families DNS (1.1.1.3).

Serveurs DNS sur le serveur Relution Decon : Un serveur DNS alternatif peut remplacer le DNS standard sur le serveur Decon. Les adresses IP (UDP) ou DNS-over-HTTPS (DoH) comme Zero ou Quad9 sont configurables.

Confidentialité

Dans les politiques Android Enterprise, la section Confidentialité propose l'option Acceptation automatique de la divulgation des données. Elle accepte la divulgation des données dans l'application Decon au nom de l'utilisateur.

Pour la version 26.4.0

Limitations

- Mise en cache : Les sites bloqués et les modifications de politique peuvent être mis en cache jusqu'à 1 minute ; les changements peuvent ne pas être appliqués immédiatement.
- Indépendance du chemin : Le DNS fonctionne au niveau du domaine, il est impossible de définir des règles différentes pour des chemins différents d'un même domaine.
- Blocage des applications : Seul l'accès Internet est bloqué ; les fonctions de base et le contenu mis en cache restent accessibles.

Gestion des applications

Relution propose une fonctionnalité complète de Gestion des applications mobiles (MAM) permettant une gestion centralisée de toutes les applications prises en charge — de manière multiplateforme et efficace.

Plateformes et formats d'applications pris en charge :

- iOS & iPadOS : applications issues d'Apps et livres (VPP dans le portail) et applications natives (`.ipa`)
- macOS : applications issues d'Apps et livres et applications natives (`.dmg`, `.pkg`)
- Android : applications Google Play Store, applications Google Play Store gérées (Android Enterprise) ainsi qu'applications natives (`.apk`)
- Windows : applications du Microsoft Store et packages d'installation dans les formats `.msix`, `.msixbundle`, `.appx`, `.appxbundle`, `.msi`, `.exe`, et via Winget
- Liens web : peuvent également être gérés et distribués de manière centralisée

Relution permet une gestion unifiée et flexible de toutes les applications au sein d'une organisation.

Pour les applications natives, il est obligatoire d'utiliser le Relution App Store, tandis que les applications issues d'Apps et livres ou des stores des fabricants peuvent être gérées de manière optionnelle via cet outil.

Pour la version 26.4.0

Vue d'ensemble du menu Apps

Le menu Apps de Relution est divisé en plusieurs sections :

- App Store - Le magasin d'applications interne de Relution pour toutes les applications et formats pris en charge mentionnés ci-dessus.
- Demandes - Demandes d'applications formulées par les utilisateurs finaux qui peuvent être approuvées par les administrateurs ou les responsables.
- Catégories - Permet de classer les applications en catégories, par exemple pour des fins éducatives.
- Apps achetées - Vue d'ensemble de toutes les applications issues d'Apps et livres, incluant les jetons VPP et les options de synchronisation.
- Médias - Vue d'ensemble de tous les livres obtenus via Apps et livres ainsi que des fichiers téléversés, comme les PDFs.

Explication de l’App Store

Le Relution App Store est un espace central pour toutes les applications prises en charge sur diverses plateformes.

Il offre une vue d’ensemble des applications disponibles selon les colonnes Nom, Plateformes, État, Modifié et d’autres critères. Des colonnes supplémentaires peuvent être affichées via le menu hamburger.

Grâce au bouton Ajouter, les applications peuvent être intégrées à partir des stores des différents fabricants ou téléchargées de manière native. Les sources suivantes sont disponibles : Appli native, Weblink, Appli Windows Store, Appli Google Play Store, Application Google Play Store gérée (Android Enterprise), Apple App Store App et Winget Store app. La source Application Google Play Store gérée (Android Enterprise) n’apparaît que si Android Enterprise est connecté dans l’organisation.

Sections de l’App Store

Lors de l’ouverture d’une application ajoutée, les options de configuration étendues et les fonctionnalités MAM deviennent accessibles.

Pour la version 26.4.0

- Informations
    - Vue d’ensemble avec le statut actuel et la version (Développement, Révision, Publiée, Archive)
    - Description de l’application (extraite du store du fabricant)
    - Journal des modifications de l’application (extrait du store du fabricant)
    - Informations supplémentaires telles que le nom interne de l’application ou sa version
- Paramètres
    - Général
        - Mise à jour automatique – uniquement pour les applications des stores ; basé sur les métadonnées du store du fabricant (mise à jour chaque semaine)
        - Catégories – permet de classer l’application, par exemple à des fins éducatives
        - Responsable – personne ou rôle en charge de l’application
        - Contact du support – adresse de contact pour le support de l’application
    - Permissions
        - Propriétaire – propriétaire de l’application
        - Examinateur – autorisation pour examiner l’application
        - Développeur – autorisation pour développer l’application
        - Utilisateurs – utilisateurs ou groupes autorisés peuvent utiliser ou installer l’application

- Déploiements automatiques – définir les utilisateurs ou groupes devant recevoir automatiquement cette application. L'onglet n'apparaît que lorsqu'une version au statut Publiée existe ; pour macOS, uniquement pour les applications issues d'Apps et livres.
- Scripts – uniquement pour les applications Windows au format `.msi` ou `.exe`
- Attributions de version et Permissions d'application – uniquement dans l'organisation globale pour les applications locales
- Historique – suivi des mises à jour et des versions de l'application
- Appareils avec cette application – vue d'ensemble de tous les appareils sur lesquels l'application est installée

---

Demandes

Grâce à l'Agent Relution → ou au Portail, les utilisateurs peuvent demander les applications souhaitées.

Cela permet à l'utilisateur autorisé ou à l'administrateur d'approuver les applications, de supprimer des demandes, de modifier leur statut, et d'acquérir des licences Apps et livres si nécessaire.

La condition préalable est le commutateur Demandeur d'application activé sous `Paramètres` → `Paramètres généraux de l'organisation`, dans la zone Demandes d'application. Il est activé par défaut et n'est pas disponible dans l'organisation globale. S'il est désactivé, l'entrée de menu Demandes n'apparaît pas et aucune application ne peut être demandée.

Pour la version 26.4.0

Catégories

Les administrateurs et les utilisateurs autorisés peuvent créer ici des catégories pour les applications et ajouter les applications correspondantes, afin de les retrouver plus facilement et rapidement dans l'application Relution Teacher.

Apps achetées

Vue d'ensemble dédiée aux applications issues d'Apps et livres pour iOS, iPadOS et macOS, incluant une fonction de synchronisation manuelle en cas de besoin.

Elle permet de filtrer via les tokens VPP et offre une vue d'ensemble du nombre total de licences, des licences disponibles, et des licences attribuées. En cliquant sur une application spécifique, il est possible d'attribuer les licences directement aux appareils, utilisateurs ou groupes. D'autres licences peuvent être achetées via le menu contextuel Acheter l'app.

Avec un jeton VPP public, les affectations affichées ne concernent que l'organisation actuelle, tandis que le nombre total de licences porte sur toutes les organisations.

Médias

Vue d'ensemble dédiée aux médias issus d'Apps et livres pour iOS, iPadOS et macOS, incluant une fonction de synchronisation manuelle en cas de besoin.

Elle permet de filtrer via les tokens VPP et offre une vue d'ensemble du nombre total de licences, des licences disponibles, et des licences attribuées. En cliquant sur un média spécifique, il est possible d'attribuer les licences directement aux appareils, utilisateurs ou groupes.

En outre, d'autres médias tels que les fichiers PDF ou EPUB peuvent être distribués. Ils sont ajoutés via Télécharger un nouveau PDF ou ePUB et remplacés via Mettre à jour le contenu des médias. Le téléversement n'est possible que si un jeton VPP est disponible dans l'organisation. D'autres livres peuvent être achetés via Acheter des livres sur l'Apple Store.

Traiter les demandes d'applications

Pour la version 26.4.0

Les applications demandées sont placées au statut Révision. Sans processus de validation actif, les propriétaires et examinateurs de l'application, c'est-à-dire par défaut les membres du groupe App Reviewer, peuvent publier ou rejeter directement la version demandée. Les utilisateurs disposant du droit de suppression peuvent supprimer la demande. Un processus de validation en plusieurs étapes peut être configuré en option ; ses étapes peuvent être limitées aux applications demandées.

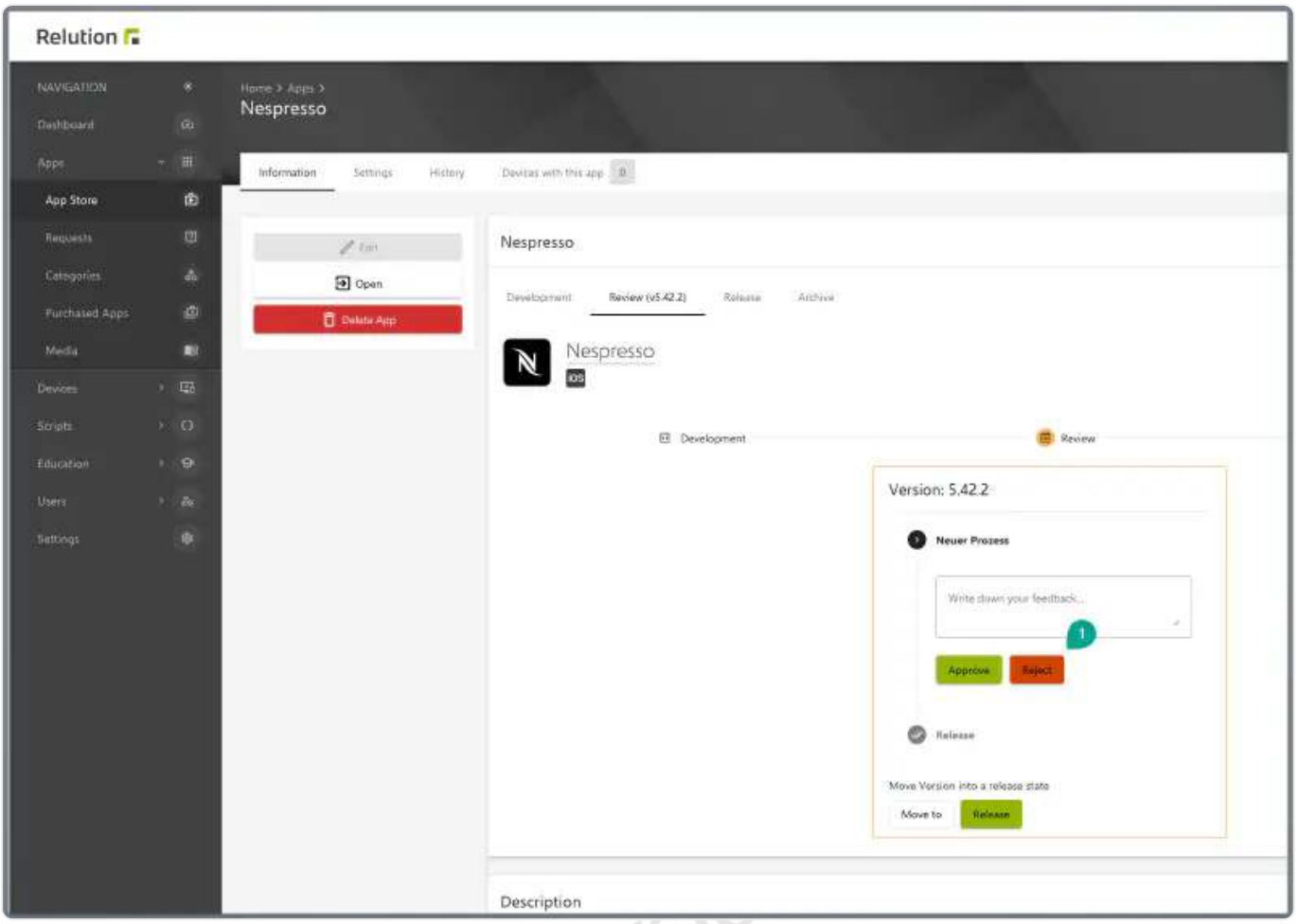
Configuration du processus

La configuration d'un processus de validation optionnel s'effectue sous `Paramètres` → `Workflow de publication d'applications`. Pour les détails sur les différentes étapes de validation, les responsabilités et la planification automatisée des dates, voir Processus de validation des applications →.

Gérer les demandes d'applications

Les applications demandées peuvent être gérées via la barre latérale sous le menu suivant : `Apps` → `Demandes`

Dans cette section, les demandes en attente peuvent être examinées puis approuvées ou rejetées.



Pour la version

Autorisations par défaut de l’App Store pour les nouvelles applications

Dans Relution, les autorisations par défaut pour les nouvelles applications peuvent être définies sous `Paramètres` → `App Store`. Cette configuration est particulièrement utile si les applications doivent être explicitement réservées à un groupe spécifique d’utilisateurs par défaut.

Configuration standard pour les nouvelles applications

Tant que le commutateur Activer est désactivé, les nouvelles applications reçoivent l’attribution par défaut suivante :

- Utilisateurs : Appstore User et Device Manager
- Développeurs : Developer
- Examinateurs : App Reviewer

Après l’activation, tous les rôles sont d’abord vides et doivent être renseignés via Utilisateur ayant téléchargé l’application ou Affecter un utilisateur ou un groupe. Sans attribution dans le rôle Utilisateur, les nouvelles applications ne sont pas disponibles pour les utilisateurs de l’App Store. Après une désactivation puis une réactivation du commutateur, le modèle est à nouveau vide.

> Si cette option est active, l'utilisateur qui télécharge l'application n'est pas autorisé à attribuer des autorisations individuelles. Les autorisations par défaut définies seront appliquées automatiquement. Les utilisateurs disposant du rôle Appstore Manager (y compris les administrateurs) font exception : pour leurs téléchargements, les autorisations par défaut sont seulement préremplies et peuvent être adaptées individuellement lors du téléchargement.

Exemple : Configuration pour le rôle Utilisateur

Au sein des paramètres, les options suivantes sont disponibles pour l’attribution :

1. Utilisateur ayant téléchargé l’application : Si cette option est active, l’utilisateur qui importe l’application est automatiquement affecté à ce rôle. Lorsqu’un utilisateur est désigné comme propriétaire, il a la permission de modifier toutes les autorisations.
2. Attribuer un utilisateur ou un groupe : Alternativement, un utilisateur spécifique ou un groupe prédéfini peut être défini pour l’utilisation de l’application.

Pour la version 26.4.0

Processus de validation des applications

Le menu `Paramètres` → `Workflow de publication d'applications` permet de définir les étapes qu'une version d'application doit franchir avant d'atteindre le statut Publiée. Le processus s'applique aux versions au statut Révision. Sans processus actif, tout utilisateur disposant de la permission Propriétaire ou Examinateur sur l'application peut publier une version directement. Dans les permissions par défaut des applications, le groupe système App Reviewer de l'organisation est enregistré comme Examinateur.

Créer des étapes de validation

Un processus de validation se compose d'un nombre quelconque d'étapes librement triables. Pour chaque étape, les paramètres suivants sont disponibles :

- Nom et Description
- Type :
  - Standard – une étape de validation classique.
  - Organiser une date de mise en production – ajoute une étape de planification de date à la version (voir ci-dessous).
- Personne ou groupe responsable : si aucun n'est défini, le propriétaire de l'application devient automatiquement responsable. Si un utilisateur désigné comme responsable est supprimé, la responsabilité passe au groupe Appstore Manager de l'organisation.
- Rendre cette étape obligatoire : si cette option est activée, la version doit obligatoirement passer par cette étape. Tant que cette étape ou une étape ultérieure est obligatoire, la version ne peut pas passer directement du statut Révision au statut Publiée. Les propriétaires de l'application disposant du rôle Appstore Manager, que les administrateurs possèdent automatiquement, font exception.
- Conditions : une étape peut être limitée à des applications spécifiques (Pour certaines applications), des types d'application (Natif, Publique, Weblink), des plateformes (iOS, Android, macOS, Windows, tvOS), des types de prix (Payant/Gratuit), des opérations de l'application spécifiques (Créer/Mettre à jour), ou exclusivement aux applications demandées (Applications demandées uniquement). Si des applications spécifiques sont sélectionnées, les conditions de type d'application, de plateforme, de type de prix et Applications demandées uniquement ne s'appliquent plus. Si Applications demandées uniquement est activé, la sélection des types d'application ne s'applique plus.

Une étape à laquelle des versions sont déjà associées ne peut être ni modifiée ni supprimée.

Pour la version 26.4.0

Si la dernière étape de validation est supprimée, le processus de validation est automatiquement désactivé.

Validation avec un processus actif

Lorsque le processus de validation est actif, chaque version au statut Révision est affectée à la première étape correspondante. Seuls la personne responsable ou les membres du groupe responsable, ainsi que les propriétaires de l'application, peuvent valider l'étape en cours. Après validation, la version passe à l'étape correspondante suivante.

Une fois la dernière étape validée, la version est publiée et reçoit le statut Publiée. Si une Date de mise en ligne future est définie pour la version, la publication a lieu automatiquement à cette date.

Pour les applications natives, une date souhaitée peut être saisie dans le champ Date de mise en ligne pour les versions au statut Développement ou Révision. Tant qu'une étape de type Organiser une date de mise en production est en cours, la date ne peut pas être modifiée.

Pour la version 26.4.0

Organiser une date de mise en production

Si le processus contient une étape de type Organiser une date de mise en production, la personne ayant téléversé l'application et la personne responsable proposent conjointement une date de publication dans la vue détaillée de la version. Une fois que les deux parties ont donné leur accord, la date est reprise comme Date de mise en ligne. Si d'autres étapes suivent dans le processus, la version les franchit d'abord. Une fois le processus terminé, elle est automatiquement publiée à la date convenue.

Activer/désactiver le processus

L'ensemble du processus de validation peut être activé ou désactivé via le menu à trois points :

- Activer le workflow : toutes les versions au statut Révision sont déplacées vers la première étape de validation correspondante. Si une version se trouvait déjà dans une étape auparavant, son historique de validation est restauré. L'activation n'est possible que si au moins une étape a été créée.
- Désactiver le workflow : les propriétaires et examinateurs de l'application, et donc par défaut aussi les membres du groupe App Reviewer, peuvent à nouveau publier des versions directement.

Mettre à disposition une application native dans le Relution App Store

Relution permet de mettre à disposition des applications natives et des packages d'installation, par exemple des fichiers IPA, PKG, DMG, APK, MSIX, MSIXBUNDLE, APPX, APPXBUNDLE, MSI et EXE. Il est ainsi possible de mettre à disposition de manière ciblée différentes versions d'une application, par exemple des versions de développement ou de test, et de les tester au préalable.

Sous `Apps` → `App Store`, la source Appli native est choisie via Ajouter, puis confirmée avec Suivant.

Le package d'installation souhaité est téléversé via Sélectionner.

Une fois le package d'installation téléversé, le formulaire s'ouvre via Ajouter des détails. Dans la section Général, le statut Publiée est sélectionné dans le champ État de la version. Le nom du statut apparaît sous forme d'info-bulle sur l'icône correspondante. Le statut Publiée n'est disponible que pour les propriétaires de l'application. Une version créée directement au statut Publiée ne passe par aucun processus de validation.

Les applications au statut Publiée peuvent être téléchargées par tous les utilisateurs autorisés via le Relution App Store.

Pour la version 26.4.0

Cette zone affiche également le nom de la version ainsi que la date de création et de modification de l'application.

Enfin, les informations sont enregistrées via Enregistrer en haut à droite.

Après l'enregistrement, une vue d'ensemble de l'application s'affiche. Elle indique notamment la plateforme pour laquelle l'application est disponible, ainsi que d'autres informations et paramètres.

Le Relution App Store indique également de quel type d'application il s'agit et pour quelle plateforme elle est mise à disposition.

Mettre à disposition une version de développement ou de test pour certains utilisateurs

Si une autre version de la même application – par exemple une version de développement ou de test – ne doit être mise à disposition que de certains utilisateurs, elle est créée au statut

Révision.

L’application souhaitée est ouverte dans le Relution App Store et une nouvelle version est créée via Ajouter une nouvelle version.

La nouvelle version est ensuite téléversée comme application native, comme décrit ci-dessus. Dans la section Général, le statut Révision est sélectionné dans le champ État de la version et les modifications sont enregistrées.

La version n’est ainsi pas visible pour les utilisateurs habituels de l’App Store. Les versions en révision ne sont visibles que pour les personnes disposant de la permission Propriétaire, Examinateur ou Développeur sur l’application, ainsi que pour les administrateurs. L’accès s’applique toujours à toutes les versions en révision de l’application, et non à une seule version.

Accès via les permissions de l’application

Les testeurs individuels obtiennent un accès ciblé via l’application elle-même : dans l’onglet Paramètres de l’application, la personne est enregistrée dans la section Permissions comme Examinateur ou Développeur via Utilisateurs et groupes. En tant que Développeur, elle voit les versions en révision mais ne peut pas les publier. Elle peut toutefois modifier les versions en révision et en développement et supprimer l’application. La section Permissions est disponible pour les propriétaires de l’application.

Pour la version 26.4.0

Accès via le groupe App Reviewer

Alternativement, l’utilisateur est ajouté au groupe système App Reviewer de l’organisation. Pour cela, l’utilisateur est ouvert sous `Utilisateurs` → `Utilisateurs`, puis le bouton Gérer les groupes est sélectionné dans la section Groupes et autorisations. Le groupe y est attribué. Son nom commence par le nom de l’organisation. Si l’organisation s’appelle par exemple « Support », le groupe s’appelle Support App Reviewer.

Les membres de ce groupe sont enregistrés comme Examinateur dans les permissions par défaut des applications. Ils voient ainsi les versions en révision de toutes les applications dont les permissions contiennent le groupe. Si un modèle de permissions par défaut est actif sous `Paramètres` → `App Store`, cela ne s’applique que si le groupe y figure (Autorisations par défaut de l’App Store →).

> En tant qu'Examinateur, les membres du groupe App Reviewer peuvent également publier des versions de ces applications, c'est-à-dire les faire passer du statut Révision au statut Publiée ou Développement. Si aucun processus de validation des applications n'est actif, cela se fait sans autre contrôle. Pour les testeurs individuels, la permission Développeur sur l'application est donc la solution la plus ciblée.

Les utilisateurs sans aucune de ces permissions ne voient que les versions au statut Publiée. Les utilisateurs ayant accès aux versions en révision voient en outre la zone Révision dans la barre supérieure du Relution App Store.

Voir aussi Traiter les demandes d'applications → pour la vérification ultérieure des applications demandées.

Pour la version 26.4.0

Gestion des utilisateurs

Relution dispose d'un système de gestion des utilisateurs interne permettant de créer des comptes manuellement ou de les ajouter via des fournisseurs externes. Les points clés et les particularités importantes sont expliqués ci-dessous.

Vue d'ensemble des utilisateurs

- Chaque utilisateur est créé dans une seule organisation de Relution.
- Un utilisateur ne peut pas appartenir à plusieurs organisations simultanément.
- La prise en charge multi-tenant est disponible pour les comptes administratifs, mais le compte utilisateur reste toujours dans le tenant d'origine.
- Tous les comptes utilisateurs sont stockés dans la base de données.
- Les adresses e-mail doivent être uniques ; la vérification porte sur toutes les organisations du serveur. Les noms d'utilisateur doivent être uniques au sein d'une organisation.

Pour la version 26.4.0

Ajout de comptes utilisateurs

Plusieurs méthodes permettent d'ajouter des comptes utilisateurs :

1. Création manuelle du compte
2. Import via fichier CSV
3. Connexion à des fournisseurs externes (par ex., LDAP → ou Microsoft Entra ID →)

Le menu contextuel de la liste des utilisateurs propose en outre l'invitation d'utilisateurs par e-mail (entrée Invitez des utilisateurs) et Création de plusieurs utilisateurs. Ces deux entrées requièrent le droit de créer des utilisateurs.

1. Création manuelle de comptes utilisateurs

- Dans la section Utilisateurs, un clic sur Ajouter ouvre le formulaire de saisie.
- Tous les champs obligatoires doivent être renseignés : nom d'utilisateur, mot de passe, prénom, nom (50 caractères maximum chacun) et adresse e-mail.
- Avec l'option Désactiver l'authentification par mot de passe, aucun mot de passe n'est défini. La connexion n'est alors possible que via un fournisseur d'identité externe (par ex. OpenID Connect ou SAML) ou un jeton API. L'option ne peut être définie qu'à la création du compte et ne peut plus être annulée ensuite.

- La section Propriétés personnalisées (repliée par défaut) propose 15 champs de 255 caractères maximum chacun. Les champs 1 à 10 peuvent être utilisés comme espaces réservés `${user.custom1}` à `${user.custom10}` dans les configurations de politiques ; les champs 11 à 15 sont enregistrés, mais ne sont pas remplacés en tant qu'espaces réservés.
- Les autorisations et groupes nécessaires devraient être définis.
- Plus d'informations sur les autorisations sont disponibles dans l'article Permissions →.

Création de plusieurs utilisateurs permet de créer jusqu'à 50 comptes utilisateurs à la fois. Le nom d'utilisateur doit contenir l'espace réservé `%N`, remplacé par un numéro croissant (par défaut `user-%N`) ; la valeur de départ est définie dans le champ Début de %N.

---

2. Import via fichier CSV

La fonction d'import CSV est disponible pour importer plusieurs comptes utilisateurs à la fois. Le déroulement complet, incluant le modèle, l'aperçu et l'attribution optionnelle de groupes ou de permissions, est décrit dans l'article Import CSV →.

> Les mots de passe indiqués dans le CSV doivent respecter la politique de mots de passe définie sous `Paramètres` → `Gestion des connexions`, en particulier la longueur minimale du mot de passe. Les lignes dont le mot de passe n'est pas conforme ne sont pas importées.

Pour la version 26.4.0

---

3. Connexion à des fournisseurs externes

- Lorsqu'un fournisseur externe (par ex., LDAP →, Microsoft Entra ID →) est connecté, le fournisseur est toujours le système principal.
- Les contenus importés sont mis à jour automatiquement en cas de modification côté fournisseur.
- Les champs nom d'utilisateur, prénom, nom, adresse e-mail, poste, téléphone et pays sont verrouillés dans le portail, car ils seront écrasés lors de la prochaine synchronisation.
- Lors de la connexion, Relution authentifie toujours l'utilisateur contre le LDAP → configuré. Si la connexion n'est pas disponible, les utilisateurs ne peuvent pas se connecter.

La configuration de la connexion aux fournisseurs externes est expliquée en détail dans les articles consacrés à chaque fournisseur. Pour les écoles, les connexions Interface OneRoster → et Import SchulConnex → sont également disponibles.

Groupes d’utilisateurs

Les groupes d’utilisateurs sont gérés sous `Utilisateurs` → `Groupes`. Les groupes rassemblent des comptes utilisateurs — par exemple pour attribuer des permissions via l’appartenance au groupe. Les rôles de permissions → peuvent être attribués aussi bien à des utilisateurs individuels qu’à des groupes — les membres reçoivent les permissions de leurs groupes.

- Ajouter un groupe : un nouveau groupe est créé via Ajouter dans la vue d’ensemble des groupes.
- Gérer les membres : les membres sont ajoutés ou retirés via Gérer les membres dans les détails du groupe. Les membres d’un groupe peuvent être des comptes utilisateurs ou d’autres groupes (groupes imbriqués). Pour les groupes synchronisés par un fournisseur (par ex. depuis LDAP), les membres sont en lecture seule.
- Supprimer : les groupes devenus inutiles peuvent être supprimés depuis la liste des groupes.
- Groupes système : ils ne peuvent pas être supprimés ; leur nom et leur description ne sont pas modifiables, et d’autres groupes système ne peuvent pas y être ajoutés comme membres.

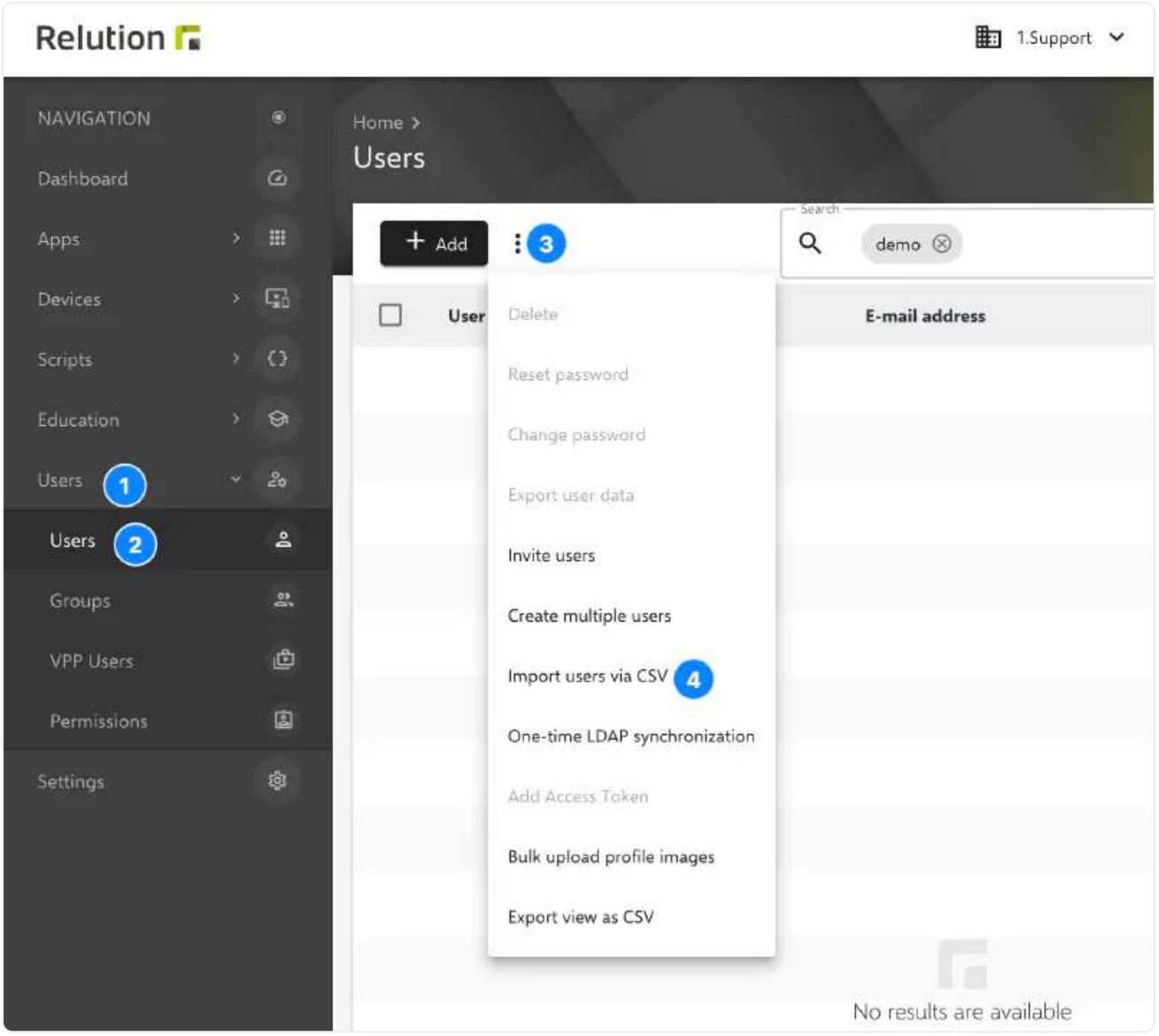
Les appartenances d’un utilisateur peuvent également être gérées directement dans les détails de l’utilisateur, dans la zone Adhésions directes sous Groupes et autorisations, via Gérer les groupes.

Pour la version 26.4.0

Import CSV

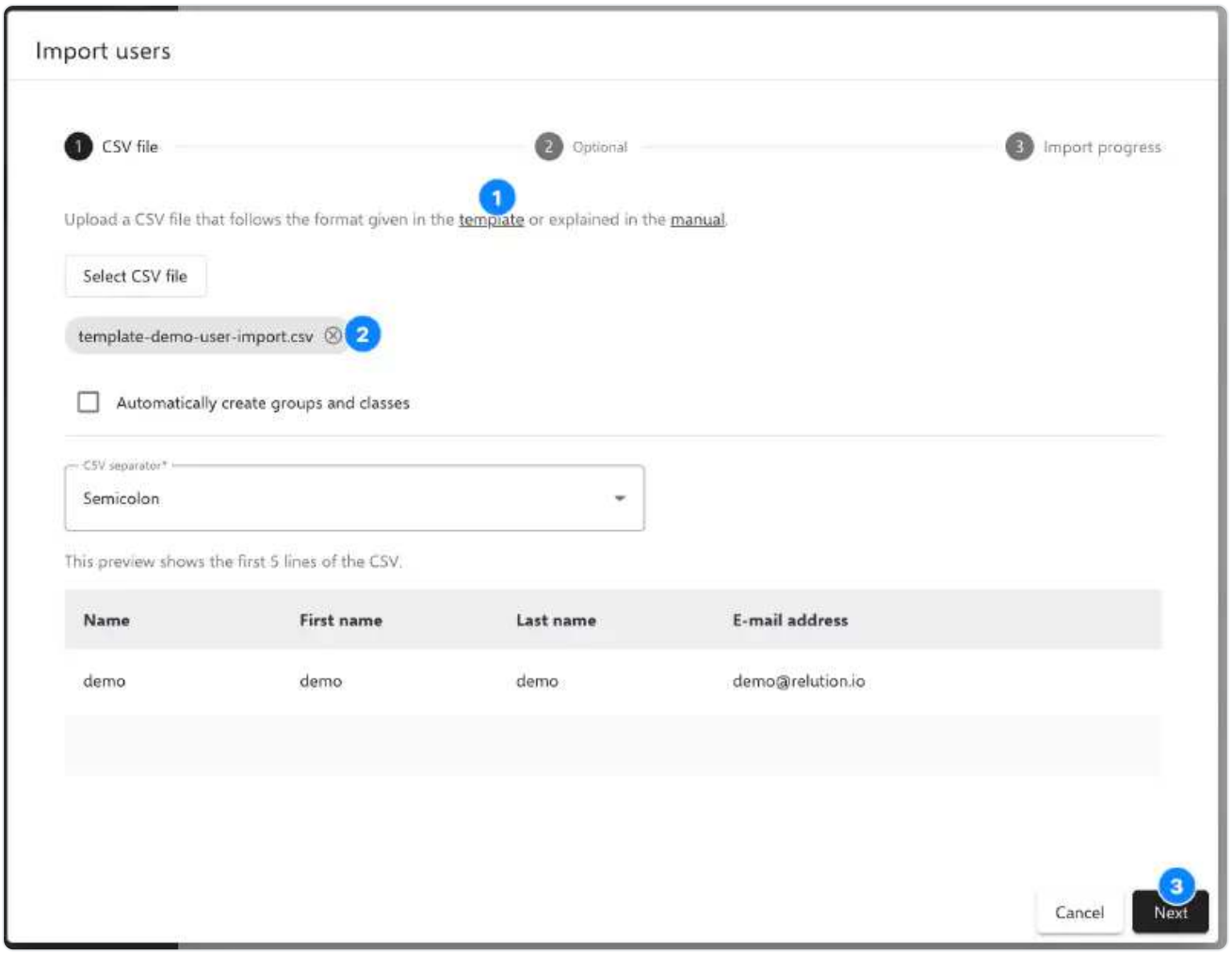
Pour gérer efficacement un grand nombre d'utilisateurs, la fonction d'import via un fichier CSV peut être utilisée. Elle nécessite les autorisations de créer et de modifier des utilisateurs. Les étapes suivantes sont nécessaires :

1. Accéder au menu : l'élément de navigation Utilisateurs est ouvert dans Relution.
2. Lancer l'import : dans le menu 3 points, Importer des utilisateurs via CSV lance l'import.



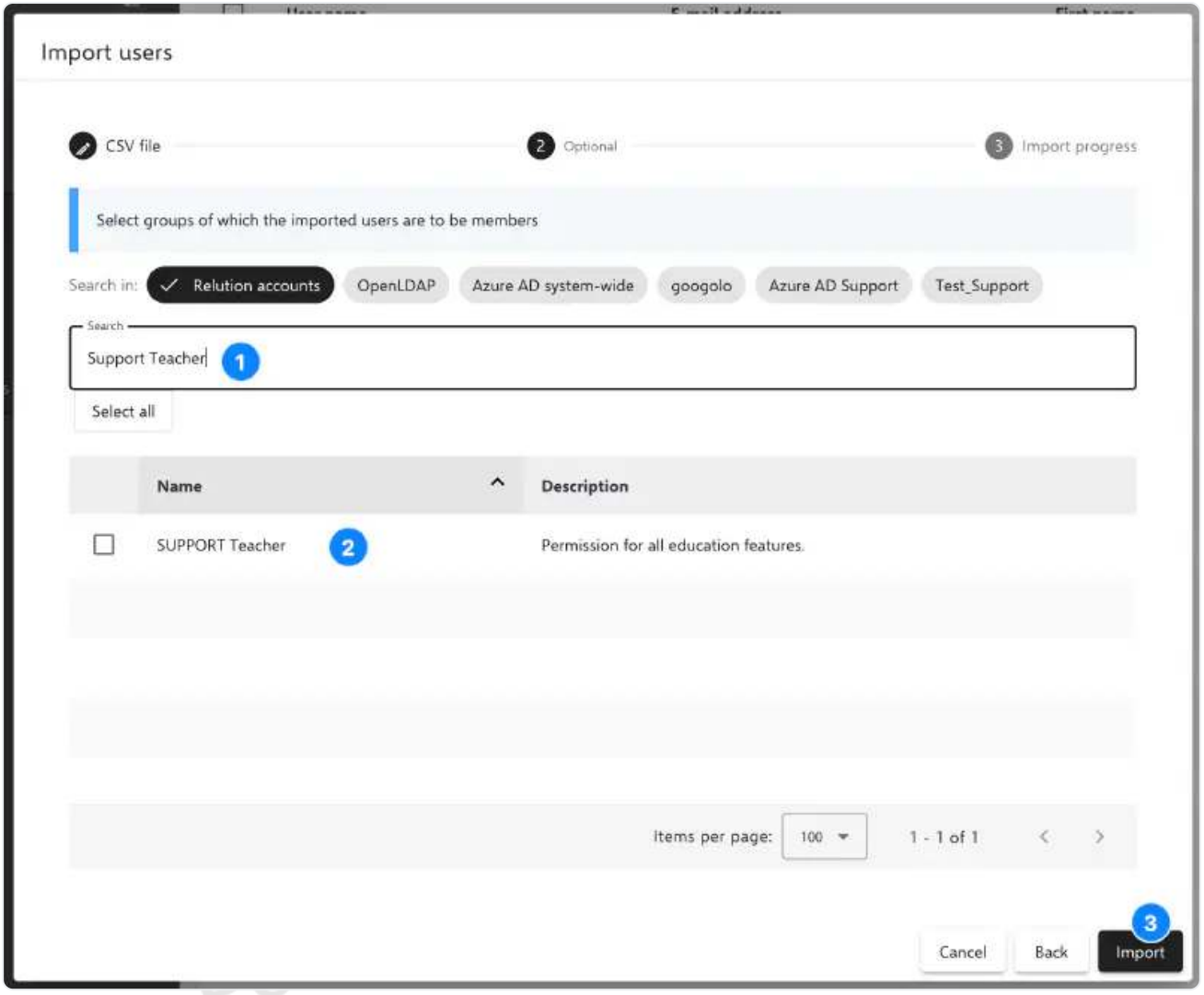
3. Utiliser le modèle : le modèle CSV fourni est téléchargé. Il utilise le séparateur choisi dans le champ Séparateur CSV (Virgule ou point-virgule) et contient les colonnes `name`, `email`, `givenName`, `surname`, `password`, `disablePasswordAuthentication`, `phone`, `position`, `country`, `managedAppleId`, `locale`, `permissions`, `memberOfGroups`, `teacherOfClasses` et `studentOfClasses`.

4. Modifier les données : le fichier est ouvert dans un éditeur au choix et les valeurs requises sont saisies.
5. Téléverser le fichier : le fichier CSV modifié est téléversé dans Relution à l'étape Fichier CSV. Cette étape contient également l'option Créer automatiquement des groupes et des classes (voir ci-dessous).
6. Vérification : l'aperçu affiche les 5 premières lignes pour contrôle.

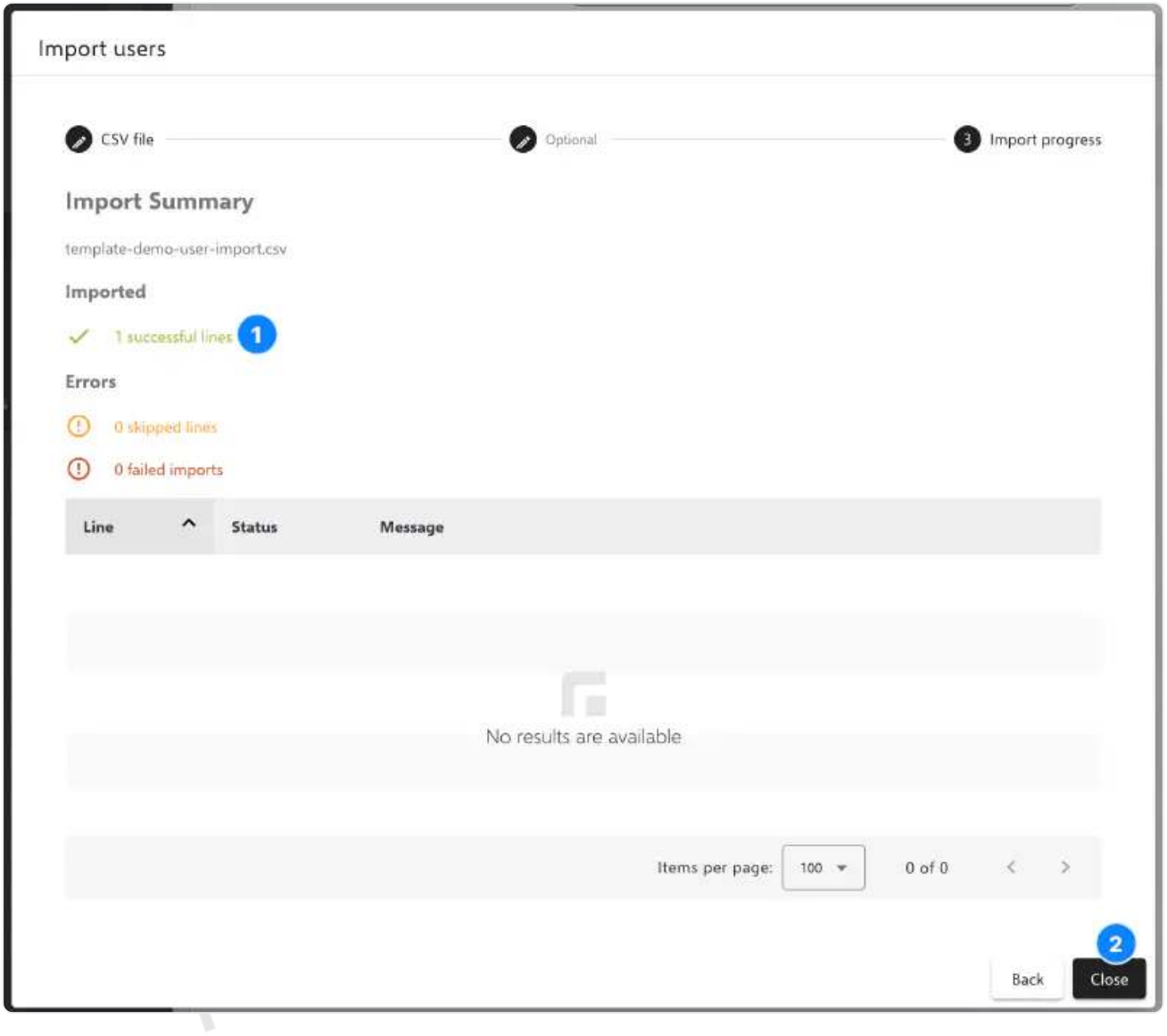


7. Attribution (facultatif) : les utilisateurs peuvent être ajoutés directement à des groupes existants au cours de ce processus. Cette étape n'est affichée qu'avec l'autorisation de lire

les groupes.



8. Finalisation : la progression de l'import affiche l'état actuel. Le résumé distingue les lignes réussies, ignorées et en échec et indique le message correspondant à chaque ligne.



Important

- Politique de mots de passe : si des mots de passe fixes sont définis, ils doivent respecter la politique de mots de passe de l'organisation concernée. Si, par exemple, la politique exige au moins 8 caractères, l'import échoue pour tous les utilisateurs dont le mot de passe est plus court.
- Attribution aux classes : les enseignants et les élèves sont attribués aux classes via les colonnes `teacherOfClasses` et `studentOfClasses`. Plusieurs classes dans une même cellule sont séparées par `|`. L'appartenance à un groupe (par exemple `UIT Teacher`) n'attribue personne à une classe. Une classe n'est enregistrée que si elle compte ensuite au moins un enseignant et au moins un élève ; pour les classes existantes, les membres actuels sont pris en compte. Dans le cas contraire, cette classe est indiquée comme ignorée dans le rapport d'import, les utilisateurs eux-mêmes étant tout de même importés. Une classe qui n'existe pas encore n'est créée que si l'option Créer automatiquement des groupes et des classes est activée ; sinon, la ligne est signalée comme en échec.

- Attribution aux groupes : les groupes (par exemple les groupes système `UIT Teacher` et `UIT Student`) sont attribués via la colonne `memberOfGroups`, les permissions de `Utilisateurs` → `Permissions` (par exemple `Self service portal - read access`) via la colonne `permissions`. Le nom exact est déterminant. Les groupes système de l'organisation portent son nom unique comme préfixe, par exemple `UIT Teacher` ; les groupes créés manuellement sont indiqués avec leur propre nom. Si le nom d'une permission figure dans `memberOfGroups`, l'import échoue pour cette ligne avec un message indiquant que le groupe est introuvable ; si Créer automatiquement des groupes et des classes est activé, un nouveau groupe vide portant ce nom est créé à la place.
- Mise à jour des utilisateurs existants : l'import CSV peut également être utilisé pour des comptes utilisateurs déjà existants. Les comptes correspondants sont identifiés par la colonne `name` (nom d'utilisateur) au sein de la même organisation et mis à jour avec les valeurs du fichier CSV, plutôt que créés en double. L'adresse e-mail n'intervient pas dans cette correspondance. Les utilisateurs gérés par un fournisseur externe (par exemple un service d'annuaire) sont ignorés. Les utilisateurs importés sont toujours activés.
- Colonnes vides lors d'une mise à jour : si une colonne existe dans le fichier CSV mais que sa valeur est vide pour une ligne donnée, le champ correspondant de l'utilisateur existant est vidé. Les colonnes `permissions`, `memberOfGroups`, `teacherOfClasses` et `studentOfClasses` font exception : une cellule vide laisse les attributions existantes inchangées. Une valeur renseignée remplace en revanche entièrement les attributions précédentes ; les permissions et groupes non listés sont retirés, de même que les classes non listées dans lesquelles l'utilisateur est inscrit comme enseignant ou élève. Les groupes sélectionnés en plus dans la boîte de dialogue d'import sont ajoutés dans tous les cas. Pour toutes les autres colonnes : les colonnes dont les valeurs existantes doivent rester inchangées doivent être entièrement supprimées du fichier CSV plutôt que simplement laissées vides.
- Mot de passe lors d'une mise à jour : si la colonne `password` est vide ou absente pour un utilisateur déjà existant, son mot de passe actuel reste inchangé. Pour les utilisateurs nouvellement créés sans mot de passe indiqué, aucun mot de passe n'est généré automatiquement ; un premier mot de passe doit alors leur être attribué séparément.
- Connexion uniquement via SSO : la colonne `disablePasswordAuthentication` ne s'applique qu'à la création d'un utilisateur ; lors d'une mise à jour, la valeur précédente est conservée.

Comportement en pratique

Quelques exemples concrets pour la mise à jour d'utilisateurs existants via le fichier CSV :

- La colonne **`email`** est présente mais laissée vide pour une ligne : l'adresse e-mail existante de l'utilisateur est alors supprimée. Pour qu'elle reste inchangée, la colonne `email` doit être entièrement supprimée du fichier CSV.

Pour la version 26.4.0

- La colonne **`memberOfGroups`** est présente mais laissée vide pour une ligne : les appartenances aux groupes existantes de l'utilisateur restent inchangées. Si la cellule contient en revanche `UIT Teacher`, l'utilisateur n'est ensuite membre que de ce groupe et des groupes sélectionnés dans la boîte de dialogue d'import.
- Comment un utilisateur existant est reconnu lors d'une mise à jour : uniquement via la colonne `name` (nom d'utilisateur) au sein de la même organisation — l'adresse e-mail n'intervient pas dans cette reconnaissance.
- La colonne **`password`** est laissée vide : pour un utilisateur déjà existant, le mot de passe actuel reste inchangé, que la colonne soit absente ou simplement vide. Pour un utilisateur nouvellement créé, aucun mot de passe n'est généré automatiquement dans ce cas.

Par exemple :

- Nom de l'organisation: `Utilisateur-Import-Test`
- Nom unique de l'organisation: `UIT`
- Groupes d'utilisateurs: `UIT Student`, `UIT Teacher`

Un fichier CSV avec un enseignant et un étudiant, auxquels un groupe est attribué via la colonne `memberOfGroups` et la classe `10a` via `teacherOfClasses` ou `studentOfClasses`, se présente par exemple comme suit :

```
name;email;givenName;surname;permissions;memberOfGroups;teacherOfClasses;stude
enseignant1;enseignant1@uit-ecole.fr;Léa;Enseignant;;UIT Teacher;10a;
etudiant1;etudiant1@uit-ecole.fr;Sam;Etudiant;;UIT Student;;10a
```

Plusieurs groupes, permissions ou classes au sein d'une même cellule sont séparés par une barre verticale (`|`), par exemple `UIT Teacher|UIT Student`. Cela s'applique aux colonnes `memberOfGroups`, `permissions`, `teacherOfClasses` et `studentOfClasses`. Un point-virgule peut également servir de séparateur au sein de la cellule ; toutefois, comme celui-ci sépare potentiellement déjà les colonnes elles-mêmes selon le Séparateur CSV choisi, l'utilisation de `|` est recommandée pour éviter toute ambiguïté. Une virgule ne sépare pas les valeurs au sein d'une cellule.

Création automatique de groupes et de classes inexistants

Les classes et les groupes d'utilisateurs inexistants peuvent être créés automatiquement lors de l'import CSV. Pour cela, l'option Créer automatiquement des groupes et des classes doit être

activée à la première étape (Fichier CSV). L'option est désactivée par défaut et ne peut être activée qu'avec les autorisations de créer des groupes et des classes. Sans cette option, les lignes contenant des groupes ou des classes inexistants sont signalées comme en échec. Les permissions de la colonne `permissions` ne sont jamais créées automatiquement ; elles doivent déjà exister. Les points suivants s'appliquent :

- Précision : l'orthographe exacte du nom est déterminante ; une orthographe différente entraîne la création d'un nouveau groupe ou d'une nouvelle classe.
- Espaces : les espaces en début et en fin de noms de groupes, de classes et de permissions sont supprimés automatiquement lors de l'import.
- Classes gérées : les classes synchronisées par un fournisseur externe sont ignorées lors de l'import.

Causes fréquentes d'un import en échec

Une cause fréquente d'un échec de l'import CSV est une adresse e-mail déjà attribuée à un autre compte utilisateur sur le serveur. Les adresses e-mail doivent être uniques sur l'ensemble du serveur, quelle que soit l'organisation à laquelle appartient l'utilisateur concerné.

Pour la version 26.4.0

Fonction d'éducation

La fonction éducative innovante de Relution facilite la préparation des cours en les intégrant de manière transparente dans l'application Relution Teacher. Cette fonction permet aux enseignants de démarrer et de gérer facilement des classes. Les classes Relution sont composées d'enseignants et d'étudiants, chacun disposant de permissions spécifiques. La structure claire et l'interface conviviale de la plateforme Relution rendent l'organisation et le déroulement des cours plus efficaces. Pour plus d'informations sur la fonction éducative et les autres fonctionnalités de Relution, consulter le site web Relution à l'adresse suivante : www.relution.io.

> L'élément de menu Éducation n'est affiché que dans les organisations disposant d'une licence Education ou Free valide. Il contient les entrées Classes et Relution Teacher ; Relution Teacher ouvre directement l'application web Teacher.

Créer un utilisateur

De nouveaux utilisateurs sont créés dans l'élément de menu Utilisateurs et se voient attribuer les autorisations correspondantes. Les méthodes de création disponibles (création manuelle, import CSV, synchronisation LDAP) ainsi que la règle relative à l'unicité de l'adresse e-mail sont décrites dans l'article sur la gestion des utilisateurs.

Pour la version 26.4.0

Gestion des utilisateurs →

Attribuer des autorisations

Dans l'élément de menu `Utilisateurs` → `Groupes`, il est possible d'assigner des groupes aux utilisateurs existants. Deux groupes standard importants sont déjà enregistrés : `<ORGANISATION> Teacher` (enseignants) et `<ORGANISATION> Student` (élèves). Le nom du groupe commence par le nom unique de l'organisation en majuscules, par exemple `ECOLE Teacher`. Ces groupes ne sont pas créés dans l'organisation système.

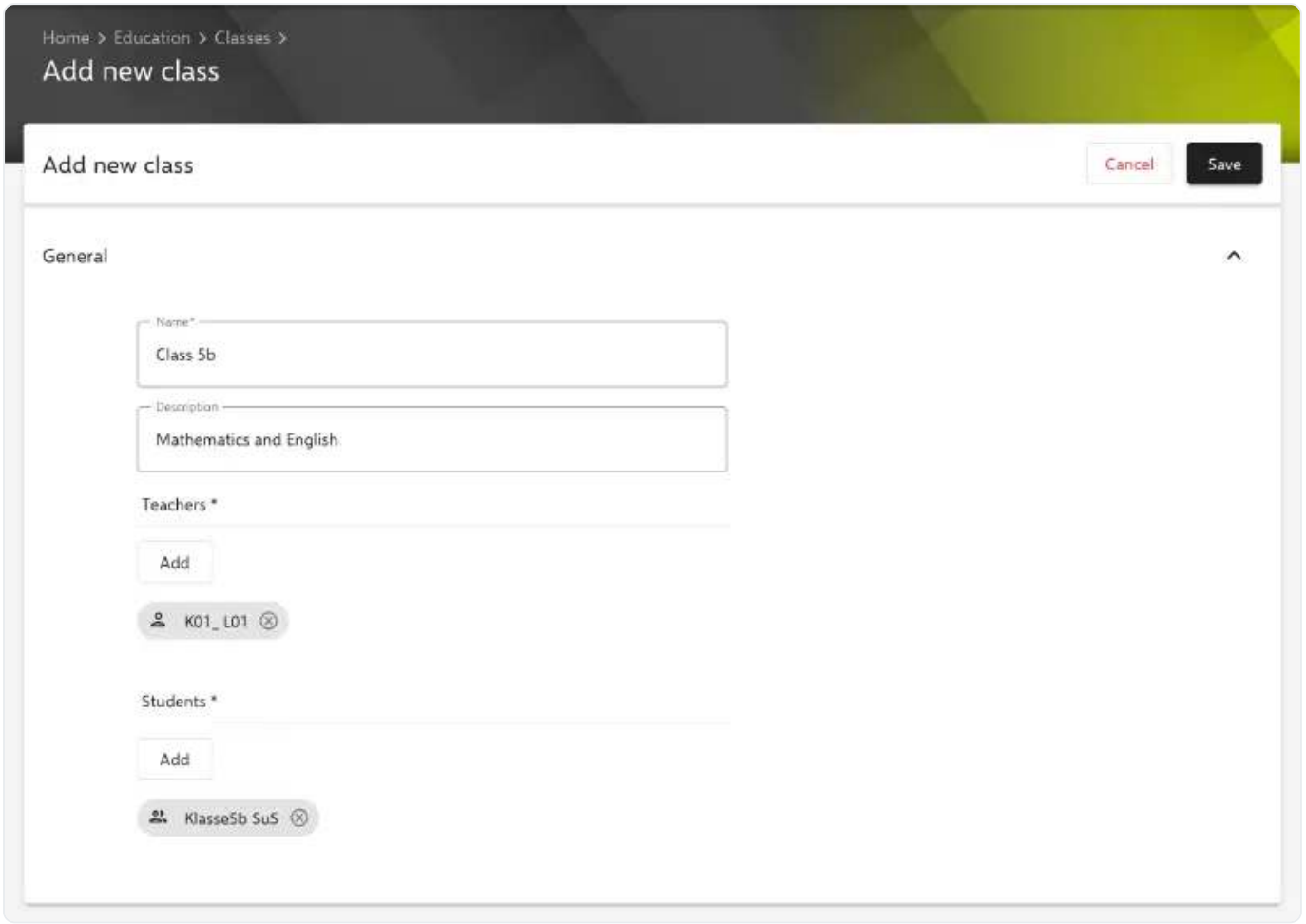
Les deux groupes se distinguent à la fois par leurs droits et par l'étendue de leurs fonctions. Par exemple, le démarrage d'une leçon via l'application Relution Teacher est réservé au groupe Teacher ; les élèves (groupe Student) ne disposent pas de ce droit. Les groupes système `Device Manager` et `Appstore Manager`, et donc aussi `Administrator`, sont membres du groupe Teacher et en héritent les droits. Cette distinction claire facilite la gestion des utilisateurs

et garantit que les droits sont attribués en fonction des tâches et des responsabilités respectives.

Si plusieurs comptes utilisateurs doivent recevoir `Teacher` ou `Student` en même temps, l'attribution peut également se faire directement lors de l'import CSV, voir Import CSV →.

Créer des classes

Dans l'élément de menu `Éducation` → `Classes`, il est possible de créer des classes manuellement et de les assigner à des utilisateurs en fonction de leur rôle. Le Nom est obligatoire ; dans l'organisation globale, l'organisation cible est également sélectionnée. Les enseignants et les élèves peuvent être attribués en tant qu'utilisateurs individuels ou en tant que groupes entiers. Il convient de noter qu'une classe doit être composée d'au moins un enseignant et d'un étudiant (chacun en tant qu'utilisateur ou groupe) pour être créée correctement.



Pour une administration efficace, il est possible de créer rapidement et facilement plusieurs classes à l'aide de la fonction d'import CSV. La synchronisation des classes depuis un système externe constitue toutefois la solution la plus pratique, car elle permet une mise à jour

automatique et une gestion uniforme des classes. Outre LDAP, les interfaces suivantes sont disponibles à cet effet :

- Import SchulConnex →
- Interface OneRoster → (par exemple pour Untis/WebUntis)
- Importation Apple School Manager →

Les classes synchronisées via une telle interface sont en lecture seule dans le portail et sont gérées exclusivement dans le système source.

Utilisation avec Relution Teacher et/ou Apple Classroom

Les classes créées peuvent être facilement préparées pour l'enseignement en utilisant l'application Relution Teacher. Plus de détails sur ce processus sont disponibles dans l'article sur l'application Relution Teacher.

Teacher →

Pour contrôler les appareils pendant les cours, il est également possible d'utiliser l'application Apple Classroom. Plus d'informations sont disponibles dans l'article sur l'application Apple Classroom.

Apple Classroom →

En résumé, on peut dire que l'application Relution Teacher est utilisée pour préparer les cours, tandis que l'application Apple Classroom permet de les contrôler pendant la leçon.

Pour la version 26.4.0

Permissions

Relution permet de configurer les permissions de manière très précise et granulaire. Cela permet de créer un ensemble de permissions spécifique pour chaque cas d'utilisation, sans fournir aux utilisateurs plus de fonctionnalités que nécessaire.

Une permission peut également imposer l'authentification multi-facteurs (MFA) à tous les utilisateurs qui la possèdent. De plus, les permissions peuvent être rendues disponibles dans toutes les organisations depuis l'organisation globale, et dans toutes les sous-organisations depuis une organisation méta.

Vue d'ensemble des permissions

Dans `Utilisateurs` → `Permissions`, des permissions par défaut sont déjà disponibles, par exemple Administrator, Teacher ou Student. Elles s'appliquent globalement à toutes les organisations, correspondent aux groupes système et sont liées à ceux-ci. Dans la liste, elles sont signalées dans la colonne Système. Ces permissions par défaut sont gérées automatiquement et ne peuvent être ni modifiées, ni supprimées, ni exportées.

Cependant, il est toujours possible de créer de nouvelles permissions personnalisées.

> Les permissions sont additives, ce qui signifie que toutes les permissions attribuées à un compte utilisateur sont combinées.

Pour la version 26.4.0

Configuration des permissions

Dans la catégorie Permissions, un nouvel élément peut être créé en cliquant sur Ajouter. Le Nom est obligatoire (255 caractères maximum) ; une Description (4000 caractères maximum) est facultative. Presque toutes les fonctions disponibles dans le portail Relution peuvent être attribuées individuellement.

En général, quatre options sont disponibles : Lire, Créer, Mettre à jour, Supprimer. Si une option en requiert une autre, celle-ci est activée automatiquement et verrouillée ; par exemple, Créer requiert Lire.

Par exemple, un utilisateur peut se voir attribuer un compte avec des permissions en lecture seule, l'empêchant d'effectuer des modifications dans le système.

Les actions sur les appareils peuvent également être configurées individuellement.

- Exemple : toutes les actions sont autorisées sauf le suivi de localisation des appareils.
- Autre cas d'usage : un utilisateur peut uniquement renouveler les tokens pour Apps et livres (VPP dans le portail) et pour l'Inscription automatisée des appareils (ADE, DEP dans le portail), sans pouvoir effectuer d'autres modifications. Pour Apps et livres, l'option Mettre à jour de l'entrée Programme d'achat en volume (VPP) est nécessaire ; pour ADE, l'option Créer de l'entrée Inscription automatique des appareils Apple. Il n'existe pas d'option Mettre à jour pour ADE ; avec Créer, l'utilisateur peut aussi ajouter de nouveaux comptes serveur ADE.

Imposer l'authentification multi-facteurs

Avec l'option Appliquer l'authentification multifactorielle pour le rôle, tous les utilisateurs disposant de cette permission doivent se connecter via MFA. La section Authentification multi-facteurs n'apparaît que si au moins une méthode MFA est activée sous `Paramètres` → `Gestion des connexions`. Les permissions par défaut ne pouvant pas être modifiées, une permission personnalisée est nécessaire. Plus de détails dans l'article Authentification multifactorielle →.

Portée

Pour la version 26.4.0

La colonne Portée indique où une permission s'applique : Locale (uniquement dans la propre organisation), Meta (dans toutes les sous-organisations d'une organisation méta) ou Mondial (dans toutes les organisations). Les nouvelles permissions sont créées localement.

Dans l'organisation globale, l'entrée de menu contextuel Définir la visibilité comme globale rend les permissions sélectionnées disponibles dans toutes les organisations ; dans une organisation méta, l'entrée Définir la visibilité à méta les rend disponibles dans toutes les sous-organisations. La permission n'est ainsi attribuée à personne ; elle devient seulement sélectionnable.

Exportation et importation des permissions

Via le menu contextuel de la liste, les permissions sélectionnées peuvent être exportées dans un fichier JSON (entrée Autorisations d'exportation) puis réimportées (entrée Autorisations d'importation), par exemple dans une autre organisation. Les permissions importées sont toujours créées localement. Les permissions par défaut ne peuvent pas être exportées.

Association des permissions aux comptes utilisateurs

Dans le compte utilisateur, une permission est attribuée dans la zone Adhésions directes sous Groupes et autorisations : le bouton Gérer les autorisations du champ Permissions ouvre la sélection.

Les permissions peuvent également être attribuées à un groupe de la même manière. Tous les membres du groupe les reçoivent alors, y compris via des groupes imbriqués.

Attribution des permissions lors de l'import CSV

Les permissions peuvent également être attribuées lors de la création de plusieurs comptes utilisateurs via l'import CSV. Le déroulement de l'import est décrit dans l'article Import CSV →.

L'attribution peut se faire de trois manières :

- Dans la colonne `permissions` du modèle CSV, les permissions sont renseignées par ligne avec leur nom exact, par exemple `Teacher` ou `Student`. Plusieurs entrées sont séparées par `|`.
- Dans la colonne `memberOfGroups`, les groupes sont renseignés avec leur nom exact, par exemple le groupe système `[Organisation] Teacher`. Le compte utilisateur reçoit les permissions du groupe via son appartenance au groupe.
- Dans l'étape optionnelle Groupes de la boîte de dialogue d'import, un ou plusieurs groupes existants sont sélectionnés. Tous les comptes utilisateurs importés en deviennent membres, en plus des groupes indiqués dans `memberOfGroups`. Cette étape n'est affichée qu'avec le droit de lecture sur les groupes.

Un nom inconnu dans `permissions` empêche l'import de la ligne concernée. Il en va de même pour `memberOfGroups`, sauf si l'option Créer automatiquement des groupes et des classes est activée ; dans ce cas, un nouveau groupe vide sans permissions est créé.

> Les noms des groupes système incluent le nom unique de l'organisation concernée, par exemple [Organisation] Teacher ou [Organisation] Student. Les permissions par défaut correspondantes s'appellent en revanche simplement Teacher, Student, etc.

Pour la version 26.4.0

Portail libre-service

Depuis la version 5.22, Relution dispose d'un portail en libre-service. Les utilisateurs de Relution peuvent y consulter leurs propres appareils, effectuer des actions individuelles et demander des détails.

Exigences

Deux permissions par défaut sont disponibles pour utiliser le portail en libre-service. Elles sont créées automatiquement lors d'une mise à jour vers Relution 5.22 ou lors de la création de la base de données. Pour mettre le portail libre-service à la disposition des utilisateurs, ceux-ci doivent avoir l'autorisation appropriée et avoir lié au moins un appareil à leur compte d'utilisateur.

Octroi de l'autorisation

Pour la version 26.4.0

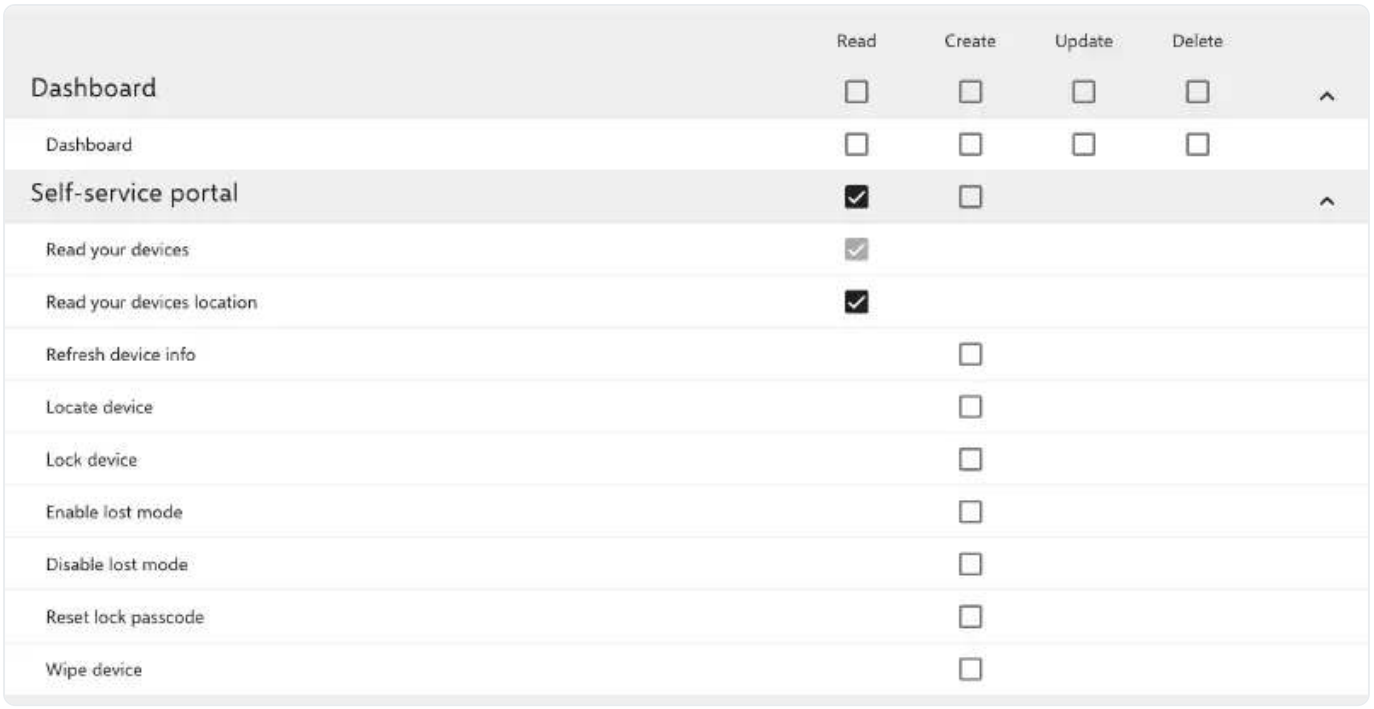
Sous `Utilisateurs` → `Permissions`, `Self service portal - full access` et `Self service portal - read access` sont disponibles comme modèles. En fonction des besoins, ils doivent être liés aux comptes souhaités.

- `Self service portal - read access` permet uniquement de consulter ses propres appareils et d'en actualiser les informations.
- `Self service portal - full access` permet en outre de lire la position, de localiser l'appareil, d'activer et de désactiver le mode perdu, de verrouiller l'appareil, de réinitialiser le code de verrouillage ainsi que d'effacer ou de supprimer l'appareil.

Pour les permissions personnalisées, les droits sont disponibles individuellement dans la catégorie Portail en libre-service, par exemple la lecture de ses propres appareils (Lisez vos appareils), Lire la localisation de vos appareils et un droit distinct pour chaque action.

L'attribution s'effectue comme suit :

1. Sous `Utilisateurs` → `Utilisateurs`, le compte utilisateur concerné est ouvert.
2. Dans la zone Adhésions directes, sous Groupes et autorisations, le bouton Gérer les autorisations du champ Permissions ouvre la sélection.
3. L'une des permissions ci-dessus y est sélectionnée.
4. Enregistrer applique l'attribution.



Lier un appareil au compte utilisateur

Un compte d'utilisateur peut être lié à un appareil soit en important un fichier CSV, soit en configurant l'inscription en conséquence avant l'inscription, soit manuellement.

Pour la méthode manuelle, il suffit de sélectionner l'appareil dans l'inventaire et de sélectionner l'icône Changer d'utilisateur d'appareil dans la barre d'outils.

Pour la version 26.4.0

Le portail libre-service

Lorsqu'une personne se connecte au portail Relution à l'aide du compte utilisateur correspondant, la fonction en libre-service est alors accessible. Les utilisateurs qui ne disposent que de droits libre-service arrivent directement sur la page Vos appareils après la connexion ; les administrateurs y accèdent via le menu de profil en haut à droite.

Depuis Relution 26.5.0, la connexion au portail libre-service passe par une portée dédiée (`/api/selfService/`). Si elle s'effectue via OpenID Connect avec des URI de redirection scopées, l'URI de redirection correspondante doit être enregistrée auprès du fournisseur d'identité, voir OIDC avec Entra → ou OIDC avec Workspace →.

Pour chaque appareil, des informations de base sont affichées, par exemple l'état de la batterie, le statut, la dernière connexion, la plate-forme, le propriétaire, le modèle, le numéro de série, le

système d'exploitation, la date d'inscription et l'état du mode perdu. Les fonctions suivantes sont également disponibles :

- Activer / désactiver le mode perdu
- Localiser l'appareil
- Afficher la position sur une carte
- Effacer l'appareil
- Verrouiller l'appareil
- Réinitialiser le code de verrouillage

Effacer l'appareil ouvre la boîte de dialogue Supprimer, qui permet de choisir entre la réinitialisation aux paramètres d'usine et la suppression de l'appareil du MDM (Supprimer). Le bouton Actualiser les informations sur tous les appareils visibles de la page Vos appareils interroge à nouveau les informations de tous les appareils affichés ; par défaut, une nouvelle interrogation n'est possible qu'au plus tôt 5 minutes après la dernière actualisation.

Les fonctions disponibles peuvent varier en fonction de la plate-forme de l'appareil. Sur les appareils iOS, le mode perdu et la localisation ne sont disponibles que sur les appareils supervisés, la localisation en outre uniquement lorsque le mode perdu est activé. Pendant la suppression ou le retrait d'un appareil, les actions sont verrouillées. Les fonctions peuvent également être limitées par des permissions.

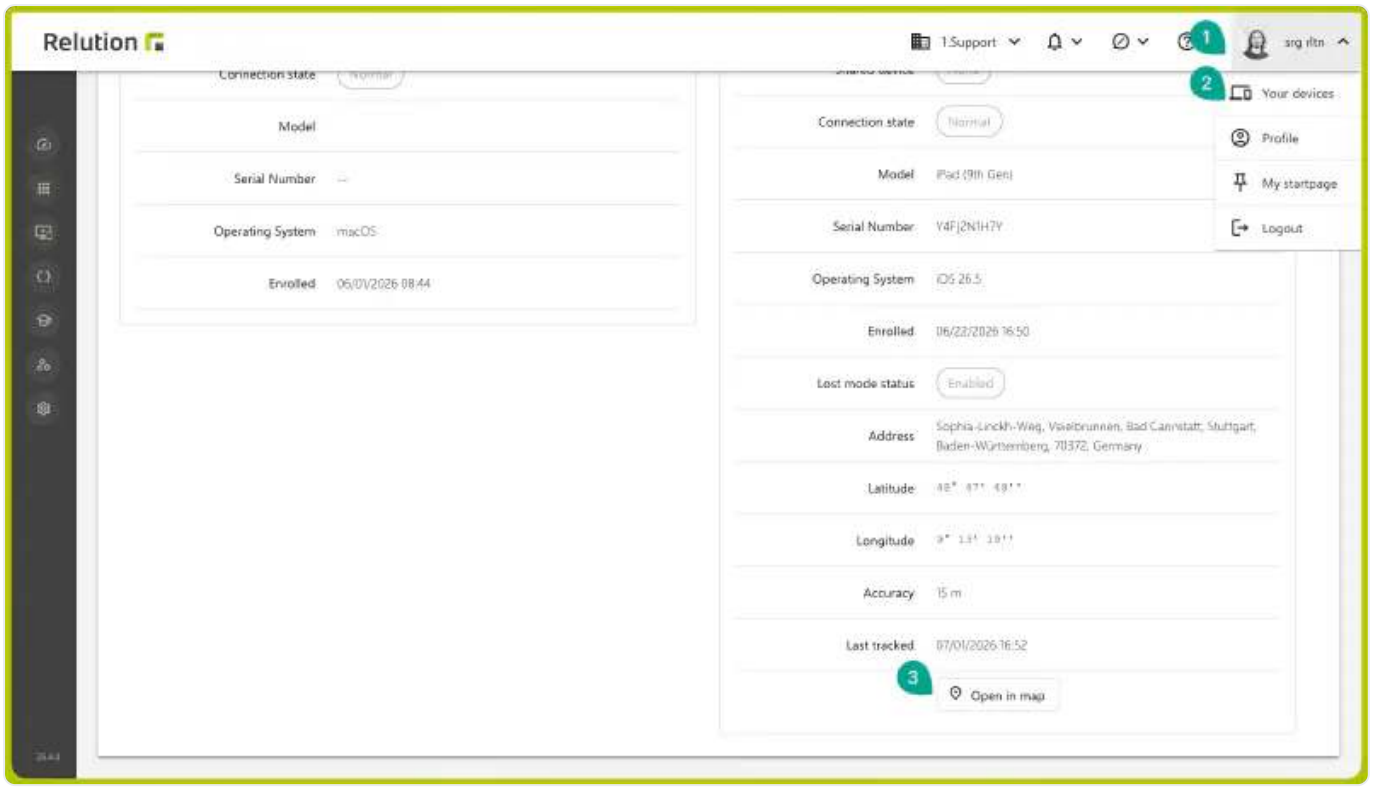
Pour la version 26.4.0

Afficher la position sur une carte

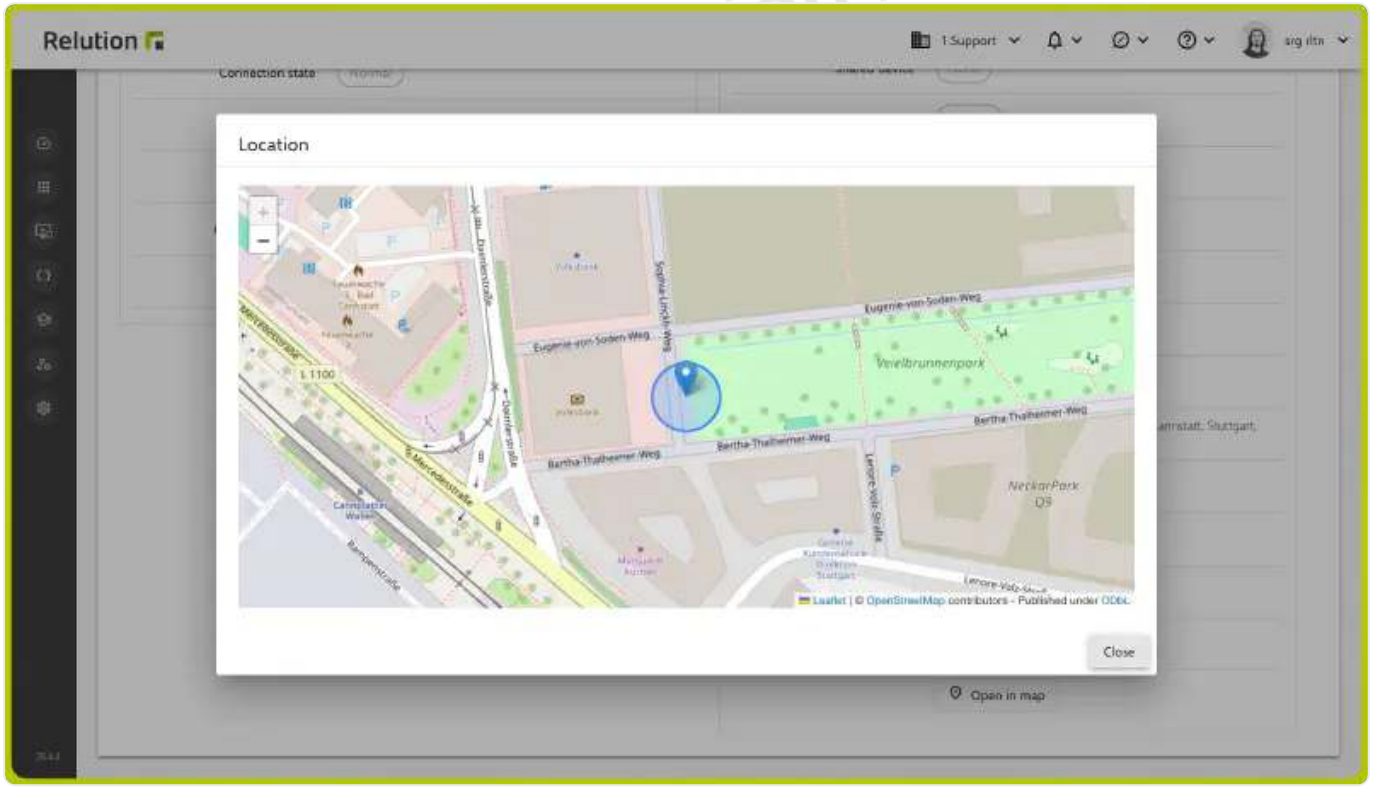
Nouveau dans 26.4

Les utilisateurs autorisés peuvent afficher directement sur une carte la dernière position connue de leur appareil.

1. L'icône de profil en haut à droite ouvre Vos appareils.
2. Dans l'appareil concerné, Ouvrir dans la carte dans la section de localisation ouvre la carte.



La dernière position connue est alors affichée sur une vue cartographique.



La permission Lire la localisation de vos appareils est requise. Elle est incluse dans `Self service portal - full access`, mais pas dans `Self service portal - read access`. En son absence, la section de localisation n'est pas affichée. La section de localisation est

disponible pour les appareils iOS, Android (y compris Android Enterprise) et Windows ; sur les appareils iOS, uniquement si l'appareil est supervisé et que le mode perdu est activé. Aucune position n'est affichée pour les appareils macOS et ChromeOS.

Pour les appareils Android Enterprise, l'activation des services de localisation ainsi que l'autorisation correspondante du compagnon Relution sont également nécessaires, voir Localiser un appareil Android → et Services de localisation →.

Pour la version 26.4.0

Espaces réservés avancés

Les espaces réservés tels que `${user.email}` ou `${device.model}` sont utilisés à plusieurs endroits dans Relution, notamment pour les noms d'appareils, les certificats, les comptes Exchange ou les configurations d'applications. Le moteur de modèles sous-jacent `FreeMarker` met à disposition des fonctions supplémentaires permettant d'adapter davantage les espaces réservés.

Sous-chaînes (substring)

La notation `[début..*longueur]` permet de n'utiliser qu'un extrait d'une valeur : au plus `longueur` caractères à partir de la position `début`. Le décompte commence à `0`. Si la valeur est plus courte, moins de caractères sont insérés ; si elle est vide, aucun. Cela suppose que `début` ne se situe pas au-delà de la fin de la valeur ; sinon, la substitution échoue comme avec `[début..fin]` (voir la remarque ci-dessous).

- `${user.givenName[0..*1]}` → première lettre du prénom
- `${device.model[0..*2]}` → deux premiers caractères du modèle d'appareil

Exemple : `${user.givenName[0..*1]}${user.surname[0..*1]}-${device.model[0..*2]}-${(device.custom1)!"00000"}` donne, pour un compte utilisateur « Max Mustermann » avec une valeur `custom1` de `00042` sur un `iPad12,1`, le résultat `MM-iP-00042`.

> La notation alternative `[début..fin]` (par exemple `[0..0]`) suppose que la valeur s'étende au moins jusqu'à la position `fin`. Si la valeur est définie mais plus courte ou vide, la substitution échoue et aucun des espaces réservés du texte concerné n'est remplacé. Il en va de même pour `[début..*longueur]` si `début` est supérieur à la longueur de la valeur.

Valeur par défaut pour un champ non défini

Si un champ n'est pas défini, l'opérateur `!` permet de définir une valeur par défaut : `${(device.custom1)!"00000"}`. Si le champ personnalisé `custom1` n'est pas défini, `00000` est utilisé à la place, au lieu que l'espace réservé reste vide. Une valeur définie mais vide est en

Pour la version 26.4.0

revanche considérée comme présente : la valeur par défaut ne s'applique pas et l'espace réservé reste vide.

Casse et remplacement de caractères

`?lower_case` et `?upper_case` convertissent intégralement une valeur en minuscules ou en majuscules. `?replace("ancien", "nouveau")` permet de remplacer des caractères ou des chaînes de caractères, par exemple pour convertir les trémas destinés à des systèmes qui n'acceptent pas de caractères spéciaux dans le nom d'utilisateur :

```
${user.surname?lower_case?replace("ä","ae")?replace("ö","oe")?replace("ü","ue")?replace("ß","ss")}
```

> Cette fonction est particulièrement pertinente pour les inscriptions macOS avec authentification de l'utilisateur, car des caractères spéciaux dans le nom de compte local peuvent faire échouer les déploiements de scripts.

Utiliser la partie locale d'une adresse e-mail

Pour n'utiliser que la partie située avant le caractère `@` de `${user.name}` (ou `${user.email}`), plusieurs variantes sont disponibles :

- `${user.name?keep_before("@")}`
- `${user.name?split("@")[0]}`
- `${user.name[0..user.name?index_of("@")-1]}`

Si la valeur ne contient pas de `@`, les deux premières variantes renvoient la valeur complète, tandis que la troisième échoue. `?keep_before` est donc recommandé.

Certificats utilisateur

Nouveau dans 26.5

Les espaces réservés de la forme `${user.certificate.…}` insèrent les certificats enregistrés dans le profil utilisateur (section Certificats utilisateur) dans une configuration, sous forme de chaîne encodée en base64 — par exemple dans une configuration d'application gérée dont les

Pour la version 26.4.0

champs attendent un certificat en base64. L'espace réservé est résolu lors de la transmission de la configuration, à partir de l'utilisateur affecté à l'appareil concerné.

Trois formes de sélection sont disponibles :

Espace réservé	Résolution
`${user.certificate.EXCHANGE}`	certificat du sous-type ayant la durée de validité restante la plus longue
`${user.certificate.EXCHANGE["mon-certificat"]}`	certificat portant exactement ce nom (sensible à la casse) ; s'il y en a plusieurs du même nom, celui ayant la durée de validité restante la plus longue
`${user.certificate.EXCHANGE[device.serialnumber]}`	le nom du certificat est calculé à partir d'un autre espace réservé

Pour la ve

Le sous-type correspond à la Catégorie sélectionnée pour le certificat dans le profil utilisateur. Le sous-type n'est pas sensible à la casse.

Catégorie dans le profil utilisateur	Sous-type
Certificat général	`GENERAL_CERTIFICATE`
Wi-Fi	`WIFI`
Exchange	`EXCHANGE`
VPN et applications	`VPN`
Cryptage S/MIME	`SMIME_ENCRYPTION`
Signature S/MIME	`SMIME_SIGNING`

Nom de certificat entre crochets

Pour les noms calculés, l'espace réservé interne s'écrit sans `${…}` englobant, donc `[device.serialnumber]` et non `[${device.serialnumber}]` — les expressions `${…}` imbriquées ne sont pas prises en charge. Pour les noms composés uniquement de lettres, de chiffres et de tirets bas, la forme pointée `${user.certificate.EXCHANGE.iPhone}` fonctionne également.

> Les noms de certificat comportant d'autres caractères (par exemple un tiret ou un espace) doivent être indiqués entre guillemets dans la forme à crochets. Une expression telle que `${user.certificate.EXCHANGE.mon-certificat}` est interprétée comme une opération de calcul et entraîne la livraison de l'ensemble de la configuration sans espaces réservés remplacés.

Mot de passe des certificats PKCS#12

Pour les certificats PKCS#12 protégés par mot de passe (par exemple une identité S/MIME), le mot de passe d'importation est fourni via la clé réservée `password` :

- `${user.certificate.SMIME_SIGNING.password}`
- `${user.certificate.SMIME_SIGNING["mon-certificat"].password}`

Pour les certificats qui ne sont pas des conteneurs PKCS#12, la valeur reste vide. `password` étant une clé réservée, un certificat portant lui-même le nom `password` ne peut pas être sélectionné via un espace réservé — dans ce cas, la forme pointée comme la forme à crochets renvoient le mot de passe. Il convient d'utiliser un autre nom pour de tels certificats.

Format de sortie

Indépendamment du format de fichier téléversé (PEM ou DER), l'espace réservé renvoie toujours la forme DER du certificat encodée en base64. Les conteneurs PKCS#12 sont livrés encodés en base64 sans modification, afin de pouvoir être importés directement par l'application destinataire avec le mot de passe. Les autres types de certificats sont également livrés tels qu'ils sont enregistrés.

Exemple d'une configuration d'application gérée pour un client de messagerie avec signature S/MIME :

Pour la version 26.4.0

```
<key>SMIMECertificate</key>
<string>${user.certificate.SMIME_SIGNING}</string>
<key>SMIMECertificatePassword</key>
<string>${user.certificate.SMIME_SIGNING.password}</string>
```

Disponibilité

Les espaces réservés de certificat utilisateur sont prévus pour les configurations dont le contenu est transmis à l'appareil de l'utilisateur affecté, en particulier les configurations d'applications gérées (iOS/macOS, Android Enterprise), les configurations Knox (Android Enterprise, Samsung KNS), les profils de configuration personnalisés (`.mobileconfig`) et Windows Custom CSP. Dans ces configurations, le portail les affiche également sous Espaces réservés disponibles. Ils ne sont pas résolus (l'espace réservé reste vide) dans les noms d'appareils, c'est-à-dire lors du renommage d'appareils et dans les configurations de nom d'appareil Apple et Windows, dans les messages d'écran de verrouillage et d'assistance, la configuration du compte professionnel et les actions de configuration Android Enterprise, dans les variables d'environnement des scripts ainsi que dans les actions webhook des groupes d'appareils. Ils ne sont pas pris en charge pour les configurations Linux. Dans les profils de configuration personnalisés (`.mobileconfig`), l'espace réservé n'est possible que dans les champs de type string, et non dans les champs de type data ; dans les configurations d'applications gérées, les deux fonctionnent.

Si aucun certificat ne peut être déterminé — par exemple en cas de sous-type inconnu, de nom inexistant ou d'absence d'affectation d'utilisateur —, l'espace réservé reste vide et la configuration est tout de même livrée. Les détails sur la cause sont consignés dans le journal du serveur.

Pour la version 26.4.0

Remarques

> Les noms de fonction et la casse doivent être utilisés exactement tels que décrits. Le portail Relution n'affichant pas d'aperçu de la valeur résolue, il est recommandé de tester la combinaison sur un appareil de test avant de déployer la configuration.

Les espaces réservés de base disponibles dans une configuration donnée (par exemple `${user.email}` , `${device.serialnumber}`) sont affichés dans le formulaire de configuration ou dans la boîte de dialogue concernée, dans la section Espaces réservés disponibles. Un clic sur une entrée la copie dans le presse-papiers.

Les valeurs non définies sont insérées sous forme de chaîne vide. En revanche, si l'évaluation d'une expression échoue — par exemple un extrait `[0..0]` d'une valeur définie mais vide ou un nom de fonction inconnu —, cela ne concerne pas seulement l'espace réservé en question : l'ensemble du texte du champ ou de la configuration est livré tel quel, c'est-à-dire avec toutes les expressions `${…}` non remplacées. La cause est consignée dans le journal du serveur.

Pour la version 26.4.0

Interface OneRoster

À partir de Relution 26.2, l'interface OneRoster est implémentée dans le portail pour les utilisateurs. Cette interface permet la synchronisation des utilisateurs et des classes, par exemple depuis Untis ou WebUntis, avec Relution. La fonctionnalité est accessible via `Paramètres` → `Gestion des utilisateurs` → `OneRoster`.

> Actuellement, Untis/WebUntis ne prend en charge qu'une seule organisation/client dans Relution. Par conséquent, il est recommandé d'intégrer l'interface OneRoster directement dans le client cible. Alternativement, l'interface peut également être intégrée dans l'organisation globale, où les écoles peuvent être mappées via des identifiants. Cependant, cela nécessite le support de l'application de gestion des utilisateurs.

Configuration de l'interface OneRoster

Une nouvelle connexion est créée dans l'aperçu `Paramètres` → `Gestion des utilisateurs` → `OneRoster` via Ajouter.

Pour la version 26.4.0

Paramètres généraux

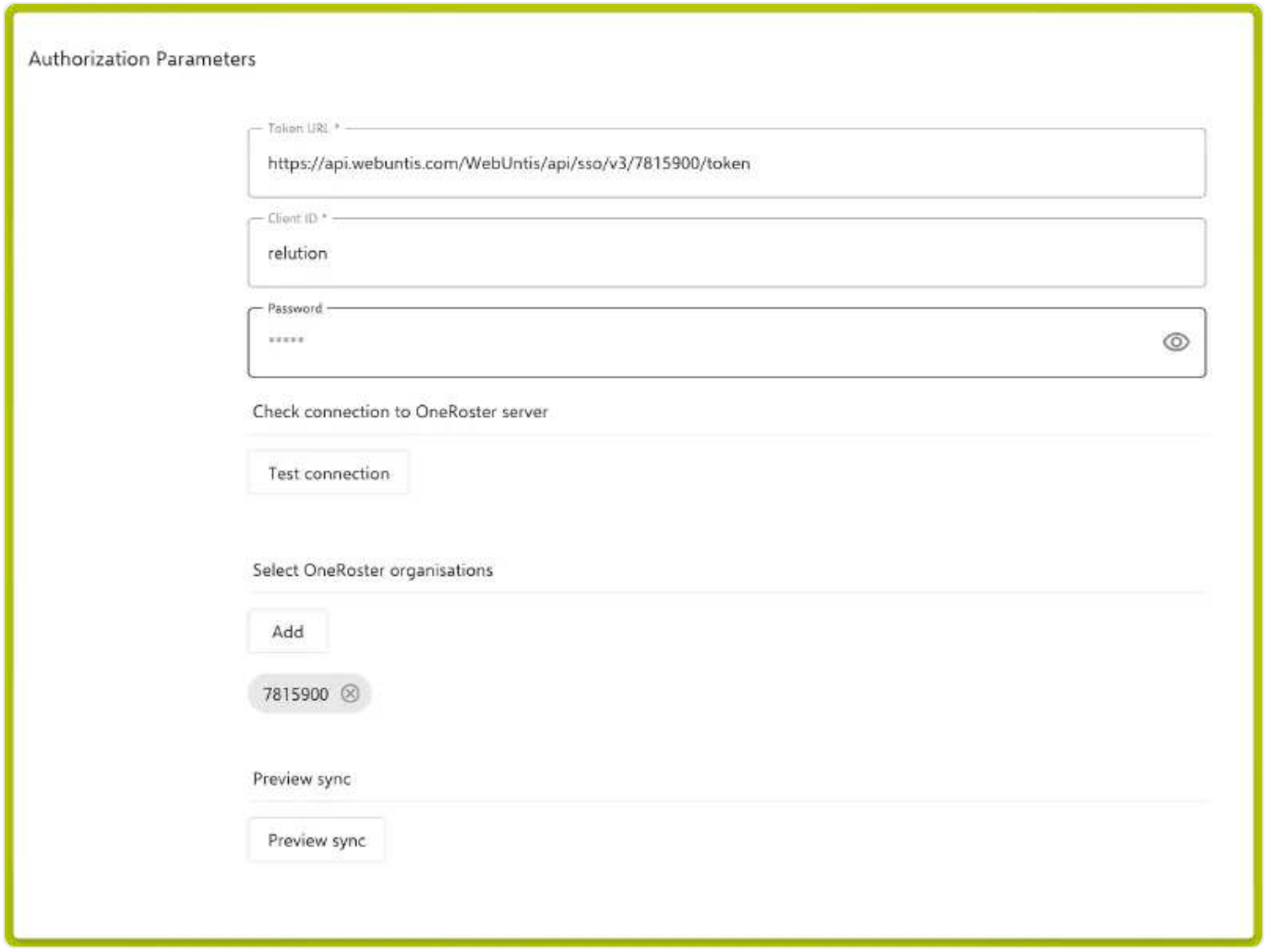
1. Nom du prestataire : nom unique de la connexion. Le nom ne doit être utilisé par aucune autre configuration de prestataire et ne peut plus être modifié après l'enregistrement.
2. Activé : cet interrupteur active l'interface. Pour une nouvelle connexion, il est désactivé ; tant qu'il reste désactivé, aucune synchronisation n'a lieu.
3. Hôte : URL du serveur OneRoster.



Paramètres d’autorisation

- URL du jeton : URL pour l’authentification par jeton.
- Client ID : identifiant client pour l’authentification.
- Mot de passe : secret client correspondant. Pour une connexion enregistrée, le champ affiche `*****` ; s’il reste vide, le mot de passe enregistré reste valable. Si l’Hôte ou l’URL du jeton est modifié, le mot de passe doit être saisi à nouveau, sinon Relution refuse le test de connexion et l’enregistrement.

Le bouton Test de connexion permet de vérifier la connexion au serveur OneRoster dès que tous les champs obligatoires sont renseignés.



Sélectionner les organisations

- Dans un client, les organisations OneRoster à synchroniser sont sélectionnées dans la section Paramètres d’autorisation via Ajouter, à côté de Sélectionner les organisations

OneRoster. Le bouton est actif dès que tous les champs obligatoires sont renseignés.
- Dans l'organisation globale ou dans une méta-organisation, la section Mappages d'organisations s'affiche à la place. Les organisations OneRoster y sont associées aux différentes organisations Relution.
- L'Aperçu de la synchronisation affiche au préalable les classes à synchroniser avec leurs enseignants et élèves. L'aperçu est disponible dès qu'au moins une organisation est sélectionnée ou associée.

Sans organisation OneRoster sélectionnée, la synchronisation échoue.

Paramètres de synchronisation

- Synchroniser les classes : importe les classes depuis OneRoster. L'option est activée par défaut.
- Action pour les utilisateurs manquants : détermine le traitement des utilisateurs déjà synchronisés qui ne sont plus fournis par le serveur OneRoster : `Aucun` (par défaut), `Désactiver` ou `Supprimer`. L'action s'applique toujours, même si Synchroniser les classes est désactivé.
- Action pour les classes manquantes : détermine le traitement des classes déjà synchronisées qui n'existent plus dans OneRoster : `Aucun` (par défaut) ou `Supprimer`. L'action ne s'applique que si Synchroniser les classes est activé.

Pour la version 26.4.0

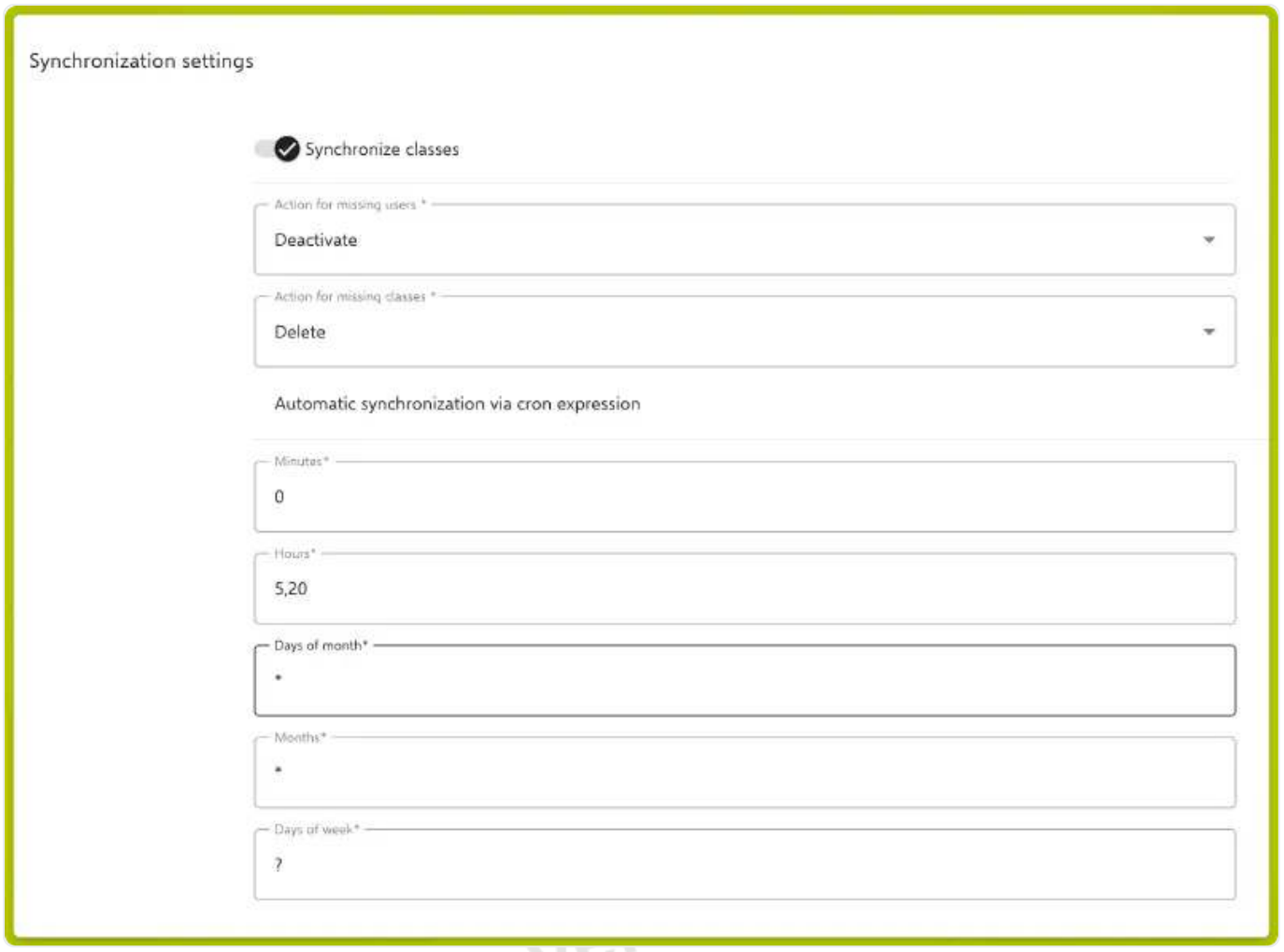
Si une synchronisation ne fournit aucun utilisateur ou aucune classe, Relution n'exécute pas l'action correspondante. Ainsi, une erreur de connexion ou de configuration n'entraîne pas la désactivation ou la suppression de tous les objets.

Les utilisateurs synchronisés sont automatiquement attribués au groupe système `<ORGANISATION> Teacher` ou `<ORGANISATION> Student` de l'organisation ainsi qu'à un groupe du prestataire. Comme nom de connexion, Relution utilise le nom d'utilisateur de OneRoster, à défaut l'adresse e-mail ou un identifiant de OneRoster.

Synchronisation automatique

La synchronisation automatique est définie à l'aide de la syntaxe Cron. Par défaut, elle s'exécute tous les jours à 5 h 00 et à 20 h 00.

- Minutes : minute à laquelle la synchronisation est effectuée.
- Heures : heure de la synchronisation.
- Jours du mois, Mois, Jours de la semaine : restrictions supplémentaires de l'intervalle de synchronisation.



Pour la ve

Vérification de la synchronisation

Une fois enregistrée, la connexion peut être ouverte dans l'aperçu. La vue détaillée liste les résultats de synchronisation séparément pour les utilisateurs et les classes : elle indique la prochaine synchronisation prévue et la dernière synchronisation effectuée, si la synchronisation a réussi, le Message d'état ainsi que le nombre d'objets synchronisés, disparus et en échec. Un clic sur le nombre sous Erreurs de synchronisation affiche les erreurs individuelles et donc leur cause.

Dans l'en-tête de la vue détaillée, l'icône de synchronisation (Synchronisation) déclenche à tout moment une synchronisation manuelle (nécessite l'autorisation de modifier les utilisateurs ou les classes). Les icônes Éditer et Supprimer s'y trouvent également.

> La plupart des erreurs de synchronisation surviennent en raison d'utilisateurs manquants dans une classe. Relution nécessite au moins un élève et un enseignant pour créer une classe. De plus, les utilisateurs sont ignorés lors de la synchronisation si leur nom d'utilisateur est déjà

attribué dans l’organisation, si leur adresse e-mail est déjà attribuée dans Relution ou s’ils n’ont pas d’adresse e-mail.

Pour la version 26.4.0

Import SchulConnex

Relution prend en charge la synchronisation des identités et des données de contexte scolaire via SchulConnex (un standard allemand d'échange de données scolaires). La fonctionnalité est accessible via `Paramètres` → `Gestion des utilisateurs` → `SchulConnex` et synchronise automatiquement les utilisateurs, les rôles de groupe ainsi que les classes/cours depuis le logiciel de gestion scolaire sous-jacent. Dans l'aperçu SchulConnex Imports, une nouvelle configuration est créée via Ajouter.

SchulConnex sert uniquement à l'import. Les utilisateurs importés se connectent à Relution via une autre méthode de connexion, par exemple un fournisseur d'identité.

Général

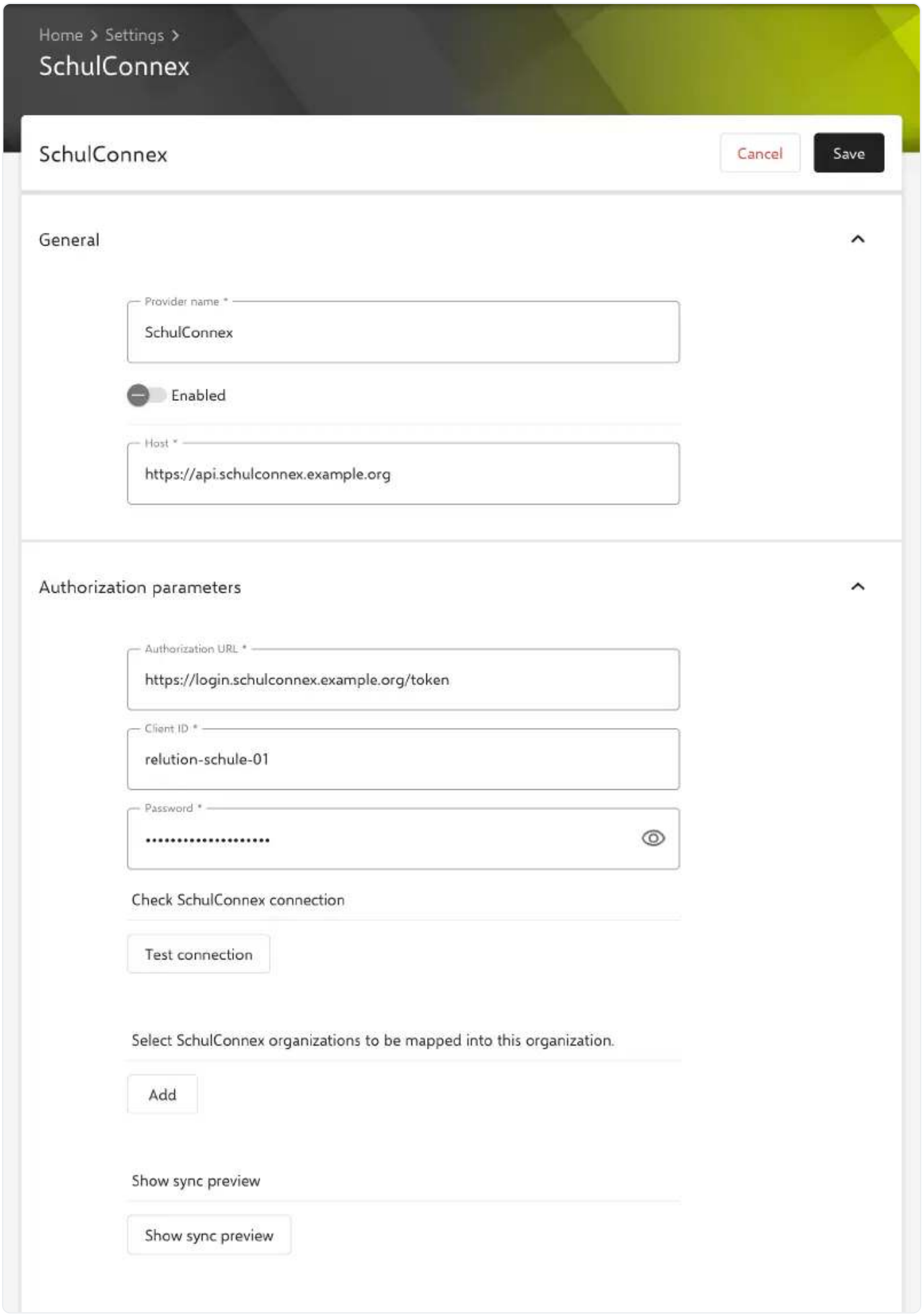
1. Nom du prestataire : nom unique de la configuration. Le nom ne doit être utilisé par aucune autre configuration de prestataire et ne peut plus être modifié après l'enregistrement.
2. Activé : active la synchronisation. Pour une nouvelle configuration, l'interrupteur est désactivé ; tant qu'il reste désactivé, aucune synchronisation n'a lieu.
3. Hôte : URL du serveur SchulConnex.

Pour la version 26.4.0

Paramètres d'autorisation

- URL d'autorisation : URL utilisée pour l'authentification OAuth.
- Identifiant du client : identifiant client pour l'authentification.
- Mot de passe : secret client du client SchulConnex. Pour une configuration enregistrée, le champ affiche `*****` ; s'il reste vide, le secret enregistré reste valable. Si l'Hôte ou l'URL d'autorisation est modifié, le secret doit être saisi à nouveau, sinon Relution refuse l'enregistrement, le test de connexion et l'aperçu de la synchronisation.

Le bouton Test de connexion (libellé Vérifier la connexion de SchulConnex) permet de tester la connexion dès que tous les champs obligatoires sont correctement renseignés.


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

Mapping des organisations

- Sur une organisation classique, les organisations SchulConnex à intégrer sont sélectionnées directement (mapping 1:1).
- Sur l'organisation globale ou une organisation méta, plusieurs organisations Relution peuvent être gérées à la fois : pour chaque organisation Relution, un ensemble dédié d'organisations SchulConnex est attribué via un assistant de mapping. Chaque organisation SchulConnex et chaque organisation Relution ne peut être associée qu'une seule fois.

Le bouton Afficher l'aperçu de la synchronisation permet de vérifier au préalable quelles classes/cours seraient importés, avec leur nombre d'enseignants et d'élèves.

Paramètres de synchronisation

- Synchroniser les classes : active l'import des classes/cours (activé par défaut).
- Action, lorsqu'un utilisateur est supprimé dans SchulConnex : définit ce qui se passe lorsqu'un utilisateur précédemment synchronisé n'existe plus dans SchulConnex : `Aucun` (par défaut), `Désactiver` ou `Supprimer`.
- Action, lorsqu'une classe est supprimée dans SchulConnex : définit ce qui advient des classes supprimées dans SchulConnex : `Aucun` (par défaut) ou `Supprimer`.
- Synchronisation automatique : planification via syntaxe Cron (minutes, heures, jours du mois, mois, jours de la semaine). Par défaut, la synchronisation s'exécute deux fois par jour, à 5 h et 20 h.

Pour la version 26.4.0

En plus de la synchronisation automatique, une synchronisation peut être déclenchée manuellement à tout moment via l'icône de synchronisation (Synchronisation) dans l'en-tête de la vue détaillée de la configuration (nécessite l'autorisation de modifier les utilisateurs ou les classes).

Mapping des rôles

Les rôles de groupe SchulConnex sont automatiquement mappés lors de l'import vers les groupes système `<ORGANISATION> Teacher` et `<ORGANISATION> Student` de l'organisation :

- Enseignants : Rôles `LEHR`, `KLLEIT`, `FOERD`, `VLEHR`, `GLEIT`
- Élèves : Rôles `LERN`, `GMIT`

Seuls les groupes SchulConnex de type classe ou cours sont pris en compte. Le rôle `SCHB` n’est attribué à aucun groupe. En outre, tous les utilisateurs importés sont attribués à un groupe du prestataire.

Vérification de la synchronisation

Après une synchronisation, les résultats peuvent être consultés dans la vue détaillée de la configuration. Elle indique séparément pour les utilisateurs et les classes la prochaine synchronisation prévue, la date de la dernière réalisation, si la synchronisation a réussi, le Message d’état ainsi que le nombre d’objets synchronisés, disparus et en échec. Un clic sur le nombre sous Erreurs de synchronisation affiche les erreurs individuelles.

> Une classe/un cours n’est créé que s’il contient au moins un élève et un enseignant. Les classes ignorées sont comptées comme des erreurs.

> Si aucune adresse e-mail n’est renseignée pour une personne, l’identifiant de personne SchulConnex est utilisé comme identifiant de connexion à la place. Si un utilisateur avec la même adresse e-mail ou le même nom d’utilisateur existe déjà, l’import de cette personne est ignoré et signalé comme une erreur.

> En cas d'échec de l'authentification (par exemple un secret expiré), l'ensemble de la synchronisation de la configuration est interrompu, car les identifiants s'appliquent à toutes les organisations mappées à la fois.

Pour la version 26.4.0

Les autres erreurs, par exemple un dépassement de délai, n’interrompent que la synchronisation de l’organisation associée concernée. Pour cette organisation, les actions relatives aux utilisateurs et classes supprimés ne sont pas exécutées ; les autres organisations sont entièrement synchronisées. Dans ce cas, la synchronisation est signalée comme ayant échoué.

Photos de profil

Relution permet de stocker des images de profil pour les utilisateurs existants au sein de la plateforme. Cette fonctionnalité offre des avantages particuliers dans l'écosystème Apple, comme pour l'application Classroom ou la connexion simplifiée sur les iPads partagés.

Lorsqu'une image de profil est attribuée à un utilisateur, les enseignants peuvent identifier plus facilement les élèves dans l'application Apple Classroom. En outre, cette fonctionnalité simplifie le processus de connexion sur les iPads partagés : les utilisateurs peuvent sélectionner leur classe et cliquer sur leur image de profil pour se connecter.

Il est important de noter que les images de profil restent stockées sur les serveurs de Relution et ne sont pas synchronisées avec les serveurs Apple.

Prérequis

- Utilisateurs existants dans Relution
- Images carrées (recommandé : `256x256` ou `512x512` pixels)
- Taille maximale de l'image : `300 Ko`

Pour la version 26.4.0

Configuration

- Les images sont nommées d'après le nom d'utilisateur de l'utilisateur concerné. C'est le nom de fichier sans extension qui compte ; il doit correspondre exactement à un nom d'utilisateur.
- Toutes les images sont regroupées dans un fichier `.zip`. Les fichiers de métadonnées macOS (`._*`) sont ignorés.
- Sous Utilisateurs, le menu à trois points ouvre l'option Téléchargement en masse d'images de profil. Le droit de mettre à jour les utilisateurs est requis.
- Après le téléversement du fichier `.zip`, un récapitulatif indique pour chaque image si elle est valide et quelles infractions existent, par exemple aucun ou plusieurs utilisateurs correspondants trouvés, image non carrée ou trop volumineuse.
- Seules les images valides sont attribuées ; une image de profil existante est alors écrasée. Les images non valides sont ignorées.

Des images de profil individuelles (JPEG ou PNG) peuvent également être téléversées dans les détails de l'utilisateur, dans le champ Image de profil. Les utilisateurs peuvent modifier leur

propre image de profil dans leur profil via l’icône de modification sur l’avatar.

Remarques

Pour que les enseignants puissent gérer les utilisateurs dans l’application Classroom, des classes doivent être définies dans Relution. Cela est également nécessaire pour la connexion simplifiée sur les iPads partagés. Les iPads partagés nécessitent en outre des comptes Apple gérés (Identifiant Apple géré dans le portail) pour permettre la connexion.

Les images de profil ne sont livrées que si, sous `Paramètres` → `Éducation` → `Paramètres des leçons`, l’accès est réglé sur Activé (par défaut) dans la section Accès aux images de profil pour les configurations Apple Education, et si l’utilisateur est membre d’une classe de la configuration Apple Education de l’appareil ; voir Paramètres des leçons →.

Pour la version 26.4.0

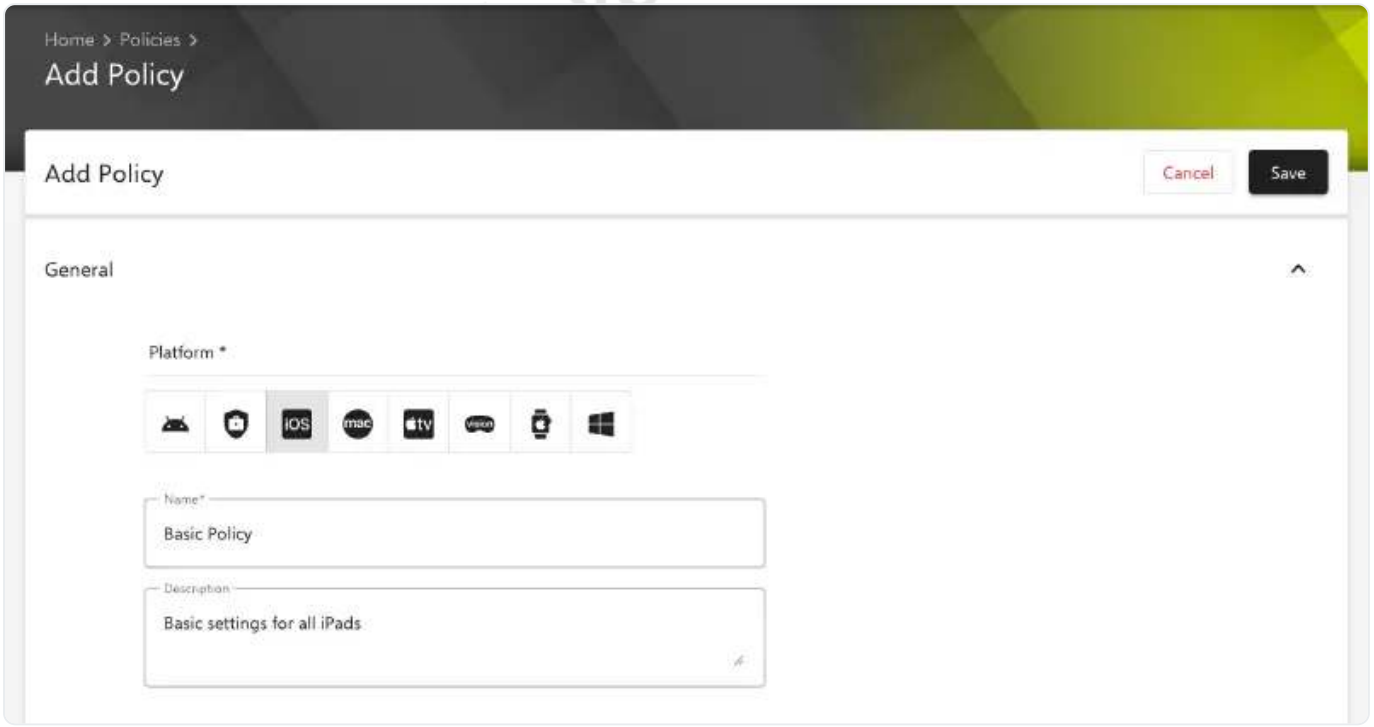
Les politiques expliquées

Une politique est un ensemble d'une ou plusieurs configurations. Chaque politique peut être appliquée à un ou plusieurs appareils en même temps. En outre, une ou plusieurs politiques peuvent être associées à chaque appareil.

Créer

Les politiques dépendent de la plate-forme. Lors de leur création, il faut veiller à déterminer la plateforme pour laquelle une politique est créée. Par exemple, une politique iOS ne peut pas être modifiée ultérieurement en une politique Android ou Windows. Au sein des systèmes d'exploitation Apple, une distinction est également faite entre les politiques iOS, macOS, tvOS, visionOS et watchOS et, de la même manière, elles ne peuvent pas être modifiées ultérieurement.

Dans le menu latéral sous `Appareils` → `Politiques`, un aperçu des politiques déjà créées est disponible. Il est possible de créer une nouvelle politique en cliquant sur le bouton Ajouter. A ce stade, un système cible doit être spécifié et un nom doit être donné.

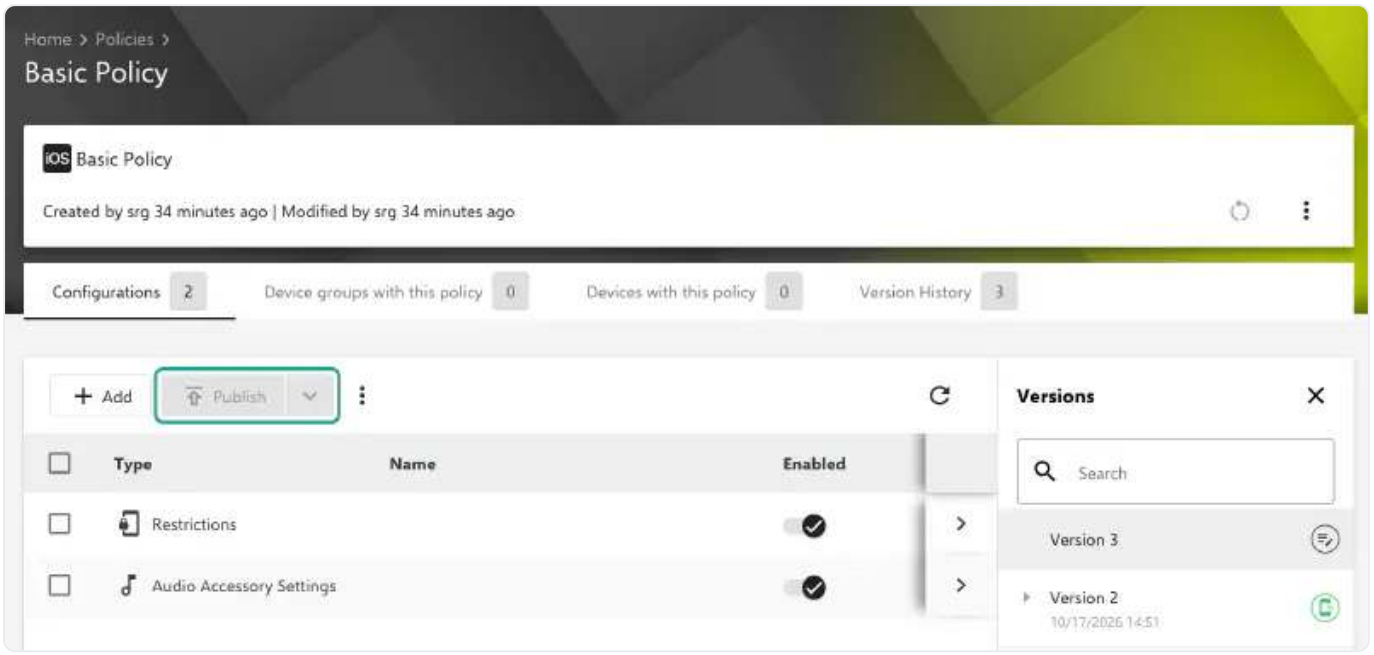


Un clic sur Enregistrer crée la nouvelle politique.

Gestion des versions des politiques

Toutes les modifications apportées à une politique ne prennent effet qu'après sa publication. Ce processus permet d'effectuer toutes les configurations et de vérifier qu'elles sont complètes sans que les changements soient directement actifs sur les appareils liés.

Une fois toutes les modifications effectuées et prêtes à être appliquées aux appareils, la version est publiée via le bouton Publier. Le bouton se trouve dans la barre d'actions de la liste des configurations, à droite de Ajouter. Seule une version modifiée depuis sa création et contenant au moins une configuration activée peut être publiée.

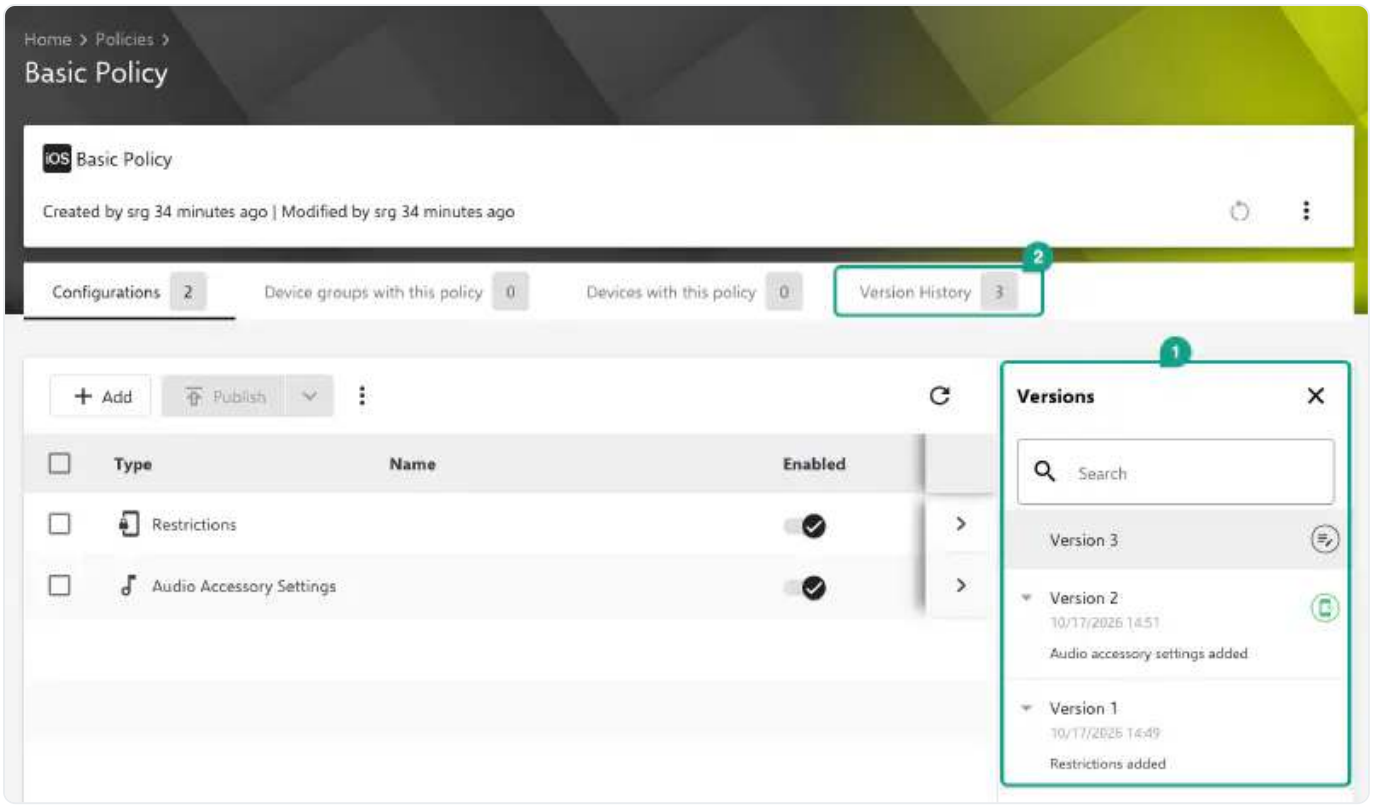


Le menu du bouton Publier propose deux variantes :

- Publier sur tous les appareils : la version est appliquée à tous les appareils auxquels la politique est attribuée.
- Publier sur des appareils de test : la version est publiée en tant que version de test (état Test) et n'est appliquée qu'aux appareils des groupes d'appareils qui utilisent la version de test. Ces groupes d'appareils sont sélectionnés dans la boîte de dialogue suivante, à condition qu'aucun groupe d'appareils n'utilise encore la version de test. Tous les autres appareils conservent la version publiée jusqu'alors. Une version de test peut ensuite être appliquée à tous les appareils via Publier.

La barre latérale des versions

La barre latérale Versions permet de consulter rapidement les versions déjà publiées d'une politique.



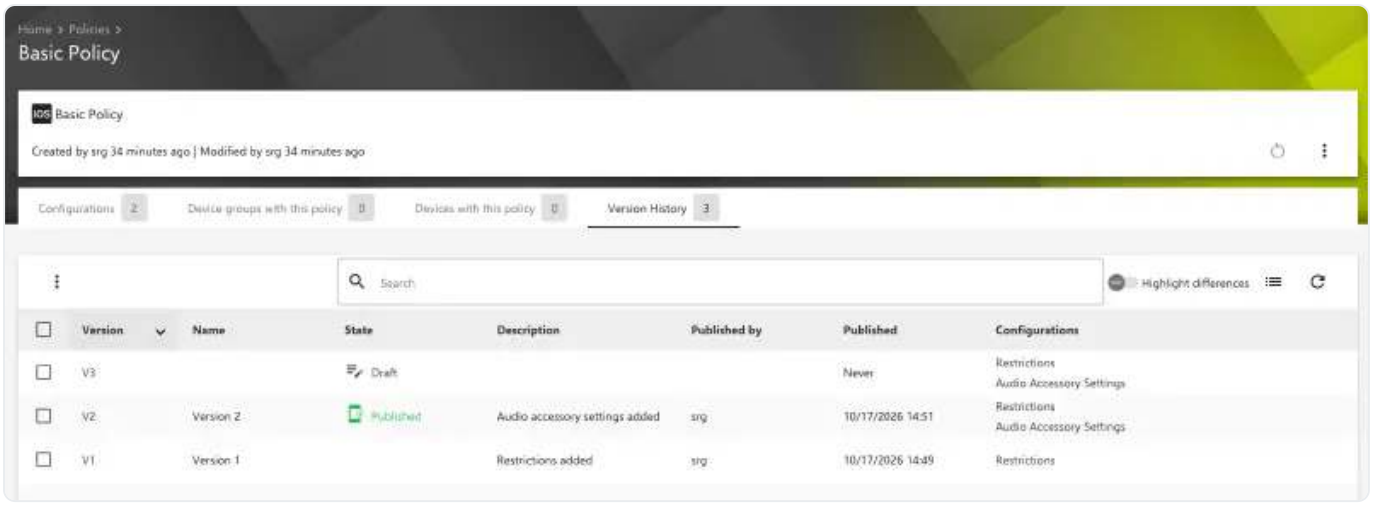
Les indications suivantes s'appliquent :

- Icône de crayon : marque le brouillon actuel – il s'agit de la version la plus récente, mais encore non publiée de la politique.
- Icône de téléphone verte : identifie la politique actuellement publiée et donc appliquée sur les appareils.
- Icône de fiole bleue : identifie une version de test, appliquée uniquement aux groupes d'appareils de test sélectionnés.
- Informations de version : lors de la publication d'une nouvelle version, un Nom et une Description peuvent être indiqués. Ils sont affichés directement dans la barre latérale afin de documenter et de suivre rapidement les modifications.

Pour la version 26.4.0

Historique de la version

Pour un suivi détaillé de toutes les modifications, l'onglet Historique de la version est également disponible.



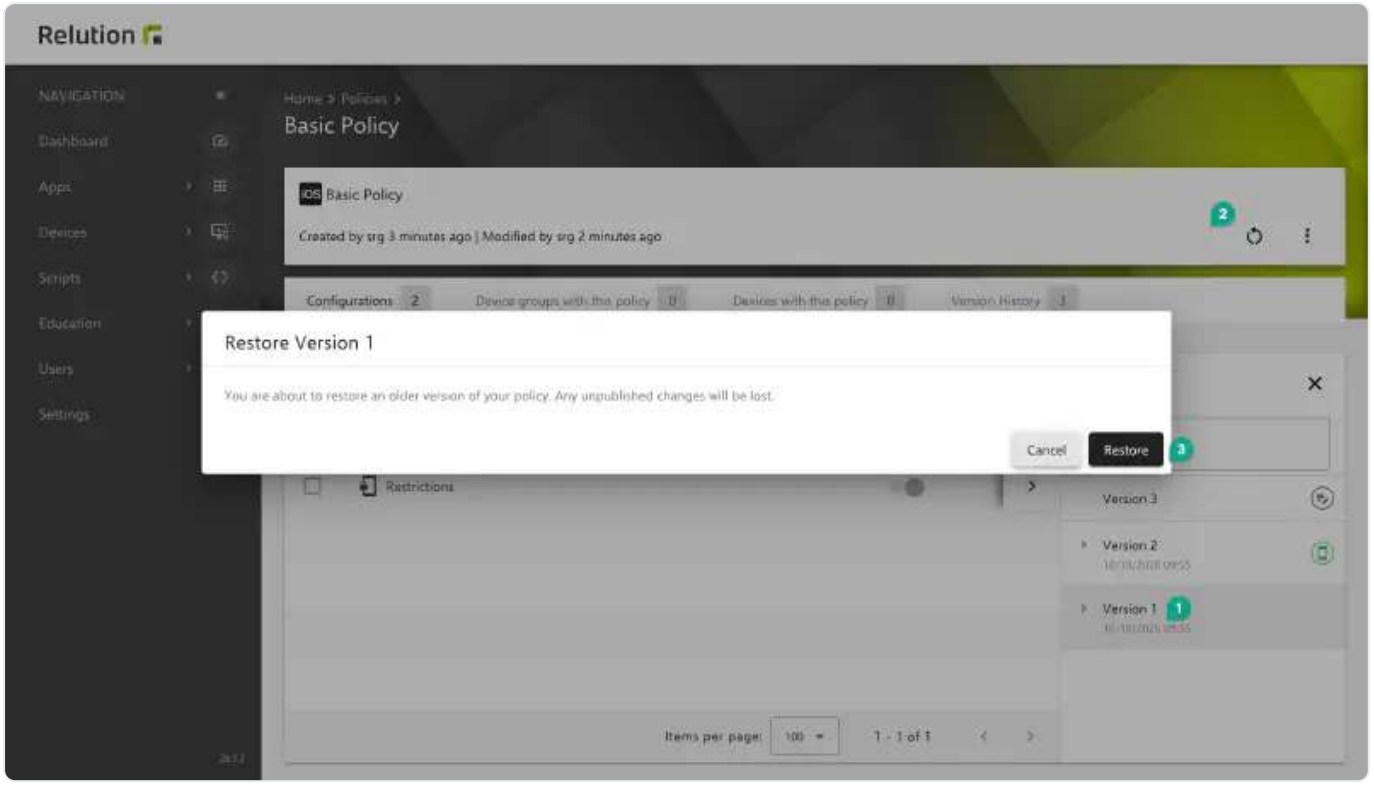
Cet aperçu répertorie toutes les versions de la politique, avec les détails suivants :

Colonne	Description
Version	L’identifiant unique de la version (par ex. V4).
Nom	Le nom attribué à la version.
État	L’état de la version : brouillon (libellé Projet dans le portail), Publié ou Test. Pour les versions obsolètes, la colonne reste vide.
Description	La remarque ajoutée lors de la publication concernant les modifications.
Publié par	L’utilisateur qui a publié la version.
Publié	Date et heure de la publication.
Les configurations	Toutes les configurations de cette version. Le commutateur Mettre en évidence les différences marque les configurations ajoutées, modifiées et supprimées par rapport à la version précédente.

Les colonnes Modifié par et Modifié le sont masquées par défaut et peuvent être affichées via la sélection des colonnes.

Restaurer des politiques

Une version antérieure d'une politique est sélectionnée dans la barre latérale Versions (1) et restaurée en tant que nouveau brouillon via le bouton Restaurer en tant que version préliminaire (2) dans l'en-tête de la politique. La fonction est également disponible dans l'onglet Historique de la version. Après confirmation avec Restaurer (3), le brouillon actuel est remplacé par une copie de la version sélectionnée ; toutes les modifications non publiées sont perdues. La politique doit posséder au moins une autre version en plus du brouillon.



Priorités

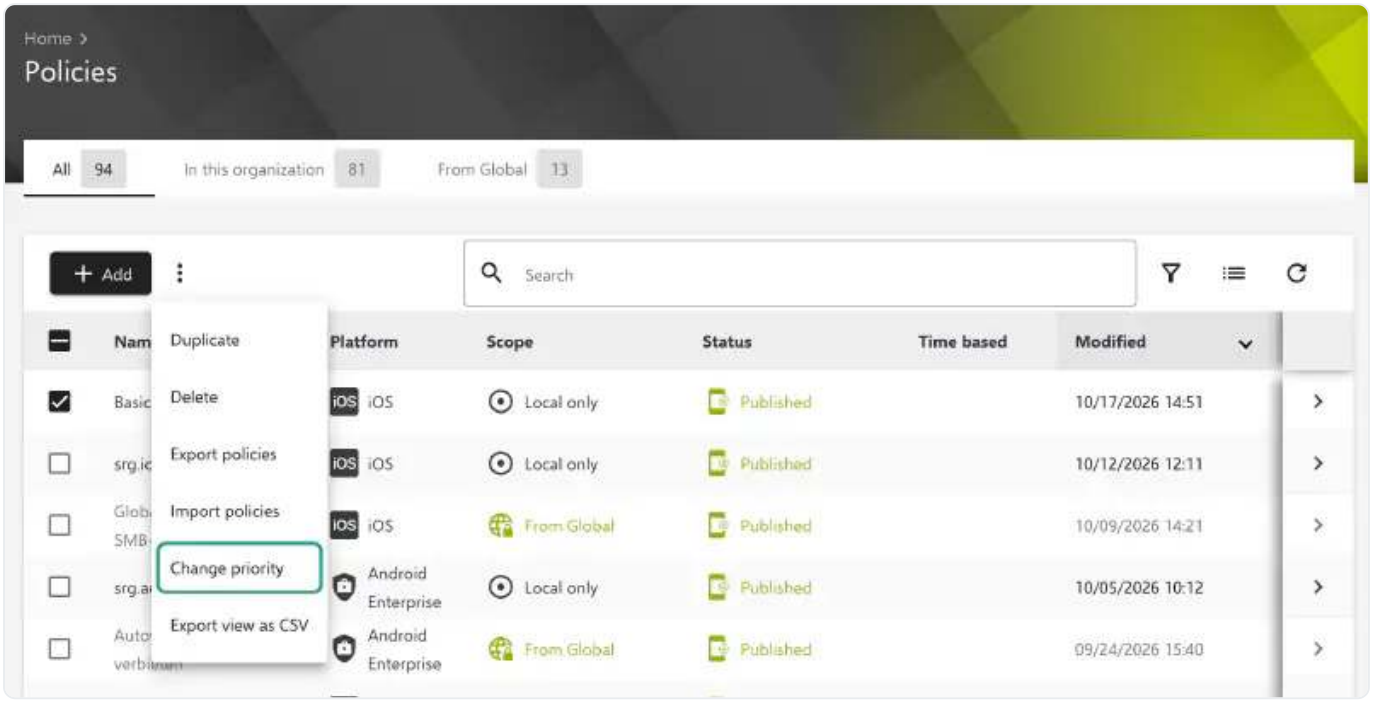
Les politiques ont des priorités. Le chiffre le plus bas l'emporte sur le plus élevé. Ainsi, la priorité 2 l'emporte sur la priorité 3. Le numéro de priorité ne s'applique qu'au sein d'un même niveau : les politiques globales → ont toujours la priorité sur les politiques partagées par une organisation Meta →, et celles-ci ont à leur tour la priorité sur les politiques de l'organisation elle-même. Une politique locale de priorité 1 ne l'emporte donc pas sur une politique globale.

Chaque plateforme a sa propre liste de priorités. Il peut donc y avoir des politiques avec la priorité 1 plusieurs fois - chacune pour iOS, macOS, tvOS, visionOS, watchOS, `Android Classic/ Legacy`, `Android Enterprise` et Windows.

Si un type de configuration qui ne peut être créé qu'une seule fois par politique (par ex. les restrictions sous `Android Classic/ Legacy`, `Android Enterprise` et Windows) figure dans plusieurs politiques de priorités différentes, seule la configuration de la politique ayant la priorité la plus élevée est retenue. Les configurations des politiques de priorité inférieure ne sont pas complétées, mais entièrement ignorées. Si une fonction est autorisée dans les restrictions d'une politique de priorité 2, mais interdite dans une politique de priorité 4, elle reste autorisée.

Certains de ces types de configuration sont en revanche transmis à l'appareil à partir de toutes les politiques, par ex. les restrictions sous iOS, macOS et tvOS ; l'appareil applique alors à chaque fois le réglage le plus restrictif. Les configurations qui peuvent être créées plusieurs fois (par ex. Wi-Fi ou certificats) sont combinées à partir de toutes les politiques. Si deux entrées entrent en conflit (par ex. des profils Wi-Fi avec le même SSID), c'est celle de la politique de priorité la plus élevée qui s'applique.

Les priorités sont modifiées dans l'aperçu des politiques via le menu à 3 points et l'entrée Changer la priorité.

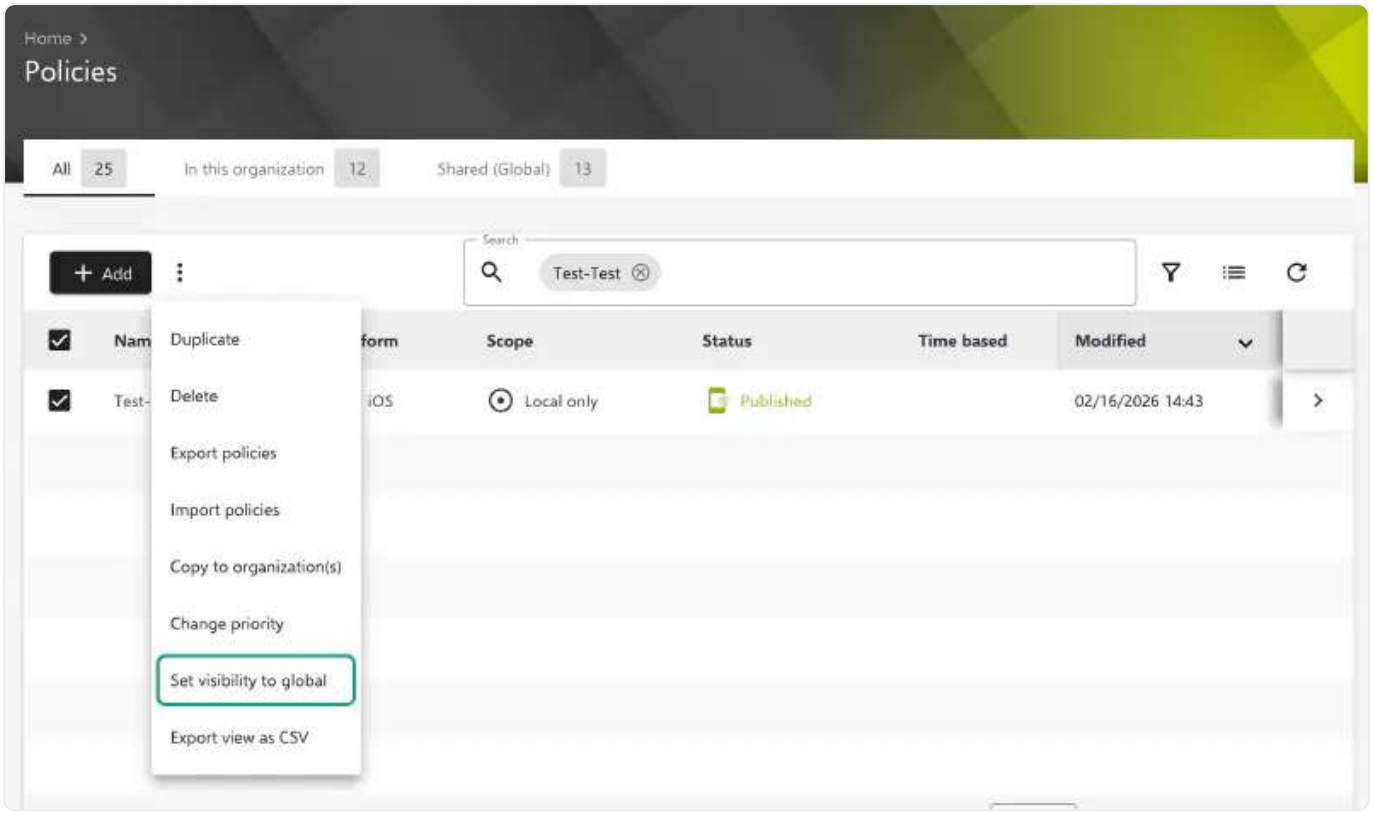


Politiques globales

De temps en temps, il peut être utile de pouvoir appliquer des configurations identiques dans plusieurs organisations de Relution. Pour ce faire, des politiques globales peuvent être créées et partagées dans l'Organisation globale →. Ces politiques peuvent être modifiées normalement dans l'organisation globale, mais ne sont disponibles qu'en lecture seule dans les autres organisations.

Le partage requiert une version publiée de la politique. La politique est ensuite sélectionnée dans l'aperçu et partagée via le menu à 3 points avec Définir la visibilité comme globale (dans la vue détaillée de la politique : Définir la visibilité des politiques auprès du public). Ce partage ne peut pas être annulé. Dans les organisations Meta →, l'entrée Définir la visibilité à méta est disponible de la même manière ; la politique est alors disponible en lecture seule dans toutes les organisations subordonnées.

> Les politiques globales ne sont pas disponibles pour Android Enterprise.



Dans l'aperçu, la colonne Champ d'application indique si une politique est partagée : dans l'organisation globale, les politiques partagées sont marquées Partagé, dans les autres organisations Depuis Mondial (ou Depuis Meta pour les politiques d'une organisation Meta). Les politiques non partagées sont marquées Local uniquement.

Désactiver les politiques

À partir de Relution 5.33, il est possible de désactiver des politiques pour des appareils individuels. Auparavant, il fallait toujours cloner et ajuster les groupes d'appareils pour retirer temporairement un appareil de l'affectation d'une politique. C'est maintenant possible en passant par `Navigation` → `Appareils` → `Inventaire` → `l'appareil concerné` →

`Politique`. Pour ce faire, il suffit de sélectionner la politique correspondante et de la désactiver/activer via le menu à 3 points.

État de la politique

L'état de la politique est affiché dans l'en-tête de la page de détails de l'appareil. Les états suivants peuvent se produire :

- `UNKNOWN = Problème`
  - L'état de la politique de l'appareil est inconnu
- `NONE = Aucun`
  - Aucune politique n'est appliquée à l'appareil
- `SENT = Aucun`
  - Une politique a été attribuée à l'appareil, mais elle n'a pas encore été appliquée
- `APPLIED = Actif`
  - Une politique est en cours d'application à l'appareil
- `UPDATE = Actif`
  - Une nouvelle version de la politique a été envoyée à l'appareil, mais l'appareil ne l'a pas encore mise à jour
- `CHANGE = Infos`
  - Une autre politique a été envoyée à l'appareil, mais l'appareil n'a pas encore modifié la politique
- `REMOVED = Infos`
  - La politique a été désattribuée à l'appareil, mais l'appareil ne l'a pas encore supprimée

Pour la version 26.4.0

Groupes d’appareils

La fonction des groupes d’appareils est disponible dans Relution depuis la version 5.21.0. Elle permet d’attribuer automatiquement des appareils à des groupes en fonction de différentes propriétés des appareils. Ces groupes peuvent ensuite être utilisés pour attribuer des politiques qui seront appliquées automatiquement.

Accès aux groupes d’appareils

Les groupes d’appareils se trouvent sous `Appareils` → `Groupes d’appareils`. Cette page présente les groupes existants et permet d’en créer de nouveaux.

Un groupe d’appareils établit un lien entre des appareils et des politiques. Ce lien peut être créé soit manuellement, soit automatiquement sur la base de certaines propriétés des appareils.

Les politiques sont associées aux appareils exclusivement via les groupes d’appareils ; une association directe n’est plus possible. Les groupes d’appareils permettent en outre de déclencher des actions par événement ou de manière planifiée : Actions de groupes d’appareils →

Pour la version 26.4.0

Création d’un nouveau groupe d’appareils

Un nouveau groupe d’appareils est créé via Ajouter. Un nom et, si nécessaire, une description sont attribués au groupe.

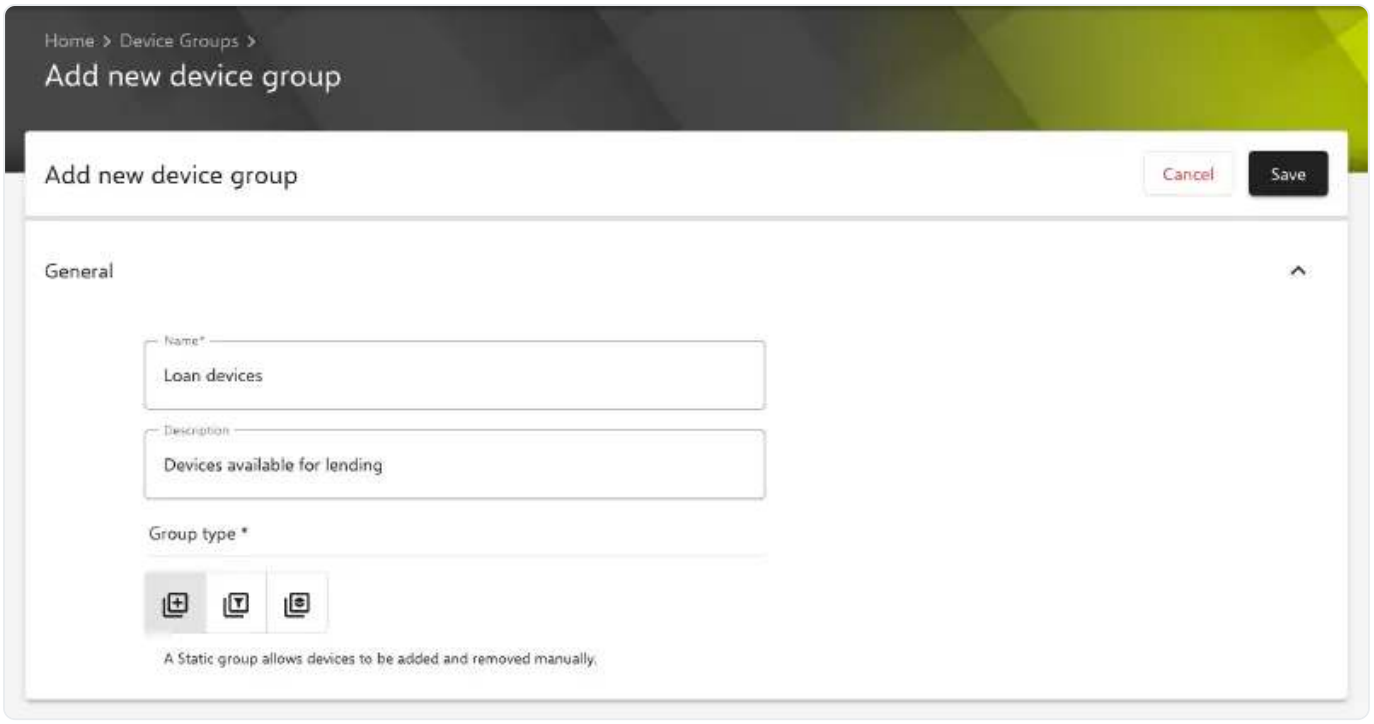
Le Type de groupe peut également être choisi :

- Statique
- Dynamique
- Éducation (uniquement avec une licence Education ou Free)

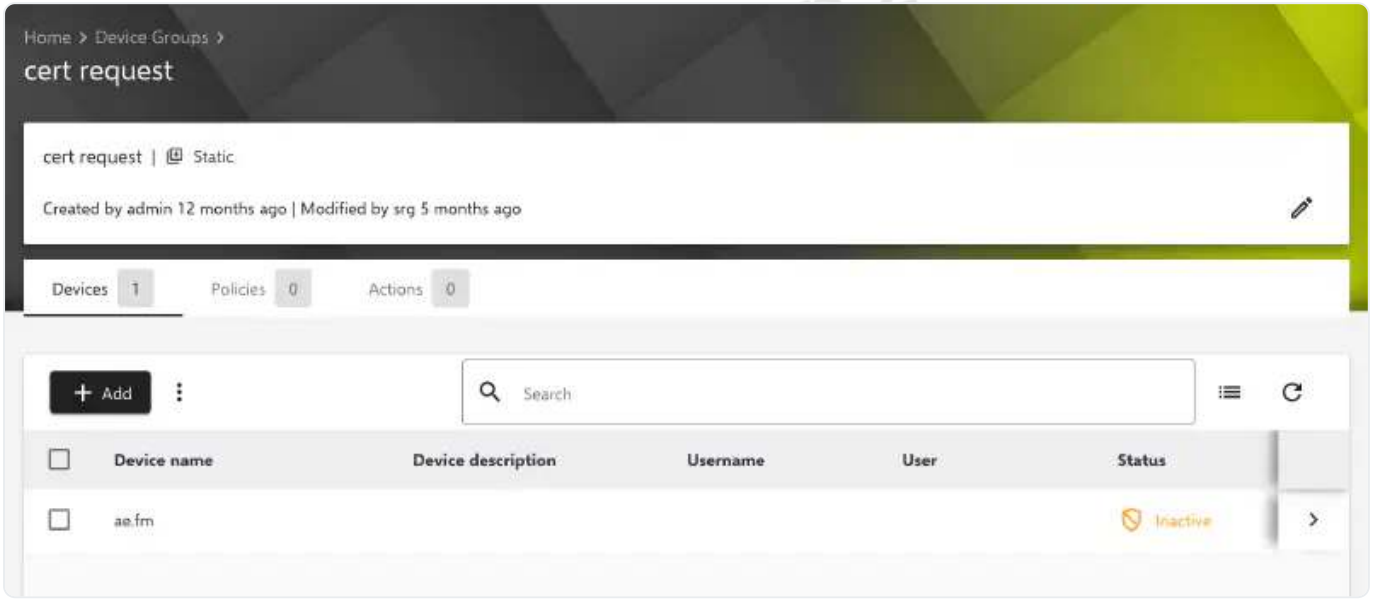
Dynamique est présélectionné.

Groupes statiques

Les groupes statiques permettent une association manuelle entre appareils et politiques.

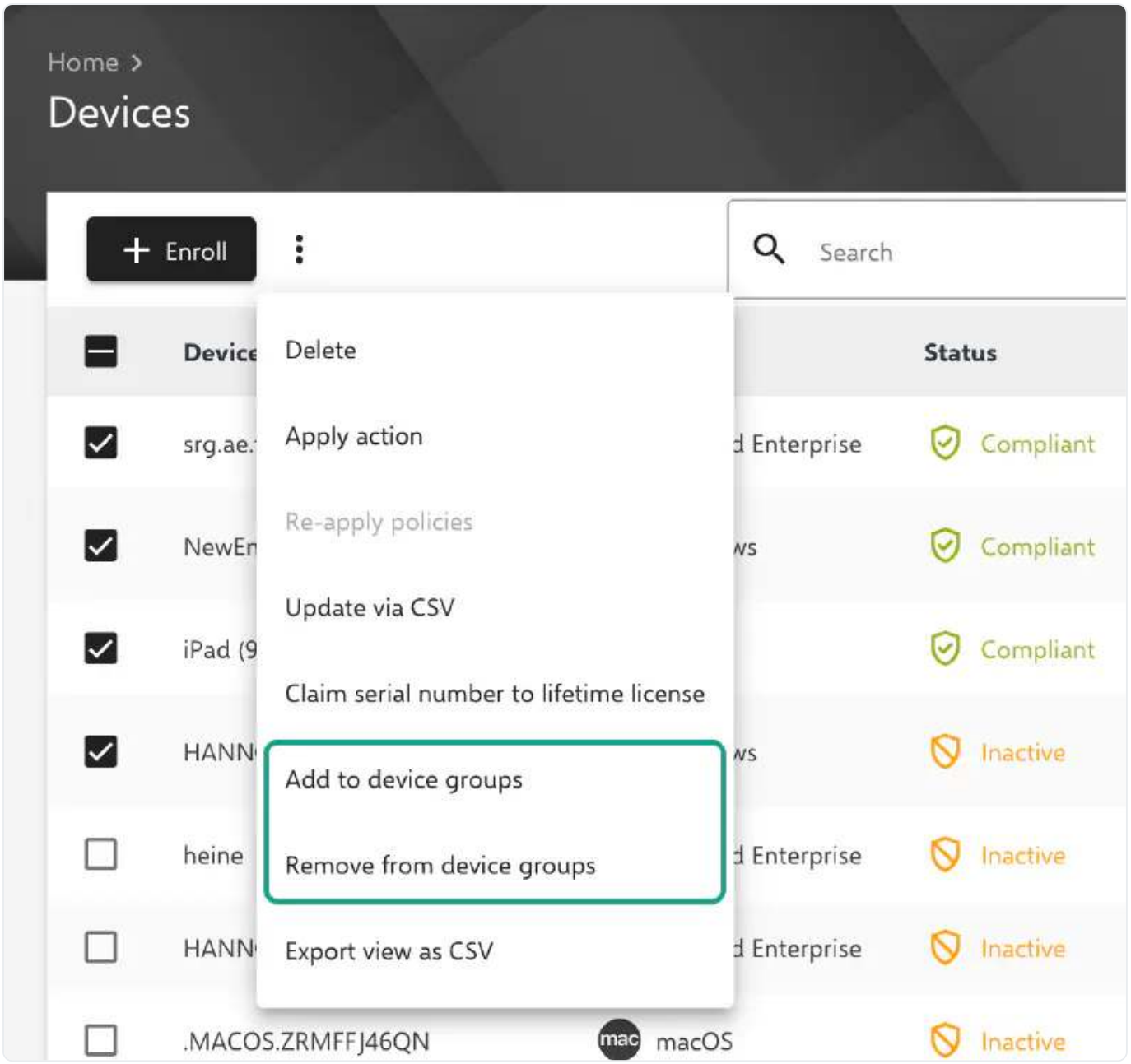


Une fois le groupe créé, des appareils et des politiques peuvent être ajoutés. Seules les politiques déjà publiées peuvent être associées.



Ajout groupé d’appareils

Depuis Relution 26.1.0, il est possible d’ajouter directement plusieurs appareils sélectionnés depuis l’inventaire ou les inscriptions automatiques à un groupe statique existant ou de les en retirer, ce qui leur attribue ou leur retire également les politiques associées. Le menu à trois points propose pour cela les entrées Ajouter aux groupes d’appareils et Supprimer des groupes d’appareils.



Les appareils peuvent déjà être attribués à des groupes statiques lors de l'inscription : les inscriptions et les inscriptions automatiques proposent pour cela le champ Groupes d'appareils statiques.

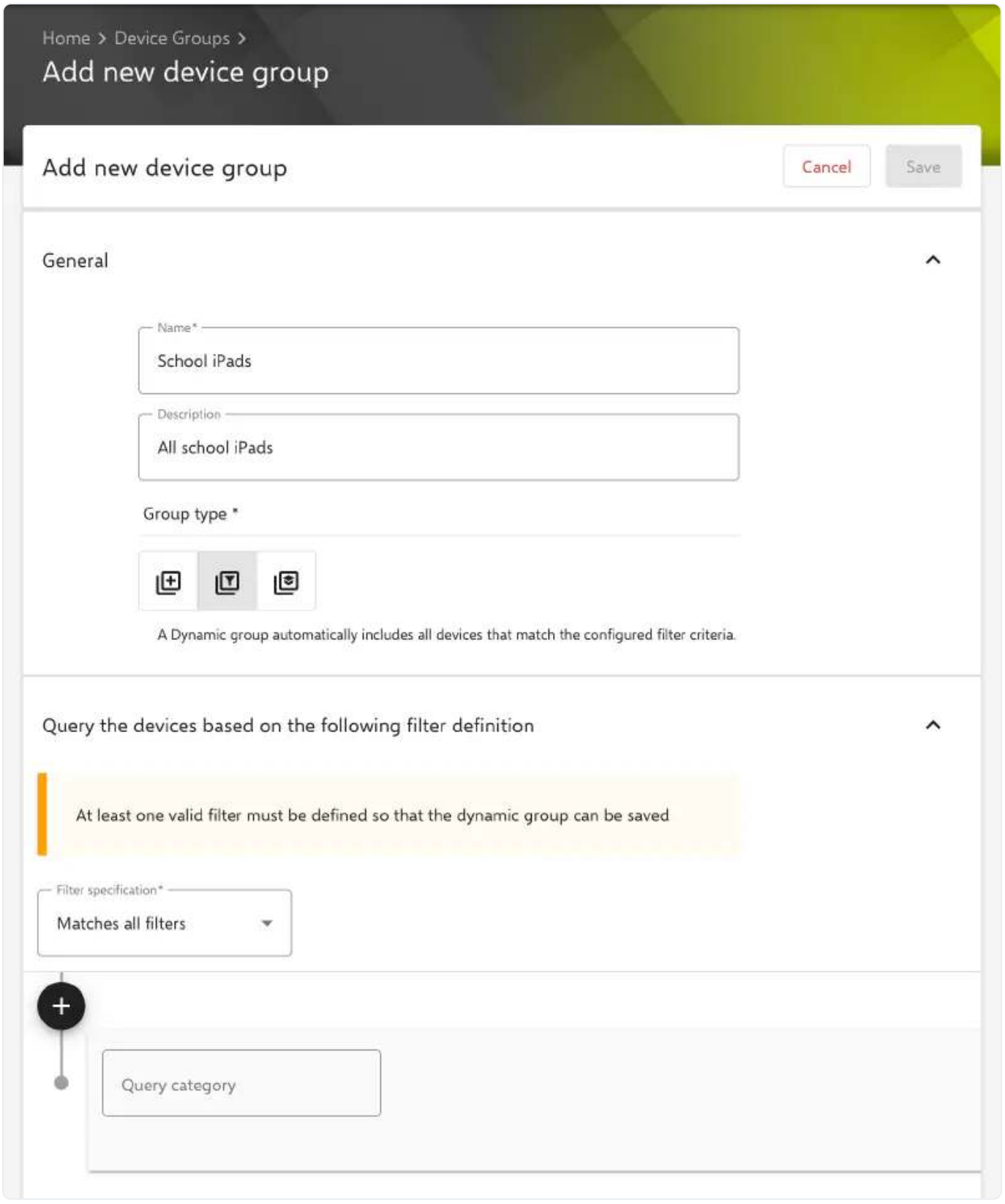
Groupes dynamiques

Dans les groupes dynamiques, des filtres doivent être définis pour déterminer quels appareils sont automatiquement attribués au groupe. Ce processus s'effectue automatiquement en arrière-plan. Pour les filtres sur des groupes d'utilisateurs ou des classes (cours), la prise en compte des modifications dans le groupe peut prendre jusqu'à une heure ; une évaluation rapide n'est

garantie que pour les connexions et déconnexions Relution Shared Device. Il n’y a aucune influence manuelle directe sur le contenu de ces groupes.

Dans la section Aperçu de l’appareil, un clic sur Actualiser indique combien et quels appareils le groupe contient avec les filtres actuels. Si l’enregistrement d’un groupe dynamique existant modifie le nombre d’appareils, Relution demande une confirmation avant l’enregistrement.

Pour la version 26.4.0



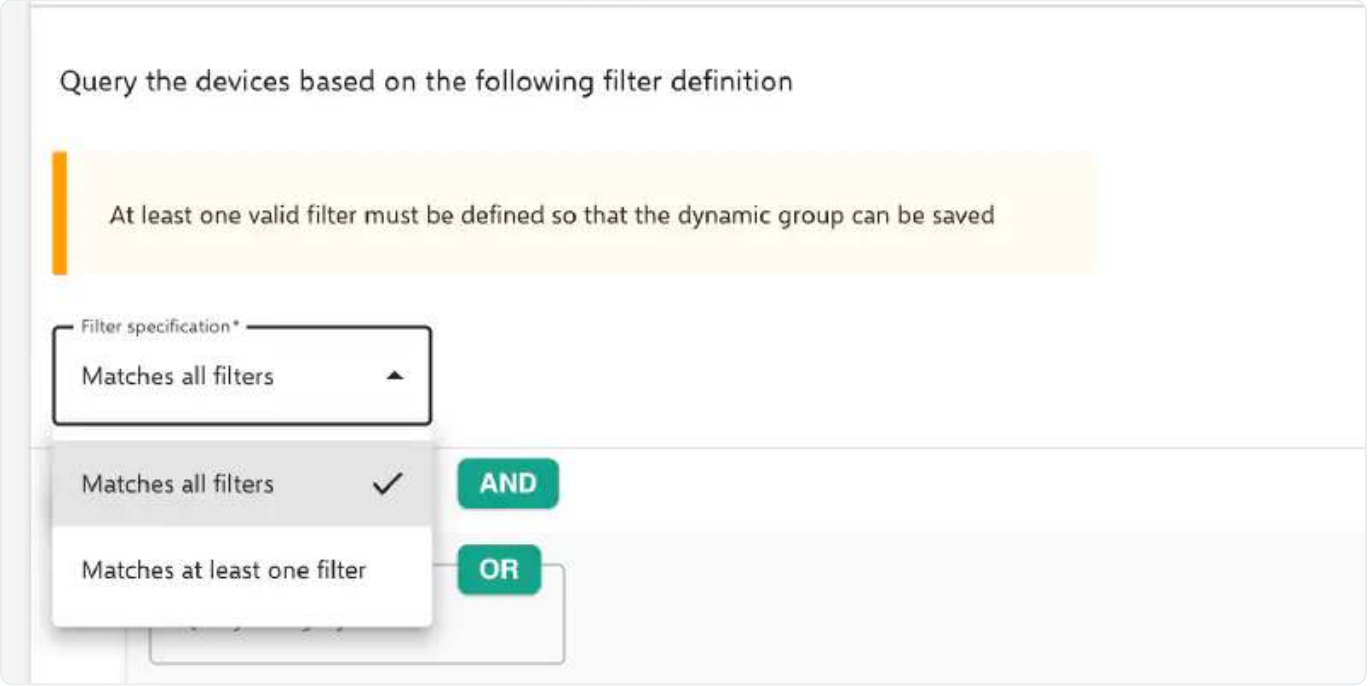
Il s'agit d'un outil complexe nécessitant une utilisation attentive. Des actions imprudentes peuvent rapidement entraîner des résultats indésirables. Les groupes dynamiques sont à utiliser avec précaution, notamment pour les politiques d'infrastructure. S'assurer par exemple qu'aucune politique Wi-Fi n'est révoquée lors d'un changement d'état d'un appareil.

Attention : lorsqu'un appareil perd son appartenance à un groupe d'appareils dynamique, les politiques attribuées via ce groupe lui sont retirées. Si l'option Désinstaller automatiquement les applications obligatoires installées automatiquement si elles ne sont plus nécessaires est activée dans une conformité des applications concernée, les applications sont supprimées avec leurs données locales. L'appartenance au groupe est rétablie automatiquement dès que la condition de filtre s'applique de nouveau, mais pas les données des applications.

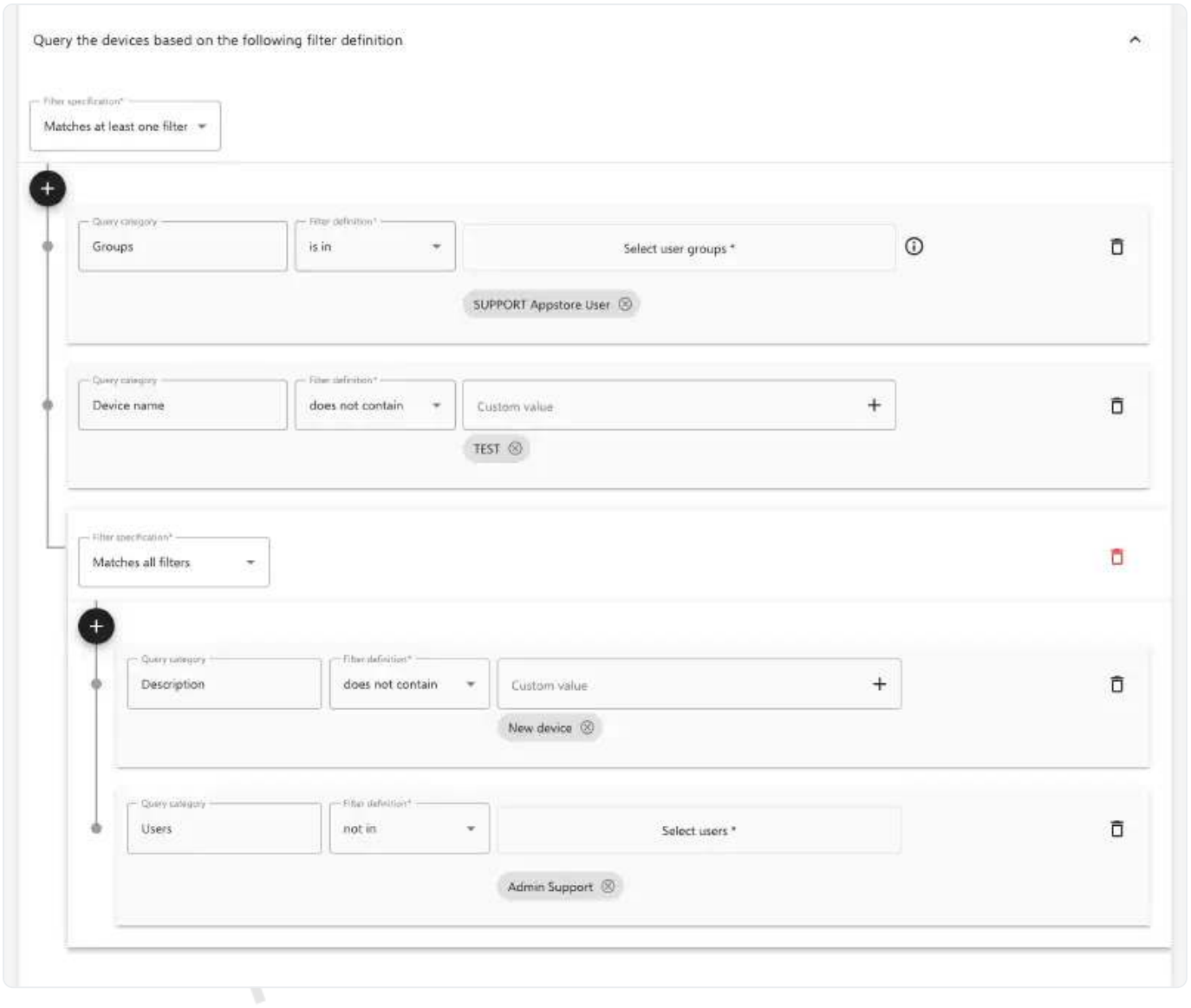
Presque toutes les propriétés filtrables peuvent changer sans intervention d'un administrateur : elles sont signalées par l'appareil ou reprises d'Apple, de Google, de Microsoft ou du fournisseur d'identité. Les champs personnalisés 1 à 5 ainsi que le nom et la description de l'appareil sont également réinitialisés lors d'une nouvelle inscription.

Pour les politiques avec désinstallation automatique, il est donc recommandé d'utiliser des groupes d'appareils statiques ou de désactiver la désinstallation automatique pour les applications contenant des données utilisateur.

Le champ Spécifications du filtre propose les options Correspond à tous les filtres (ET) et Correspond à au moins un filtre (OU). Via le symbole plus, Ajouter un filtre crée d'autres filtres et Ajouter un groupe crée des groupes de filtres imbriqués. Chaque groupe de filtres possède ses propres Spécifications du filtre, ce qui permet de regrouper des conditions comme dans l'exemple suivant.



Dans l'exemple, un filtre a été défini à partir de plusieurs propriétés et opérateurs logiques.



Le filtre inclut les appareils suivants :

- L'utilisateur associé doit être membre du groupe `SUPPORT Appstore User`.

OU

- Le nom de l'appareil ne contient pas `TEST`.

OU

- La description ne contient pas `New device`.

ET

- L'utilisateur n'est pas `Admin Support`.

Le filtre peut également être formulé comme suit :

```
Groupes = "SUPPORT Appstore User" OU Nom de l’appareil NE CONTIENT PAS "TEST"
OU (Description NE CONTIENT PAS "New device" ET Utilisateur N’EST PAS "Admin S
```

Les spécifications de filtre fonctionnent comme des opérations logiques classiques.

Pour éviter toute erreur, il est par exemple possible d’ajouter le numéro de série d’un appareil spécifique comme valeur de filtre fixe afin d’appliquer une politique uniquement à cet appareil et de vérifier si le résultat correspond aux attentes.

Groupes d’appareils dynamiques avec filtre de groupe

Depuis la version 5.33, Relution prend en charge l’utilisation de groupes d’appareils comme filtres dans les groupes dynamiques. Cela permet d’utiliser des groupes statiques ou dynamiques existants comme conditions dans de nouveaux groupes, afin d’inclure ou d’exclure spécifiquement des appareils.

Pour ce type de filtre, Groupe d’appareils est sélectionné sous Catégorie de requête et au moins un groupe existant est ajouté comme condition. Les définitions de filtre est dans, pas dans et tous les (l’appareil est membre de tous les groupes sélectionnés) sont disponibles. Le groupe en cours de modification n’est pas proposé à la sélection.

Pour la version 26.4.0

Avantages du filtre de groupe

- Formation plus précise des groupes cibles, par exemple : `tous les iPads sauf les appareils de test`
- Moins d’efforts de maintenance, car les politiques n’ont plus besoin d’être dupliquées manuellement
- Gestion plus claire des politiques, profils et actions

Avec ce nouveau type de filtre, il est possible d’inclure ou d’exclure explicitement un ou plusieurs autres groupes d’appareils au sein d’un groupe dynamique. Par exemple, un groupe de test peut facilement être exclu d’un groupe de production dynamique sans définir de critères supplémentaires.

La configuration des groupes dynamiques nécessite une planification rigoureuse.

- Éviter de créer des groupes dépendants les uns des autres.
- Ne pas supprimer accidentellement des configurations de base critiques, telles que des profils Wi-Fi.
- Toujours tester les modifications de politiques avec des appareils pilotes.

Des erreurs de configuration peuvent entraîner la perte d’appareils dans des groupes ou même provoquer des boucles infinies.

Groupes Éducation

Nouveau dans 26.5

Le type de groupe Éducation applique automatiquement les politiques liées aux appareils des élèves participants pendant la durée d’un cours. L’appartenance découle des cours en cours dans Relution Teacher ; l’affectation manuelle d’appareils n’est pas possible. Détails sous Groupes Éducation →.

Dupliquer des groupes d’appareils

Depuis Relution 5.33, les groupes d’appareils peuvent être dupliqués afin de simplifier et d’accélérer la gestion.

Pour la version 26.4.0

Pour cela, un ou plusieurs groupes peuvent être sélectionnés sous `Appareils` → `Groupes d’appareils` et dupliqués via le menu à trois points. Un message demande alors quels éléments du groupe d’origine doivent être copiés.

Options disponibles :

- Inclure les actions du groupe d’appareils (uniquement avec l’autorisation de créer des actions de groupes d’appareils)
- Inclure les dispositifs (uniquement pour les groupes statiques)
- Inclure les filtres, si désactivé un groupe statique sera créé (uniquement pour les groupes dynamiques ; si l’option est désactivée, un groupe statique sans appareils est créé)
- Inclure les politiques

Si un seul groupe est dupliqué, la boîte de dialogue demande en outre le Nom du groupe d’appareils dupliqué. Lorsque plusieurs groupes sont dupliqués, les doublons reçoivent automatiquement le nom `<nom d’origine> - dupliquer`.

Supprimer des groupes d’appareils

Les groupes d’appareils devenus inutiles peuvent être sélectionnés sous `Appareils` → `Groupes d’appareils` et supprimés via le menu à trois points. Lors de la suppression d’un groupe, les appareils restent inscrits, mais les politiques qui leur étaient attribuées uniquement via ce groupe leur sont retirées. Si l’option Désinstaller automatiquement les applications obligatoires installées automatiquement si elles ne sont plus nécessaires est activée dans une conformité des applications concernée, les applications sont supprimées avec leurs données locales.

Activer les groupes d’appareils

Obsolète depuis Relution 26.0.0

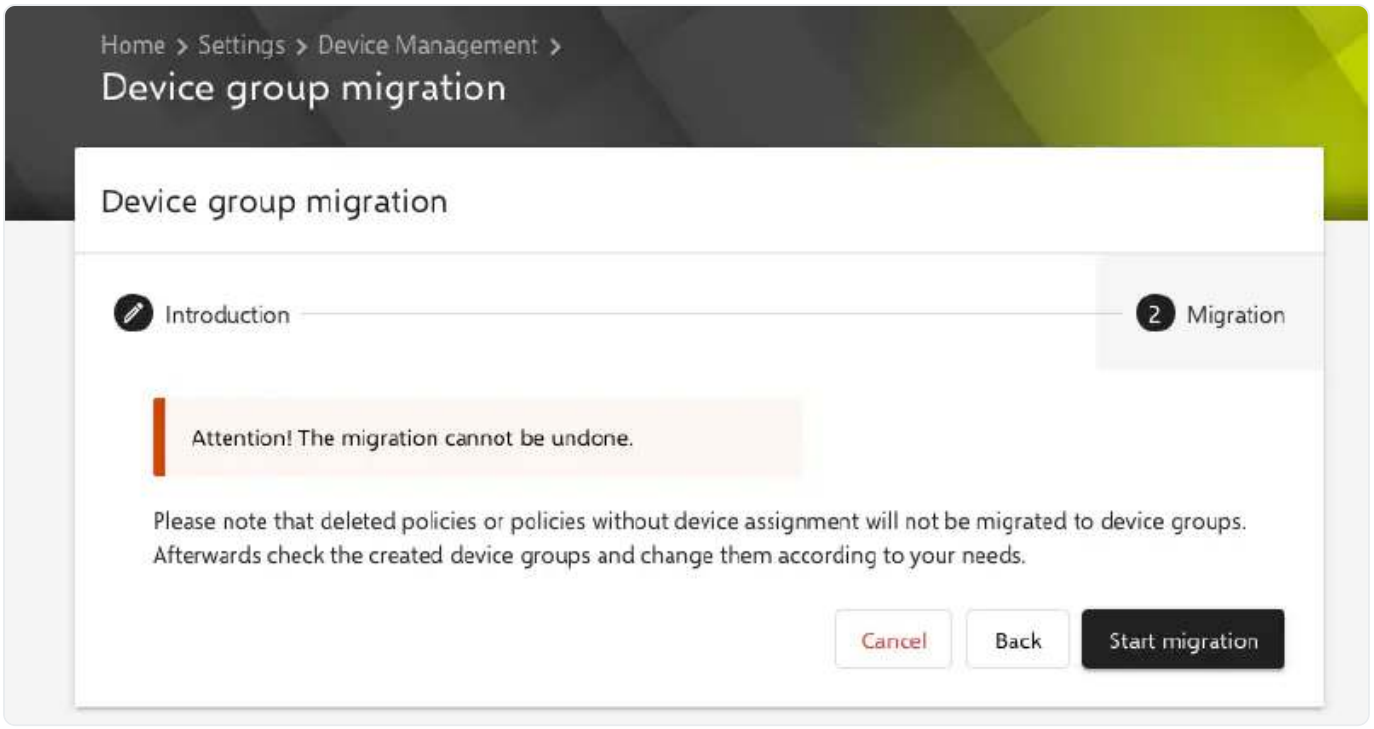
Auparavant, la fonctionnalité des groupes d’appareils devait être activée manuellement via `Paramètres` → `Gestion des appareils` → `Migration des groupes de dispositifs`.

L’attribution des politiques aux groupes d’appareils ne pouvait pas être annulée.



Après avoir cliqué sur Commencer la migration, un message présentant les modifications à venir s’affiche. Il convient de le lire attentivement avant de cliquer sur Suivant.

Dans la boîte de dialogue suivante, la migration peut être exécutée.



Pour la version 26.4.0

Politiques basées sur l'utilisateur

Dans Relution, les politiques sont attribuées par défaut à des groupes d'appareils. Toutefois, grâce aux groupes d'appareils dynamiques et au filtrage basé sur l'utilisateur, les politiques peuvent également être liées de manière ciblée à un utilisateur individuel ou à un groupe d'utilisateurs entier.

Le principe fonctionne comme suit :

1. Un groupe d'appareils dynamique est configuré avec un filtre utilisateur.
2. Dès que l'utilisateur concerné (ou un membre du groupe d'utilisateurs) est attribué à l'appareil en tant qu'utilisateur de l'appareil, celui-ci est automatiquement ajouté à ce groupe d'appareils. L'attribution a généralement lieu lors de l'inscription ou manuellement dans les détails de l'appareil.
3. Les politiques attribuées au groupe d'appareils deviennent actives et sont appliquées à l'appareil.
4. Si l'attribution est supprimée ou si un autre utilisateur est attribué, l'appareil quitte à nouveau le groupe – les politiques sont désactivées.

> Une connexion sur l'appareil ne modifie l'utilisateur de l'appareil que dans les cas suivants : sur les Relution Shared Devices (connexion et déconnexion) et sur les appareils Windows pour lesquels le changement d'utilisateur de l'appareil est activé dans le Windows Companion. Sous Windows, la connexion attribue l'utilisateur ; celui-ci reste attribué jusqu'à la connexion suivante.

Pour plus de détails, voir les articles Appareil partagé Relution → et Changement d'utilisateur à la connexion →.

Prérequis

- Les utilisateurs sont créés dans Relution et, si nécessaire, affectés à un groupe d'utilisateurs
- Les appareils sont inscrits et peuvent être affectés à un utilisateur
- Autorisations dans l'organisation concernée pour créer des groupes d'appareils, lire les utilisateurs ou les groupes (sans cette autorisation, la sélection dans le filtre est désactivée) et attribuer des politiques

Pour la version 26.4.0

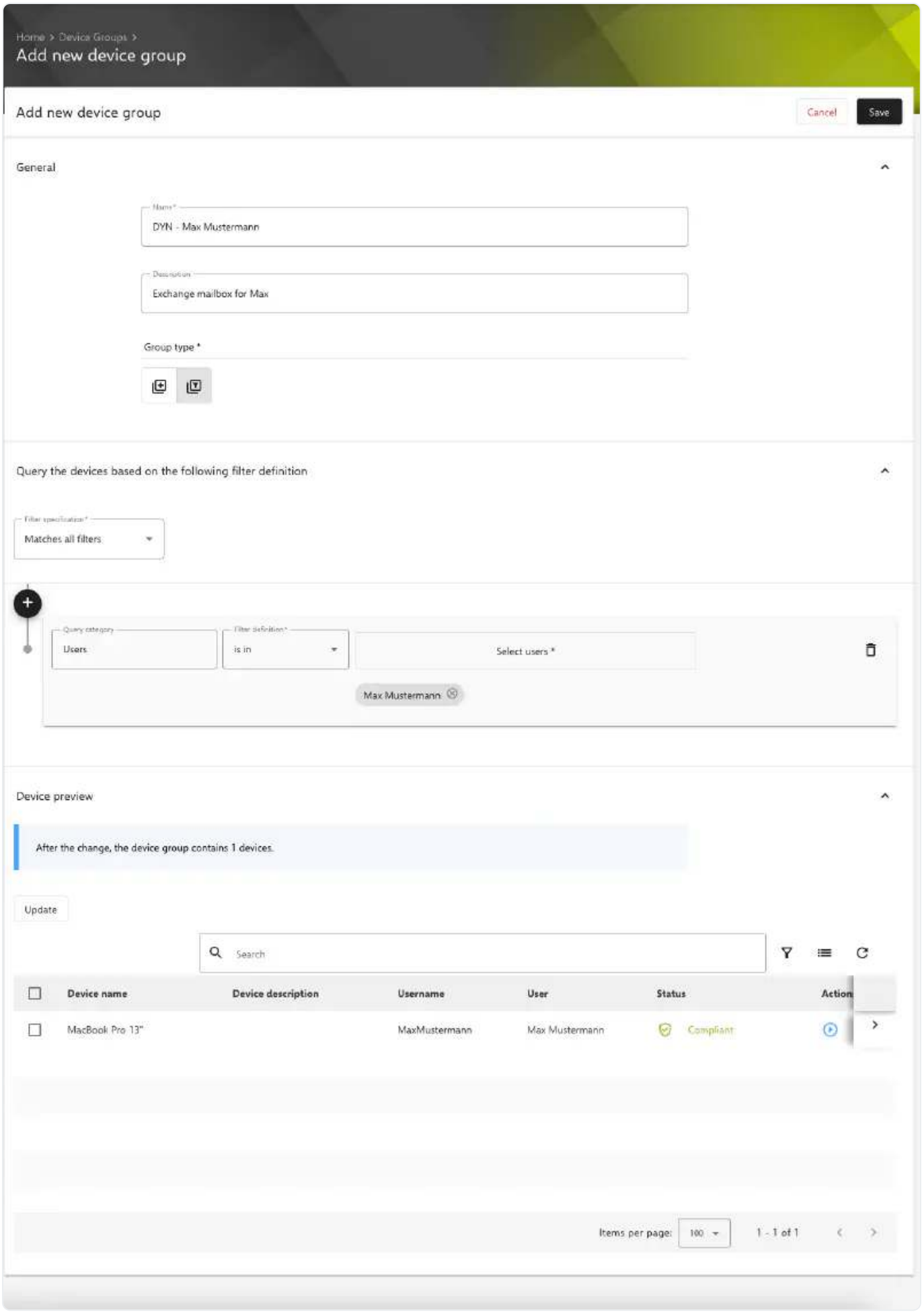
Cas d’utilisation

Scénario	Catégorie de requête	Description
Un utilisateur individuel reçoit une politique spécifique	Utilisateurs	par ex. un développeur a besoin de restrictions allégées, profil Exchange privé
Un département reçoit une configuration uniforme	Groupes	par ex. tous les enseignants reçoivent un profil Exchange partagé
Scénario BYOD	Groupes	Politiques de profil professionnel uniquement pour les utilisateurs BYOD enregistrés

Pour la version 26.4.0

Pour un utilisateur individuel

1. Accéder à `Appareils` → `Groupes d'appareils`.
2. Cliquer sur Ajouter.
3. Attribuer un nom explicite, par ex. `DYN – Jean Dupont`.
4. Sous Type de groupe, sélectionner Dynamique (réglage par défaut). Les options sont affichées sous forme d’icônes ; le libellé apparaît au survol de la souris.
5. Dans la section Interroger les dispositifs sur la base de la définition de filtre suivante, sélectionner les valeurs suivantes dans la ligne de filtre existante :
   - Catégorie de requête : `Utilisateurs`
   - Définition du filtre : opérateur « est dans » (libellé `est en` dans le portail)
   - Cliquer sur Sélectionner les utilisateurs et choisir l’utilisateur souhaité dans la boîte de dialogue (sélection multiple possible).
6. Enregistrer le groupe d’appareils.


Home > Device Groups >
Add new device group
Add new device group
Cancel
Save
General
DYN - Max Mustermann
Exchange mailbox for Max
Group type *
Query the devices based on the following filter definition
Matches all filters
Users
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

Si plusieurs appareils sont attribués à l'utilisateur, tous ces appareils sont ajoutés au groupe.

Pour un groupe d’utilisateurs

1. Accéder à `Appareils` → `Groupes d'appareils`.
2. Cliquer sur Ajouter.
3. Attribuer un nom explicite, par ex. `DYN – Enseignants`.
4. Sous Type de groupe, sélectionner Dynamique (réglage par défaut).
5. Dans la section Interroger les dispositifs sur la base de la définition de filtre suivante, sélectionner les valeurs suivantes dans la ligne de filtre existante :
   - Catégorie de requête : `Groupes`
   - Définition du filtre : opérateur « est dans » (libellé `est en` dans le portail)
   - Cliquer sur Sélectionner des groupes d’utilisateurs et choisir le groupe d’utilisateurs souhaité (sélection multiple possible).
6. Enregistrer le groupe d’appareils.

Le filtre prend également en compte les membres des sous-groupes imbriqués du groupe d’utilisateurs sélectionné.

Pour la version 26.4.0

Les groupes d'utilisateurs peuvent être synchronisés via LDAP/AD. Les modifications apportées à l'appartenance aux groupes sont automatiquement reprises dans Relution. Jusqu'à ce que les groupes d'appareils dynamiques filtrant sur des groupes d'utilisateurs soient réévalués, il peut s'écouler par défaut jusqu'à une heure (en plus de l'intervalle de synchronisation LDAP). Seules les connexions et déconnexions sur les Relution Shared Devices sont évaluées rapidement.

Autres options de filtre

Outre « est dans », les définitions de filtre `pas dans`, `est vide` et `n'est pas vide` sont disponibles pour les catégories Utilisateurs et Groupes. Avec `est vide`, il est par exemple possible de créer un groupe pour tous les appareils sans utilisateur.

D’autres filtres peuvent être ajoutés via + → Ajouter un filtre, par ex. un filtre avec la catégorie Propriété pour le scénario BYOD. Le champ Spécifications du filtre détermine si un appareil doit correspondre à tous les filtres (Correspond à tous les filtres) ou à au moins un filtre (Correspond à au moins un filtre). Après un clic sur Actualisation, l’Aperçu de l’appareil indique quels

appareils remplissent actuellement les filtres. Les détails de tous les filtres figurent dans l'article Groupes d'appareils →.

Attribuer des politiques au groupe d'appareils dynamique

Une fois le groupe d'appareils dynamique créé, les politiques souhaitées lui sont attribuées :

1. Ouvrir le groupe d'appareils nouvellement créé.
2. Passer à l'onglet Politiques.
3. Cliquer sur Ajouter.
4. Dans la boîte de dialogue Ajouter des politiques, sélectionner une ou plusieurs politiques et confirmer.

Les politiques sont désormais liées au groupe d'appareils dynamique et sont appliquées automatiquement dès qu'un appareil remplit la condition de filtre.

Recommandations et bonnes pratiques

Pour la version 26.4.0

- Convention de nommage : Un préfixe uniforme pour les groupes d'appareils dynamiques, par ex. `DYN –`, permet de les distinguer clairement des groupes statiques dans l'aperçu.
- Ordre des politiques : Les conflits possibles doivent être pris en compte lorsqu'un appareil est membre de plusieurs groupes dynamiques en même temps.
- Tests : Les nouveaux groupes dynamiques doivent d'abord être testés avec un seul appareil et un utilisateur de test avant que la configuration soit déployée en production.
- Synchronisation LDAP : En cas d'utilisation de groupes LDAP, il convient de vérifier si les intervalles de synchronisation sont adaptés au cas d'utilisation concerné.

Articles associés

- Les politiques expliquées →
- Groupes d'appareils →
- Gestion des utilisateurs →
- Politiques par réseau (BYOD) →
- Configuration LDAP →

Actions de groupes d’appareils

Avec Relution 5.22, il est possible de déclencher non seulement des politiques mais aussi des actions et des travaux CRON par le biais de l’appartenance à des groupes d’appareils. Cette fonction a entièrement remplacé les ensembles de règles avec Relution 26.0. Les ensembles de règles existants n’ont pas été transférés à la nouvelle fonctionnalité.

> Les groupes d'appareils sont indépendants de la plate-forme. Pour cette raison, il peut être impossible d'appliquer des actions individuelles à certains appareils.

La fonctionnalité de base des groupes d’appareils est expliquée ici : Groupes d’appareils →

Créer des actions

Les actions appartiennent toujours à un groupe d’appareils. Elles sont créées sous `Appareils` → `Groupes d'appareils`, dans la vue détaillée du groupe, onglet Actions, via Ajouter. L’autorisation de créer ou de modifier des actions de groupes d’appareils est nécessaire.

Pour la version 26.4.0

Le formulaire Ajouter une action comprend deux sections :

- Général : Nom, Description (facultative) et Déclencheur. Le champ Déclencheur propose les options Basé sur des événements et Programmé par CRON.
- Action : Le champ Type d’action définit ce qui est exécuté sur les appareils (voir la section Principaux types d’actions).

Dans la liste des actions, chaque action peut être activée ou désactivée via l’interrupteur Activé. Les actions désactivées ne sont pas exécutées.

Basé sur des événements

Les actions basées sur des événements réagissent aux changements d’appartenance au groupe :

1. Déclenchement de l’exécution définit quand l’action est exécutée : Pas de déclencheur, Lorsqu’un appareil entre dans le groupe, Lorsqu’un appareil quitte le groupe ou Les deux.
2. Retard d’exécution propose Immédiatement et Retardé. Avec Retardé, le délai est indiqué en Jours, Heures et Minutes ; la valeur par défaut est de 90 minutes. Si un appareil entré dans le groupe n’en est plus membre à l’expiration du délai, ou si un appareil sorti du groupe en

est de nouveau membre, l'action n'est pas exécutée. Cela évite des exécutions pour des appareils qui n'appartiennent au groupe que brièvement.

Les actions basées sur des événements ne s'appliquent qu'aux entrées et sorties futures. Les appareils qui sont déjà membres du groupe lors de la création de l'action ne déclenchent pas l'action.

Programmé par CRON

1. Les actions peuvent être déclenchées selon un calendrier défini par une expression CRON WIKI CRON →. À chaque échéance, l'action est exécutée pour tous les appareils qui sont alors membres du groupe.
2. Tous les champs sont obligatoires. Les virgules séparent des valeurs individuelles ; les plages et les valeurs de pas sont acceptées. Jours du mois et Jours de la semaine ne peuvent pas contenir tous deux des valeurs concrètes ; l'un des deux est réglé sur `*` ou `?`.
3. Par défaut, l'action est exécutée tous les jours à 06:00 et 21:00 (Minutes `0`, Heures `6,21`, Jours du mois `*`, Mois `*`, Jours de la semaine `?`). Les heures se réfèrent au fuseau horaire du serveur Relution.

Pour la version 26.4.0

Champ	Description	Valeurs autorisées
Minutes	Moment dans l'heure	0 à 59
Heures	Moment dans la journée	0 à 23
Jours du mois	Jour calendaire	1 à 31
Mois	Mois de l'année	1 à 12 (ou JAN-DEC)
Jours de la semaine	Jour de la semaine	0 à 6 (0 = dimanche à 6 = samedi, ou SUN-SAT)

Compléments sur la syntaxe

Les valeurs sont saisies sans espaces ; sinon, le portail refuse la saisie comme non valide.

- Astérisque (`*`) : signifie « chaque » (p. ex. chaque minute, chaque jour).
- Point d'interrogation (`?`) : uniquement pour Jours du mois et Jours de la semaine ; signifie « aucune valeur précise ».
- Virgule (`,`) : sépare des valeurs individuelles (p. ex. `1,15,30` pour les 1re, 15e et 30e minutes).
- Trait d'union (`-`) : définit une plage (p. ex. `1-5` pour lundi à vendredi).
- Barre oblique (`/`) : définit des intervalles (p. ex. `*/5` pour toutes les 5 unités).

Crontab Guru →

Ces configurations sont directement valides et sont appliquées après l'enregistrement.

Principaux types d'actions

Le champ Type d'action propose les types suivants :

1. Supprimer un appareil
2. Action du dispositif
3. Action de notification
4. Modifier le nom de l'appareil
5. Actualiser la politique de l'appareil
6. Webhook

Pour la version 26.4.0

Supprimer un appareil

Description :

- Cette action retire l'appareil de la gestion de Relution. Ce qui se passe sur l'appareil dépend du type d'inscription :
  - Les appareils Android Enterprise entièrement gérés sont réinitialisés aux paramètres d'usine.
  - Sur les appareils Android Enterprise avec profil professionnel ou avec profil personnel, seul le profil professionnel est supprimé ; les applications et données personnelles sont conservées.
  - Sur toutes les autres plates-formes, la gestion est retirée (p. ex. le profil MDM sur les appareils Apple ou l'inscription sous Windows), mais l'appareil n'est pas réinitialisé.
- Important : Cette action ne peut pas être annulée.
- Pour les appareils inscrits via KME (Knox Mobile Enrollment), il faut s'assurer qu'aucun profil n'est attribué dans le portail d'inscription Samsung Knox, car l'appareil serait sinon automatiquement réinscrit après la suppression (Android uniquement).

Options :

- Android :
  - Conserver l’application client Relution : oui/non
- Appareil géré (Android Enterprise, entièrement géré) :
  - Conserver la protection contre la réinitialisation d’usine (FRP) activée : oui/non
  - Effacer également le stockage externe de l’appareil (comme les cartes SD) : oui/non
  - Message : texte affiché aux utilisateurs d’appareils personnels avec profil professionnel avant la suppression du profil professionnel. Il n’a aucun effet sur les appareils appartenant à l’entreprise.

Action du dispositif

Description :

- Permet d’effectuer diverses actions individuelles sur les appareils.

Après la sélection, la section Détails indique les plates-formes sur lesquelles l’action est disponible.

Pour la version 26.4.0

Sous-actions :

1. Activer le mode perdu
   - Verrouille l’appareil et permet de le localiser. Peut être utilisé lorsqu’un appareil a été perdu.
   - Champs : Message, numéro de téléphone, note de bas de page, courriel, adresse, nom de l’organisation
2. Désactiver le mode perdu
   - Annule le Mode Perdu.
3. Redémarrer l’appareil
   - Redémarre l’appareil.
   - Champ : Motif du redémarrage (uniquement appareils Android sans Android Enterprise et tableaux blancs interactifs)
   - Options : Mise hors tension (uniquement appareils Android sans Android Enterprise et tableaux blancs interactifs), Notifier à l’utilisateur de redémarrer l’appareil (pas de redémarrage forcé), uniquement macOS 11 ou version ultérieure
4. Actualiser les informations sur l’appareil
   - Actualise les informations sur l’appareil stockées dans Relution.
5. Alerte
   - Déclenche une alarme sur l’appareil.
   - Champ : Durée (en secondes)
6. Activer ou désactiver le Bluetooth

- Active ou désactive le Bluetooth.
- Option : Activer Bluetooth

7. Analyser l'appareil
   - Lance une analyse antivirus Microsoft Defender sur les appareils Windows.
   - Champ : Type de balayage (Balayage rapide ou Balayage complet)
8. Supprimer des utilisateurs locaux
   - Supprime tous les comptes et données des utilisateurs locaux.
   - Option : Forcer la suppression des comptes
9. Activer ou désactiver le point d'accès personnel
   - Active ou désactive le point d'accès personnel.
   - Option : Activer le point d'accès personnel
10. Plan cellulaire eSIM
    - Configure un plan mobile eSIM.
    - Champ : URL du serveur
11. Supprimer le raccourci
    - Supprime un raccourci de l'appareil.
    - Champs : Label, URL
12. Démarrer la lecture AirPlay
    - Lance la lecture AirPlay sur une Apple TV ou un autre appareil compatible AirPlay.
    - Champs : Nom, adresse MAC, durée de balayage (secondes), mot de passe
13. Return to Service
    - Réinitialise l'appareil aux paramètres d'usine. L'appareil tente ensuite de se réinscrire automatiquement dans Relution ; le verrouillage d'activation doit pour cela être désactivé. Disponible pour iOS 17 ou version ultérieure et tvOS 18 ou version ultérieure.
    - Champ : Configuration Wi-Fi (obligatoire ; sélection parmi les configurations Wi-Fi activées des politiques publiées)
    - Option : Conserver le plan de données existant (iOS uniquement)
14. Envoyer un fichier à l'appareil
    - Envoie un fichier à l'appareil.
    - Champs : Sélectionner le fichier, le répertoire, ne pas décompresser les archives ZIP
15. Effacer l'appareil
    - Réinitialise l'appareil aux paramètres d'usine.
    - Options : Conserver la protection contre la réinitialisation d'usine (FRP) activée, Effacer également le stockage externe de l'appareil, Message, PIN, Conserver le plan de données existant, Désactiver la configuration de la proximité
16. Installer la mise à jour de Prowise
    - Installe une mise à jour de Prowise.
    - Champ : Mise à jour sur
17. Verrouiller l'appareil
    - Verrouille l'appareil avec le mot de passe actuel.
    - Champs : Message, numéro de téléphone, code PIN

Pour la version 26.4.0

18. Ajouter un raccourci
    - Ajoute un raccourci à l'appareil.
    - Champs : Label, URL, Ouvrir en plein écran, Icône
19. Réinitialiser le code de verrouillage
    - Réinitialise le mot de passe de l'appareil.
    - Champ : Nouveau mot de passe
    - Options : Verrouiller immédiatement, Exiger la saisie avant la prochaine réinitialisation, Ne pas demander au démarrage
20. Réinitialiser le mot de passe (Windows)
    - Réinitialise le mot de passe d'un compte utilisateur Windows.
    - Champs : Nom d'utilisateur, Mot de passe, Répéter le mot de passe
    - Action : Générer un exemple de mot de passe
21. Arrêter l'appareil
    - Arrête l'appareil.
22. Arrêter la lecture AirPlay
    - Met fin à la lecture AirPlay.
23. Localiser l'appareil
    - Déclenche la localisation de l'appareil.
24. Effacer le mot de passe des restrictions
    - Supprime le code Temps d'écran.
25. Activer ou désactiver l'itinérance des données
    - Active ou désactive l'itinérance des données sur les appareils iOS. L'utilisateur peut modifier de nouveau ce paramètre sur l'appareil.
    - Option : Activer l'itinérance des données
26. Continuer dans l'Assistant Configuration de l'appareil
    - Poursuit la configuration de l'appareil dans l'Assistant Configuration.
27. Installer le média
    - Installe le média sur l'appareil.
    - Champ : Sélection du jeton
28. Supprimer les médias
    - Supprime le média de l'appareil.
    - Champ : Sélection du jeton
29. Exécuter le script PowerShell
    - Exécute un script PowerShell sur les appareils Windows.
30. Déconnexion de l'utilisateur
    - Déconnecte l'utilisateur actuel.
31. Exécuter un script shell
    - Exécute un script shell sur les appareils macOS et Linux. La sous-action n'est disponible que si le compagnon macOS est activé (`Paramètres` → `Applications` `client Relution`, interrupteur Activer le compagnon macOS).
32. Demande d'informations sur l'appareil

Pour la version 26.4.0

    - Demande des informations spécifiques sur l'appareil (Android Enterprise, profil professionnel sur un appareil personnel, Android 13 ou version ultérieure). L'utilisateur est invité à approuver la divulgation de ces informations.
    - Champ : Type (Identifiant eSIM (EID))
33. Enterprise Wipe (Nettoyage d'entreprise dans le portail)
    - Supprime le profil professionnel et toutes les politiques, en laissant l'appareil à un usage personnel. Les applications et les données du profil personnel sont conservées (Android Enterprise, appareil d'entreprise avec profil personnel, Android 8 ou version ultérieure).
34. Définir les applications par défaut
    - Définit les applications par défaut pour les appels, la messagerie et la navigation web sur les appareils iOS.
    - Champs : Application d'appel par défaut et Application de messagerie par défaut (iOS 26 ou version ultérieure), Application du navigateur par défaut (iOS 18.2 ou version ultérieure)
35. Activer le bureau à distance
    - Active sur les Mac la gestion à distance via Apple Remote Desktop : accès pour tous les utilisateurs, réception d'événements à distance ainsi que les options Observer, Contrôler et Montrer que l'on observe. Toutes les autres options restent inchangées (macOS 10.14.4 ou version ultérieure).
36. Désactiver le bureau à distance
    - Désactive sur les Mac la gestion à distance via Apple Remote Desktop (macOS 10.14.4 ou version ultérieure).

Pour la version 26.4.0

Action de notification

Description :

- Envoie des notifications aux utilisateurs de l'appareil ou à d'autres personnes.

Destinataires :

- Notifier l'utilisateur de l'appareil
- Notifier les autres utilisateurs : sélection d'utilisateurs et de groupes d'utilisateurs
- Destinataires supplémentaires du courrier électronique : autres adresses e-mail

Message :

- Notification par courrier électronique : envoi d'un e-mail basé sur un modèle. Remise au modèle rétablit le texte par défaut.
- Notification par message push : les destinataires reçoivent le message push sur tous les appareils inscrits qui leur sont attribués.

Des espaces réservés peuvent être utilisés dans les textes ; les espaces réservés disponibles sont affichés dans le formulaire : Espaces réservés avancés →

Modifier le nom de l'appareil

Description :

- Modifie le nom de l'appareil.

Champ : Nom de l'appareil. Les espaces réservés tels que `${device.serialnumber}` sont résolus pour chaque appareil. Si le résultat est un nom vide, le nom actuel de l'appareil est conservé.

Actualiser la politique de l'appareil

Description :

- Met à jour les politiques appliquées à l'appareil.

Webhook

Description :

- Envoie une requête à un service externe (par exemple, un autre système).

Pour la version 26.4.0

Champs : URL, Méthode (GET, POST ou PUT ; POST est présélectionné), En-têtes (en-têtes de requête sous forme de liste), Corps

Sous Tester les paramètres du webhook, Vérifier la connectivité fait envoyer par le serveur une requête OPTIONS à l'URL indiquée et affiche la réponse. Cela permet de vérifier si l'hôte cible est accessible depuis le serveur Relution.

Géo-zones

Cet article décrit comment attribuer automatiquement des politiques en fonction de l'emplacement de l'appareil. Ces géofences doivent être créées à l'avance, puis attribuées à l'aide de groupes d'appareils dynamiques.

Restrictions et notes

> La fonction de géofence nécessite une connexion Internet permanente, un module GPS sur l'appareil et l'Agent Relution installé. Les plateformes prises en charge sont iOS (iPhone et iPad avec module cellulaire, p. ex. Cellular iPad →), Android et Android Enterprise.

- Sur les appareils Android, la détection peut être retardée selon l'état de l'appareil, dans des cas exceptionnels jusqu'à 30 minutes.
- Dans le portail, le rayon d'une géofence est fixé à 100 mètres autour de l'emplacement défini.

Si la géo-zone est modifiée sans connexion internet et sans GPS, une synchronisation manuelle des données de localisation doit être déclenchée sur l'appareil dans l'Agent de Relution.

Pour la version 26.4.0

Préparation

Pour que les géofences fonctionnent, l'Agent Relution doit être installé sur l'appareil et avoir été ouvert au moins une fois. En outre, les autorisations relatives aux notifications push et aux services de localisation doivent être accordées à l'Agent Relution ; l'utilisateur ne doit pas les retirer. Cela s'applique aux appareils iOS et Android. Sous Android, l'Agent Relution a besoin de l'autorisation de localisation en permanence, c'est-à-dire également en arrière-plan.

Sur les appareils iOS, l'autorisation de localisation ne peut pas être accordée automatiquement via l'interface MDM. Par conséquent, les utilisateurs doivent configurer ce paramètre eux-mêmes.

> Pour ce faire, la valeur Allow access to location (Autoriser l'accès à la localisation) doit être réglée sur Always (Toujours) sous `Settings` → `Apps` → `Relution Agent` → `Location` sur l'appareil iOS.

Si ce n'est pas le cas, l'Agent de Relution ne peut pas transmettre l'emplacement actuel au serveur et l'attribution automatique des politiques n'est pas possible.

Si des zones ou des iBeacons sont configurés dans l'organisation, Relution crée une notification de conformité (Permission de localisation ou Services de localisation) pour les appareils dont l'Agent Relution n'a pas l'autorisation de localisation ou dont les services de localisation sont désactivés. L'appareil reste conforme.

Mise en place d'une géofence

Les géofences sont gérées sous `Paramètres` → `Attribution dynamique des politiques` → `Zones`. Une nouvelle géofence est créée via Ajouter.
Dans la section Général, un Nom est saisi (champ obligatoire). Dans la section Adresse, l'emplacement est défini : via la barre de recherche de la carte (adresse ou coordonnées au format latitude, longitude, p. ex. `48.7968, 9.2211`), par un clic droit ou un appui long sur la carte, ou directement via les champs Latitude et Longitude. Le bouton Plan du centre (centrer la carte) centre la carte sur le marqueur défini.
Enregistrer crée la géofence ; le bouton n'est actif que lorsque le nom et les coordonnées sont définis. Relution détermine automatiquement l'adresse affichée à partir des coordonnées lors de l'enregistrement.
Une entrée devrait maintenant avoir été ajoutée à l'aperçu de la géofence.

Pour la version 26.4.0

Lorsqu'une géofence est créée, modifiée ou supprimée, Relution envoie automatiquement l'action de rechargement des zones (Zones de rechargement dans le portail) à tous les appareils iOS, Android et Android Enterprise, afin que l'Agent Relution charge les zones actuelles. L'action apparaît dans l'historique des actions de l'appareil et ne peut pas être déclenchée manuellement.

L'affichage, la création, la modification et la suppression de géofences nécessitent, dans le rôle, les permissions pour Zones dans la section Attribution dynamique des politiques : Permissions →

Ce que l'Agent Relution affiche à l'utilisateur au sujet des zones et des iBeacons à portée est défini par le paramètre Affichage d'informations sur les iBeacons et les zones à portée sous `Paramètres` → `Gestion des appareils`, dans la section Relution Agent (Agent de relution dans le portail) : Masquer (par défaut), Informations complètes ou Représentation occultée.

Configuration du groupe d'appareils

Pour pouvoir appliquer la géofence à un groupe d'appareils dynamique, celui-ci doit être configuré avec un filtre.
Sous `Appareils` → `Groupes d'appareils`, un nouveau groupe d'appareils dynamique est

créé ou un groupe existant est modifié.
Comme Catégorie de requête, Zones saisies (zones dans lesquelles l'appareil se trouve) est sélectionné et, par exemple, l'opérateur d'inclusion est en comme Définition du filtre ; les géofences souhaitées sont choisies via Sélectionner les zones. Les appareils qui se trouvent dans au moins une de ces zones deviennent alors automatiquement membres du groupe. La politique souhaitée est ensuite attribuée au groupe.

Autres définitions de filtre : avec tous les, l'appareil doit se trouver dans toutes les zones sélectionnées, avec pas dans, dans aucune d'entre elles ; n'est pas vide et est vide incluent les appareils situés dans une zone quelconque ou dans aucune zone et ne nécessitent pas de sélection de zone.

Groupes d'appareils →

Les zones dans lesquelles un appareil se trouve actuellement sont indiquées dans la liste des appareils par la colonne et le filtre Zones de géofence saisies, ainsi que dans les détails de l'appareil, sur la carte Emplacement de l'appareil, sous Zones saisies.

Outre la position géographique, les politiques peuvent également être attribuées en fonction de signaux radio dans l'espace : iBeacons →

Pour la version 26.4.0

iBeacons

Outre les géozones →, Relution permet également d'attribuer des politiques en fonction des iBeacons. Un iBeacon est un émetteur Bluetooth dont le signal est reçu par les appareils situés à proximité. Lorsqu'un appareil se trouve à portée d'une balise enregistrée, il peut recevoir automatiquement une autre politique via un groupe d'appareils dynamique.

Dans le portail, les deux approches relèvent de la section `Paramètres` → `Attribution dynamique des politiques` : les Zones s'appuient sur la position géographique, les iBeacons sur des signaux radio dans l'espace. Les iBeacons conviennent donc également là où le GPS n'est pas disponible de manière fiable — à l'intérieur des bâtiments, par exemple.

Limites et remarques

Les conditions suivantes doivent être remplies pour utiliser la fonction :

- L'application Relution Agent doit être installée et avoir été ouverte au moins une fois.
- Les autorisations relatives aux notifications push, aux services de localisation et au Bluetooth doivent être activées pour l'application Relution Agent et ne doivent pas être désactivées par les utilisateurs.
- Sur les appareils Android, la détection peut être retardée selon l'état de l'appareil. Dans des cas exceptionnels, cela peut prendre jusqu'à 30 minutes.

Pour la version 26.4.0

Les appareils iOS, Android et Android Enterprise sont pris en charge. Relution n'évalue pas les iBeacons sous macOS et Windows, même si un Relution Agent y est installé.

Si des iBeacons ou des zones sont configurés dans l'organisation, Relution crée une notification de conformité (Permission de localisation ou Services de localisation) pour les appareils dont le Relution Agent n'a pas l'autorisation de localisation ou dont les services de localisation sont désactivés. L'appareil reste conforme.

Les balises elles-mêmes sont du matériel tiers et ne font pas partie de Relution. Relution gère uniquement leurs identifiants et évalue lesquels un appareil reçoit.

Créer un iBeacon

Accéder à `Paramètres` → `Attribution dynamique des politiques` → `iBeacons` et créer une nouvelle entrée via Ajouter. Un iBeacon est identifié par trois valeurs définies par le matériel utilisé :

- Identifiant unique (UUID) — un UUID spécifique à l'application et au cas d'utilisation du déploiement.
- Major ID — précise un iBeacon et un cas d'utilisation particuliers, par exemple une sous-région au sein de la région définie par l'UUID.
- ID mineur — permet de subdiviser davantage la région ou le cas d'utilisation.

S'y ajoute un nom, libellé lisible par l'homme sous lequel la balise apparaîtra ensuite dans les filtres.

Le Nom et l'Identifiant unique (UUID) sont obligatoires ; Major ID et ID mineur sont facultatifs et acceptent des valeurs de 1 à 65535.

> La combinaison UUID, Major ID et ID mineur doit être unique. Si une entrée comportant ces trois mêmes valeurs existe déjà, la création est refusée avec un message.

Une répartition courante consiste à utiliser un UUID commun par site, le Major ID par bâtiment ou par étage et l'ID mineur par salle. Les filtres peuvent ensuite être construits à la granularité souhaitée.

Pour la version 26.4.0

Les entrées existantes peuvent être modifiées via Éditer et supprimées via Supprimer dans la liste. L'affichage, la création, la modification et la suppression nécessitent, dans le rôle, les permissions pour iBeacons dans la section Attribution dynamique des politiques : Permissions →

Lorsqu'un iBeacon est créé, modifié ou supprimé, Relution envoie automatiquement l'action Recharger les iBeacons à tous les appareils iOS, Android et Android Enterprise, afin que le Relution Agent charge les définitions iBeacon actuelles. L'action apparaît dans l'historique des actions de l'appareil, mais ne peut pas être déclenchée manuellement.

Suivre les iBeacons sur l'appareil

Les balises actuellement reçues par un appareil sont visibles à deux endroits :

- Dans l'aperçu de l'inventaire, via la colonne iBeacons à portée. Le filtre du même nom restreint la liste à certaines balises, la valeur de filtre Pas d'iBeacons aux appareils sans réception.

- Dans les détails de l’appareil, sur la carte Emplacement de l’appareil, également sous iBeacons à portée. Y figurent les iBeacons qui sont suffisamment proches pour que l’appareil puisse recevoir leur signal. La carte n’apparaît que si l’appareil reçoit des balises, a pénétré dans une zone ou signale l’état du service de localisation.

Ce que le Relution Agent affiche à l’utilisateur au sujet des iBeacons et des zones à portée est défini par le paramètre Affichage d’informations sur les iBeacons et les zones à portée sous `Paramètres` → `Gestion des appareils`, dans la section Relution Agent (Agent de relution dans le portail) : Masquer (par défaut), Informations complètes ou Représentation occultée.

Configurer le groupe d’appareils

Pour qu’une balise déclenche une politique, elle est définie comme filtre dans un groupe d’appareils dynamique.

Accéder à `Appareils` → `Groupes d'appareils` et créer un nouveau groupe d’appareils dynamique ou en modifier un existant. Comme Catégorie de requête, iBeacons à portée est sélectionné et, comme Définition du filtre, l’opérateur d’inclusion est en ; les balises souhaitées sont ensuite choisies via Sélectionner les iBeacons. Les appareils qui reçoivent au moins l’un de ces signaux deviennent alors automatiquement membres du groupe et reçoivent la politique qui y est attribuée.

Autres définitions de filtre : avec tous les, toutes les balises sélectionnées doivent être à portée simultanément, avec pas dans, aucune d’entre elles ; n’est pas vide et est vide incluent les appareils ayant une balise quelconque ou aucune balise à portée et ne nécessitent pas de sélection de balise.

Groupes d’appareils →

Sujets connexes

- Géo-zones → — attribuer des politiques en fonction de la position géographique.
- Groupes d’appareils → — groupes dynamiques et leurs filtres.

Pour la version 26.4.0

Politiques par réseau (BYOD)

Dans les scénarios BYOD, les appareils sont utilisés à la fois à l'intérieur et à l'extérieur de l'établissement.
Un pilotage purement basé sur le temps des politiques est souvent peu flexible et implique une charge de maintenance élevée.

Une alternative éprouvée est l'attribution de politiques basée sur le réseau, où les politiques sont automatiquement appliquées dès qu'un appareil se trouve sur le réseau de l'établissement. La détection s'effectue via l'adresse IP publique du réseau.

Cette approche est particulièrement adaptée au BYOD, car les appareils ne sont pas inutilement restreints en dehors de l'établissement, tout en réduisant la charge administrative.

Principe de base

Pour la version 26.4.0

L'emplacement d'un appareil BYOD est déterminé indirectement via son adresse IP publique.

La configuration se compose de :

- Une politique qui ne doit s'appliquer que sur le réseau de l'établissement
- Un groupe d'appareils dynamique qui rassemble les appareils en fonction de leur adresse IP publique

Lorsqu'un appareil contacte Relution depuis le Wi-Fi de l'établissement, Relution détecte l'adresse IP publique du réseau de l'établissement. L'appareil est alors automatiquement affecté au groupe d'appareils dynamique et reçoit la politique correspondante.

> L'appareil doit rester connecté au Wi-Fi de l'établissement pour que la configuration soit appliquée et maintenue.

Groupe de base BYOD recommandé

Indépendamment du groupe dynamique pour le réseau de l'établissement, les appareils BYOD doivent toujours être affectés à un groupe d'appareils de base.

Celui-ci contient des configurations qui s'appliquent de façon permanente, par exemple :

- Profils Wi-Fi de l’établissement
- Applications obligatoires
- Restrictions de base qui s’appliquent également en dehors de l’établissement

Cela garantit que les appareils restent fonctionnels en permanence.

Configurer le groupe d’appareils dynamique

Un nouveau groupe dynamique est créé. Comme Catégorie de requête, Dernière adresse IP est sélectionnée et, comme Définition du filtre, l’opérateur d’inclusion est en. L’adresse IPv4 publique ou la plage IPv4 du réseau de l’établissement est saisie dans le champ Adresse IP ou CIDR (p. ex. `203.0.113.25` ou `203.0.113.0/24`) ; plusieurs entrées sont possibles.

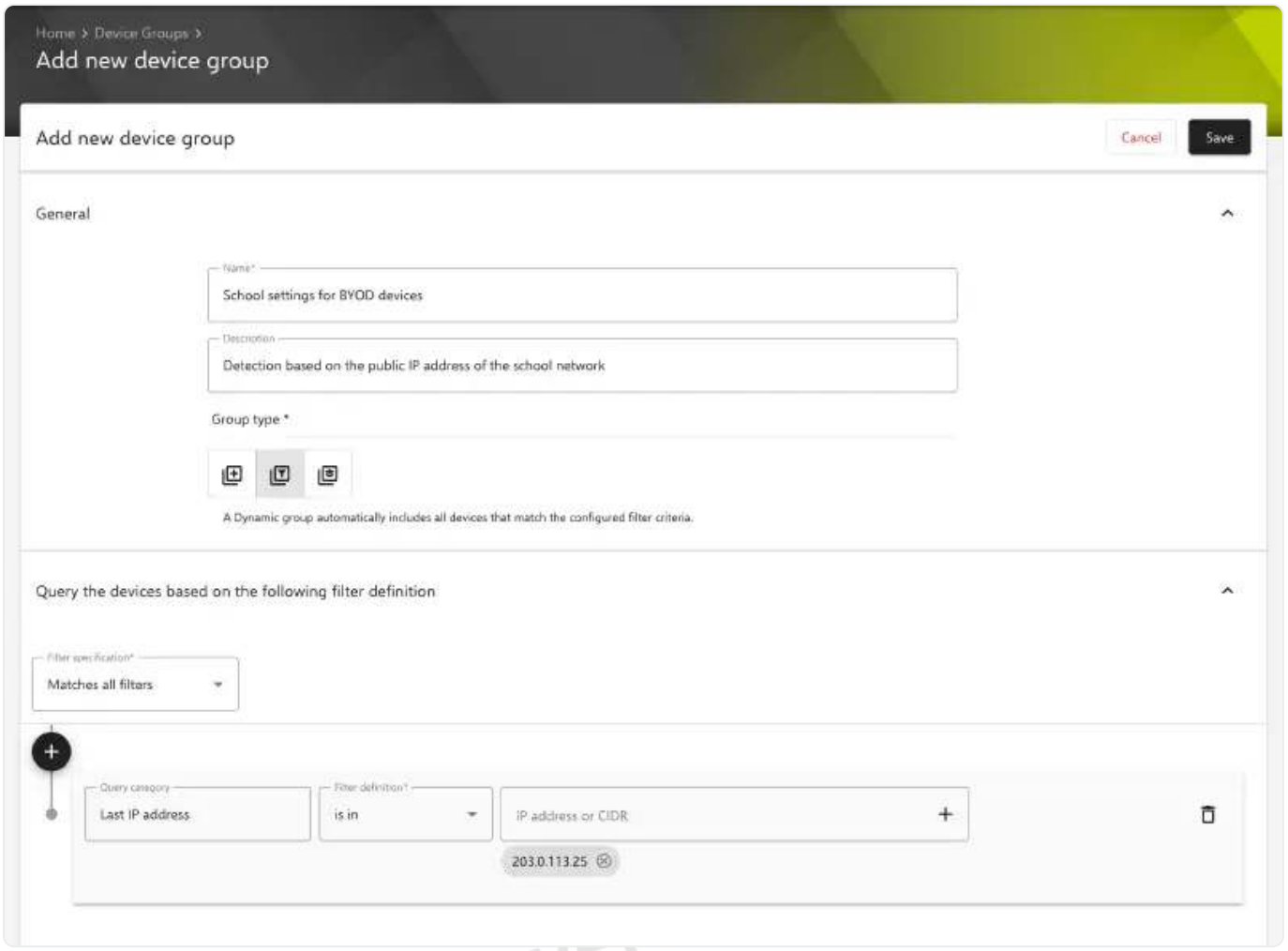
Le filtre doit couvrir la plage d’adresses IP publiques du réseau de l’établissement.
Tous les appareils dont la dernière adresse IP détectée se situe dans cette plage sont automatiquement ajoutés au groupe.

Le filtre n’évalue que les adresses IPv4. Si un appareil atteint le serveur Relution via IPv6, sa dernière adresse IP est enregistrée en tant qu’adresse IPv6 et l’appareil n’est pas pris en compte par le groupe.

La dernière adresse IP détectée par Relution pour un appareil figure dans les détails de l’appareil, sur la carte Réseau sous Dernière adresse IP, ainsi que dans la colonne du même nom de la liste des appareils. Cela permet de déterminer la plage publique appropriée.

Groupes d’appareils →

Pour la version 26.4.0



Pour la ve

Mise à jour de l’adresse IP

Relution reprend l’adresse IP publique de la connexion dès que l’appareil contacte le serveur. L’action Actualiser les informations sur l’appareil permet de le déclencher de manière ciblée.

Une actualisation a lieu notamment dans les cas suivants :

- Lors de l’exécution de politiques
- Lors du ping périodique de vérification de disponibilité, si Vérifiez la disponibilité des appareils est activé (une fois par jour par défaut, réglable via Intervalle ping en minutes sous `Paramètres` → `Gestion des appareils` ; pas pour Android Enterprise)
- Via une action de groupe d’appareils avec le déclencheur programmé par CRON
- Lorsqu’un administrateur exécute l’action Actualiser les informations sur l’appareil pour l’appareil dans le portail
- Lorsque l’utilisateur lance une actualisation dans le portail libre-service (au plus tôt 5 minutes après la dernière actualisation)

- Lorsque l’utilisateur déclenche manuellement l’action dans le Relution Agent via l’onglet Paramètres

---

Recommandation : action programmée par CRON dans le groupe de base

Dans la plupart des environnements BYOD, une action de groupe d’appareils du type Action du dispositif avec Actualiser les informations sur l’appareil et le déclencheur programmé par CRON est recommandée. L’action est créée dans le groupe de base BYOD, dans lequel l’appareil se trouve durablement, et non dans le groupe dynamique basé sur l’adresse IP. Une action CRON n’est exécutée que pour les appareils qui sont actuellement membres du groupe. Dans le groupe dynamique, elle n’atteindrait jamais les appareils situés hors du réseau de l’établissement, qui ne seraient donc pas ajoutés automatiquement au groupe. Le groupe de base garantit que les appareils actualisent régulièrement leur adresse IP, sans qu’une intervention de l’utilisateur soit nécessaire.

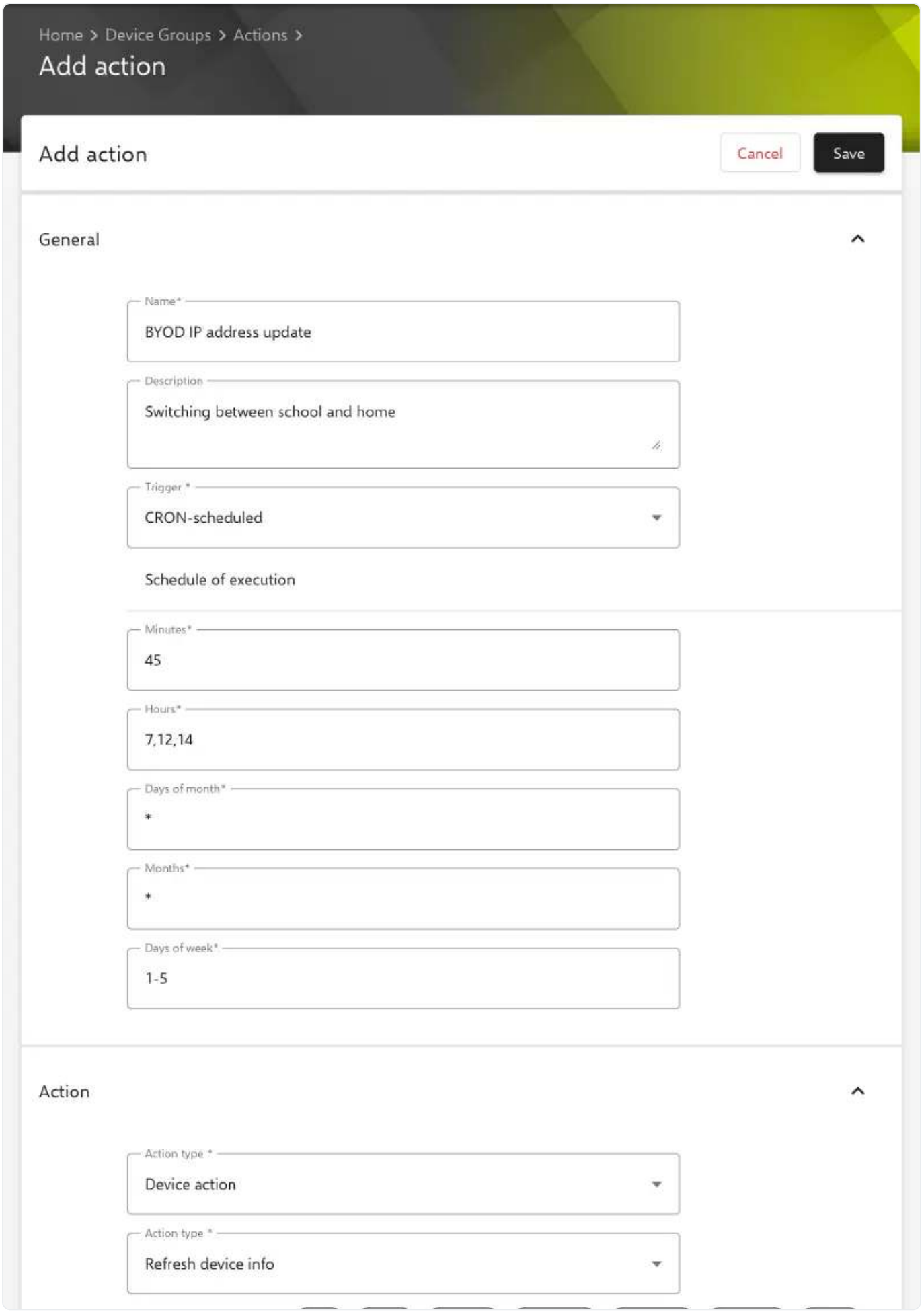
Remarques sur l’utilisation des actions CRON

- Ne pas utiliser d’intervalles très courts
- Ne pas configurer de fréquence de répétition élevée

Par exemple, une exécution horaire de Actualiser les informations sur l’appareil peut entraîner des problèmes de performance importants pour un grand nombre d’appareils.

Un intervalle modéré est suffisant et garantit un fonctionnement stable.
Dans l’exemple de configuration suivant, l’action est exécutée tous les jours de la semaine à 7 h 45, 12 h 45 et 14 h 45.

Pour la version 26.4.0


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

Avantages de l’attribution basée sur le réseau (BYOD)

- Aucun planning complexe nécessaire
- Les politiques ne s’appliquent que sur le réseau de l’établissement
- Moins de politiques par rapport aux approches basées sur le temps
- Idéal pour les appareils à usage privé

Limitations et remarques

- Les appareils doivent être connectés au réseau de l’établissement
- La méthode dépend de plages d’adresses IP publiques stables
- Seul IPv4 est pris en charge ; les appareils qui atteignent Relution via IPv6 ne sont pas détectés
- Les modifications ne prennent parfois effet qu’après la prochaine actualisation des informations sur l’appareil
- Si un reverse proxy est placé devant Relution, il doit transmettre l’IP du client dans l’en-tête `X-Forwarded-For` et être déclaré comme proxy fiable (Relution évalue les en-têtes transférés via `server.forward-headers-strategy=native`) ; sinon, Relution ne voit que l’adresse du proxy, voir Déclarer l’IP du reverse proxy comme fiable →

Pour la version 26.4.0

Résumé

L’attribution de politiques basée sur le réseau via l’adresse IP publique est une solution fiable et nécessitant peu de maintenance pour les environnements BYOD.

Elle permet d’appliquer les politiques de l’établissement de manière ciblée uniquement lorsque les appareils se trouvent réellement sur le réseau, tout en restant utilisables sans restriction à l’extérieur.

Aperçu de l'inventaire

L’aperçu de l’inventaire dans Relution offre de nombreuses informations et possibilités de personnalisation. Un aperçu des fonctions disponibles est proposé ci-après. L’inventaire des appareils fournit toutes les informations et fonctions pertinentes nécessaires à la gestion des appareils.

Colonnes disponibles

- Nom de l’appareil
- Description
- Organisation (visible uniquement avec des droits de lecture sur les appareils d’autres organisations)
- Utilisateur
- Nom d’utilisateur
- Adresse e-mail
- État
- Actions (nombre d’actions en attente)
- Mises à jour disponibles (Windows)
- État de la connexion
- État de la politique
- Plateforme
- Type d’inscription
- Téléphone
- Fabricant
- Modèle
- Propriété
- Dernière connexion
- Date de la dernière connexion à Companion
- Inscrit
- Créé le
- Groupes d’appareils
- Stratégies à installer
- Politiques actives
- Type d’inscription automatique
- Numéro de série
- Version de l’OS
- Édition OS

Pour la version 26.4.0

- État de mise à jour
- MAC Wi-Fi
- MAC Ethernet
- État du mode perdu
- Supervisé
- Bootstrap Token
- iPad partagé
- Niveau de batterie
- IMEI
- ICCID(s)
- Roaming
- Dernière adresse IP
- Dernier lieu connu (pays déterminé à partir de la dernière adresse IP)
- iBeacons à portée
- Zones de géorepérage actives
- Date d'expiration du certificat d'identité (dans la sélection des colonnes : Le certificat d'identité a expiré)
- Faire confiance aux certificats d'identité expirés
- FDE
- Niveau de correctif de sécurité
- Politiques désactivées
- Prêt à (uniquement si le système de prêt est activé, voir Prêt →)
- Prêt jusqu'au (uniquement si le système de prêt est activé)

Pour la version 26.4.0

De plus, cinq colonnes personnalisées sont disponibles ; elles peuvent être activées et nommées dans les paramètres, voir Propriétés personnalisées de l'appareil →.

L'ordre et la visibilité de toutes les colonnes peuvent être configurés individuellement par l'utilisateur. Dans la sélection des colonnes, l'ordre se modifie par glisser-déposer. Les largeurs de colonnes ajustées sont enregistrées.

Options de recherche et de filtrage

Les colonnes peuvent être triées par ordre croissant ou décroissant. Par défaut, la liste est triée par Dernière connexion dans l'ordre décroissant. Il est également possible de restreindre la liste et de la rendre plus claire à l'aide de termes de recherche.

Les options de filtrage suivantes sont disponibles :

- Organisation (uniquement avec des droits de lecture sur les appareils d'autres organisations)

- Plateforme
- Type d’inscription
- Version de l’OS
- Niveau de correctif de sécurité
- Mise à jour de l’OS en attente (oui / non)
- Modèles d’appareils
- État
- État du mode perdu
- Édition OS
- Groupe d’appareils
- Propriété
- Stratégies à installer
- Politiques actives
- État de la connexion
- Roaming (oui / non)
- Dernier lieu connu (sélection du pays)
- Fabricant
- Le certificat d’identité a expiré (oui / non)
- Faire confiance aux certificats d’identité expirés (oui / non)
- Actions (nombre d’actions en attente)
- iPad partagé (oui / non)
- Supervisé (oui / non)
- Bootstrap Token (oui / non)
- Politiques désactivées (oui / non)
- Type d’inscription automatique
- iBeacons (uniquement avec le droit de lecture sur les iBeacons)
- Zones de géorepérage actives (uniquement avec le droit de lecture sur les zones de géorepérage)
- Nom de la politique KSP et message KSP (uniquement si Android Enterprise est disponible et avec le droit de lecture sur les politiques d’appareil)
- un filtre par colonne personnalisée activée (nommé d’après la colonne)

Pour la version 26.4.0

Par défaut, le filtre État est réglé sur Conforme, Inactif et Non conforme. Les appareils à l’état Inscription en attente… ne s’affichent donc que lorsque cet état est sélectionné dans le filtre.

Pagination

Les listes peuvent contenir 50, 100, 250 ou 500 entrées par page. Par défaut, 100 entrées sont affichées par page.

Fonctions supplémentaires

Depuis l’inventaire, les appareils peuvent être sélectionnés et associés directement à des actions. Pour les appareils sélectionnés, des options telles que Supprimer, Appliquer l’action, le déplacement vers une autre organisation, Réappliquer les politiques, Attribuer le numéro de série à la licence Lifetime, Ajouter aux groupes d’appareils et Supprimer des groupes d’appareils sont disponibles.

De plus, Mise à jour via CSV permet de mettre à jour le nom de l’appareil, l’utilisateur (adresse e-mail) et les champs personnalisés activés ; les appareils sont identifiés par leur numéro de série.

Exporter la vue au format CSV exporte un fichier CSV incluant toutes les colonnes affichées. Au-delà de 500 entrées, une boîte de dialogue propose le choix entre Exporter la page actuelle (uniquement la page affichée) et Exporter toutes les données.

Les appareils supprimés sont d’abord déplacés dans la corbeille (`Appareils` → `Poubelle`). Les colonnes supplémentaires Supprimé le et Supprimé par y sont disponibles.

Pour la version 26.4.0

Déplacer un appareil vers une organisation

Les appareils enrôlés peuvent être déplacés d'une organisation source vers une organisation cible. Au cours de ce processus, les données relatives à l'utilisateur et à l'organisation seront adaptées ou supprimées.

Conditions préalables

- Au moins la version `5.23.0` de Relution
- La fonctionnalité n'est disponible que dans l'organisation du magasin
- L'utilisateur exécutant doit avoir la permission de mettre à jour les appareils.
- L'organisation cible dispose d'une licence valide pour les appareils, qui n'est pas dépassée. Les appareils dont le numéro de série est attribué à une licence Lifetime → font exception.
- Appareils Apple : l'organisation cible utilise le même certificat APNs que celui avec lequel l'appareil est inscrit. Il peut également s'agir d'un certificat hérité de l'organisation parente.
- Plateformes supportées
  - Android Legacy
  - Apple (iOS, iPadOS, macOS, tvOS)
  - Tableaux blancs interactifs
  - Windows

Pour la Version 26.4.0

Si une condition n'est pas remplie pour un appareil, cet appareil n'est pas déplacé, tandis que les autres appareils sélectionnés le sont.

Adaptation des données de l'appareil

Les données spécifiques à l'utilisateur et à l'organisation ne peuvent pas être déplacées dans une autre organisation. Par conséquent, les données correspondantes sont soit supprimées de l'appareil, soit adaptées à l'organisation cible.

Les actions non terminées de l'appareil sont annulées avant le déplacement.

Les données suivantes sont toujours supprimées :

- Toutes les actions de l'appareil
- Tous les ensembles de règles attribués
- L'utilisateur assigné
- Tous les certificats de formation délivrés

Les données suivantes sont supprimées si elles appartiennent à l'organisation source :

- Certificats d'appareil délivrés
- Informations relatives à la fonctionnalité de prêt de l'appareil
- Zones attribuées
- Balises iBeacons attribuées

Les données correspondantes de l'organisation du magasin sont conservées. Si un appareil est déplacé depuis l'organisation du magasin, ces données sont donc entièrement conservées.

D'autres adaptations de l'appareil sont décrites dans les sections suivantes.

Adaptations pour toutes les plateformes

Groupes d'appareils

- L'appareil est retiré des groupes d'appareils locaux statiques et dynamiques de l'organisation source.
  - Si un appareil quitte un groupe d'appareils, les politiques appliquées sont supprimées.
- L'appareil sera automatiquement ajouté aux groupes d'appareils locaux dynamiques correspondants de l'organisation cible.
  - Si un appareil entre dans un groupe d'appareils, les politiques correspondantes sont appliquées.
- L'appareil n'est pas retiré des groupes d'appareils publics.

Pour la version 26.4.0

Historique des appareils

- L'historique de l'appareil est complètement supprimé.
- En outre, un nouvel historique de l'appareil est créé pour le transfert réussi dans l'organisation cible.

Inscription

- Les inscriptions uniques sont déplacées vers l'organisation cible.
- Pour les inscriptions multiples, une nouvelle inscription unique inutilisable sera créée dans l'organisation cible.
- En outre, l'utilisateur référencé, les jeux de règles, les politiques et les notifications sont supprimés de l'appareil.
- Une attribution à une inscription automatique, par ex. via l'Inscription automatisée des appareils (ADE, DEP dans le portail), n'est conservée que si elle provient de l'organisation du magasin.

Adaptations pour Windows

- L'historique des scripts locaux de l'organisation source est supprimé de l'appareil. L'historique des scripts publics et des scripts de l'organisation Meta est conservé.

Adaptations pour Apple

- Les licences Apps et livres (VPP dans le portail) liées à un jeton VPP de l'organisation source (jeton VPP local) sont supprimées de l'appareil.
- Les licences qui appartiennent à un jeton VPP de l'organisation du magasin sont déplacées dans l'organisation cible.
- Les licences qui appartiennent à un jeton VPP d'une organisation Meta → sont déplacées dans l'organisation cible si l'organisation source et l'organisation cible font partie de la même organisation Meta. Dans le cas contraire, elles sont supprimées de l'appareil.
- Le Managed Media n'est pas supprimé de l'appareil et sera visible dans l'organisation cible.
  - Sauf si le Managed Media a été appliqué par une configuration et que l'appareil quitte le groupe d'appareils correspondant.
  - Le Managed Media de l'organisation source peut être retiré de l'appareil dans l'organisation cible.
- Le certificat de supervision ne peut pas être déplacé vers l'organisation cible. Le certificat ne peut être téléchargé à partir de l'appareil déplacé que si l'autorisation de lecture des appareils existe à la fois dans l'organisation cible et dans l'organisation à laquelle appartient le certificat (généralement l'organisation source).

Pour la version 26.4.0

Processus

Dans l'inventaire des appareils de l'organisation du magasin, un ou plusieurs appareils peuvent être déplacés vers une organisation cible. Les appareils doivent d'abord être sélectionnés. Ensuite, l'entrée Passer à (déplacement vers une autre organisation) du menu à 3 points peut être cliquée. Pour un appareil individuel, l'entrée est également disponible dans le menu à 3 points de la ligne de l'appareil. L'entrée n'est pas disponible si la sélection contient des appareils supprimés, des appareils avec le statut `WITHDRAWN` ou des appareils d'une plateforme non prise en charge.

Dans la boîte de dialogue, l'organisation cible doit être sélectionnée. En général, les appareils peuvent être déplacés vers toutes les organisations, à l'exception de l'organisation du magasin, de l'organisation du système, des organisations Meta et de l'organisation source. Les organisations Meta sont certes proposées à la sélection, mais le déplacement vers celles-ci est refusé et les appareils restent dans leur organisation d'origine. Si seuls les appareils d'une

organisation source sont sélectionnés, cette organisation n’est pas affichée dans la boîte de dialogue. Si des appareils de plusieurs organisations ont été sélectionnés, toutes ces organisations peuvent être choisies comme organisation cible. Cependant, les appareils sélectionnés qui appartiennent déjà à l’organisation cible ne seront pas pris en compte.

La deuxième étape de la boîte de dialogue contient une boîte d’information avec des conseils sur les conséquences possibles et un lien vers la documentation.

Après confirmation, les appareils sélectionnés seront déplacés vers l’organisation cible. Chaque appareil est déplacé individuellement. Si un appareil ne peut pas être déplacé, il reste dans son organisation d’origine, par ex. si l’organisation cible ne dispose d’aucune licence d’appareil libre ou si, pour les appareils Apple, le certificat APNs de l’organisation cible ne correspond pas à celui de l’organisation source. Le portail n’affiche aucun message d’erreur dans ce cas. Le résultat doit donc être vérifié dans la colonne Organisation de l’inventaire des appareils.

Pour la version 26.4.0

Prêt

Le système de prêt Relution aide les écoles à assurer une gestion efficace des appareils prêtés. Le système permet aux administrateurs de définir les conditions de prêt, de suivre les périodes de prêt et de surveiller l'état des appareils.

L'objectif est de garantir un processus transparent, sécurisé et fluide pour la remise et la restitution des appareils.

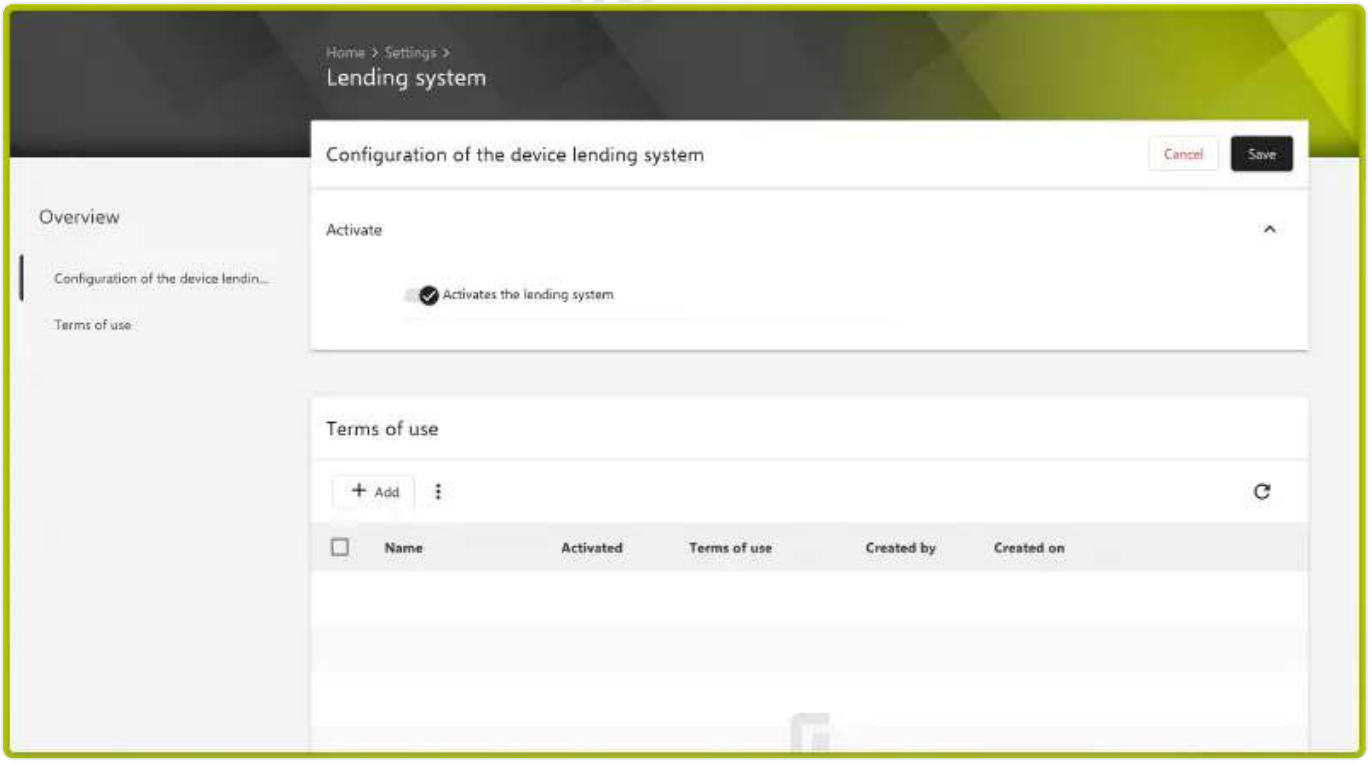
Une nouvelle fonctionnalité permet désormais d'effectuer les restitutions d'appareils avec l'application Relution Assets, voir Assets →.

Activer le système de prêt

Le système de prêt peut être activé dans Relution pour le tenant souhaité via le chemin suivant :

`Paramètres` → `Système de prêt`

Le système de prêt n'est pas disponible dans l'organisation globale.



Conditions d’utilisation

Avant de remettre des appareils aux élèves ou aux enseignants, des conditions d’utilisation claires doivent être définies.

Celles-ci comprennent notamment :

- conditions générales d’utilisation
- règles de remise et de restitution des appareils prêtés
- responsabilité en cas de dommage ou de perte
- configuration initiale des appareils
- respect des règles de protection des données et de protection des mineurs

Ces conditions peuvent être enregistrées dans Relution sous `Paramètres` → `Système de prêt` (section Conditions d’utilisation, bouton Ajouter des conditions d’utilisation) et formatées en Markdown pour une meilleure lisibilité.

Il est possible d’enregistrer plusieurs variantes de conditions pouvant être sélectionnées lors du prêt.

Les conditions documentées sont disponibles tout au long du processus de prêt et peuvent être sélectionnées pour chaque prêt. Il est ainsi toujours possible de retracer dans quelles conditions un appareil a été prêté.

Pour la version 26.4.0

Seules les conditions d’utilisation activées avec l’interrupteur Activé peuvent être sélectionnées. Le texte d’une condition d’utilisation ne peut plus être modifié après sa création ; lors de la modification, seuls le nom et l’activation peuvent être changés. Pour une nouvelle version, une nouvelle condition d’utilisation est créée et l’ancienne est désactivée.

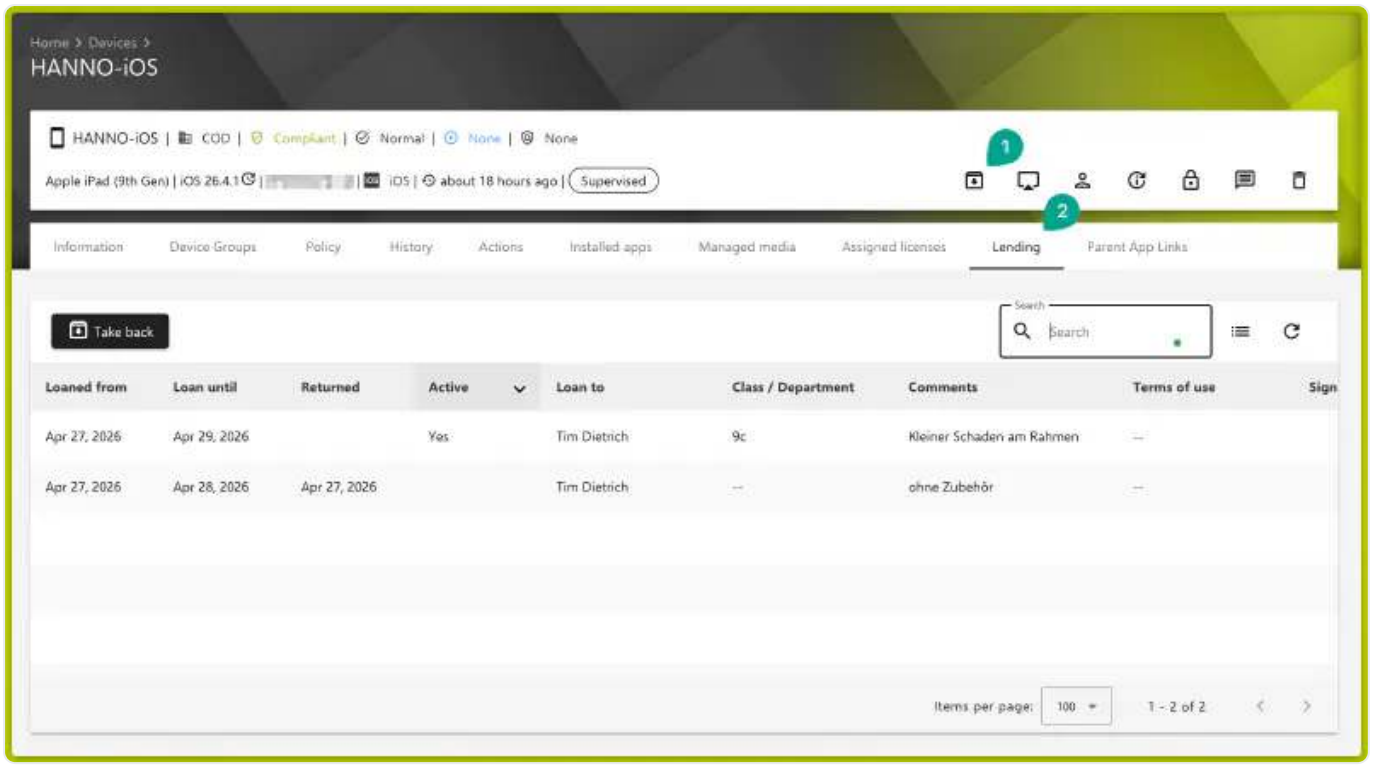
En complément, un document signé, p. ex. un contrat de prêt physique, peut être téléversé dans le champ Signature lors du prêt.

Prêter des appareils

Pour représenter le prêt de manière structurée dans Relution, les appareils peuvent être prêtés depuis l’Inventaire.

Deux points d’accès sont disponibles dans les détails de l’appareil :

- Accès rapide Prêter l’appareil dans l’encadré d’information (1)
- Onglet Prêts avec le bouton Prêter (2)



Dans la boîte de dialogue suivante, la période de prêt est définie via les champs obligatoires Prêté à partir du (prérempli avec la date du jour) et Prêt jusqu'au. La période de prêt court jusqu'à la fin du jour sélectionné sous Prêt jusqu'au.

L'appareil est attribué à un élève ou à un enseignant. Dans le champ obligatoire Prêt à, le nom de l'emprunteur est saisi.

Une fonction de suggestion permet de sélectionner des noms déjà saisis ainsi que des utilisateurs Relution existants.

Le champ facultatif Classe/département permet d'indiquer la classe ou le département de l'emprunteur. Les entrées déjà utilisées y sont également proposées.

Pour la version 26.4.0

Informations supplémentaires lors du prêt

Le champ Commentaires permet d'enregistrer des remarques, par exemple :

- objectif du prêt
- projet ou mesure
- remarques sur l'état de l'appareil

Si des accessoires tels qu'un chargeur, une housse ou un stylet sont remis, cela peut être documenté et vérifié lors de la restitution.

En complément, il est possible de :

- sélectionner des conditions d'utilisation enregistrées dans le champ Conditions d'utilisation
- téléverser un document signé (p. ex. le contrat de prêt) au format PDF, JPG ou PNG dans le champ facultatif Signature

Dans l'onglet Prêts des détails de l'appareil, un prêt en cours est marqué dans la colonne Actif. L'appareil n'est plus disponible jusqu'à sa restitution et ne peut être prêté à nouveau qu'ensuite. L'onglet affiche également l'historique complet des prêts de l'appareil avec les informations saisies, p. ex. Prêt à, Classe/département, Conditions d'utilisation, Signature (téléchargeable) et Prêt par.

Dans l'aperçu de l'inventaire, les appareils prêtés sont identifiables via les colonnes Prêt à et Prêt jusqu'au. Celles-ci sont masquées par défaut et peuvent être affichées via la sélection des colonnes.

Restituer des appareils

La restitution s'effectue également via la page de détails de l'appareil :

- Accès rapide Restituer l'appareil dans l'encadré d'information
- Onglet Prêts avec le bouton Restituer

Pour la version 26.4.0

Dans la boîte de dialogue suivante, les informations du prêt sont verrouillées ; seul le champ Commentaires peut encore être modifié. La restitution est confirmée avec Retourner, et l'heure actuelle est enregistrée comme date de restitution.

Après une restitution réussie, le prêt n'est plus marqué comme actif dans l'onglet Prêts ; la date de restitution est affichée dans la colonne correspondante.

L'appareil est ensuite de nouveau disponible comme appareil de prêt et peut être prêté à nouveau.

Dépassement de la durée de prêt

Si la durée de prêt est dépassée et que l'appareil n'est pas restitué à temps, la date Prêt jusqu'au apparaît en rouge dans l'aperçu de l'inventaire et dans l'onglet Prêts. De plus, une icône de cloche avec l'info-bulle Période de prêt dépassée à côté du nom de l'appareil dans la liste d'inventaire signale le dépassement.

Une fois la durée de prêt expirée, l'appareil reçoit automatiquement la violation de conformité Période de prêt dépassée et est considéré comme non conforme. Relution le vérifie

régulièrement (par défaut toutes les heures) ainsi qu'à chaque enregistrement d'un prêt. Lorsque l'appareil est restitué, la violation est de nouveau supprimée.

Règles en cas de dépassement de durée de prêt

D'autres réactions automatiques sont configurées via un groupe d'appareils dynamique avec des actions : le groupe filtre sur Violations de conformité avec la valeur Période de prêt dépassée (ou sur Prêt jusqu'au), et les actions du groupe sont exécutées pour les appareils de ce groupe, p. ex. dès qu'un appareil entre dans le groupe. Voir Groupes d'appareils → et Actions de groupes d'appareils →.

Les réactions suivantes peuvent être liées à cet état via les actions de groupe :

- Grâce à une Action de notification avec l'option Notifier les autres utilisateurs, les administrateurs peuvent être informés automatiquement.
- Grâce à une action de l'appareil (Action du dispositif dans le portail), les appareils prêtés peuvent être verrouillés ou réinitialisés aux paramètres d'usine.

Cela garantit une utilisation sécurisée et contrôlée des appareils prêtés.

Enregistrer les accessoires

Pour la version 26.4.0

Relution permet de définir jusqu'à cinq champs supplémentaires personnalisés sous Propriétés personnalisées de l'appareil →.

Exemples :

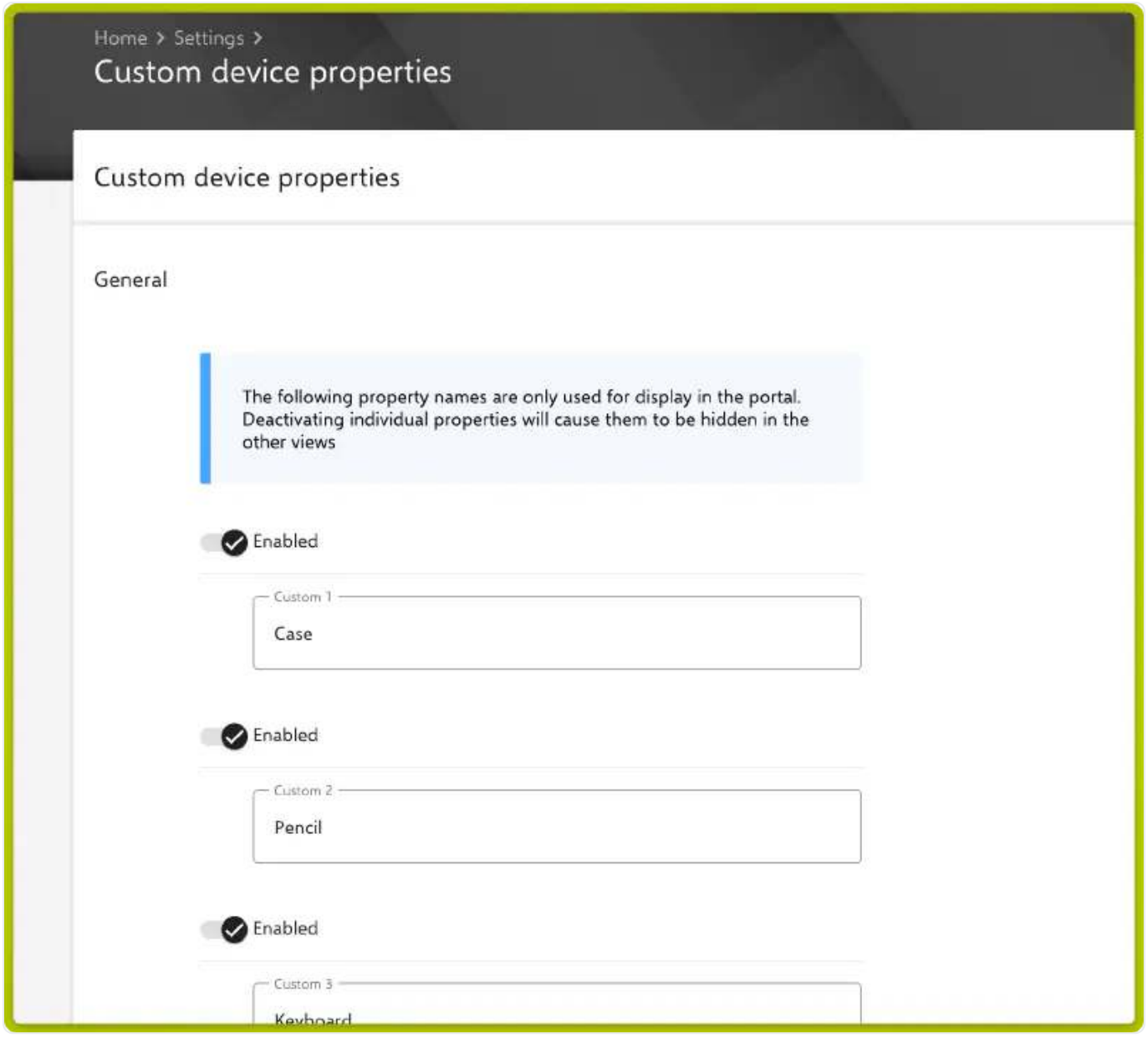
- chargeurs
- sacs
- stylos / stylets
- adaptateurs
- autres accessoires

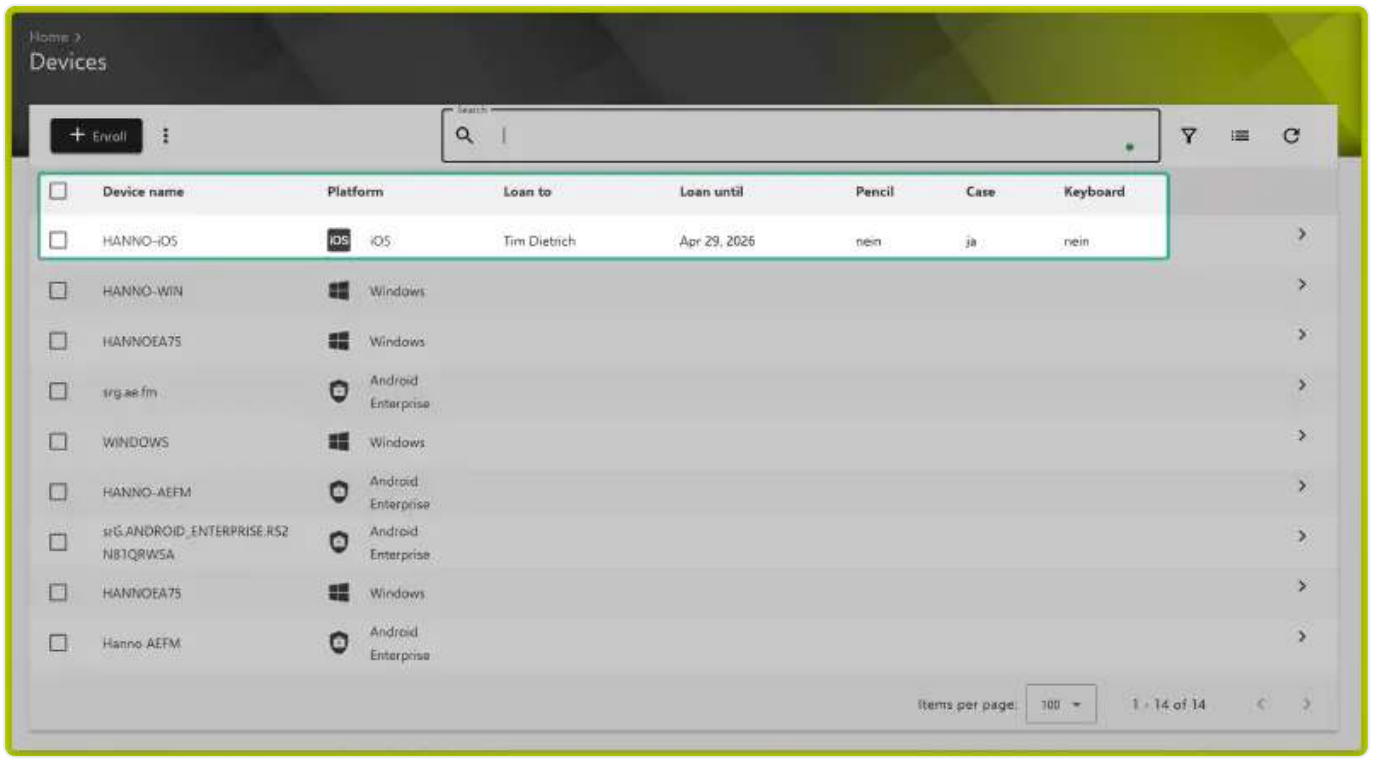
Ces propriétés définies peuvent être configurées dans les détails de l'appareil et vérifiées spécifiquement lors de la restitution.

Une fois activées, les propriétés personnalisées apparaissent dans les détails de l'appareil sous Informations en bas de la page.

Les propriétés personnalisées activées peuvent également être affichées dans l'aperçu de l'inventaire du portail Relution.

Il est ainsi possible d’enregistrer facilement quels accessoires appartiennent à un appareil. Lors de la restitution, il peut être rapidement vérifié si tous les objets remis ont été retournés intégralement.





Pour la version 26.4.0

Propriétés personnalisées de l'appareil

Sous `Paramètres` → `Propriétés personnalisées de l'appareil`, cinq champs de texte libre librement nommables (`Personnalisé 1`–`5`) sont disponibles, permettant d'enrichir les appareils avec des informations propres – par exemple un centre de coûts, un site ou des accessoires fournis.

Activer et nommer les champs

Chacun des cinq champs dispose de son propre interrupteur d'activation et d'un libellé modifiable. Le libellé ne peut être saisi qu'une fois le champ activé. Si un champ activé est enregistré sans libellé, il apparaît partout sous son nom par défaut (p. ex. 1 personnalisé). Le libellé sert uniquement à l'affichage dans le portail ; désactiver un champ le masque à nouveau dans toutes les vues. Les valeurs enregistrées sur les appareils sont conservées.

> Il n'existe pas de types de champs (nombre, date, liste déroulante, etc.) – les cinq champs sont de simples champs de texte libre.

Pour la version 26.4.0

Utilisation

Les champs activés sont disponibles aux endroits suivants :

- Vue détaillée de l'appareil : une carte dédiée Propriétés personnalisées, avec des valeurs directement modifiables via l'icône de crayon (avec le droit de modifier les appareils).
- Inscriptions et inscriptions automatiques : un champ de saisie par champ activé dans le formulaire et une colonne optionnelle dans la liste ; les valeurs enregistrées sont transférées à l'appareil lors de l'inscription.
- Liste d'inventaire : sous forme de colonnes optionnelles pouvant être affichées et de filtres à sélection multiple parmi les valeurs existantes, voir Aperçu de l'inventaire →.
- CSV : export depuis la liste des appareils et celle des inscriptions automatiques (colonnes `custom1`–`custom5`) ; les appareils et inscriptions automatiques existants sont mis à jour via Mise à jour via CSV (identification par numéro de série, en-tête de colonne = libellé configuré ou `custom1`–`custom5`, les cellules vides ne modifient rien).
- Groupes d'appareils dynamiques : comme critère de filtre, avec le libellé configuré ici comme nom d'affichage.

- Espaces réservés : `${device.custom1}` à `${device.custom5}`, p. ex. dans les noms d’appareils, voir Espaces réservés avancés →.

Pour un exemple d’application, voir Prêt : Enregistrer les accessoires →.

Pour la version 26.4.0

Télécharger les journaux des appareils

Les journaux de débogage des appareils individuels peuvent être activés et téléchargés directement via le portail Relution.

Il est possible de télécharger les journaux de débogage pour des appareils spécifiques directement depuis le serveur via le portail Relution. Cela facilite considérablement l'analyse des erreurs, car un accès direct au système de fichiers du serveur n'est plus nécessaire.

Prérequis

- Organisation : La fonction n'est disponible que dans l'organisation globale.
- Autorisations : Administrateur système ou un utilisateur dont le rôle comprend l'autorisation Journalisation dans la section Appareils (sélectionnable uniquement pour l'organisation globale).

Pour la version 26.4.0

Instructions

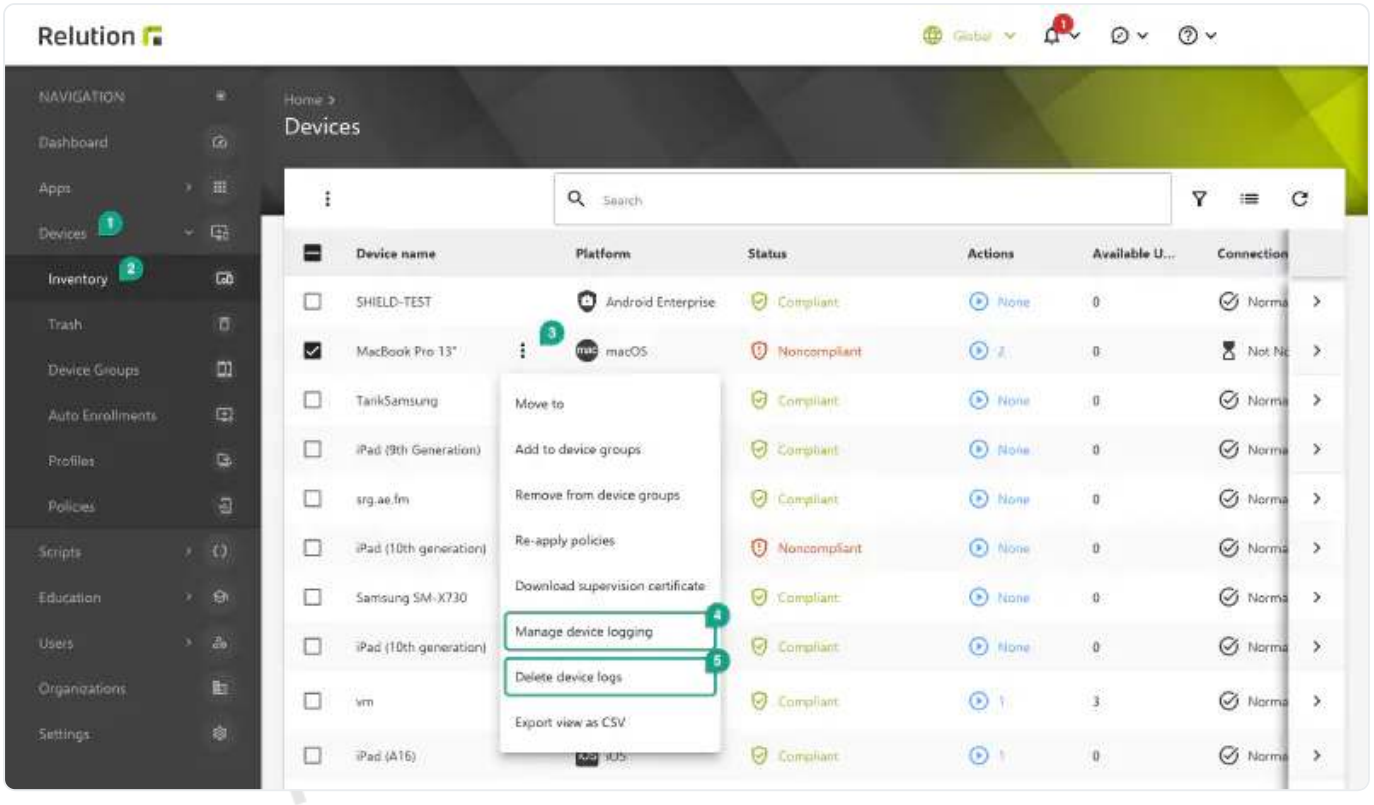
Voici les étapes pour activer la journalisation ou télécharger les journaux existants :

1. Connexion : La connexion au portail Relution s'effectue avec un compte administrateur de l'organisation globale.
2. Sélection de l'appareil : L'appareil concerné est sélectionné sous `Appareils` → `Inventaire`.
3. Ouvrir le menu contextuel : Le menu contextuel s'ouvre dans la ligne de l'appareil via le menu à trois points (Actions).
4. Gérer la journalisation : L'option Modifier la journalisation des appareils ouvre la boîte de dialogue correspondante.
    - Activer la journalisation : L'interrupteur Activer la journalisation basée sur l'appareil active la journalisation et affiche le champ Durée (en minutes), qui définit combien de temps la journalisation détaillée reste active (par défaut : 60 minutes, minimum : 1). Confirmer applique le réglage. Lorsque la journalisation est active, la boîte de dialogue affiche l'Heure de début et l'Heure de fin. Pour mettre fin à la journalisation plus tôt, l'interrupteur est désactivé et la modification est appliquée avec Confirmer.
    - Téléchargement : La section Journaux des appareils propose, via Télécharger, l'archive des journaux (fichier ZIP) collectée par le serveur pour cet appareil. Dans un environnement en cluster, l'archive ne contient les journaux de toutes les instances que

si Spring Boot Admin est activé ; sinon, seuls les journaux d'une seule instance sont téléchargés.

5. Nettoyage : L'option Supprimer les journaux de l'appareil du menu contextuel permet de retirer du serveur les journaux collectés des appareils sélectionnés.

Les options du menu sont également disponibles dans la liste des appareils d'un groupe d'appareils.



Remarques sur le stockage

- Les journaux sont conservés uniquement dans la mémoire du serveur et sont perdus lors d'un redémarrage du serveur.
- Un nombre limité d'événements de journal est enregistré par appareil (10 000 par défaut). En cas de longue durée de journalisation ou d'appareils très actifs, les messages plus anciens sont ignorés.
- Un jour après la fin de la journalisation, le système supprime automatiquement les journaux.

Configurer DEP

L’inscription automatisée des appareils (ADE, DEP dans le portail ; anciennement `Device Enrollment Program`) d’Apple permet aux organisations d’inscrire et d’approvisionner leurs propres appareils Apple. L’ADE rationalise le processus d’approvisionnement et de gestion des appareils à grande échelle en permettant de préconfigurer les appareils avant qu’ils ne soient distribués. Les utilisateurs reçoivent leurs appareils entièrement configurés et prêts à l’emploi, tandis que les données restent confidentielles et que le système est sécurisé. Tous les paramètres préconfigurés sont contrôlés par les administrateurs via la gestion à distance, et la conformité est maintenue sans fil, sans jamais nécessiter d’intervention manuelle sur site.

Appareils compatibles avec l’ADE

Tous les iPhones, iPads, ordinateurs Mac ou Apple TV achetés à partir du 1er mars 2011, soit directement auprès d’Apple, soit auprès d’un revendeur agréé Apple participant, sont éligibles à l’ADE. Les iPhones et iPads doivent fonctionner sous iOS/ iPadOS 7 ou une version ultérieure, les ordinateurs Mac doivent fonctionner sous OS X 10.9 ou une version ultérieure, et les Apple TV doivent fonctionner sous tvOS 10.2 ou une version ultérieure. L’Apple Vision Pro (visionOS) peut également être inscrit dans Relution via l’ADE. Des appareils Apple peuvent être ajoutés à l’ADE à l’aide de `Apple Configurator`, quel que soit l’endroit où ils ont été achetés. Lors de la configuration d’un appareil Apple enregistré manuellement, celui-ci se comporte comme n’importe quel autre appareil enregistré, avec une supervision obligatoire et un enregistrement de gestion des appareils mobiles (MDM). Pour les appareils Apple qui n’ont pas été achetés directement, les utilisateurs disposent d’une période de transition de 30 jours pour retirer l’appareil de l’inscription MDM et de la supervision.

Pour la version 26.4.0

Avantages de l’ADE

Le principal avantage de l’ADE est la simplicité du processus d’inscription automatique. Ce processus garantit que tous les appareils Apple sont configurés conformément aux exigences de l’organisation et que tous les utilisateurs disposent des mêmes applications, réglages, restrictions et autorisations sur leurs appareils avant même qu’ils ne leur soient remis.

Autres avantages

- Installation de profils MDM que les utilisateurs ne peuvent pas supprimer, de sorte que les appareils restent gérés à distance. Pour cela, l'option L'utilisateur peut supprimer l'inscription MDM est désactivée dans le profil DEP (activée par défaut).
- Possibilité d'activer la supervision sans fil.
- Préconfiguration d'une installation initiale, évitant aux utilisateurs finaux de perdre du temps.
- Installation silencieuse d'applications et fonctionnalités "push".
- Plus de contrôle pour le service informatique.
- Moins de problèmes de sécurité.

Appareils iOS supervisés, DEP et MDM →

Migration des appareils via Apple Configurator

`Apple Configurator` est une solution pour les petites organisations qui n'ont que quelques appareils Apple à gérer ou qui n'ont besoin que d'une configuration de base pour leurs appareils. Comme `Apple Configurator` ne fournit pas de capacités sans fil, les appareils gérés avec `Apple Configurator` doivent être physiquement connectés à un ordinateur Mac pour pouvoir effectuer des changements. Cela peut être avantageux pour les organisations qui ont besoin d'une approche pratique.

Pour la version 26.4.0

La migration de `Apple Configurator` vers l'ADE avec Relution est la solution pour les organisations de toute taille qui veulent un système convivial pour gérer n'importe quel nombre d'appareils mobiles Apple. La migration fournit une solution conviviale et sans fil avec des fonctionnalités avancées qui peuvent être personnalisées pour répondre aux besoins des organisations de toute taille.

Ajouter des appareils DEP avec Apple Configurator 2 →

Restrictions sur l'ajout d'appareils à l'ADE

Les appareils Apple achetés le 1er mars 2011 ou après cette date peuvent être inscrits à l'ADE après une réinitialisation d'usine. La seule autre restriction est que l'appareil doit être inscrit à l'ADE dans les trois ans suivant la date d'achat.

Supprimer des appareils de l’ADE

Il est possible à tout moment de retirer des appareils de l’ADE. Les appareils endommagés, perdus ou volés peuvent et doivent être retirés de l’ADE dès que possible. Une fois qu’un appareil a été retiré de l’ADE, il ne peut plus être attribué automatiquement via le revendeur ; il ne peut être ajouté à nouveau que manuellement à l’aide de `Apple Configurator`.

Ajouter des appareils de revendeurs agréés à l’ADE

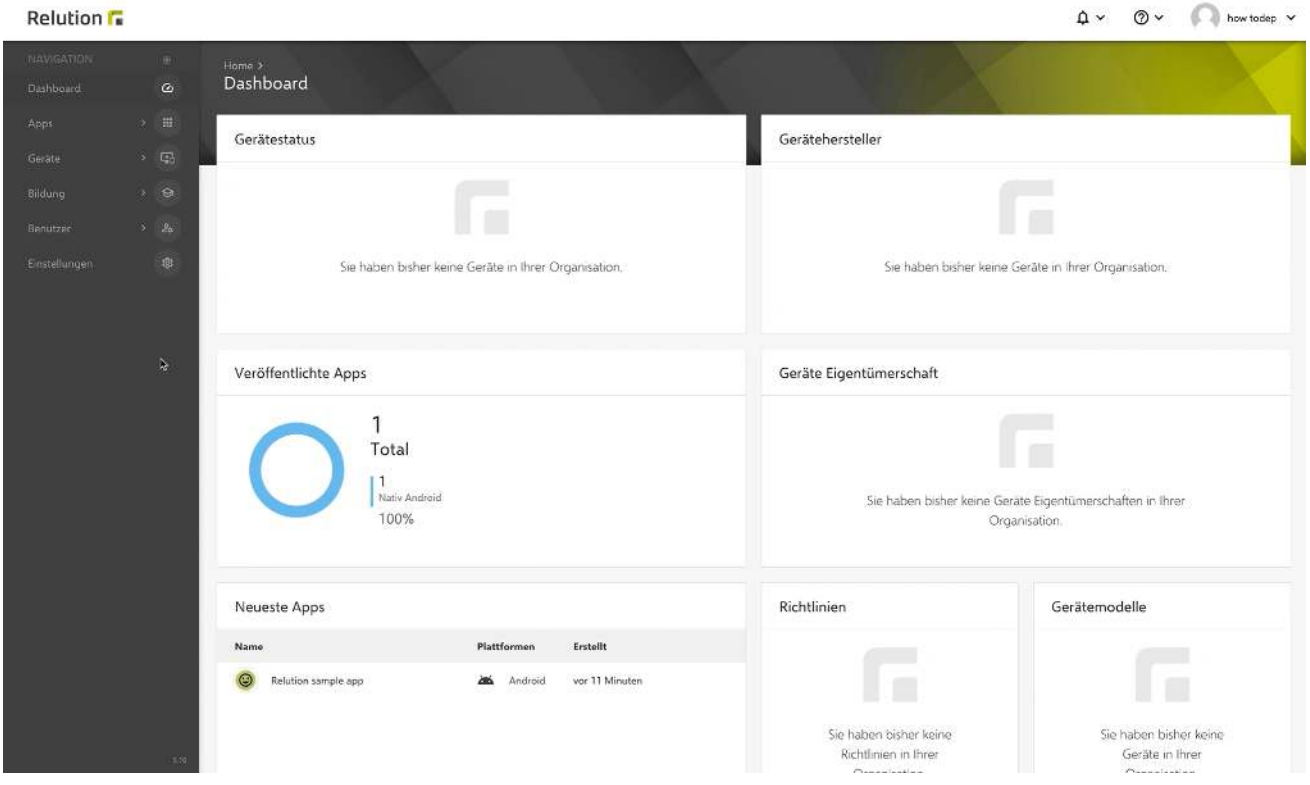
L’ADE fonctionne avec les appareils Apple compatibles avec l’ADE lorsqu’ils sont achetés auprès de revendeurs et d’opérateurs agréés. Il est recommandé de se renseigner auprès du revendeur avant d’acheter un appareil Apple. Pour s’inscrire à l’ADE auprès d’Apple, un numéro de client Apple ou un ID de revendeur DEP doit être saisi. Si un revendeur n’a pas ce numéro, l’accès à l’ADE n’est pas possible.

Comment faire

Pour la version 26.4.0

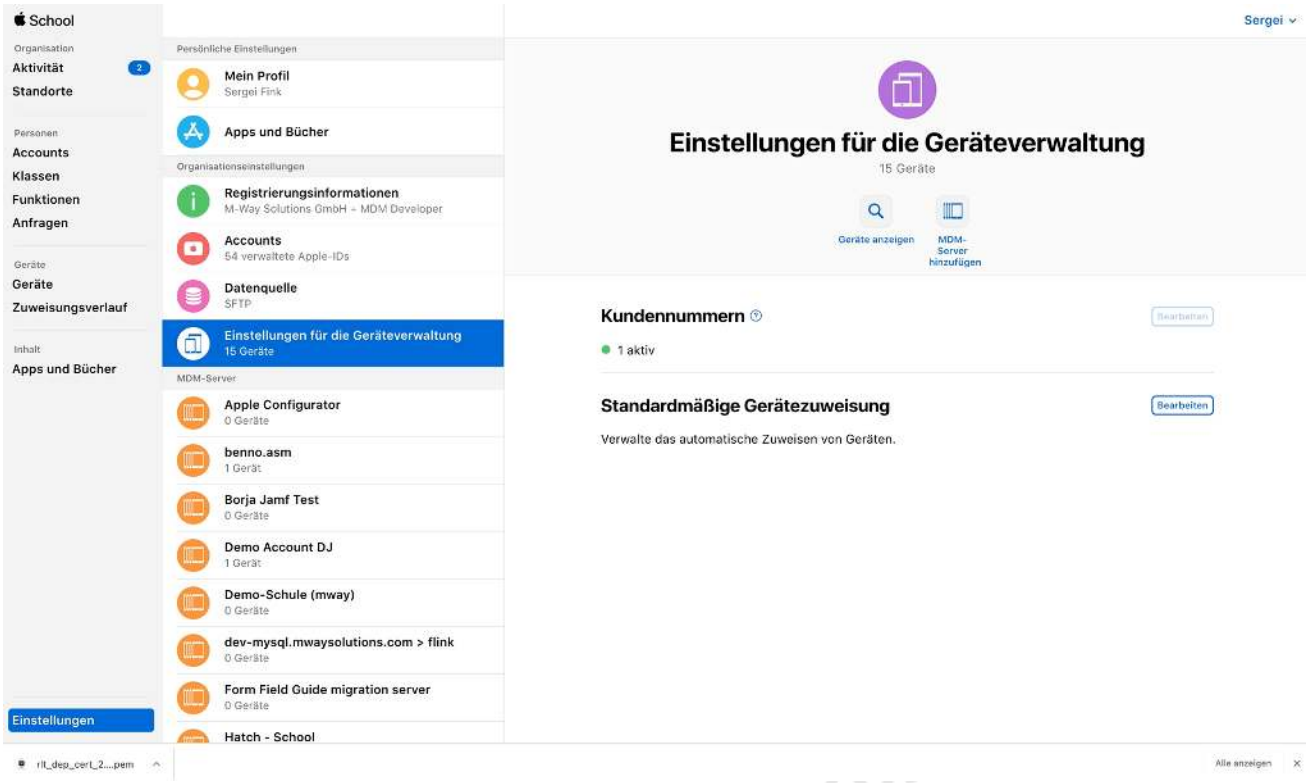
Le compte DEP est configuré dans Relution sous `Paramètres` → `Apple Automated Device Enrollment` (section Spécifique à la plate-forme de l’appareil).

1. Télécharger le certificat du serveur dans Relution via Télécharger le certificat.

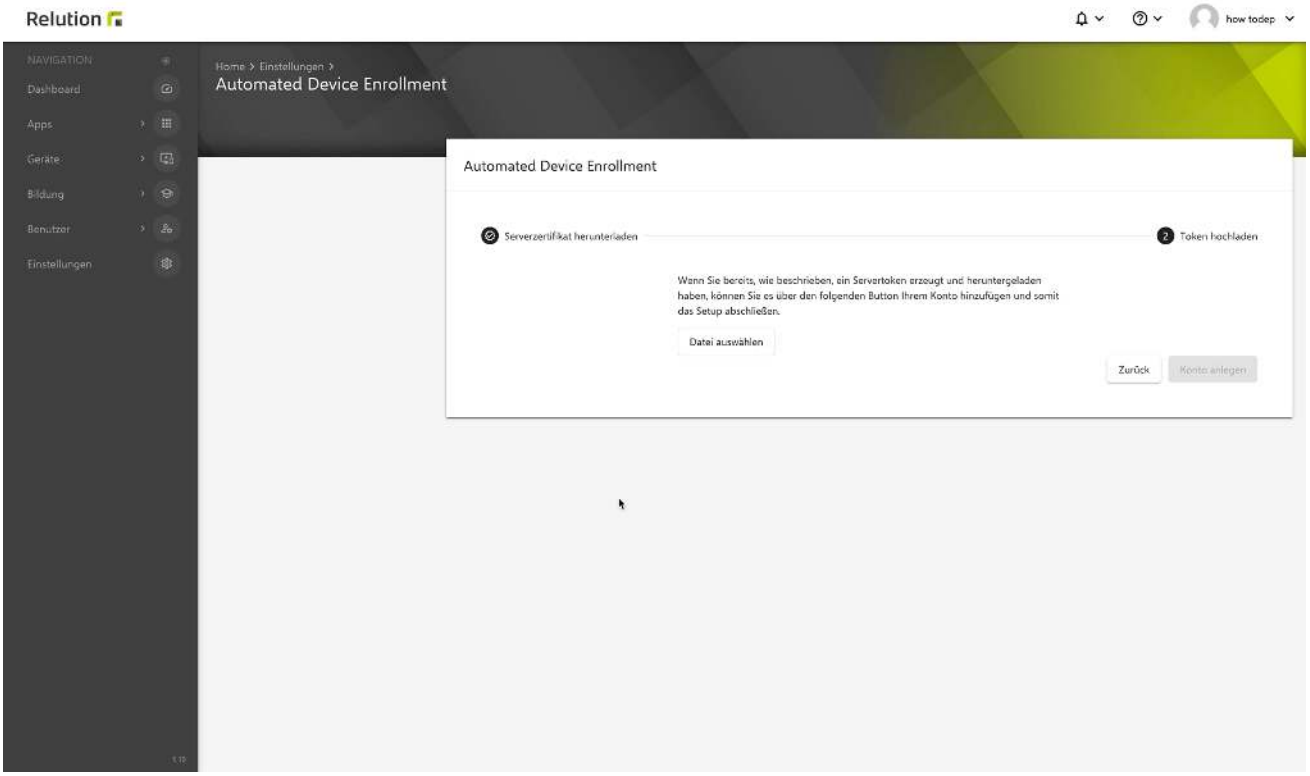


2. Créer un serveur MDM dans Apple School/ Business Manager.

3. Téléverser le certificat dans Apple School/Business Manager et télécharger le jeton.



4. Téléverser le jeton dans Relution (bouton Jeton de téléchargement dans le portail) et vérifier sa validité.

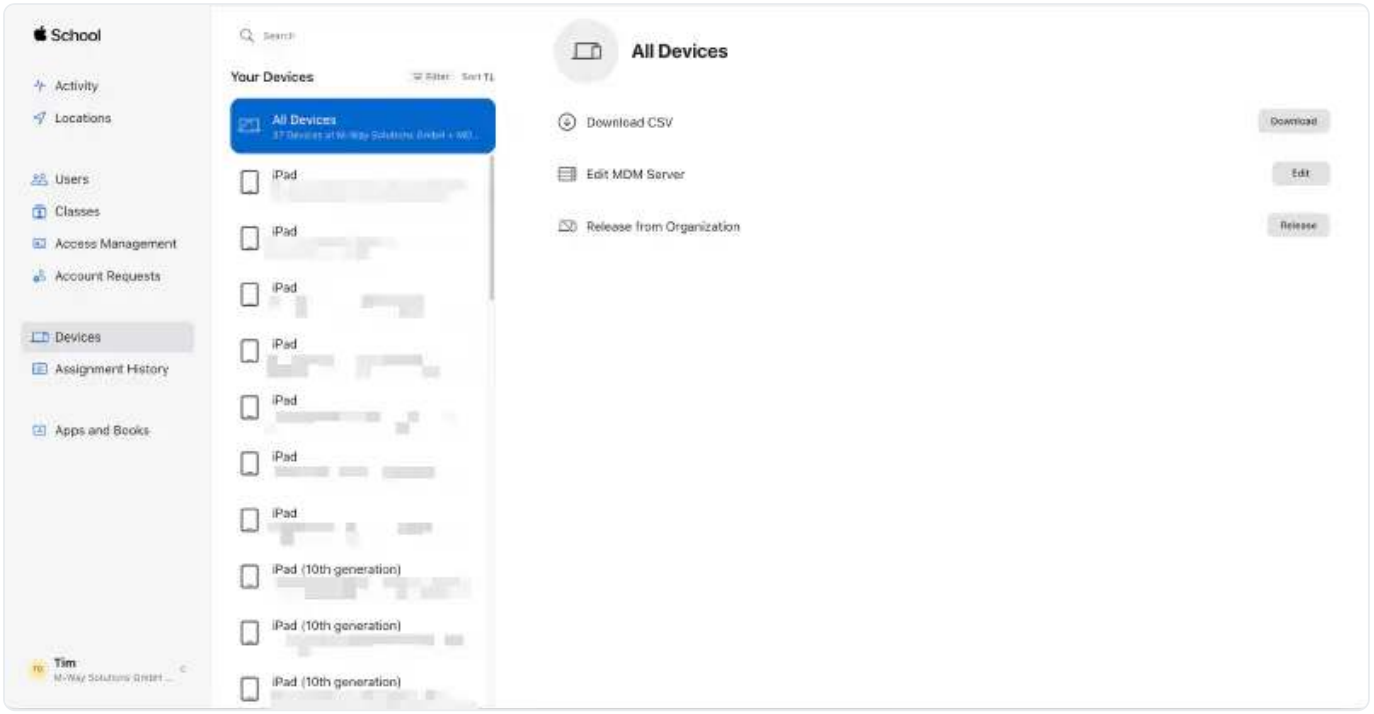


Les erreurs fréquentes lors de l'importation du jeton, les extensions de fichiers et les causes d'invalidation prématurée sont décrites sous Remarques importantes et dépannage →.

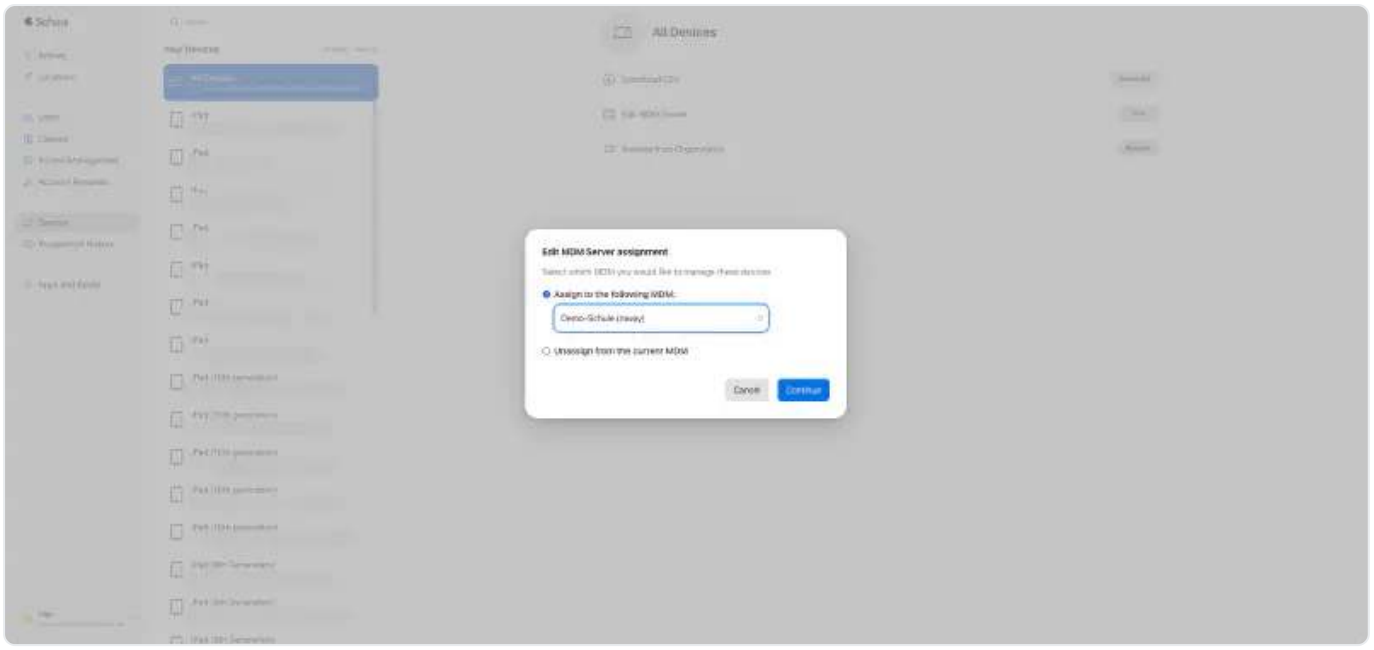
Le jeton DEP est valable un an et doit ensuite être renouvelé. La procédure est décrite sous Renouveler les jetons DEP (Jetons de serveur) →.

Affecter les appareils au serveur MDM

L'affectation des appareils Apple au serveur MDM dans Apple School/Business Manager nécessite un accès avec les autorisations appropriées. Dans Apple School/ Business Manager, la section Devices est ouverte.



Les appareils souhaités sont sélectionnés et affectés au serveur approprié.



Synchroniser les appareils

Les appareils Apple deviennent ensuite visibles dans Relution sous `Appareils` → `Inscriptions automatiques`. Par défaut, Relution synchronise les appareils automatiquement une fois par jour (la nuit, vers 3 h, heure du serveur). Le bouton Synchroniser les appareils déclenche immédiatement la synchronisation ; tous les services d'inscription automatique configurés sont alors synchronisés.

Pour la version 26.4.0

Si un profil DEP a été précédemment créé et marqué avec Utiliser comme profil par défaut, il est automatiquement attribué aux nouveaux appareils lors de la synchronisation. Sinon, le profil DEP est attribué manuellement via Définir le profil — un profil DEP est obligatoire. Les profils DEP sont créés sous `Appareils` → `Profils`, voir Profil pour l'ADE →.

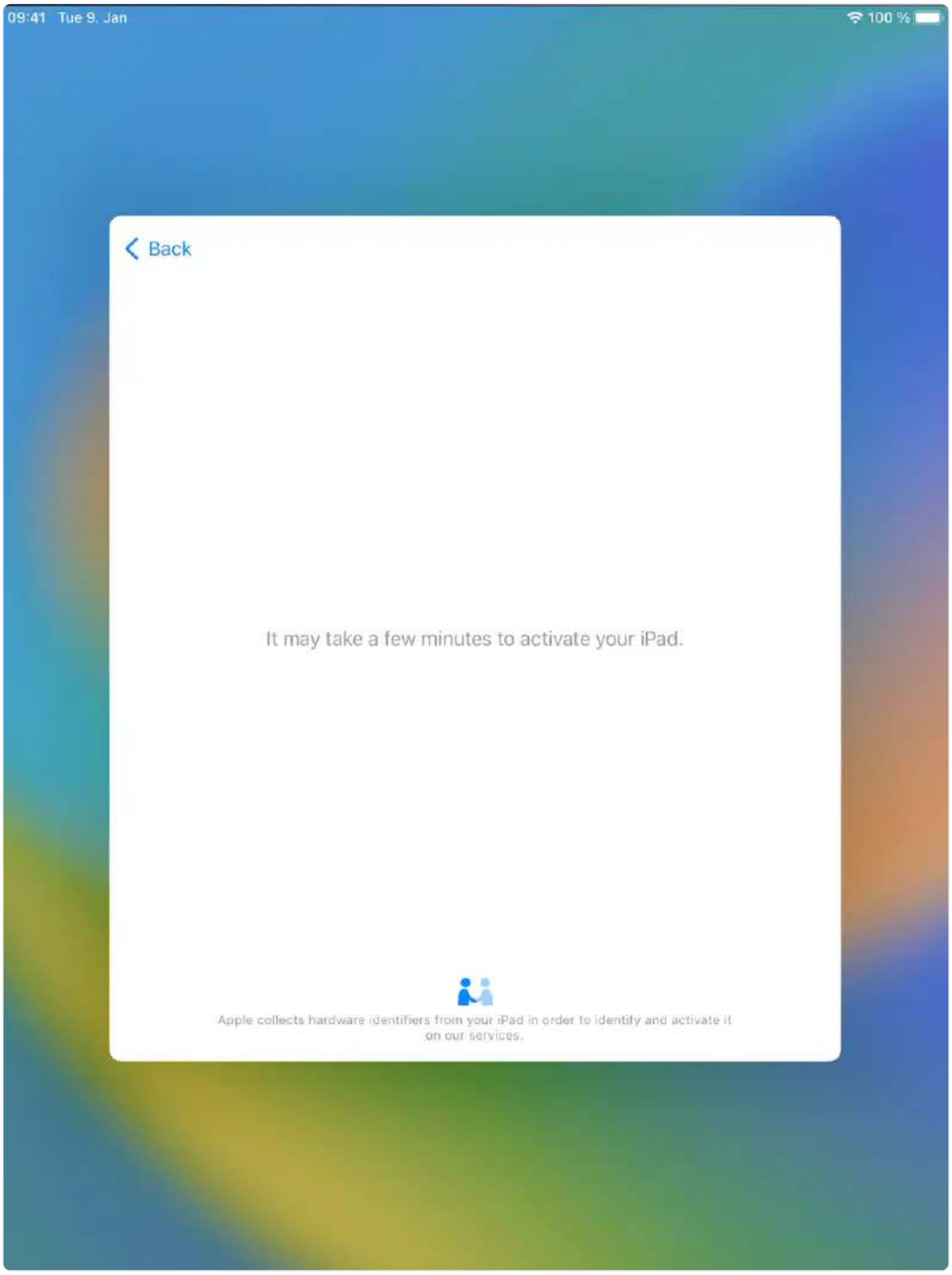
Les actions suivantes sont également disponibles pour les appareils sélectionnés dans les inscriptions automatiques :

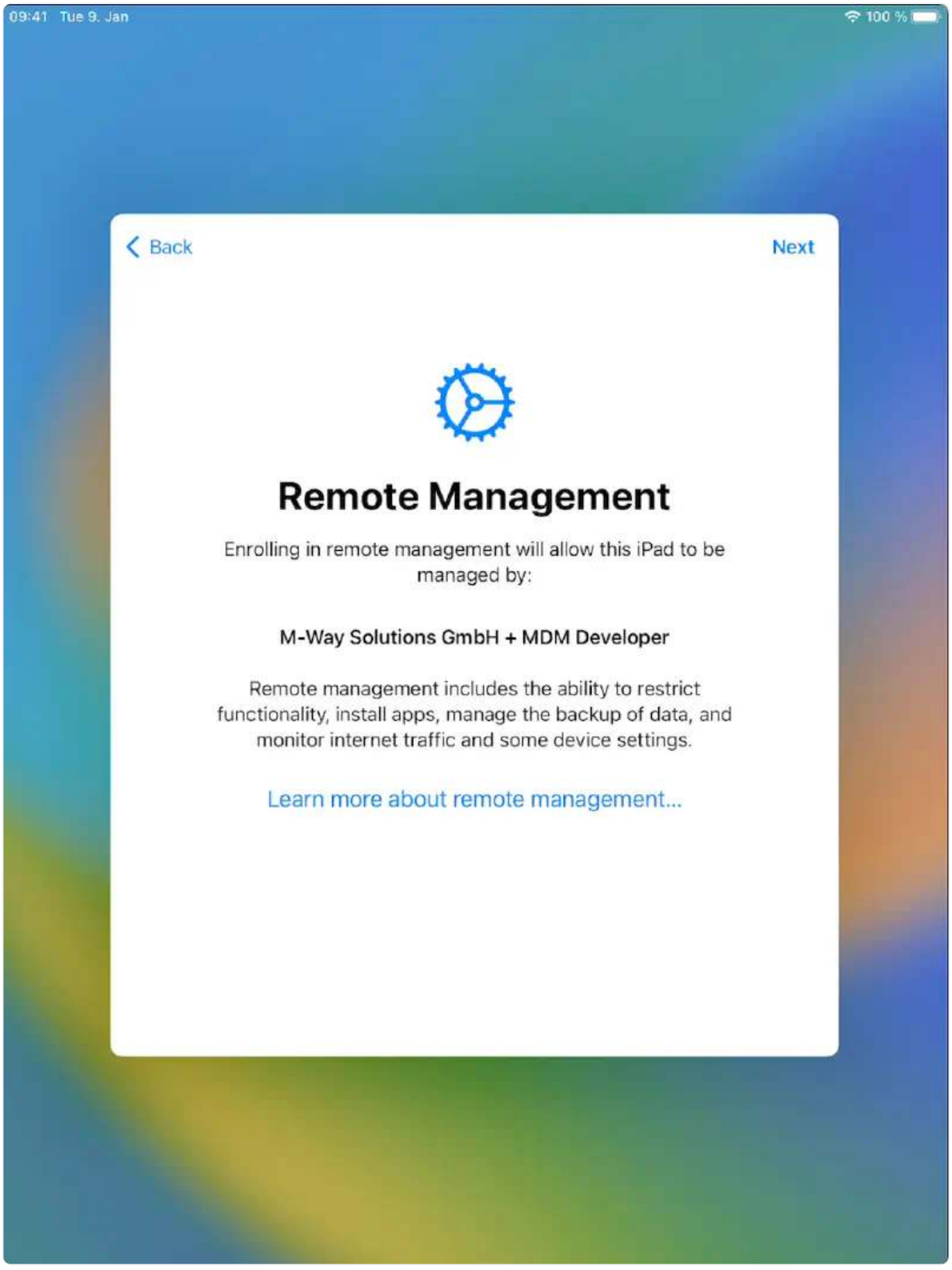
- Attribuer un utilisateur et Désassigner un utilisateur : attribue un utilisateur aux appareils ou supprime l'attribution.
- Utiliser le nom d'utilisateur comme nom d'appareil : reprend le nom de l'utilisateur attribué comme nom d'appareil.
- Ajouter aux groupes d'appareils et Supprimer des groupes d'appareils : affecte les appareils à des groupes d'appareils statiques. Les politiques de ces groupes sont appliquées automatiquement lors de l'inscription.

Mise en service des appareils DEP

Lorsqu'un des appareils est mis en service, ou lorsqu'une réinitialisation d'usine est effectuée s'il est déjà opérationnel, l'appareil se connecte à Apple et télécharge le profil DEP, à condition qu'une connexion Internet soit disponible. Il suffit de suivre les instructions affichées à l'écran : à la fin de l'assistant, l'appareil Apple est enrôlé et l'agent `Relution Agent` devrait être installé.

Pour la 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...

Si le message d’erreur `Profil n'a pas pu être chargé` s’affiche, il est vérifié s’il reste suffisamment de licences d’appareil libres et si un profil DEP est associé à l’appareil.

Pour la version 26.4.0

Profil pour l'ADE

Si les appareils Apple doivent être enrôlés via l'inscription automatisée des appareils (ADE, DEP dans le portail), un profil (anciennement profil DEP) est utilisé. Ce profil est transféré de Relution au serveur Apple et est appliqué aux appareils avant l'inscription proprement dite.

> Un seul profil peut être appliqué par appareil à la fois. En outre, le profil n'est transmis aux appareils qu'une seule fois lors de l'inscription. Si des modifications doivent être transmises ultérieurement, les appareils doivent être réinitialisés aux valeurs d'usine pour recevoir le profil mis à jour.

Un profil ne peut être créé que si l'ADE (anciennement DEP) est configurée dans l'organisation Relution et qu'un jeton DEP valide est enregistré.

Configurer DEP →

Les nouveaux profils sont créés sous `Appareils` → `Profils` via Créer. Si d'autres types d'inscription automatique sont également configurés, le type de profil est demandé d'abord ; DEP y est sélectionné. Cette zone offre également une vue d'ensemble des profils existants.

L'option Utiliser comme profil par défaut fait d'un profil le profil par défaut. Il est automatiquement attribué aux nouvelles inscriptions automatiques auxquelles aucun autre profil n'est encore attribué. Pour les appareils dont la migration MDM est en cours, cela ne se produit que si Attendre la configuration et Conserver toutes les applications installées sont activées dans le profil par défaut. Il est recommandé de définir un profil par défaut. Le nom du profil doit être significatif afin qu'il puisse être facilement identifié.

Sous Accords, il est possible de sélectionner des accords créés sous `Paramètres` → `Général` → `Accords`. Relution met leurs textes à la disposition de l'appareil pendant l'inscription. La sélection n'est affichée qu'aux utilisateurs disposant d'un droit de lecture sur les accords.

Le Nom d'appareil par défaut (255 caractères maximum) est appliqué aux appareils dans les Inscriptions automatiques lors de l'inscription. Des espaces réservés peuvent également être utilisés et combinés ici, voir Espaces réservés avancés →. Les champs Numéro de téléphone du support, Adresse e-mail du support, Nom du département (125 caractères maximum) et Invite d'authentification (255 caractères maximum) contiennent des informations affichées lors de l'inscription.

Pour la version 26.4.0

Forcer l’inscription MDM

Cette option rend obligatoire l’enrôlement des appareils au démarrage. Il n’est pas possible d’ignorer ou d’annuler le processus d’enrôlement. Par exemple, si les appareils sont volés, ils ne peuvent pas être mis en service sans l’inscription MDM.

Authentification de l’utilisateur lors de l’inscription

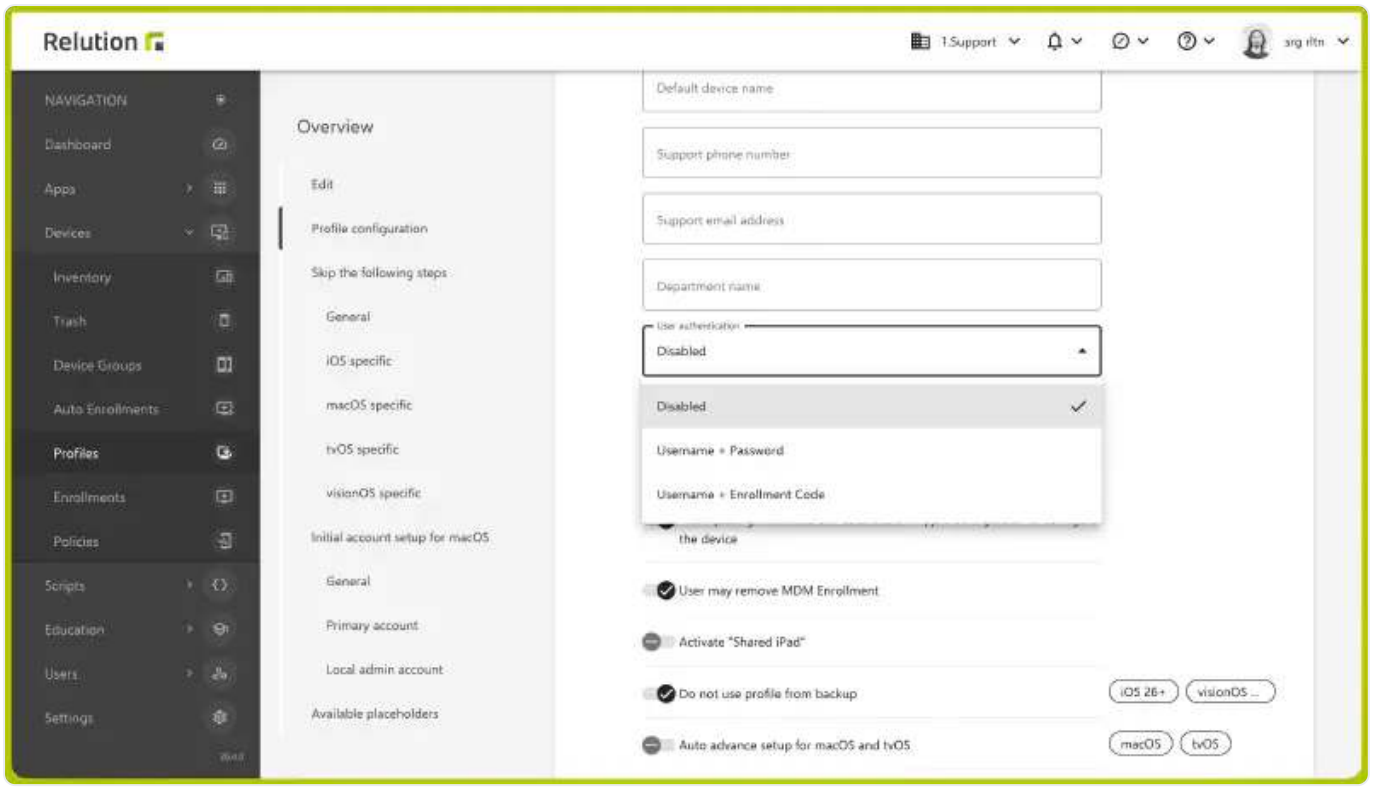
Nouveau dans 26.4

Le champ Authentification utilisateur détermine si et comment les utilisateurs doivent s’authentifier lors de l’inscription. Trois options sont disponibles :

- Désactivé : aucune authentification utilisateur n’a lieu.
- Nom d’utilisateur + mot de passe : l’inscription doit être authentifiée avec un compte utilisateur Relution. Un compte Apple n’est pas nécessaire pour cela et n’est pas pris en charge ici.
- Nom d’utilisateur + Code d’inscription (depuis la version 26.4) : au lieu d’un mot de passe, un code d’inscription à usage unique généré par Relution est demandé.

Si des appareils sont attribués à des utilisateurs individuels dans la liste Inscriptions automatiques, seuls ces derniers pourront s’authentifier et mettre en service les appareils correspondants.

Pour la version 26.4.0



> L’option Nom d’utilisateur + Code d’inscription nécessite qu’un compte utilisateur avec une adresse e-mail renseignée soit affecté à l’inscription automatique de l’appareil. Le code est généré lors de l’inscription et envoyé exclusivement par e-mail à cette adresse. Pour que cela fonctionne, l’envoi de mails doit être configuré et fonctionnel sur le serveur. Configurer l’envoi de mails →

Pour la version 26.4.0

Avec Nom d’utilisateur + Code d’inscription, l’adresse e-mail de l’utilisateur attribué est également acceptée à la place du nom d’utilisateur. Le code à huit caractères n’est valable qu’une seule fois et devient invalide après plus de cinq tentatives erronées. Si la page de connexion est rouverte, Relution génère un nouveau code et l’envoie.

Autoriser le couplage avec des Mac ou des PC et autoriser Apple Configurator à configurer l’appareil

Cette option est activée par défaut ; si elle est désactivée, le portail affiche un avertissement. Si cette option est désactivée, il ne sera pas possible de se connecter ultérieurement à un PC ou à un Mac, par exemple pour copier des photos ou créer une sauvegarde des appareils. Il est recommandé d’activer cette option et d’interdire la connexion avec des ordinateurs dans les restrictions, si cela est souhaité. L’avantage est que les restrictions dans les politiques peuvent être modifiées à tout moment. Le profil, quant à lui, ne peut pas l’être. Dans ce cas, il faudrait obligatoirement réinitialiser les appareils pour modifier l’option.

L’utilisateur peut supprimer l’inscription MDM

Si l’option est activée, les utilisateurs des appareils peuvent supprimer le profil MDM et donc la possibilité de gestion par Relution.

Cette option est activée par défaut pour les nouveaux profils. Pour empêcher la suppression du profil MDM, elle doit être désactivée avant l’inscription des appareils ; une modification ultérieure nécessite la réinitialisation des appareils.

Activer l’iPad partagé

L’option Activer « iPad partagé » est la seule possibilité d’activer le mode multi-utilisateurs d’Apple, iPad partagé. Si cette option est activée, toutes les cases cochées ci-dessous pour les étapes de configuration à sauter deviennent redondantes, car elles sont sautées automatiquement.

Pour la version 26.4.0

Ne pas utiliser le profil de sauvegarde

Cette option concerne les appareils à partir d’iOS/iPadOS 26 ou de visionOS 26. Si elle est activée, l’appareil n’utilise pas le profil contenu dans la sauvegarde lors de la restauration d’une sauvegarde. Détails sur le transfert via une sauvegarde : Sauvegarde →

Avance automatique de la configuration pour macOS et tvOS

Si l’option Configuration avancée automatique pour macOS et tvOS est activée, l’assistant de configuration des appareils macOS et tvOS passe automatiquement d’un écran à l’autre. L’appareil a besoin pour cela d’une connexion Ethernet. Tant que l’option est activée, les étapes de configuration à sauter ne peuvent pas être sélectionnées.

Attendre la configuration

Si Attendre la configuration est activée, l’appareil reste dans l’assistant de configuration jusqu’à ce que toutes les applications et configurations aient été installées. L’action d’appareil Continuer

dans l'Assistant Configuration de l'appareil informe l'appareil que la préconfiguration est terminée et qu'il peut continuer dans l'assistant de configuration.

L'option Conserver toutes les applications installées n'est disponible qu'avec Attendre la configuration et est activée par défaut. Elle est nécessaire pour préserver les applications gérées et leurs données lors de la migration d'appareils gérés entre serveurs MDM.

Version minimale du système d'exploitation

Nouveau dans 26.5

L'option Version minimale du système d'exploitation impose aux appareils de se mettre d'abord à jour vers une version spécifique pendant l'Assistant de configuration, avant de pouvoir être inscrits. Une version minimale peut être définie indépendamment pour chaque plateforme :

- Version minimale d'iOS/iPadOS
- Version minimale de macOS
- Version minimale de visionOS

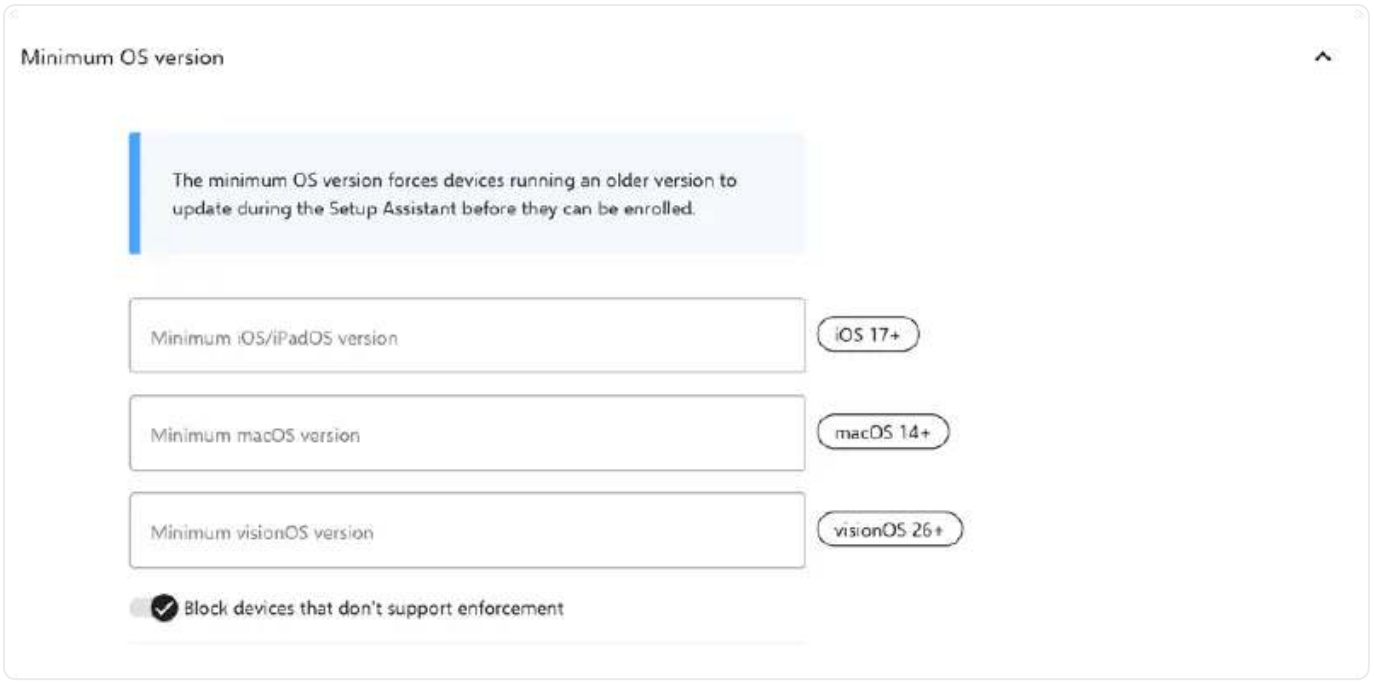
Si un champ reste vide, aucune version minimale n'est appliquée pour la plateforme correspondante. tvOS n'est pas pris en charge par cette fonctionnalité.

Pour la version 26.4.0

Si un appareil satisfait déjà le minimum configuré, l'inscription n'est pas affectée. Si un appareil signale, lors de l'inscription, une version inférieure au minimum configuré, il lui est d'abord demandé de se mettre à jour pendant l'Assistant de configuration. L'inscription ne se poursuit qu'une fois la mise à jour effectuée et l'Assistant de configuration relancé. Relution demande automatiquement la version la plus basse actuellement proposée par Apple qui satisfait le minimum requis — pas nécessairement la dernière version disponible. Cette application obligatoire suppose également que l'appareil puisse effectivement se voir demander une mise à jour, ce qu'Apple prend en charge à partir d'iOS/iPadOS 17, de macOS 14 et de visionOS 26.

> Si Apple ne propose actuellement aucune version satisfaisant le minimum configuré, l'inscription de l'appareil est refusée plutôt que de le diriger vers une version indisponible. Cela évite que des appareils restent bloqués dans l'Assistant de configuration.

L'option Bloquer les appareils qui ne prennent pas en charge l'application obligatoire (activée par défaut) détermine comment sont traités les appareils auxquels aucune mise à jour ne peut être demandée pendant l'inscription, par exemple parce qu'ils exécutent une version trop ancienne du système d'exploitation. Si l'option est activée, ces appareils sont exclus de l'inscription. Si elle est désactivée, ils sont inscrits sans application de la version minimale du système d'exploitation.



Sauter les étapes de configuration suivantes

Toutes les options activées seront ignorées lors de la configuration initiale de l'appareil.

Les étapes de configuration affichées à nouveau après la configuration initiale, p. ex. après une mise à jour logicielle, ne sont pas concernées. Elles peuvent être masquées via la configuration Assistant d'installation dans une politique, voir Assistant d'installation (iOS) → et Assistant d'installation (macOS) →.

Si Services de localisation n'est pas activé, l'étape est affichée pendant la configuration. La localisation de l'appareil peut y être autorisée afin que les appareils règlent automatiquement le bon fuseau horaire. L'option ne concerne que l'assistant de configuration et n'a aucune influence sur la localisation ultérieure des appareils.

Configuration initiale du compte pour macOS

Cette section permet d'ajouter des comptes d'utilisateur et d'administrateur aux appareils macOS, qui sont automatiquement créés au démarrage. Des espaces réservés sont également disponibles dans cette section, voir Espaces réservés avancés →.

Pour la version 26.4.0

Ajouter des appareils au DEP

À l'origine, seuls les appareils Apple achetés directement auprès d'Apple ou de revendeurs de confiance pouvaient être ajoutés à Apple School/Business Manager. Si des appareils étaient achetés auprès d'autres sources, ils ne pouvaient pas être automatiquement inscrits dans Relution via l'inscription automatisée des appareils (ADE, DEP dans le portail).

Appareils iOS / tvOS via Apple Configurator 2

Apple permet désormais d'ajouter manuellement des appareils iOS et tvOS à Apple School/Business Manager à l'aide de l'Apple Configurator. Cela permet de bénéficier de tous les avantages de l'inscription automatique via l'ADE, quel que soit l'endroit où les appareils ont été achetés. Ajouter les appareils Apple au DEP à une date ultérieure →

Appareils macOS via Apple Configurator (mobile)

Avec l'Apple Configurator pour appareils mobiles (iOS/iPadOS), Apple a fourni un moyen facile d'ajouter des appareils macOS à l'Apple School/ Business Manager. Manuel du configurateur Apple →
Apple Configurator App →

Pour la version 26.4.0

Instructions

1. Installer Apple Configurator sur un appareil iOS/iPadOS avec au moins iOS 16.
2. Sur l'appareil, se connecter à Apple Configurator avec un compte Apple School/Business Manager valide.
3. Démarrer l'appareil macOS et s'arrêter dans l'Assistant de configuration lorsque la section pour le Pays ou la Région s'affiche.
4. Tenir l'appareil iOS/iPadOS près du Mac, et sur le Mac, cliquer sur Jumeler Manuellement en bas à gauche de l'Assistant de configuration.
5. Entrer la combinaison de 6 chiffres sur l'appareil iOS/iPadOS.
6. Une fois que l'appareil macOS a terminé le processus, un redémarrage ou une extinction est proposé.
7. Attribuer l'appareil à un emplacement dans Apple School/Business Manager.
8. Dans Relution, sous `Appareils` → `Inscriptions automatiques`, déclencher la synchronisation via Synchroniser les appareils (sans déclenchement manuel, elle a lieu

automatiquement une fois par jour). Un profil DEP marqué Utiliser comme profil par défaut est alors attribué automatiquement aux appareils sans profil ; sinon, sélectionner l'appareil et lui attribuer un profil DEP via Définir le profil.

9. Terminer la procédure d'accueil Apple habituelle sur l'appareil.

Les profils DEP sont créés sous `Appareils` → `Profils`, voir Profil pour l'ADE →.

Remarque sur le statut dans les Inscriptions automatiques

- Bleu - Profil attribué - Un profil DEP a été attribué à l'appareil, mais n'a pas encore été appliqué.
  - Cela peut se produire lors de modifications du profil pour des appareils déjà inscrits ou pour des appareils qui n'ont pas encore terminé la configuration.
- Vert - Profil poussé - Le profil a été appliqué et l'appareil a signalé son exécution.
- Rouge - Profil supprimé - Le profil a été retiré de l'appareil.
- Gris - Pas de profil - Aucun profil DEP n'est attribué à l'appareil ou un profil attribué a été supprimé.
- Gris - Profil inconnu - Apple a signalé un statut de profil que Relution ne peut pas attribuer.

Supprimer des appareils

Pour la version 26.4.0

Il arrive souvent que des appareils appartenant à des utilisateurs finaux aient été ajoutés à l'ADE à des fins éducatives, par exemple, mais qu'ils soient ensuite renvoyés à un usage privé. Dans ce cas, les appareils doivent être correctement retirés du MDM et de l'ADE pour garantir une utilisation continue sans problème.

L'ordre suivant doit être respecté :

1. Sauvegarder les données.
2. Libérer l'appareil de l'organisation dans Apple School/Business Manager ou le dissocier du serveur MDM Relution.
3. Seulement ensuite, réinitialiser l'appareil, soit par l'utilisateur, soit dans Relution via l'action Effacer l'appareil.

> Si l'appareil est réinitialisé avant l'étape 2, l'attribution ADE est conservée et l'appareil s'inscrit à nouveau dans Relution dans l'Assistant de configuration.

Sauvegarde des données

La manière la plus simple de sauvegarder les données de l'utilisateur entre la réinitialisation et la nouvelle configuration est d'utiliser Apple iCloud avec un compte Apple privé. Pour ce faire, il faut s'assurer que l'option Autoriser la modification du compte est activée dans la configuration Restrictions dans Relution et qu'elle a été appliquée à l'appareil. L'option est activée par défaut ; une intervention n'est nécessaire que si une restriction attribuée la désactive. Cela permet à l'utilisateur de se connecter à l'appareil avec un compte Apple privé et d'effectuer la sauvegarde de données souhaitée.

Suppression de l'Apple School / Business Manager

La libération ou la dissociation peut facilement être effectuée dans le portail Apple ASM/ABM sans avoir d'effet immédiat sur l'appareil. Ce n'est qu'à la prochaine réinitialisation complète aux paramètres d'usine que l'appareil reçoit d'Apple l'attribution actuelle et n'est plus inscrit automatiquement. Dans Relution, l'inscription automatique est supprimée lors de la synchronisation suivante, dès qu'Apple signale l'appareil comme retiré. La synchronisation a lieu automatiquement une fois par jour ou immédiatement via Synchroniser les appareils sous `Appareils` → `Inscriptions automatiques`.

Pour la version 26.4.0

Suppression du MDM

Dans Relution, l'option Effacer tout le contenu et les paramètres doit être autorisée dans la configuration Restrictions (activée par défaut). De cette façon, l'utilisateur peut réinitialiser l'appareil après la sauvegarde. Il est conseillé d'informer l'administrateur Relution, car un réseau Wi-Fi précédemment déconnecté sur l'appareil peut empêcher la communication avec le MDM, auquel cas aucune information sur l'état de l'appareil n'est disponible. Sinon, l'action Effacer l'appareil peut être déclenchée dans Relution, ce qui déplace l'appareil dans la Poubelle et met à jour les informations relatives à l'appareil en conséquence.

> Les modifications de l'attribution ADE et du profil DEP ne prennent effet qu'après une réinitialisation d'usine.

Configurer le VPP

Lors de l'acquisition et de la distribution d'applications aux utilisateurs, l'administrateur d'un système MDM est confronté à certains défis. Lorsque les utilisateurs obtiennent une application sur l'App Store d'Apple, que ce soit à partir d'un appareil de l'école ou de l'entreprise ou d'un appareil personnel, l'application doit être téléchargée individuellement à l'aide d'un identifiant Apple personnel. La licence de l'application n'appartient alors pas à l'école ou à l'entreprise, mais est attribuée à l'identifiant Apple personnel.

Le problème se pose principalement pour les applications payantes lorsque la licence de l'application achetée est remboursée aux utilisateurs sous forme de remboursement de frais ou de bons d'achat. En effet, les utilisateurs conservent toujours la propriété de la licence de l'application via leur identifiant Apple personnel. En cas de changement d'école ou de départ de l'entreprise, la licence d'application est irrévocablement perdue pour les étudiants ou les employés. Si une application doit être distribuée à un grand nombre d'appareils, l'utilisation d'identifiants Apple personnels crée rapidement une situation confuse et difficile à contrôler pour l'administrateur.

Pour la version 26.4.0

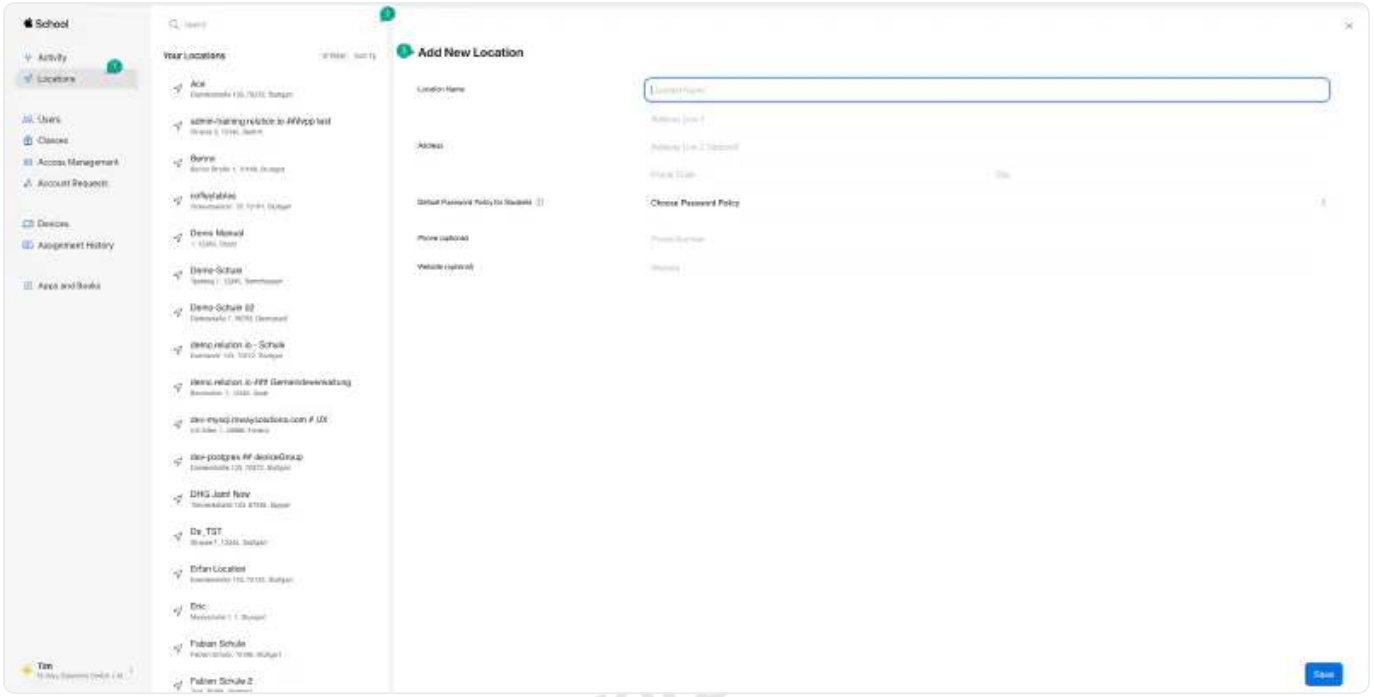
À quoi sert Apps et livres (VPP) ?

Pour résoudre les problèmes décrits ci-dessus et pouvoir distribuer des applications de l'App Store d'Apple via Relution sans avoir besoin d'un identifiant Apple sur l'appareil mobile, il existe le programme Apps et livres d'Apple (VPP dans le portail), anciennement appelé Programme d'achat en volume d'Apple (Apple Volume Purchase Program). Ce programme permet d'acheter des applications en grandes quantités de manière centralisée et de les distribuer indépendamment de l'utilisateur, sans avoir besoin d'un identifiant Apple sur l'appareil. Les licences d'applications issues d'Apps et livres, appelées licences VPP dans le portail, sont ainsi gérées de manière centralisée sans jamais changer de propriétaire et peuvent être retirées à tout moment par l'administrateur.

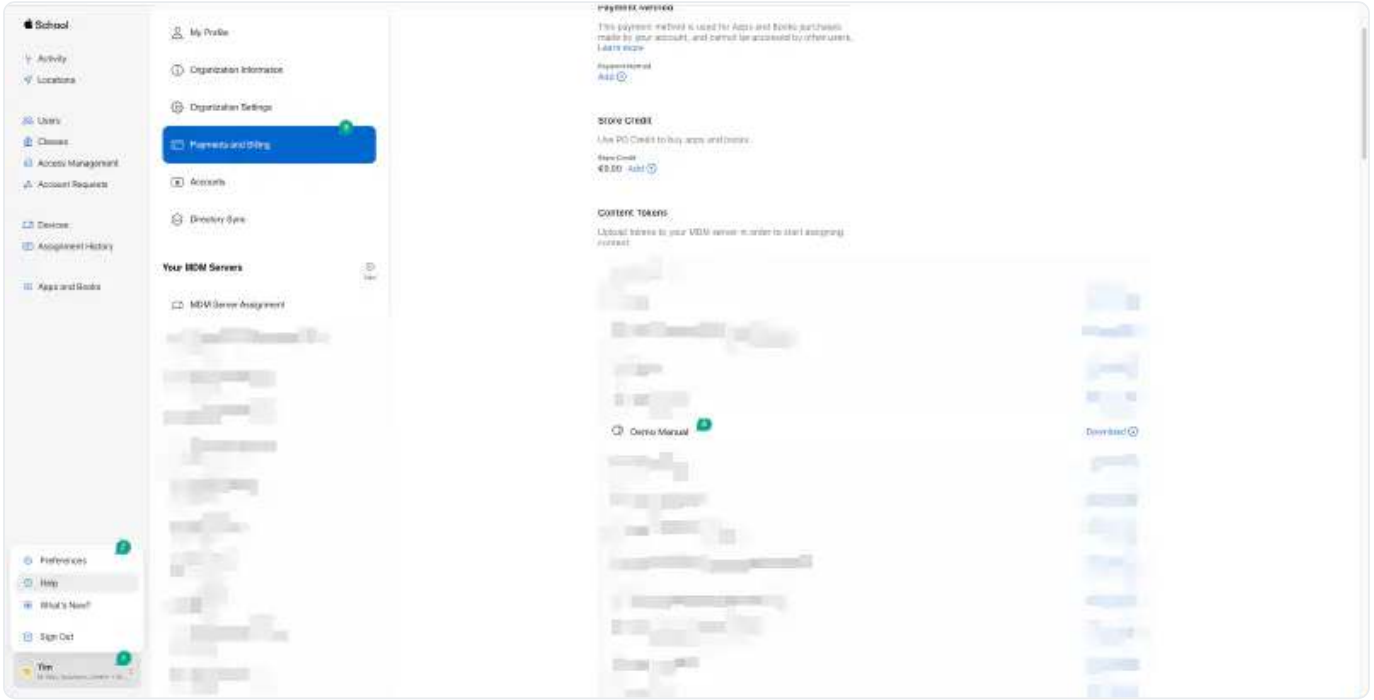
Apps et livres est cartographié et configuré via l'Apple Business Manager ou l'Apple School Manager. C'est également là que les licences d'application sont achetées de manière centralisée à l'aide de l'identifiant Apple de l'école ou de l'entreprise. Ce programme s'applique aux applications gratuites et payantes.

Comment le VPP est-il lié à Relution ?

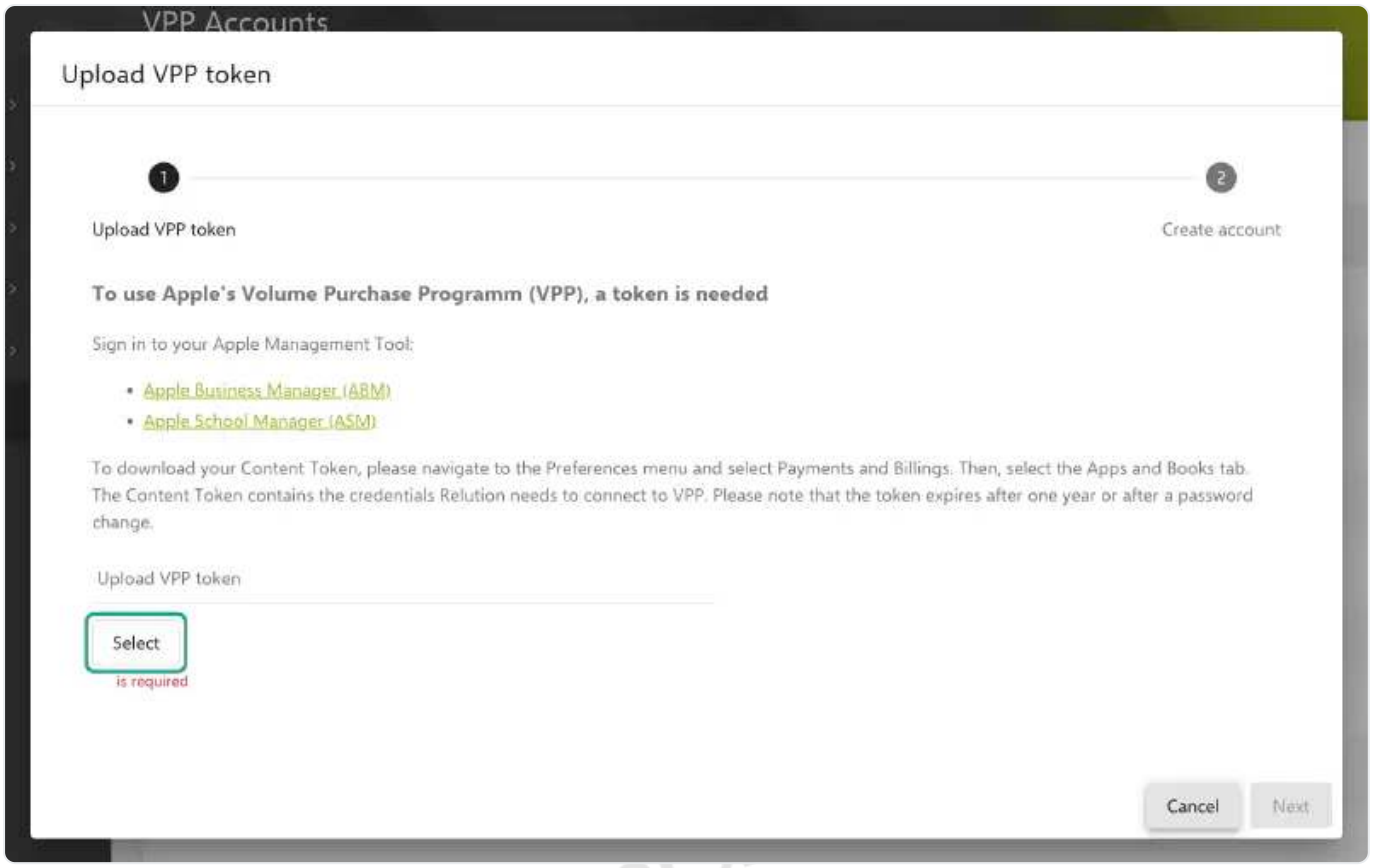
Pour distribuer les licences VPP achetées via Relution, les deux systèmes doivent être liés. Dans Apple Business Manager ou Apple School Manager, un nouvel emplacement est d'abord créé sous Emplacements.

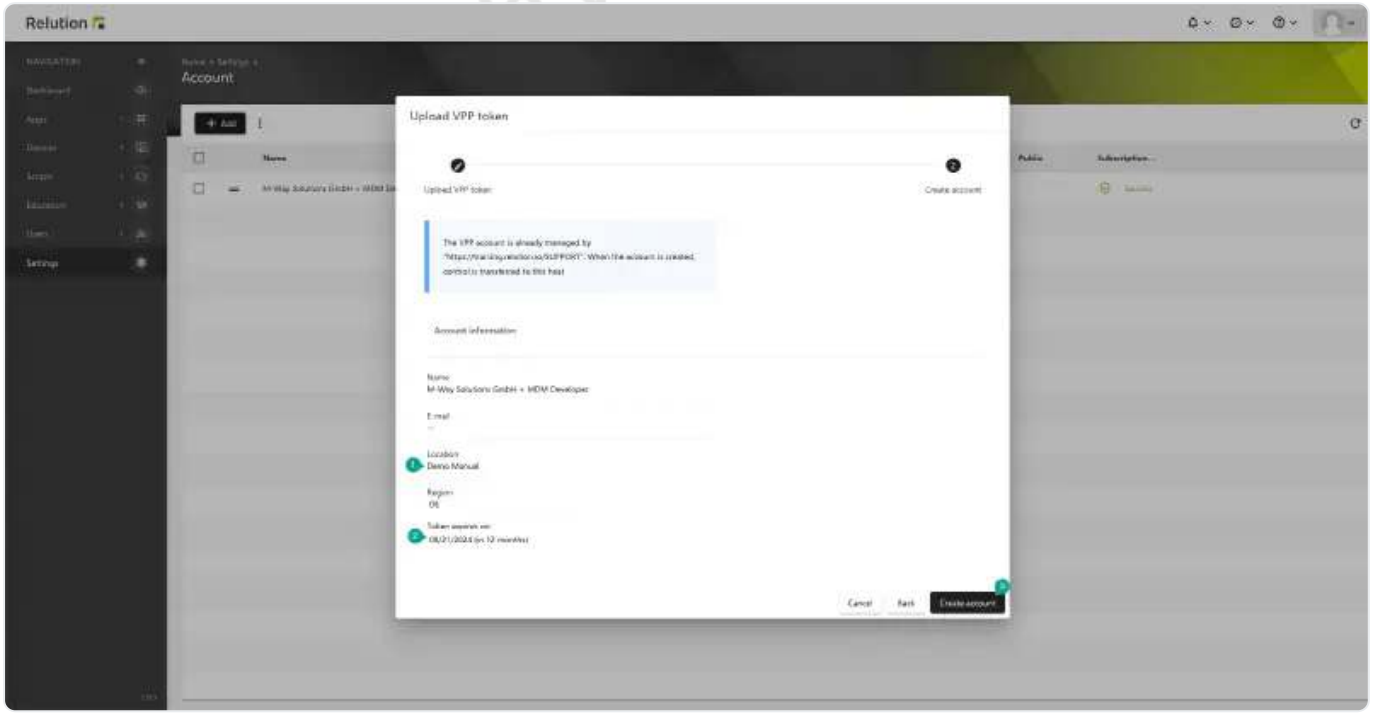


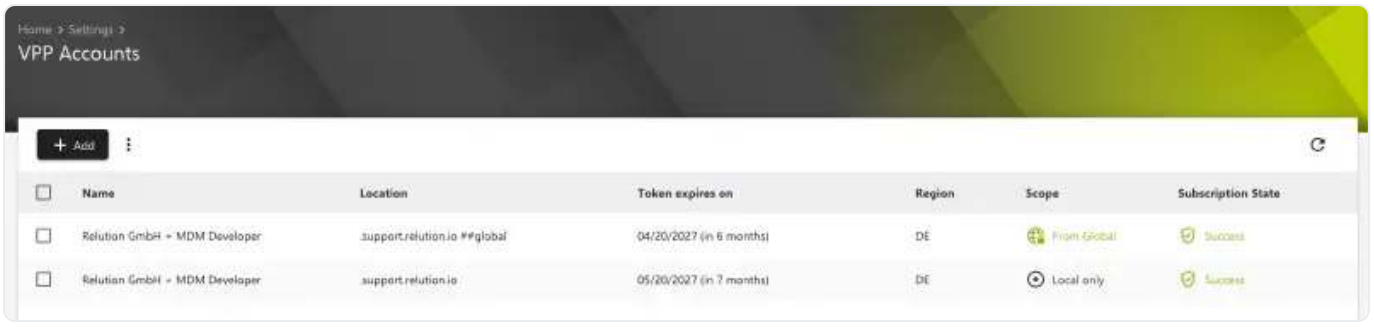
Pour connecter cet emplacement à un serveur MDM, un jeton VPP doit être généré pour l'emplacement concerné sous `Préférences` → `Apps et livres`.



Une fois que le jeton VPP est téléchargé dans Relution sous `Paramètres` → `Programme d'achat en volume (VPP)` → `Compte`, les deux systèmes sont liés.







Si le jeton est déjà géré par un autre serveur MDM, la boîte de dialogue le signale lors de la création du compte. Avec la création du compte, Relution reprend la gestion du jeton. La colonne État de l'abonnement de la liste des comptes indique si Relution est inscrit auprès d'Apple pour recevoir les notifications concernant ce compte. Pour cela, le serveur Relution doit être accessible depuis les serveurs Apple.

> Chaque jeton VPP est valable pendant un an. Il doit ensuite être téléchargé à nouveau dans Apple Business Manager ou Apple School Manager pour l'emplacement concerné. Le nouveau jeton est importé dans le compte existant dans Relution via le menu à trois points → Mettre à jour le jeton (voir Renouveler les jetons VPP (Jetons de contenu) →). La suppression du compte efface toutes les données VPP, et un deuxième compte pour le même emplacement ne peut pas être créé dans la même organisation. Le centre de notification de Relution alerte en temps voulu en cas d'expiration prochaine d'un jeton VPP.

Pour la version 26.4.0

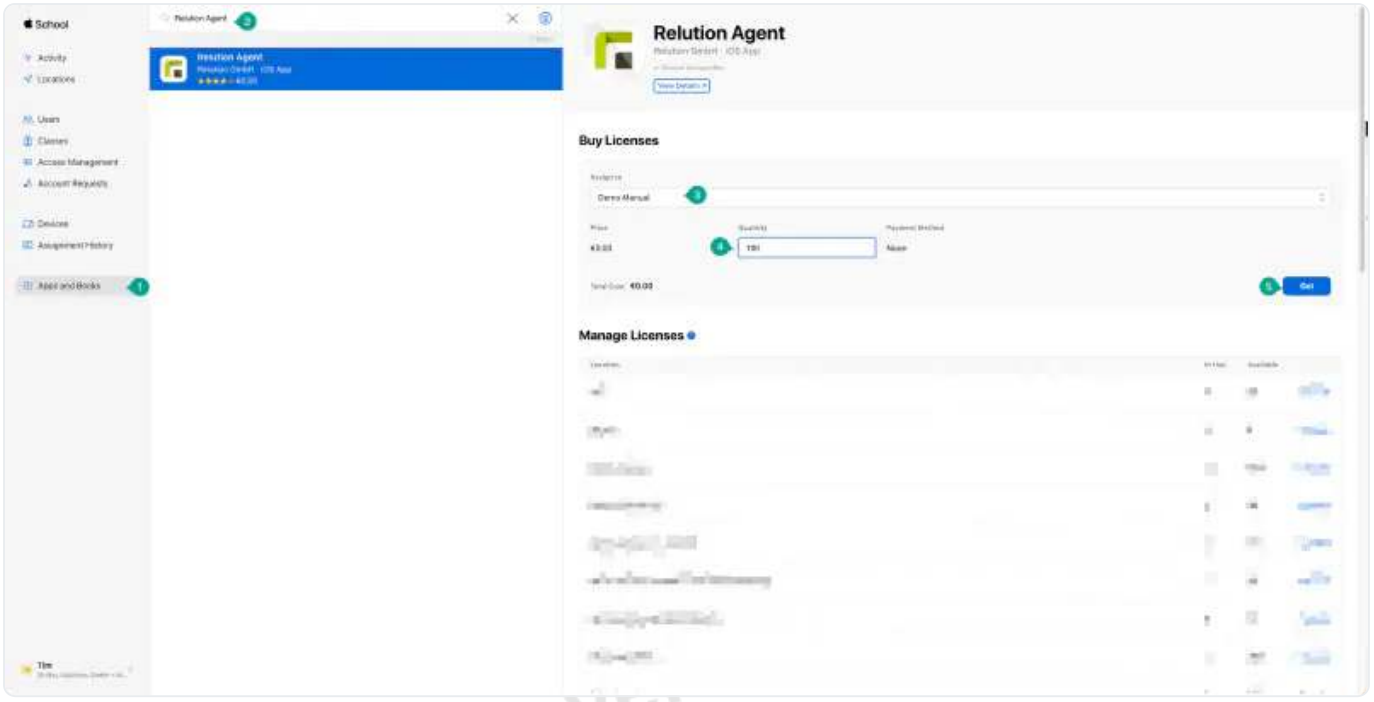
Les notifications par e-mail concernant l'expiration prochaine et l'expiration des jetons VPP et DEP sont activées par défaut et peuvent être ajustées sous `Paramètres` → `Les notifications` via Le jeton VPP va bientôt expirer, Le jeton VPP a expiré, Le jeton DEP va bientôt expirer et Le jeton DEP a expiré. Le premier rappel est envoyé 30 jours avant l'expiration, puis quotidiennement à partir de 15 jours avant l'expiration. Les e-mails sont adressés aux utilisateurs autorisés à gérer les paramètres VPP ou DEP.

L'utilisation de plusieurs jetons VPP dans une organisation Relution est décrite dans une section séparée.

Après l'appairage, les éléments de menu Apps achetées et Les médias apparaissent dans Relution sous Apps. Apps achetées liste toutes les apps achetées via Apps et livres et les licences VPP correspondantes (nombre), Les médias contient les livres achetés. Les licences VPP sont automatiquement synchronisées à intervalles réguliers. En outre, les licences VPP pour l'organisation peuvent également être mises à jour manuellement via Synchroniser. L'historique des synchronisations, y compris les opérations échouées, est affiché sous `Paramètres` → `Programme d'achat en volume (VPP)` → `Historique de synchronisation`.

Comment les licences d’application sont-elles obtenues dans VPP ?

Dans Apple Business Manager ou Apple School Manager, les licences d’application peuvent être obtenues sous Apps et livres et attribuées à un emplacement configuré.

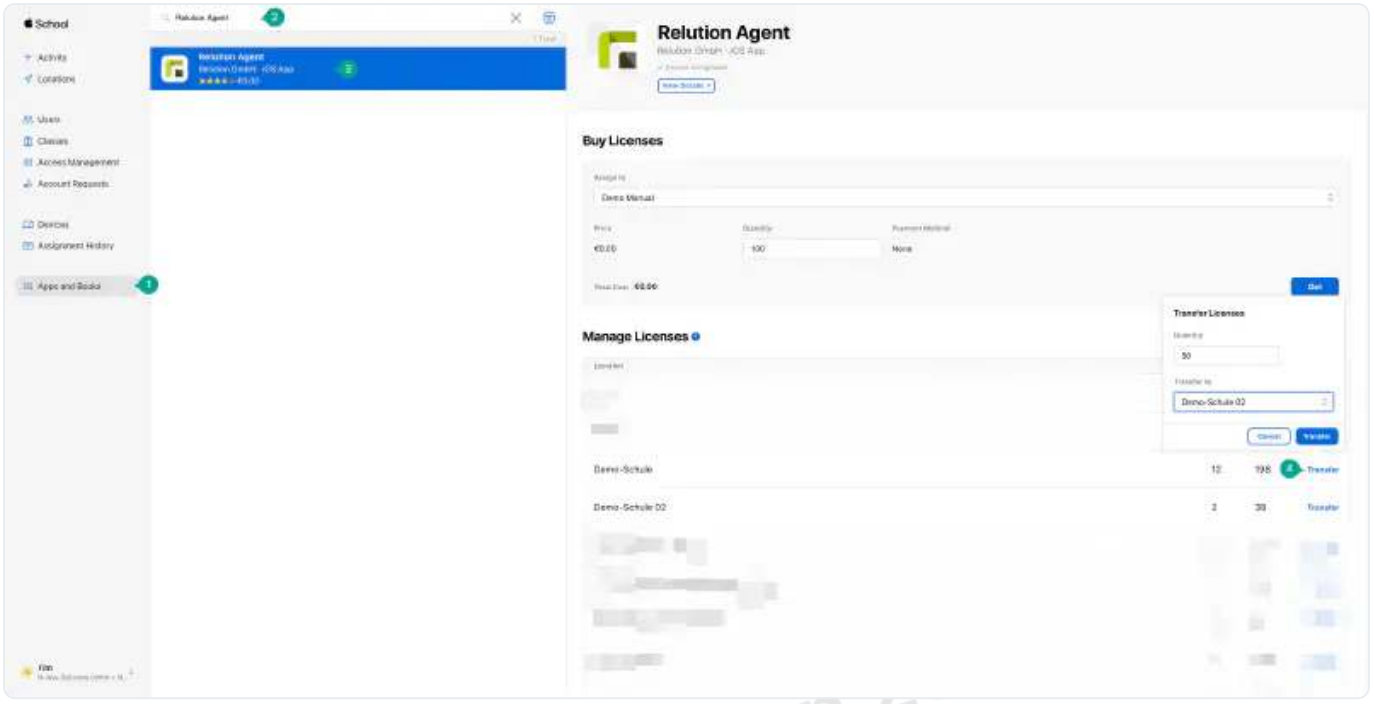


Une fois chargées, elles sont disponibles dans Apple Business Manager ou Apple School Manager. En outre, les licences d’application peuvent être distribuées aux appareils de l’organisation appropriée dans Relution associé à l’emplacement sélectionné via un jeton VPP.

Le VPP peut-il également être utilisé pour gérer des licences d’application pour différentes organisations ou différents lieux ?

Si plusieurs organisations sont gérées dans Relution via la fonctionnalité multi-client, comme c’est le cas, par exemple, pour un conseil scolaire avec plusieurs écoles, les licences d’application peuvent être achetées de manière centralisée avec un Apple ID du conseil scolaire et distribuées aux écoles respectives. Pour ce faire, un emplacement doit être créé dans Apple School Manager pour chaque école et le jeton VPP doit être stocké dans l’organisation Relution correspondante de chaque école. Cela s’applique de manière analogue à Apple Business Manager dans le contexte de l’entreprise.

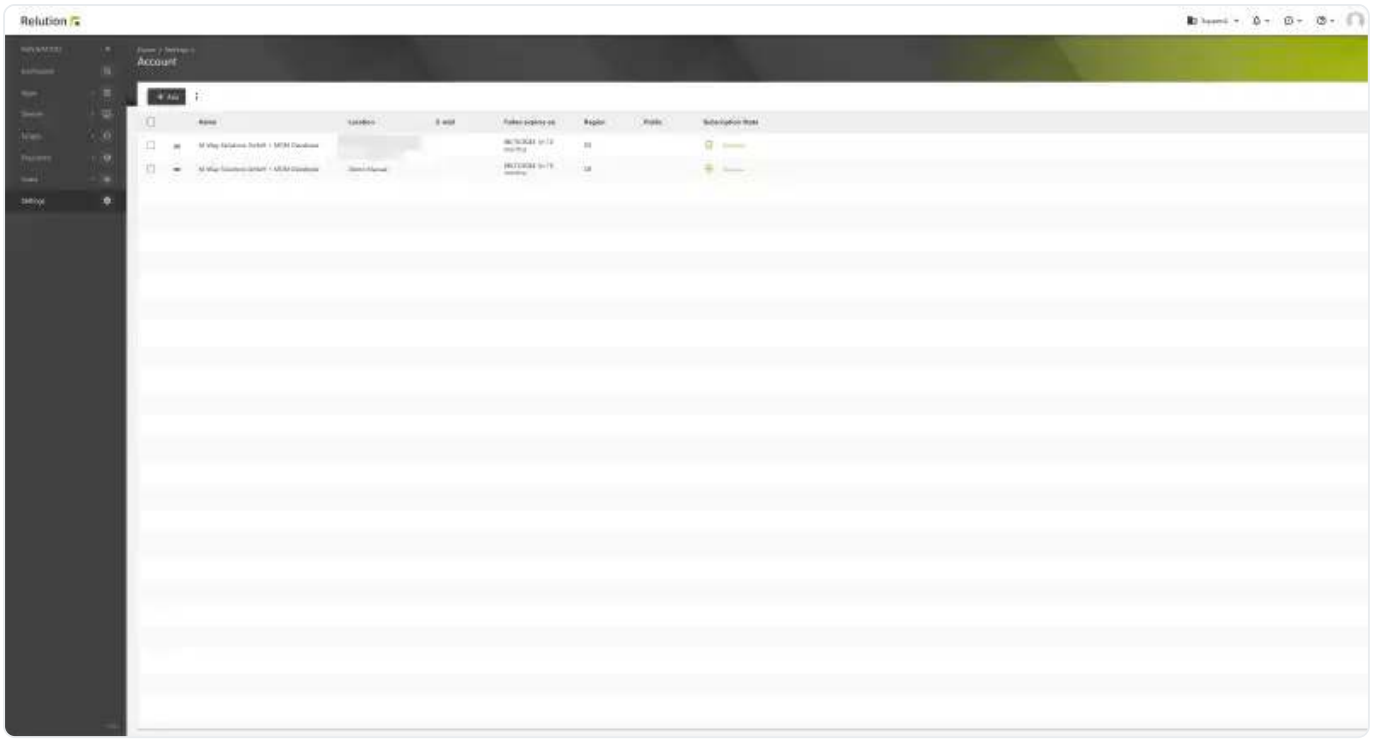
Les licences VPP achetées peuvent être gérées dans Apple Business Manager ou Apple School Manager et transférées vers d'autres sites. Il est ainsi possible d'acheter des licences d'application de manière centralisée pour un site principal et de les distribuer ensuite à d'autres sites sous forme de paquets.



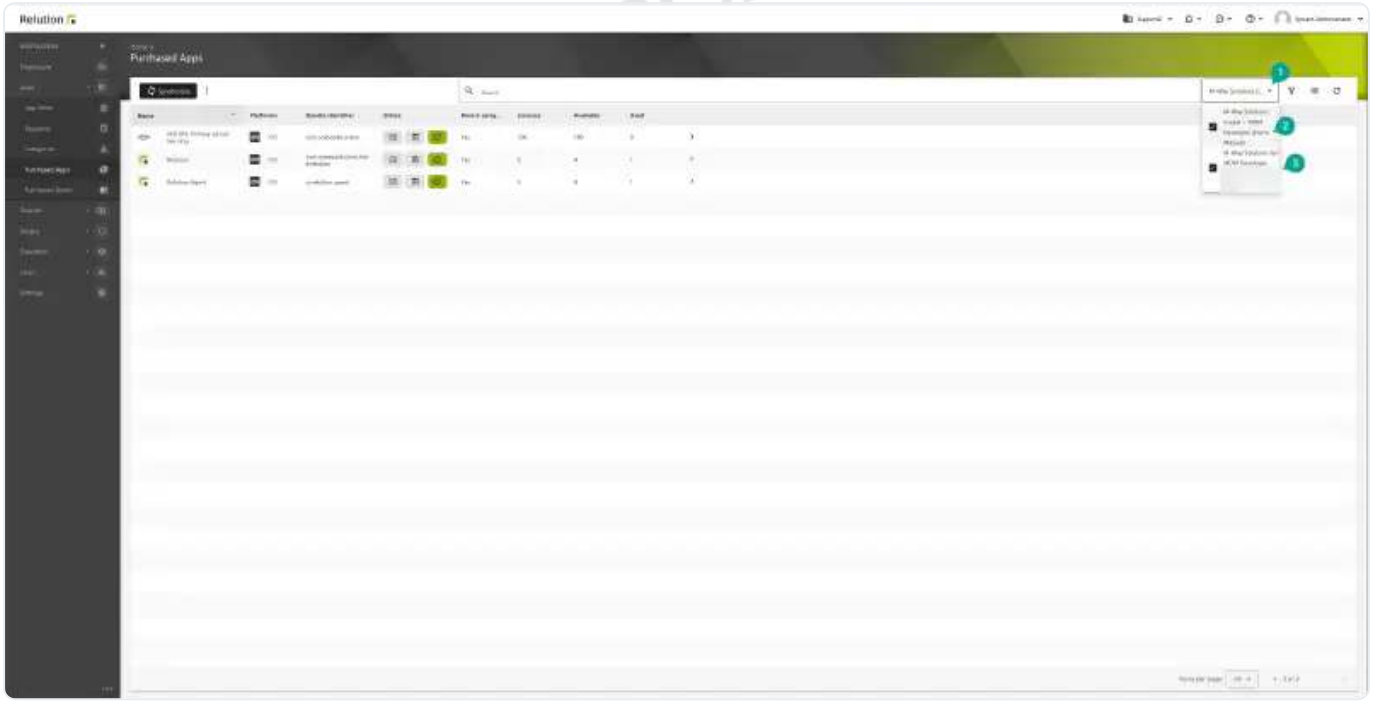
pour la version 2

Est-il possible d'utiliser plusieurs jetons VPP au sein d'une organisation Relution ?

Au sein de Relution, il est possible de stocker plusieurs jetons VPP sous `Paramètres` → `Programme d'achat en volume (VPP)` → `Compte`. L'objectif est de relier différents comptes Apple School Manager, par exemple si une école est équipée d'applications VPP par un conseil scolaire, mais qu'en même temps elle possède et utilise ses propres licences VPP. Par analogie, cela fonctionne également avec Apple Business Manager.



La somme de toutes les licences d'application provenant de plusieurs jetons VPP pour une organisation est affichée sous forme agrégée dans la vue Apps achetées. Un menu déroulant peut être utilisé pour filtrer les licences VPP selon l'emplacement dans Apple School Manager.



Les licences VPP sont attribuées sous `Apps` → `Apps achetées` : après la sélection d'une application, Associer une licence ouvre une boîte de dialogue dans laquelle des appareils, des utilisateurs ou des groupes sont sélectionnés. Si la licence de l'application existe dans plus d'un

jeton VPP stocké, le jeton à partir duquel la licence de l'application doit être utilisée est d'abord sélectionné. Révoquer la licence annule une attribution.



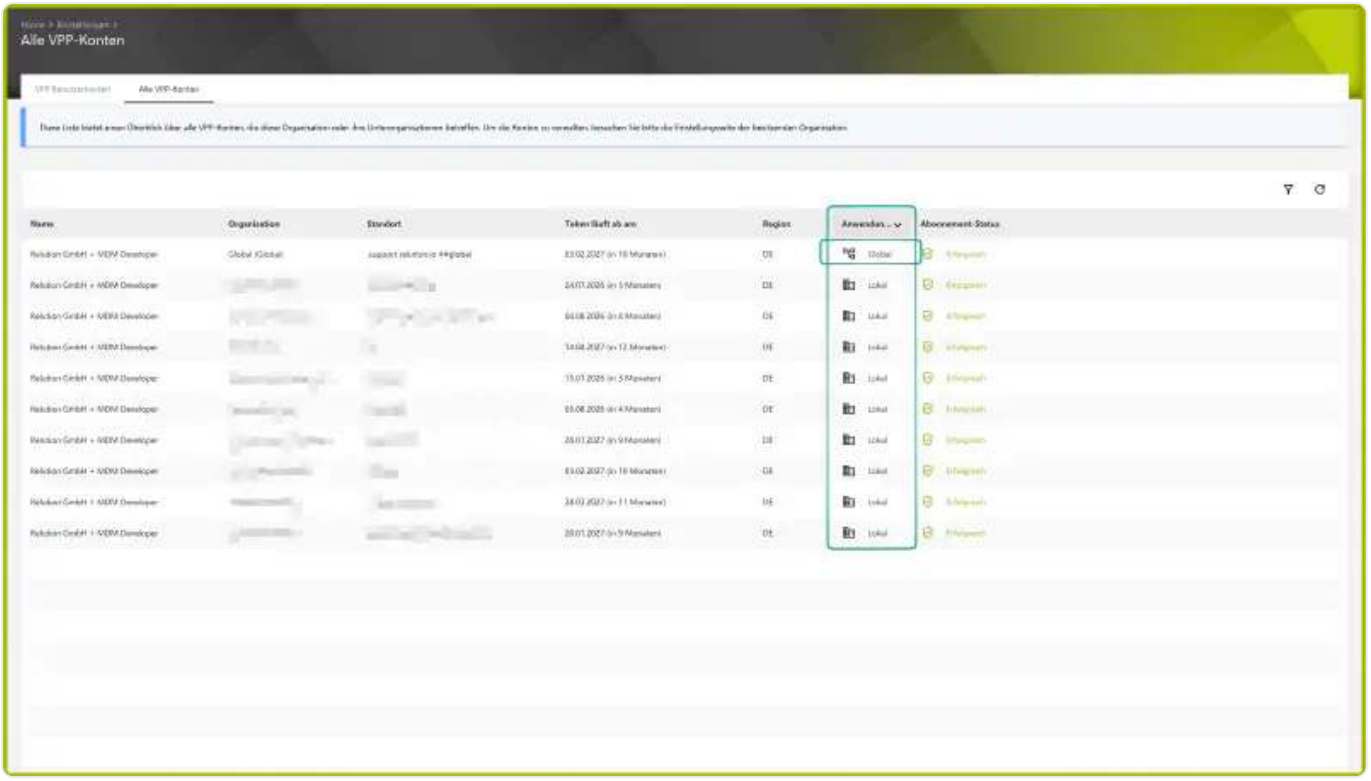
VPP global

Avec Relution, il est possible d'intégrer des jetons VPP dans l'organisation globale. Cela permet de distribuer des applications achetées de manière centralisée vers les tenants.

Un jeton VPP de l'organisation globale est automatiquement disponible dans toutes les organisations, un jeton VPP d'une méta-organisation dans ses sous-organisations. Les applications issues des comptes VPP de l'organisation globale remplacent automatiquement les applications existantes dans les autres organisations ; cette opération est irréversible. Dans l'organisation subordonnée, le jeton hérité n'est pas modifiable (y compris les paramètres de mise à jour des applications) ; seul son ordre peut être modifié. Dans Apps achetées et Les médias, les attributions affichées concernent l'organisation actuelle, tandis que le nombre total de licences s'applique à toutes les organisations.

Cela évite la mise en place multiple dans Apple School Manager / Apple Business Manager ainsi que la mise à jour répétée de plusieurs jetons. Dans le meilleur des cas, un seul jeton doit être renouvelé une fois par an.

Pour la version 26.4.0



Remarque importante concernant les licences

Il est essentiel de disposer d'un nombre suffisant de licences VPP pour tous les appareils et tenants.

Exemple :

- Organisation 1 : 250 appareils
- Organisation 2 : 100 appareils
- Organisation 3 : 1000 appareils

Dans ce cas, au moins 1350 licences VPP globales doivent être acquises.

Jetons VPP spécifiques aux tenants

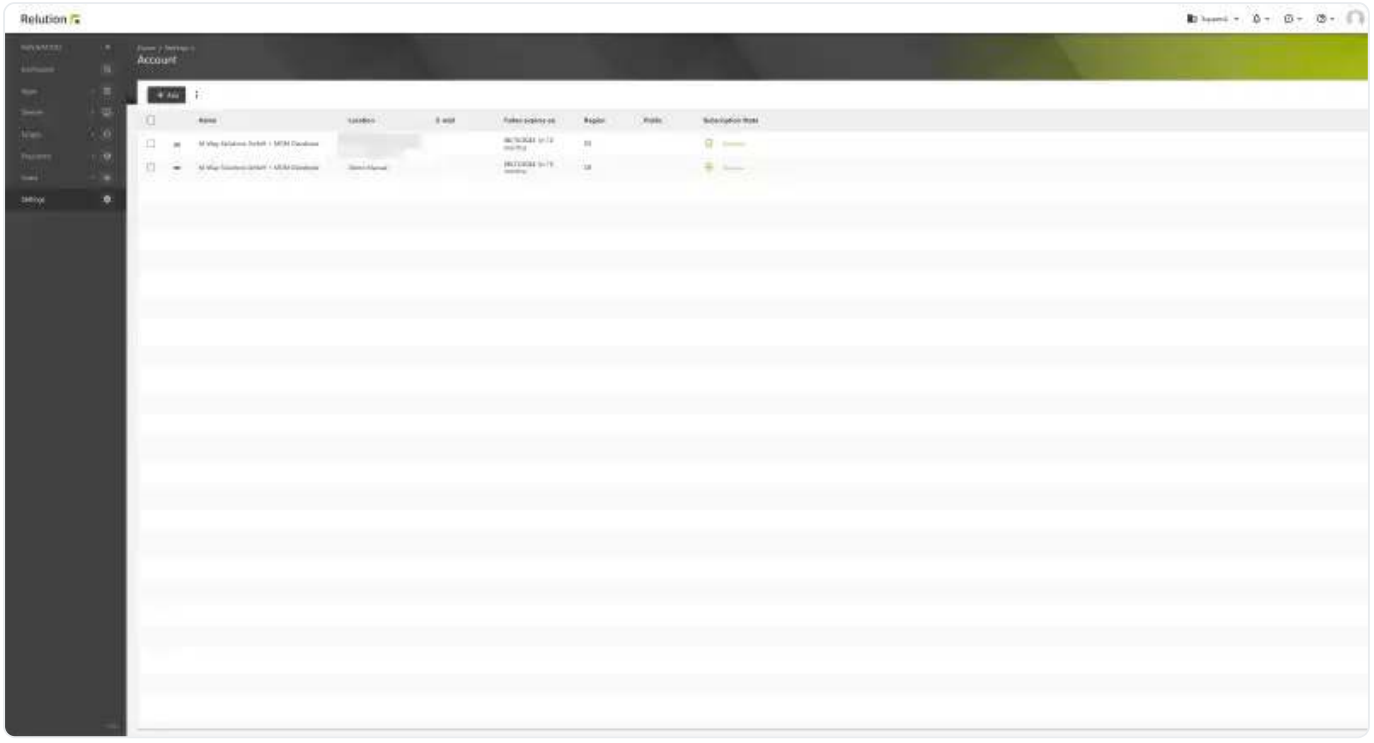
Si un site nécessite des applications payantes ou un jeton VPP supplémentaire avec ses propres applications, celui-ci peut être intégré directement dans le tenant concerné.

Cela permet une séparation claire des coûts et des licences entre la gestion globale et locale.

Pour la version 26.4.0

Les licences VPP dans Relution peuvent-elles aussi être automatiquement assignées à des appareils ?

Si des applications sont automatiquement installées sur des périphériques via des déploiements automatiques ou une politique (conformité des applications), Relution vérifie si une licence VPP est disponible pour cette application. Si c'est le cas, la licence VPP est automatiquement assignée à l'appareil. Pour les apps de l'App Store qui ne prennent en charge que macOS ou que tvOS, les licences VPP sont une condition préalable à un déploiement automatique : sans licences VPP disponibles dans l'organisation, aucun déploiement automatique ne peut être configuré pour ces apps. Pour les apps iOS, la licence VPP est facultative. Si plusieurs jetons VPP sont stockés pour l'organisation et que la licence de l'application est présente dans chacun d'entre eux, la licence VPP du premier jeton VPP de la liste est utilisée. Sous `Paramètres` → `Programme d'achat en volume (VPP)` → `Compte`, l'ordre des jetons VPP peut être modifié afin de déterminer de quel jeton la licence VPP est utilisée lors d'une attribution automatique via des déploiements automatiques.



L'installation par Relution des mises à jour disponibles des apps issues d'Apps et livres sur les appareils est définie sous `Paramètres` → `Programme d'achat en volume (VPP)` → `Les mises à jour` avec Mettre à jour les applications : Jamais, Immédiatement après la détection d'une mise à jour d'application ou Planifié. Pour une planification, les jours de la semaine et l'Heure de début sont indiqués.

Les erreurs fréquentes lors du téléversement des jetons, un aperçu des extensions de fichier et les raisons d’une perte de validité anticipée sont décrits sous Remarques importantes et dépannage →.

Pour la version 26.4.0

Renouveler les jetons DEP / VPP

Les jetons pour l'Inscription automatisée des appareils (ADE, DEP dans le portail) et pour Apps et livres (VPP dans le portail) ont une durée de validité maximale de 1 an et doivent être renouvelés régulièrement pour garantir la gestion des appareils et l'attribution des applications sans interruption. Ce guide explique comment renouveler facilement ces jetons.

Les jetons ADE et Apps et livres sont indépendants les uns des autres : chaque jeton expire un an après sa propre création. Seul le jeton dont l'expiration approche est donc renouvelé. Relution envoie des rappels par e-mail pour les jetons qui vont expirer ou qui ont expiré, une première fois 30 jours avant l'expiration, puis quotidiennement à partir de 15 jours avant l'expiration (voir Configurer le VPP →). Dans la liste des comptes DEP, la colonne Le jeton expire le signale un jeton par une icône d'avertissement à partir de 60 jours avant l'expiration et un jeton expiré par une icône rouge.

> Apple a renommé Apple Business Manager (ABM) en Apple Business en avril 2026.

De plus, à partir de la version 5.33, Relution offre la possibilité d'afficher tous les jetons DEP et VPP connectés dans un aperçu centralisé. Les administrateurs de l'organisation `Global` ou d'une méta-organisation peuvent ainsi voir en un coup d'œil :

Pour la version 26.4.0

- Quels jetons DEP et VPP sont valides ou expirés
- La date d'expiration de chaque jeton

Aperçu des jetons dans le portail Relution

Les deux types de jetons sont gérés à des endroits différents du portail.

Accéder aux comptes DEP

Pour accéder à l'aperçu central des comptes DEP, procéder comme suit :

1. Se connecter à l'organisation `Global` ou à une méta-organisation.
2. Ouvrir les Paramètres dans la barre latérale gauche.
3. Naviguer vers la section Spécifique à la plate-forme de l'appareil.
4. Sélectionner Inscription automatique des appareils Apple.
5. Ouvrir l'onglet Tous les comptes DEP (disponible à partir de la version 5.33.0).

Accéder aux comptes VPP

Pour accéder à l'aperçu des comptes VPP, procéder comme suit :

1. Se connecter à l'organisation `Global` ou à une méta-organisation.
2. Ouvrir les Paramètres dans la barre latérale gauche.
3. Naviguer vers la section Programme d'achat en volume (VPP).
4. Sélectionner Compte.
5. Ouvrir l'onglet Tous les comptes VPP (disponible à partir de la version 5.33.0).

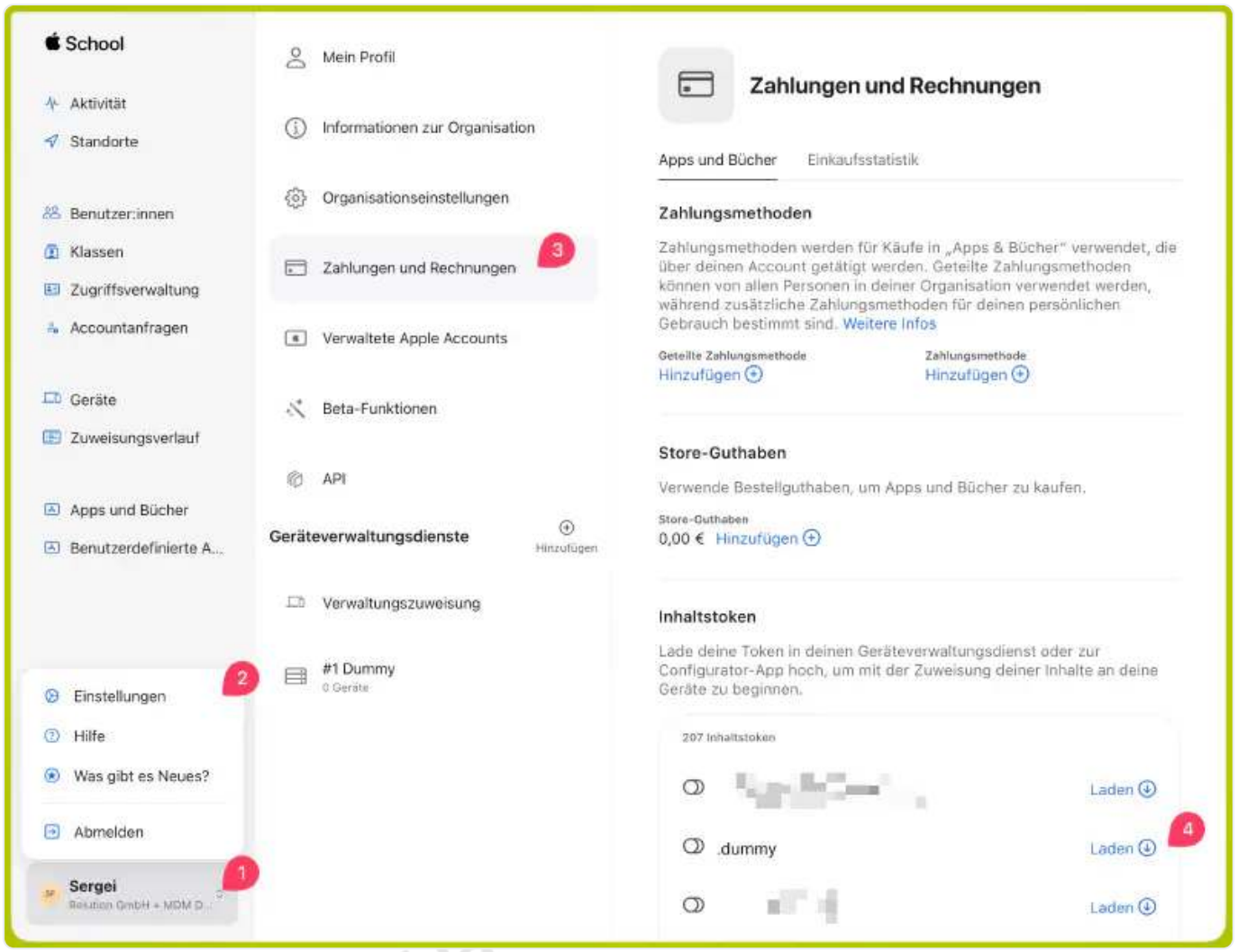
Renouveler les jetons VPP (Jetons de contenu)

Le jeton VPP est d'abord téléchargé chez Apple, puis importé dans Relution.

Téléchargement depuis Apple School Manager (ASM)

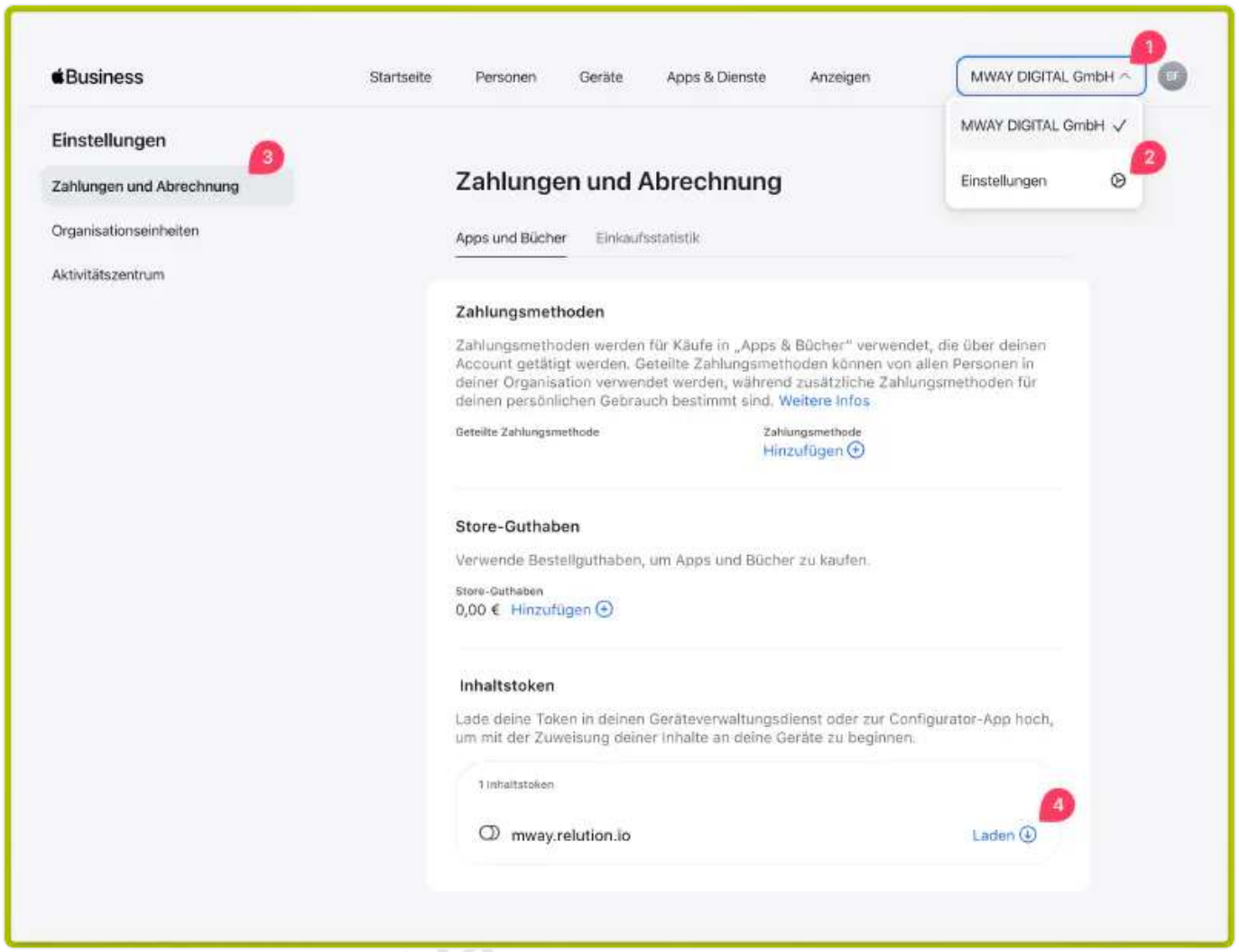
1. Se connecter à Apple School Manager →.
2. Cliquer sur le nom de l'utilisateur connecté en bas à gauche.
3. Ouvrir les Préférences.
4. Sélectionner Paiements et facturation.
5. Sous Jetons de contenu, cliquer sur Télécharger pour le jeton souhaité.
    - *Format du fichier :* `sToken_for_[Lieu].vpptoken`

Pour la version 26.4.0



Téléchargement depuis Apple Business (anciennement ABM)

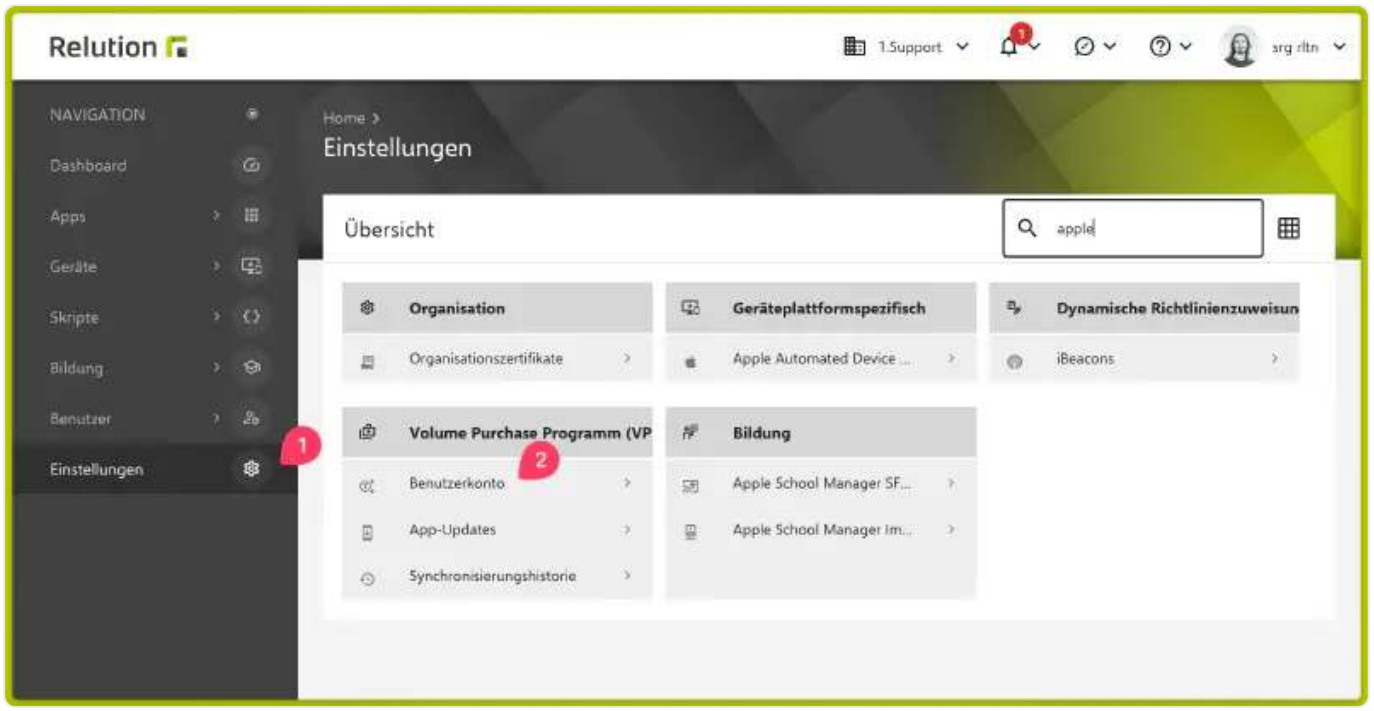
1. Se connecter à Apple Business →.
2. Cliquer sur le nom de l'organisation en haut à droite.
3. Ouvrir les Réglages.
4. Sélectionner Paiements et facturation.
5. Dans la section des jetons de contenu, cliquer sur Télécharger pour le jeton souhaité.
    - *Format du fichier :* `sToken_for_[Lieu].vpptoken`

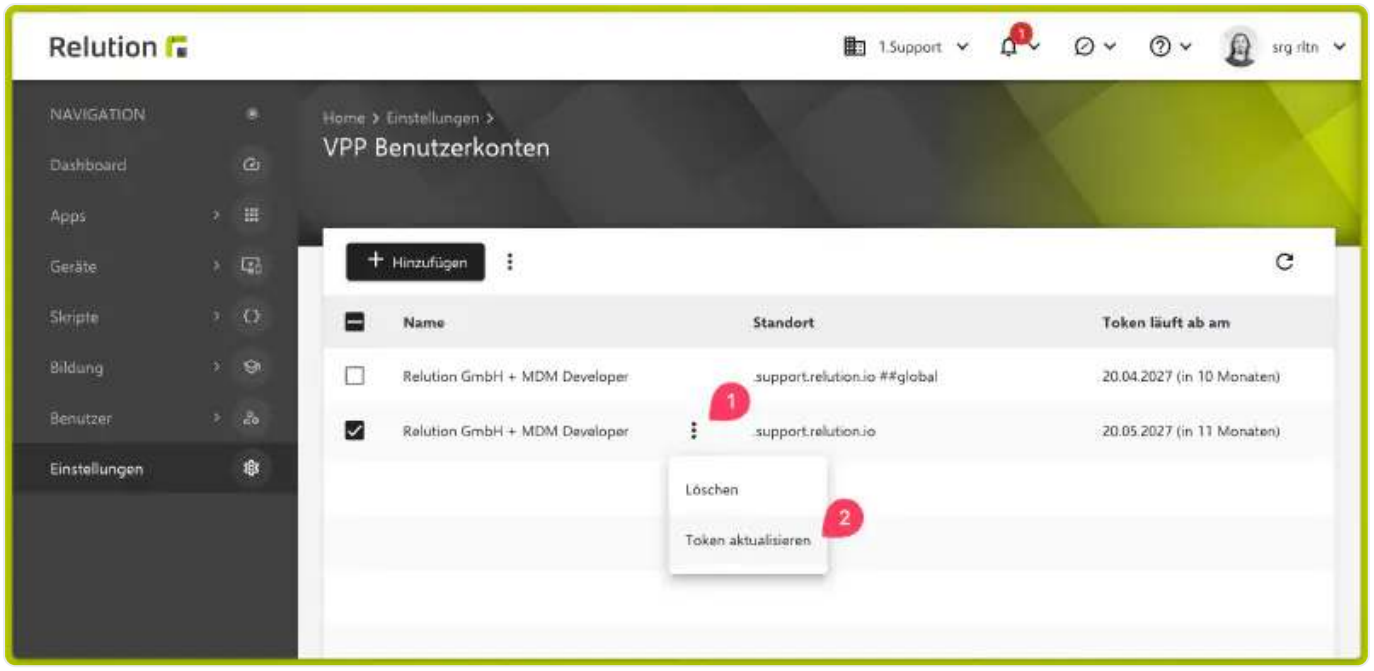


Pour la

Importation dans Relution

1. Se connecter au portail Relution et basculer vers l'organisation correspondante.
2. Ouvrir les Paramètres.
3. Naviguer vers Programme d'achat en volume (VPP) → Compte.
4. Sélectionner le jeton à renouveler via le menu à trois points.
5. Cliquer sur Mettre à jour le jeton.
6. Télécharger le fichier précédemment récupéré (`*.vpptoken`).
7. Finaliser l'opération en cliquant sur Mettre à jour le jeton.





Dans l'organisation `Global`, la boîte de dialogue signale que les applications issues de comptes VPP globaux remplacent les applications existantes dans d'autres organisations. Si le compte est déjà géré par un autre serveur MDM, un avis s'affiche également ; avec la mise à jour, Relution reprend la gestion.

Renouveler les jetons DEP (Jetons de serveur)

Apple chiffre le nouveau jeton avec la clé publique enregistrée dans ABM/ASM lors de la configuration initiale. Relution conserve le certificat correspondant pour chaque compte DEP ; la clé publique n'a donc pas besoin d'être téléversée à nouveau lors du renouvellement. Si le certificat est malgré tout nécessaire, il peut être enregistré via Télécharger le certificat dans la boîte de dialogue de téléversement du jeton (ouverte via Mettre à jour le jeton).

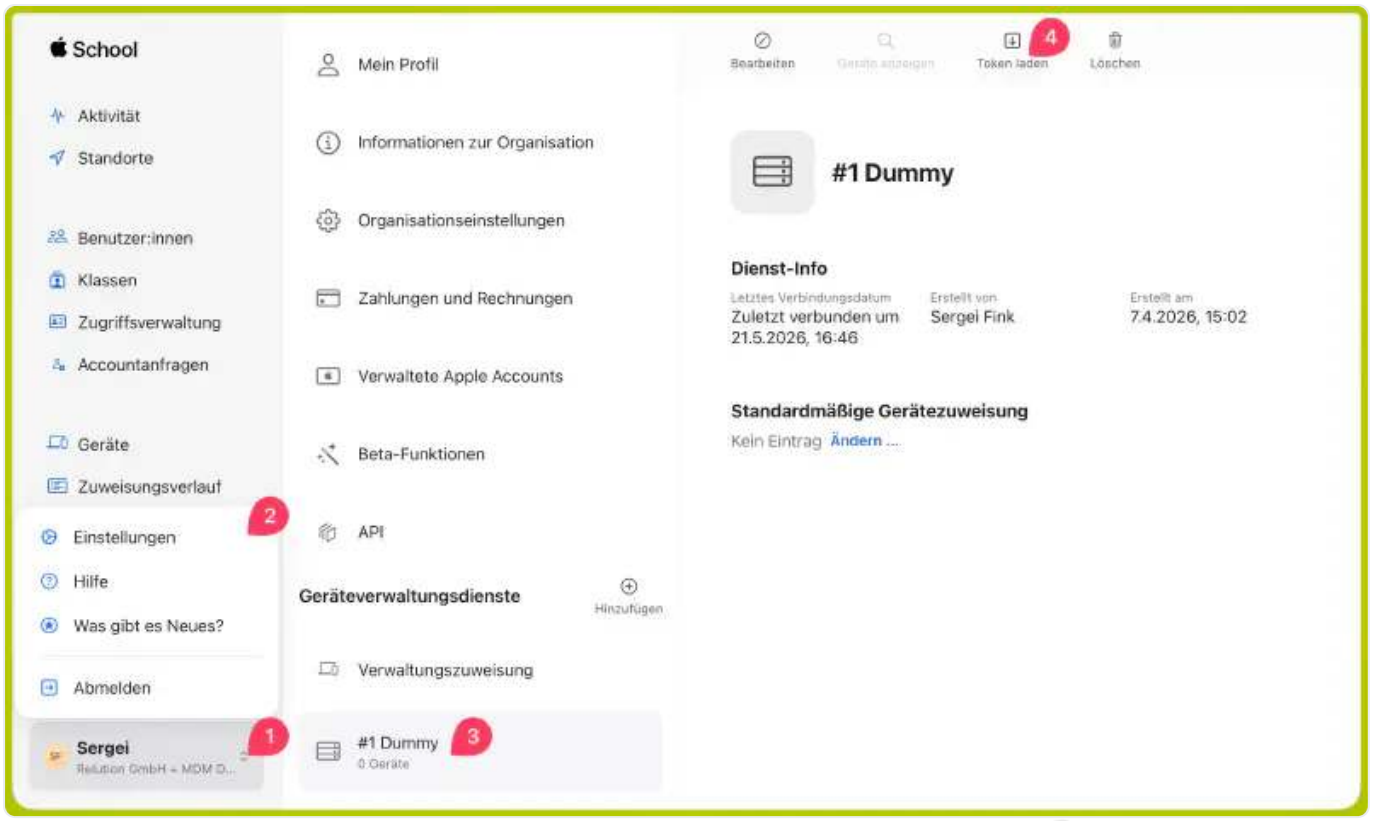
Téléchargement depuis Apple School Manager (ASM)

1. Se connecter à Apple School Manager →.
2. Cliquer sur le nom de l'utilisateur connecté en bas à gauche.
3. Ouvrir les Préférences.
4. Dans la liste des services de gestion des appareils, sélectionner le service de gestion des appareils connecté à Relution.
5. Télécharger le jeton.

   > Le téléchargement d'un nouveau jeton réinitialise le jeton existant.

   - *Format du fichier :* `*_smime.p7m`

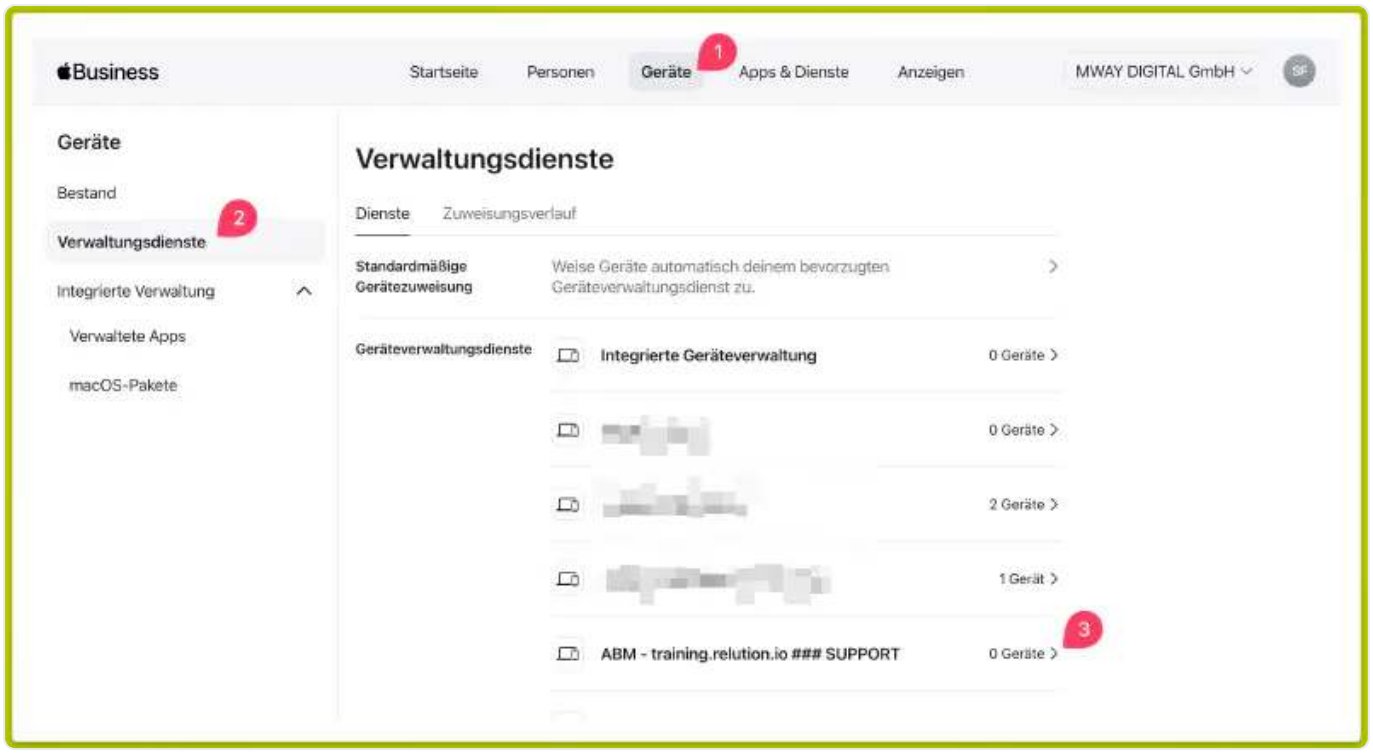
Pour la version 26.4.0

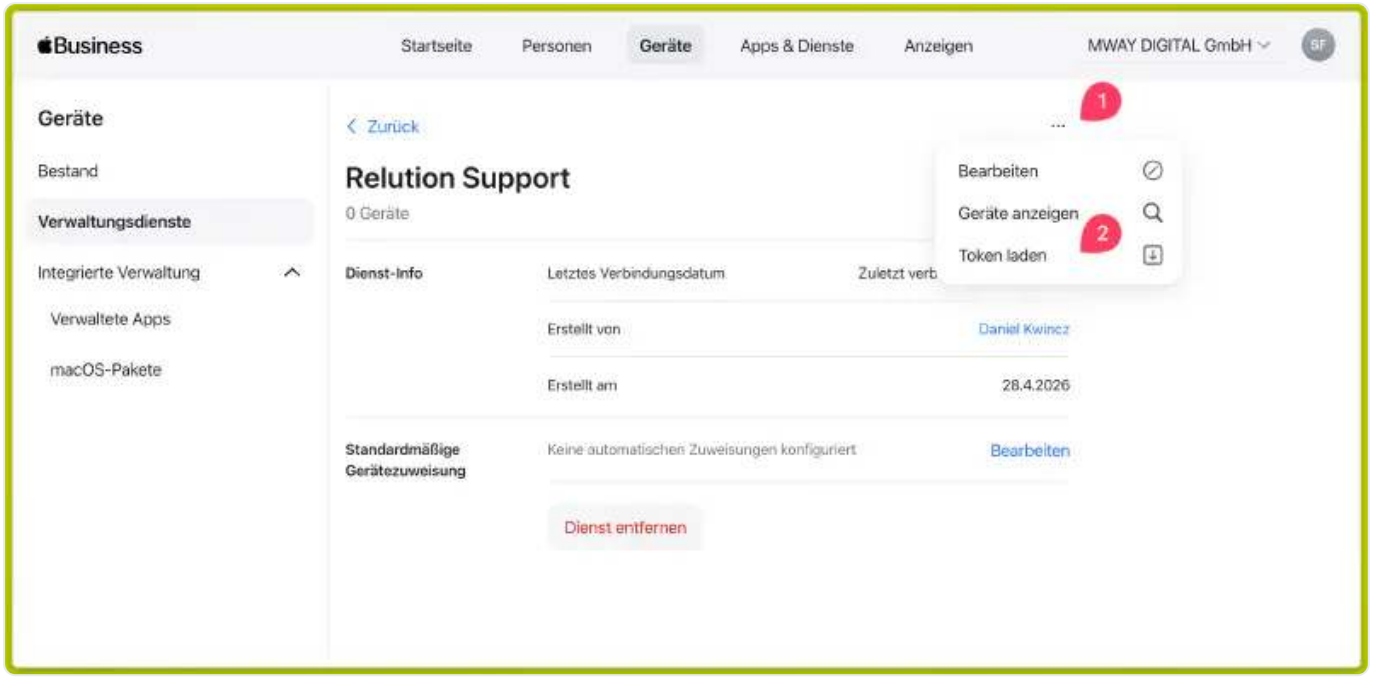


Pour la version 26.4.0

Téléchargement depuis Apple Business (anciennement ABM)

1. Se connecter à Apple Business →.
2. Cliquer sur Appareils en haut au centre.
3. Dans la barre latérale gauche, sélectionner Services de gestion.
4. Dans la liste des services de gestion des appareils, sélectionner le service souhaité.
5. Ouvrir le menu à trois points (⋯) en haut à droite et télécharger le jeton.
   - *Format du fichier :* `*_smime.p7m`

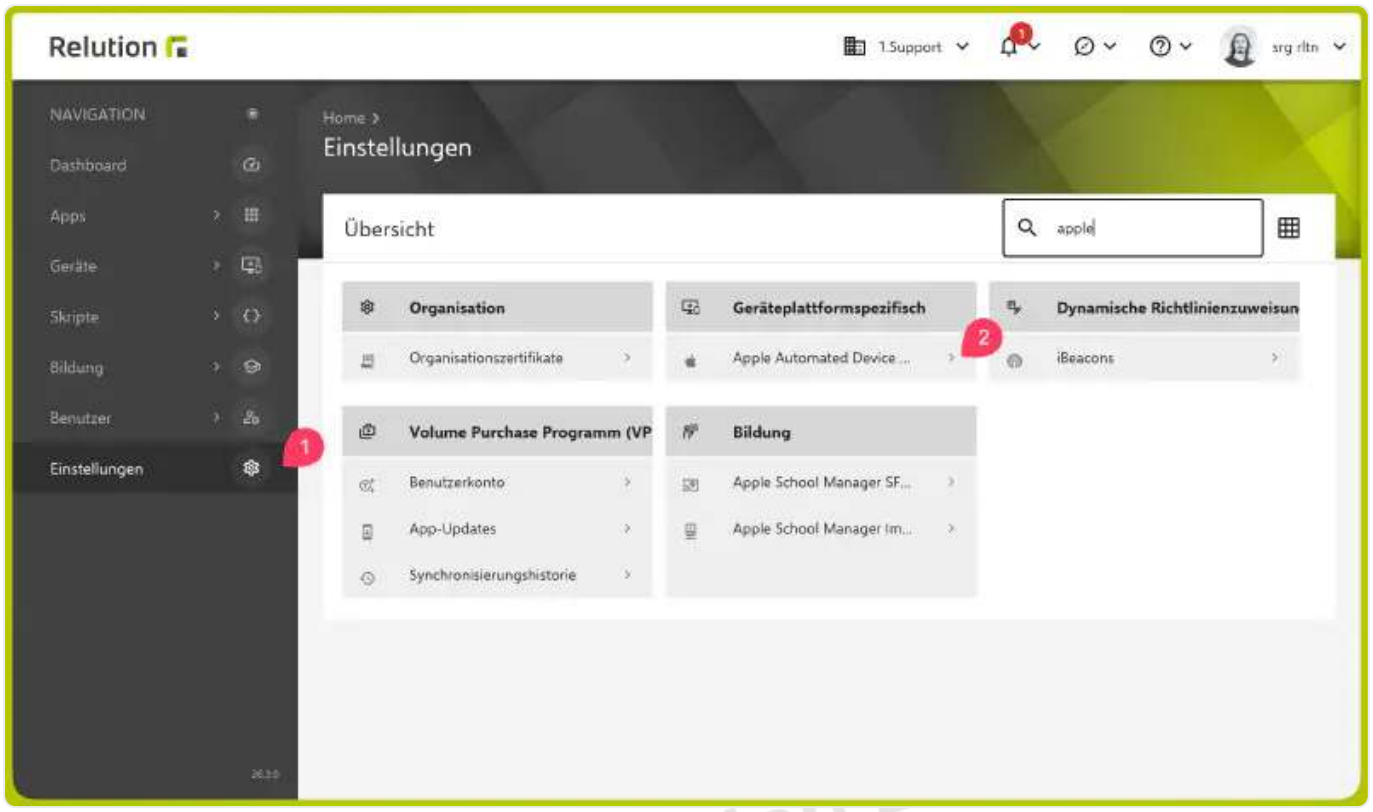


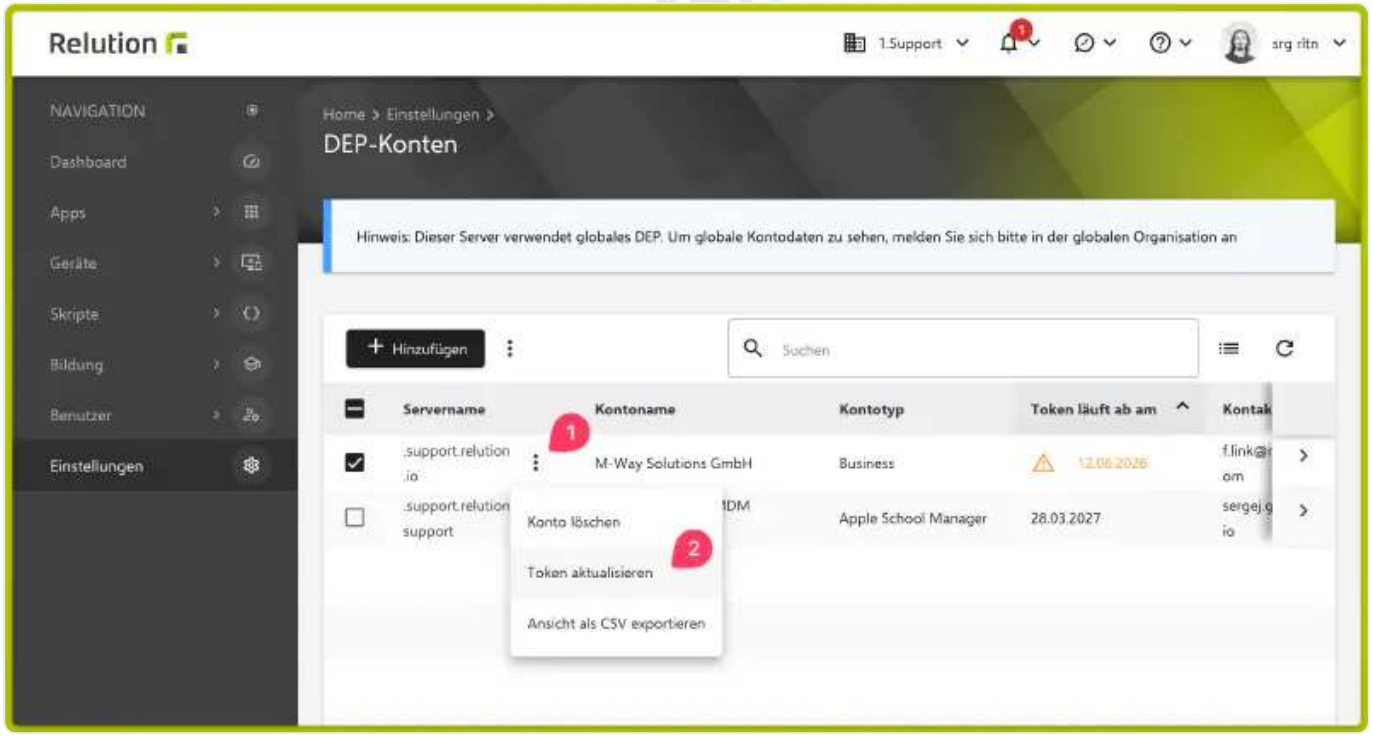


Importation dans Relution

1. Se connecter au portail Relution et basculer vers l’organisation correspondante.
2. Ouvrir les Paramètres.
3. Naviguer vers Spécifique à la plate-forme de l’appareil → Inscription automatique des appareils Apple.
4. Sélectionner le jeton souhaité via le menu à trois points.
5. Cliquer sur Mettre à jour le jeton.

6. Télécharger le fichier `*_smime.p7m` via Sélectionner.
7. Finaliser l'opération en cliquant sur Enregistrer.





Remarques importantes et dépannage

Les points suivants sont, d'expérience, les causes les plus fréquentes d'échec du renouvellement des jetons.

Erreurs fréquentes

En pratique, il arrive souvent que les jetons VPP (`.vpptoken`) et les jetons DEP (`.p7m`) soient confondus et téléchargés dans les mauvais menus. Dans le menu DEP, Relution refuse un fichier `.vpptoken` avec le message Données non valides fournies. Dans le menu VPP, un fichier `.p7m` n'est pas accepté : le fichier est rejeté sans message et le champ de téléversement reste vide. Si un fichier `.p7m` n'est pas un jeton DEP valide, Relution affiche La ressource n'est pas prise en charge ou la ressource est endommagée.

Si un jeton DEP appartient à un autre service de gestion des appareils que celui lié au compte DEP, Relution le refuse avec le message Le jeton téléchargé n'appartient pas au serveur MDM lié à ce compte DEP. Dans ce cas, le jeton est téléchargé depuis le bon service de gestion des appareils dans ABM/ASM.

Si le téléversement du jeton DEP échoue avec le message Erreur inconnue ou Le jeton n'est pas valide. Veuillez mettre à jour le jeton dans les paramètres, Apple a refusé la requête. Une cause possible est une heure du serveur non synchronisée ; elle est vérifiée et corrigée en premier. Si l'erreur persiste, le jeton n'est pas valide (par exemple parce qu'un nouveau jeton a entre-temps été généré pour le serveur MDM dans Apple Business Manager ou Apple School Manager). Dans ce cas, un nouveau jeton est téléchargé puis téléversé.

Pour la version 26.4.0

Aperçu des extensions de fichiers

Type de jeton	Usage	Extension de fichier
Jeton DEP	Inscription automatisée des appareils (ADE)	`*_smime.p7m`
Jeton VPP →	Licences d'applications et de livres (VPP)	`*.vpptoken`
Clé publique	Certificat de chiffrement fourni par Relution pour ABM/ASM	`*.pem` *(Requis uniquement lors de la configuration initiale)*

Invalidation prématurée du jeton

Un jeton peut devenir invalide avant sa date d’expiration normale d’un an. Les causes courantes sont :

- Changement de mot de passe : Le mot de passe du compte Apple géré (Identifiant Apple géré dans le portail) utilisé dans ABM/ASM a été modifié.
- Statut du compte : Le compte administrateur utilisé pour générer le jeton a été supprimé, désactivé ou ses droits ont été restreints.
- Nouvelles conditions générales Apple : Apple a publié de nouvelles conditions générales dans le portail ABM/ASM. La communication du jeton est alors temporairement bloquée jusqu’à ce qu’un administrateur principal accepte les nouvelles conditions sur le portail d’Apple.

Pour la version 26.4.0

Ajouter à DEP rétroactivement

Apple Configurator 2 est une application gratuite disponible sur le Mac App Store, utilisée pour la configuration manuelle des appareils Apple (connectés via USB) avant leur distribution aux utilisateurs. Elle permet de créer et d'installer des profils sur les appareils. De plus, Apple Configurator 2 permet l'ajout rétroactif d'appareils Apple au Device Enrollment Program (DEP) qui n'avaient pas déjà été assignés par un revendeur agréé.

Ce processus est exclusivement possible pour les appareils iOS, iPadOS et tvOS. Les appareils macOS doivent impérativement être achetés auprès d'un revendeur agréé pour bénéficier des avantages de l'inscription automatique au DEP. De manière générale, il est recommandé d'acquérir directement des appareils compatibles DEP, car l'ajout rétroactif implique plusieurs étapes manuelles.

Quelles sont les préparations nécessaires avant d'ajouter un appareil à DEP rétroactivement ?

Pour assurer une inscription DEP confortable et automatique, il est conseillé de créer au préalable un profil Wi-Fi. Ce profil peut être créé sur le Mac via le menu `Fichier` → `Nouveau profil` → `Wi-Fi` puis enregistré sous forme de fichier.

Pour la version 26.4.0

Comment ajouter des appareils Apple rétroactivement à l'aide d'Apple Configurator 2 ?

Connecter les appareils Apple à un Mac via un câble USB et lancer Apple Configurator 2. La boîte de dialogue suivante apparaîtra :

Faire un clic droit sur l'appareil affiché et sélectionner Préparer…. À l'étape suivante, choisir les options suivantes :

- Ajouter à Apple Business Manager (pour les entreprises) ou Apple School Manager (pour les établissements d'enseignement)
- Autoriser les appareils à se jumeler avec d'autres ordinateurs

Remarque : L'option Activer et terminer l'inscription ne doit PAS être sélectionnée, car cela entraînerait une tentative directe d'inscription de l'appareil. Après l'ajout à DEP, des

configurations supplémentaires sont encore nécessaires dans Apple Business Manager/Apple School Manager et Relution.

À l'étape suivante, sélectionner Nouveau serveur… et cliquer sur Suivant.

Maintenant, spécifier le nom et l'URL du serveur Relution correspondant. Le nom peut être choisi librement. L'URL commence par `https://`. Par exemple, pour le système de test Relution en conjonction avec les appareils iOS, c'est `https://live.relution.io/`.

Pour les appareils tvOS à gérer dans le système de test Relution, le chemin suivant doit être spécifié : `https://live.relution.io/api/enrollment/v1/appleMdm/depenroll`

Ensuite, sélectionner le certificat affiché. S'il y a plusieurs certificats, choisir le premier.

Le serveur est maintenant défini, enregistré dans Apple Configurator 2, et sera de nouveau disponible pour l'ajout ultérieur d'autres appareils au programme d'inscription des appareils.

Dans la boîte de dialogue suivante, sélectionner Nouvelle organisation… et confirmer avec Suivant.

L'étape suivante implique la connexion au serveur DEP d'Apple. Saisir l'identifiant Apple et le mot de passe du compte Apple Business Manager ou Apple School Manager respectif.

Si nécessaire, cette connexion doit être confirmée par une authentification à 2 facteurs (saisie d'un code à 4 chiffres envoyé par SMS).

Pour la version 26.4.0

Maintenant, sélectionner Créer une nouvelle identité de supervision et confirmer avec Suivant. Les données de l'organisation seront également enregistrées par Apple Configurator 2, afin de pouvoir être réutilisées ultérieurement, et une nouvelle organisation n'aura pas besoin d'être créée.

Ensuite, dans la boîte de dialogue suivante, sélectionner les étapes de configuration qui ne doivent PAS être ignorées pendant la configuration de l'appareil. L'option Services de localisation doit être choisie pour garantir une attribution correcte du fuseau horaire à l'appareil Apple.

À l'étape suivante, sélectionner un profil de configuration Wi-Fi créé précédemment dans Apple Configurator 2 via `Fichier` → `Nouveau profil`. Ce profil sera automatiquement adopté par l'appareil après le redémarrage, établissant ainsi une connexion Internet.

Cela permet à l'appareil Apple de transmettre l'inscription DEP rétroactive aux serveurs d'Apple. Alternativement au profil Wi-Fi, la connexion Internet du Mac peut également être partagée avec l'appareil connecté via la connexion USB.

Si aucun profil n'est sélectionné, les paramètres Wi-Fi devront être saisis manuellement lors du redémarrage des appareils. En cliquant sur Préparer, l'appareil redémarrera. Il s'inscrira

automatiquement à DEP, puis sera manuellement assigné au serveur MDM Relution correspondant dans Apple Business Manager ou Apple School Manager (par défaut, il est assigné à Apple Configurator 2).

Quelles configurations sont nécessaires dans Apple Business Manager ou Apple School Manager ?

Après l'ajout manuel d'appareils Apple à DEP, ceux-ci doivent être assignés au serveur MDM souhaité dans Apple Business Manager ou Apple School Manager. Alternativement, une option peut être configurée dans Apple Business Manager ou Apple School Manager pour assigner automatiquement les Nouveaux appareils à un serveur MDM défini. Toutes les options de configuration sont décrites dans la documentation en ligne d'Apple.

Une fois que les appareils Apple sont assignés à un serveur MDM dans Apple Business Manager ou Apple School Manager, ils peuvent ensuite être synchronisés dans l'organisation Relution correspondante sous `Appareils` → `Inscriptions automatiques`.

Comment l'inscription des nouveaux appareils DEP est-elle terminée ?

Pour la version 26.4.0

Une fois qu'un appareil Apple a été ajouté rétroactivement à DEP, assigné à un serveur MDM dans Apple Business Manager ou Apple School Manager, et qu'un profil DEP a été attribué à l'inscription automatique correspondante dans Relution, l'inscription automatique peut être effectuée sur l'appareil.

Si aucun profil DEP par défaut n'est configuré dans Relution ou si un profil DEP différent doit être utilisé, un profil DEP doit être attribué aux appareils nouvellement synchronisés. Pour plus de détails, consultez l'aperçu sur l'inscription automatique des appareils Apple DEP dans Relution.

Quelles sont les limites de l'utilisation de l'application Apple Configurator 2 ?

La préparation des appareils peut prendre plusieurs minutes. Si le processus en cours est interrompu ou arrêté, Apple Configurator 2 a besoin d'un certain temps pour terminer toutes les opérations en toute sécurité. Le Mac sur lequel Apple Configurator 2 est exécuté ne doit pas être éteint pendant la préparation de l'appareil, car cela pourrait endommager les appareils.

Les profils de configuration créés avec Apple Configurator 2 ne peuvent être installés sur les appareils Apple que via une connexion USB. La gestion à distance des appareils n'est donc pas possible rétroactivement. Pour de nombreux appareils, cela entraîne également un effort administratif manuel important. L'utilisation de Relution comme système MDM central peut réduire considérablement l'effort administratif.

Pour les appareils Apple ajoutés rétroactivement à DEP, il existe un délai de grâce de 30 jours concernant la suppression de l'inscription MDM sur l'appareil. Ce n'est qu'après l'expiration de cette période que l'option Supprimer la gestion sera supprimée des paramètres de l'appareil et ne pourra plus être effectuée manuellement par les utilisateurs.

Pour la version 26.4.0

Types d'inscription

Pour gérer les appareils iOS dans Relution, il faut d’abord les inscrire. Ce processus d’inscription peut être effectué de trois manières différentes. Les types d’inscription diffèrent et ont un effet durable sur les fonctions ultérieures.

Inscription manuelle

Cette inscription est réalisée en téléchargeant et en installant manuellement un profil MDM sur les appareils. Pour ce faire, il faut soit scanner un code QR sur les appareils, soit accéder manuellement à l’URL correspondante. Ensuite, le profil MDM doit être installé sur les appareils.

Avantages

- Cette inscription peut être effectuée sans avoir à réinitialiser les appareils aux paramètres d’usine.

Inconvénients

- L’inscription peut être supprimée à tout moment dans les paramètres des appareils (profil MDM).
- Ne convient que partiellement aux appareils BYOD, car les administrateurs peuvent voir quelles applications sont installées.
- Toutes les actions et configurations de politiques ne sont pas possibles.
- Les appareils ne sont souvent pas supervisés (mode supervisé).

Pour l’inscription manuelle →
Supervision →

Automatiquement via Apple DEP.

Les appareils iOS se connectent au serveur Apple au démarrage et, s’il s’agit d’appareils qui ont été enrôlés dans le DEP, sont automatiquement redirigés vers le serveur MDM et enrôlés. Ce processus peut être forcé afin que les utilisateurs ne puissent pas l’ignorer. De même, la fonction d’iPad partagé d’Apple peut être activée et le profil MDM sur les appareils peut être

Pour la version 26.4.0

protégé contre la suppression. Cela nécessite un accès avec les autorisations appropriées pour Apple School/Business Manager.

Avantages

- L’inscription est en grande partie automatique.
- Les appareils sont protégés contre le vol.
- L’enrôlement (profil MDM sur l’appareil) ne peut pas être supprimé.
- Les appareils sont en mode supervisé.
- L’iPad partagé d’Apple (Shared iPad) peut être activé.

Inconvénients

- Les appareils doivent être réinitialisés aux paramètres d’usine au préalable.

Pour l’enrôlement automatique →
Profil pour l’ADE →

Inscription via Apple User Enrollment.

Il s’agit de l’inscription typique pour les appareils Bring Your Own Device (BYOD). Les utilisateurs peuvent s’inscrire eux-mêmes et les appareils iOS n’ont pas besoin d’être réinitialisés aux valeurs d’usine.

Pour la version 26.4.0

Avantages

- Les administrateurs ne peuvent pas voir les applications installées de manière privée.
- Les appareils restent sous le contrôle de l’utilisateur.

Inconvénients

- Toutes les actions et configurations de politique ne sont pas possibles.
- Des identifiants Apple gérés sont nécessaires.

Aller à Apple User Enrollment for iOS →

Inscription des utilisateurs

L'enrôlement des utilisateurs permet d'enrôler des appareils iOS et macOS privés sans que leur propriétaire n'ait à renoncer à tout contrôle sur ces appareils. Sur la base de l'approche BYOD (Bring Your Own Device), les appareils privés des étudiants ou des employés peuvent être intégrés et utilisés dans le contexte de l'école ou de l'entreprise tout en maintenant la protection des données privées.

> Les appareils ne doivent pas être en mode surveillé ou supervisé pour l'inscription des utilisateurs Apple.

Deux variantes d'inscription sont disponibles : basée sur le compte et basée sur le profil (inscription manuelle conventionnelle).

> L'inscription de l'utilisateur basée sur le profil n'est plus prise en charge à partir de iOS 18.

Pour la version 26.4.0

Avantages

- Les administrateurs ne peuvent pas voir les applications installées de manière privée.
- Les appareils restent sous le contrôle des utilisateurs.

Inconvénients

- Toutes les actions et configurations de politique ne sont pas possibles.
- Des identifiants Apple gérés sont nécessaires.

Préparer l'inscription à Relution

À partir de l'organisation Relution, une inscription manuelle pour les appareils iOS ou macOS peut être créée classiquement et le lien d'inscription peut être envoyé aux étudiants ou employés souhaités.

La condition préalable à la création d'une inscription d'utilisateur est l'affectation d'utilisateurs. Pour cela, un "Managed Apple ID" ou une "adresse e-mail" doivent être enregistrés dans les détails de l'utilisateur. Ensuite, les utilisateurs correspondants peuvent être ajoutés et

l'inscription peut être complétée. Les utilisateurs affectés à des appareils ne peuvent plus être modifiés ou supprimés des appareils inscrits via l'inscription des utilisateurs.

Inscription d'utilisateurs basée sur l'utilisateur (seulement jusqu'à iOS 17)

Le lien d'inscription reçu effectuera l'inscription de l'appareil sur l'appareil iOS ou macOS en utilisant les Apple ID gérés des utilisateurs et l'appareil apparaîtra automatiquement dans l'inventaire des appareils de l'organisation Relution correspondante.

Inscription de l'utilisateur basée sur le compte

Relution prend en charge l'inscription des utilisateurs basée sur le compte pour les appareils iOS et macOS qui ne sont pas en mode supervisé.

Pour utiliser l'inscription des utilisateurs basée sur le compte, les éléments suivants sont nécessaires :

- Service Discovery Well-Known Hosts

Pour la version 26.4.0

Une découverte de service doit être configurée afin qu'Apple puisse transférer les appareils vers le bon serveur MDM. Pour ce faire, un fichier de ressources bien connues http doit être stocké sur le domaine que les utilisateurs utiliseront pour se connecter. Apple doit pouvoir récupérer ce fichier via un HTTP GET à l'URL suivante :

```
https://yourdomain.com/.well-known/com.apple.remotemanagement
```

Le domaine également utilisé pour les Apple ID doit être renseigné sous `votredomaine.com`.

Le fichier créé doit être stocké sur un domaine qui peut gérer les requêtes HTTP GET. Créer le fichier au format JSON avec un contenu de type application/json.

Pour entrer les informations correctes dans le fichier, il est possible de copier les informations requises directement à partir du portail Relution. Pour ce faire, ouvrir :

1. Paramètres
2. Gestion des appareils / Gestion des appareils

3. Enregistrement de l’utilisateur Apple basé sur un compte
4. Régler le curseur sur on
5. Copier le texte entre crochets et l’insérer dans le fichier.

> Important : pour que le fichier fonctionne correctement, il ne doit pas avoir d'extension.

Exemple : maxmustermann@musterhausen.de

Dans cet exemple, le domaine de l’ID serait `musterhausen.de` c’est donc là qu’il faut stocker la découverte des services.

L’option 2 facilite grandement l’enregistrement des appareils personnels dans Relution. Dès que les utilisateurs de Relution s’enregistrent sur des appareils privés via l’option “Connexion au compte professionnel ou scolaire…” dans `VPN & Gestion des appareils` des paramètres généraux, les inscriptions des utilisateurs sont automatiquement générées dans Relution. En utilisant l’Apple ID géré des utilisateurs respectifs, l’URL d’inscription de la solution MDM respective est automatiquement identifiée. Après s’être connecté avec les identifiants de connexion des utilisateurs de Relution, les appareils apparaissent automatiquement dans l’inventaire des appareils de l’organisation Relution correspondante après une authentification réussie.

Pour la version 26.4.0

Inscription manuelle

L'enrôlement s'effectue en téléchargeant et en installant manuellement un profil MDM sur les appareils iOS. Pour ce faire, il faut soit scanner un code QR sur les appareils, soit accéder manuellement à l'URL correspondante. Ensuite, le profil MDM doit être installé sur les appareils.

Avantages

- L'enrôlement peut être effectué sans avoir à réinitialiser les appareils aux paramètres d'usine.

Inconvénients

- L'inscription peut être supprimée à tout moment dans les paramètres des appareils (profil MDM).
- Ne convient que partiellement aux appareils BYOD, car les administrateurs peuvent voir quelles applications sont installées.
- Toutes les actions et configurations de politiques ne sont pas possibles.
- Les appareils ne sont souvent pas supervisés (mode supervisé).

Pour la version 26.4.0

Pour effectuer une inscription manuelle, il faut d'abord la créer dans Relution. Pour ce faire, passer à "Appareils > Enrôlements" dans le menu et cliquer ensuite sur "Ajouter".

Les inscriptions dépendent du système d'exploitation. Par conséquent, sélectionner soit `iOS, macOS ou tvOS` comme `Platform` et l'inscription `Device` comme `Type`. La `propriété` peut être choisie en fonction de cela.

Pour associer un `Utilisateur` à l'appareil à enrôler, le sélectionner. Les utilisateurs doivent avoir le rôle Device User pour cela.

Chaque enrôlement ne peut être utilisé qu'une seule fois, sauf si le commutateur pour l'inscription multiple est activé. Dans ce cas, de nouveaux appareils peuvent être inscrits via le lien d'inscription jusqu'à ce que la date de validité soit dépassée ou qu'il n'y ait plus de licences d'appareils disponibles dans Relution.

Sous `Politiques` et `Règles`, la même chose peut être liée à l'inscription. Si l'appareil est enrôlé, ces règles sont appliquées directement.

Une fois l'enrôlement enregistré et créé, il est ensuite possible de scanner le code QR créé sur l'appareil iOS, ou d'entrer l'URL manuellement dans le navigateur. Le profil MDM est téléchargé via le bouton `Enrollment` et doit être installé sur l'appareil à l'étape suivante dans les `Settings` sous `VPN and Device Management`.

Instructions pas à pas

1. Démarrer l'inscription en appuyant sur le bouton "Inscription".
2. Appuyer ensuite sur le bouton "Autoriser".
3. Fermer la fenêtre suivante.
4. Passer aux "Réglages".
5. Là, dans la section `Général`.
6. Appuyer sur `VPN and Device Management` tout en bas.
7. Sélectionner le profil MDM chargé.
8. Vérifier le profil MDM, appuyer sur `Installer` et confirmer la boîte de dialogue à nouveau en appuyant sur `Installer`.
9. Un message de sécurité s'affiche. Appuyer à nouveau sur `Install`.
10. Faire confiance à l'administration à distance.
11. En appuyant sur `Done`, le profil MDM est installé.

L'inscription est terminée. <L'agent Relution est maintenant installé sur l'appareil et une nouvelle entrée devrait apparaître dans l'inventaire de l'appareil sur le portail Relution.

Pour la version 26.4.0

Migrer des appareils Apple

Avec la sortie d'iOS 26, Apple propose désormais la migration d'appareils Apple gérés d'une solution de gestion des appareils mobiles (MDM) comme Jamf ou iServ vers Relution. L'objectif est de reprendre entièrement les appareils sans les réinitialiser, sans nouvel enregistrement manuel et sans perte des configurations, applications ou identifiants Apple gérés existants.

Conditions relatives à l'appareil

- Un iPhone, iPad ou Mac géré (profil MDM actif) via DEP par l'intermédiaire d'Apple Business Manager (ABM) ou d'Apple School Manager (ASM).
- L'appareil doit être en mode Supervisé (supervision complète).
- Version du système d'exploitation iOS/iPadOS 26+ ou macOS 26+.
- L'iPad ne doit pas être exploité en mode iPad partagé (Shared iPad) – la migration n'est pas disponible pour les iPad partagés ; ces appareils doivent être réinitialisés et réinscrits.
- L'appareil ne doit pas être en mode application unique (Single App Mode / mode kiosque) – ce mode doit être désactivé avant la migration, sinon la migration ne peut pas être effectuée.

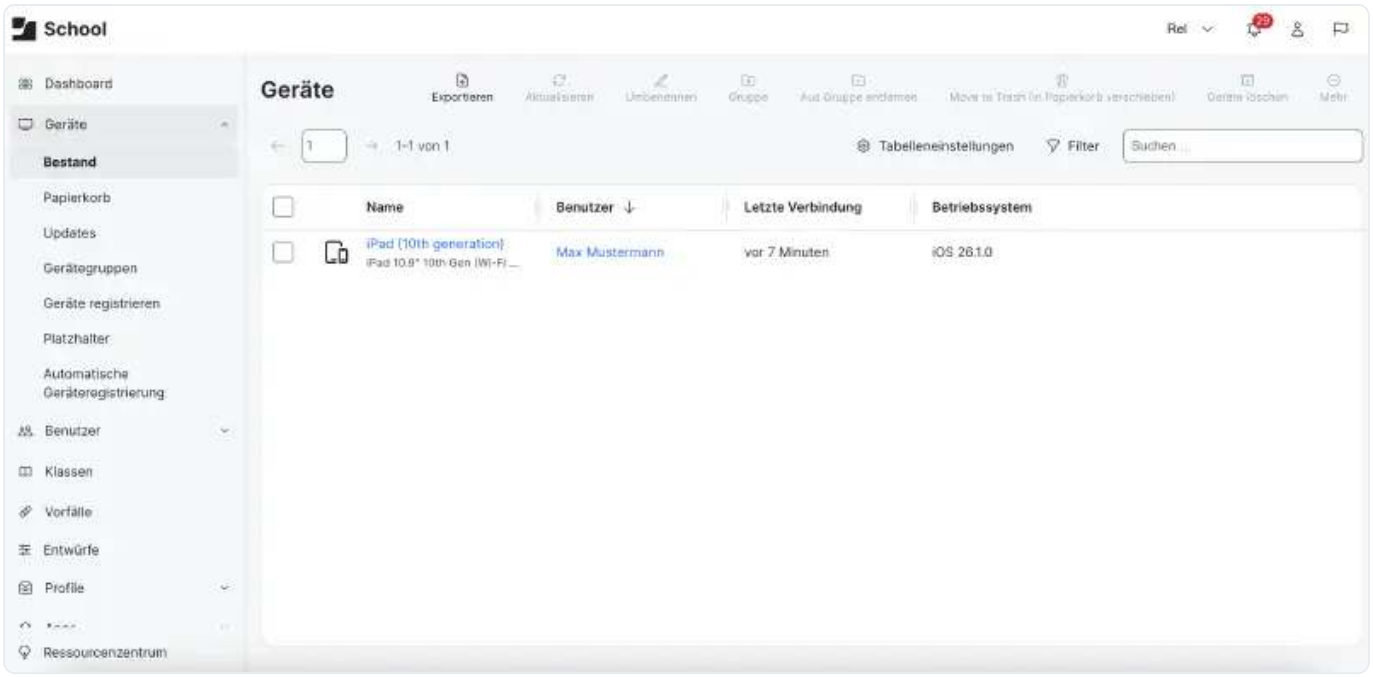
Pour la version 26.4.0

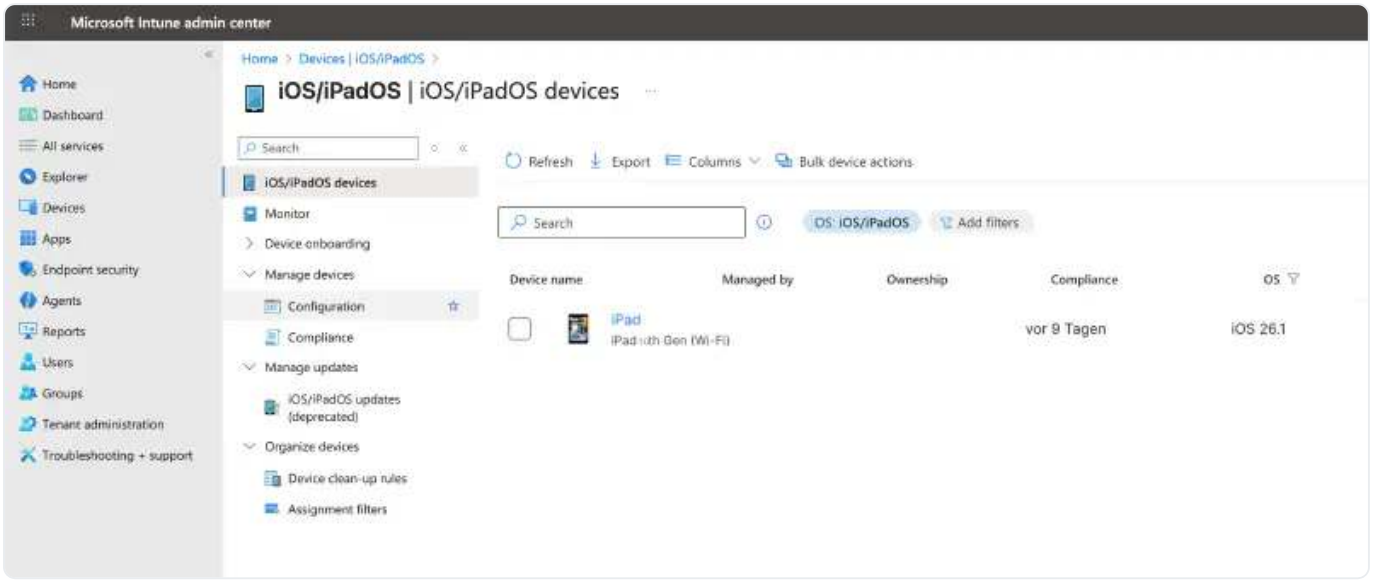
Conditions relatives au MDM

- La solution MDM tierce existante doit autoriser l'attribution d'appareils ou le transfert via ABM/ASM. Cette fonctionnalité est prise en charge dans Relution depuis la version `5.34`.
- Relution est enregistré comme serveur MDM dans ABM/ASM et est opérationnel.

Vérifier les appareils dans le MDM tiers

- Les appareils devant être migrés vers Relution doivent être visibles dans le MDM tiers, comme illustré dans les exemples suivants.
- Aucune configuration supplémentaire dans l'ancien MDM n'est nécessaire pour la migration des appareils vers Relution.



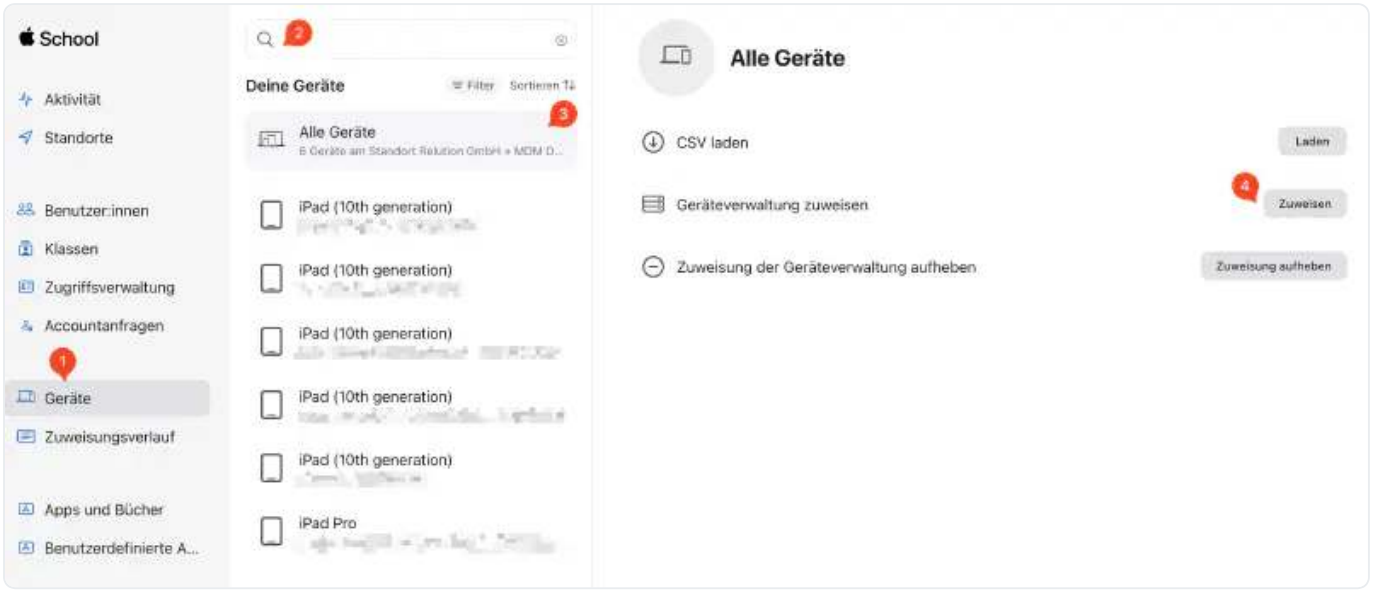


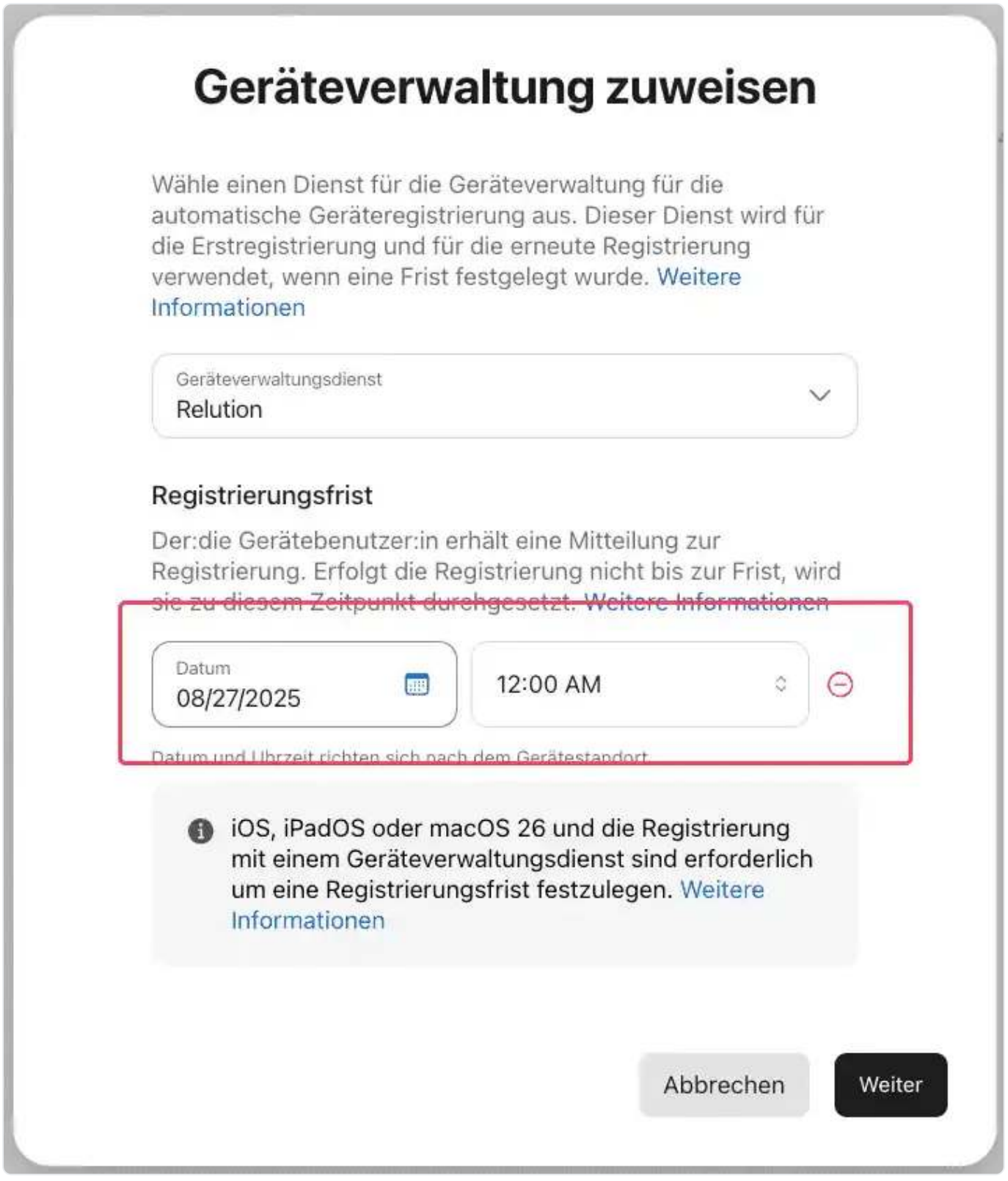
Préparation dans Relution

- Dans Relution, vérifier que les jetons DEP → et VPP → sont disponibles et valides.
- Créer ou identifier un groupe d’appareils devant contenir les appareils à migrer.
- Créer dans Relution toutes les configurations nécessaires (profils, certificats, applications).
- Pour éviter les erreurs de configuration, il est recommandé d’effectuer d’abord la migration avec des appareils de test.
- Adapter dans le profil DEP le réglage Installer et configurer les applications avant de continuer avec l’assistant de configuration. Sinon, aucun profil ne sera automatiquement attribué à l’appareil lors de l’inscription.

Attribution dans l’ABM/ASM

- Se connecter à Apple Business Manager ou à Apple School Manager.
- Accéder à `Appareils` → `Tous les appareils` et filtrer selon les numéros de série des appareils à migrer.
- Sélectionner les appareils → Attribuer la gestion des appareils.
- Dans la boîte de dialogue : sélectionner Relution comme nouveau serveur.
- Un délai de migration doit être défini ; l’utilisateur dispose ainsi de temps jusqu’à ce délai pour terminer la migration, après quoi il doit effectuer la migration pour continuer à utiliser l’appareil.
- Confirmer la modification – Apple marque désormais les appareils pour Relution.



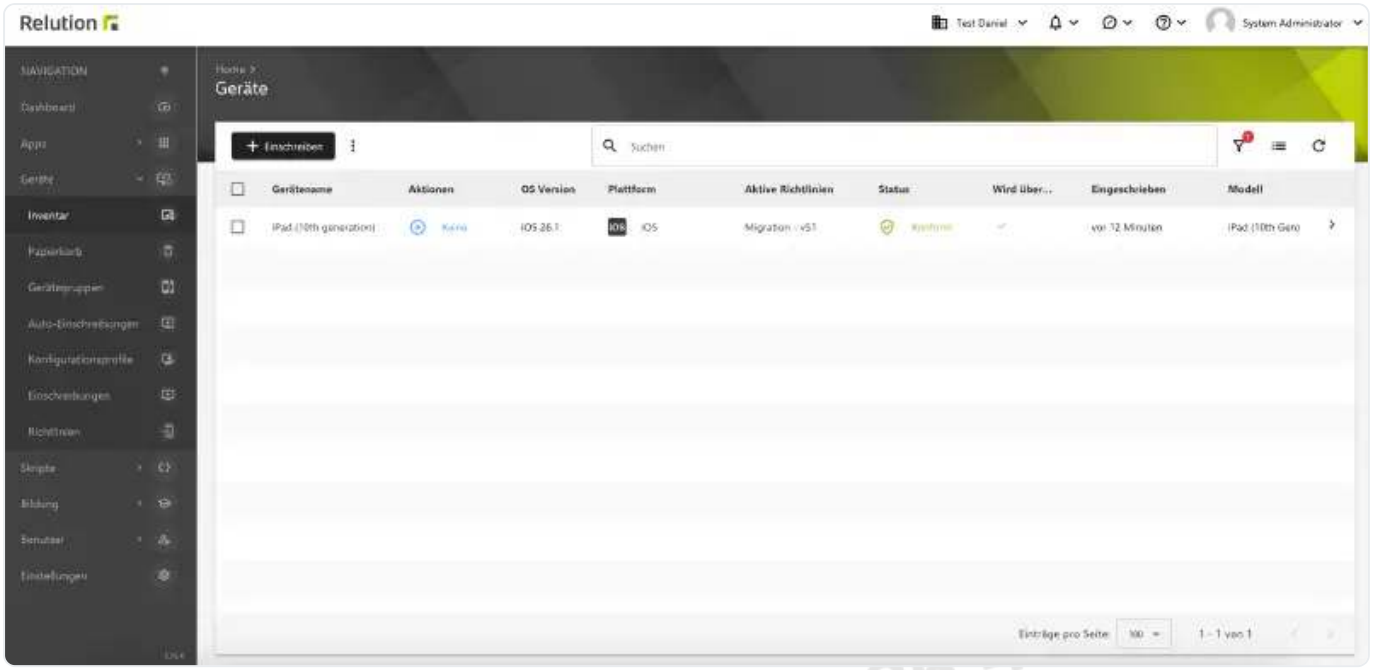


Migration sur l’appareil

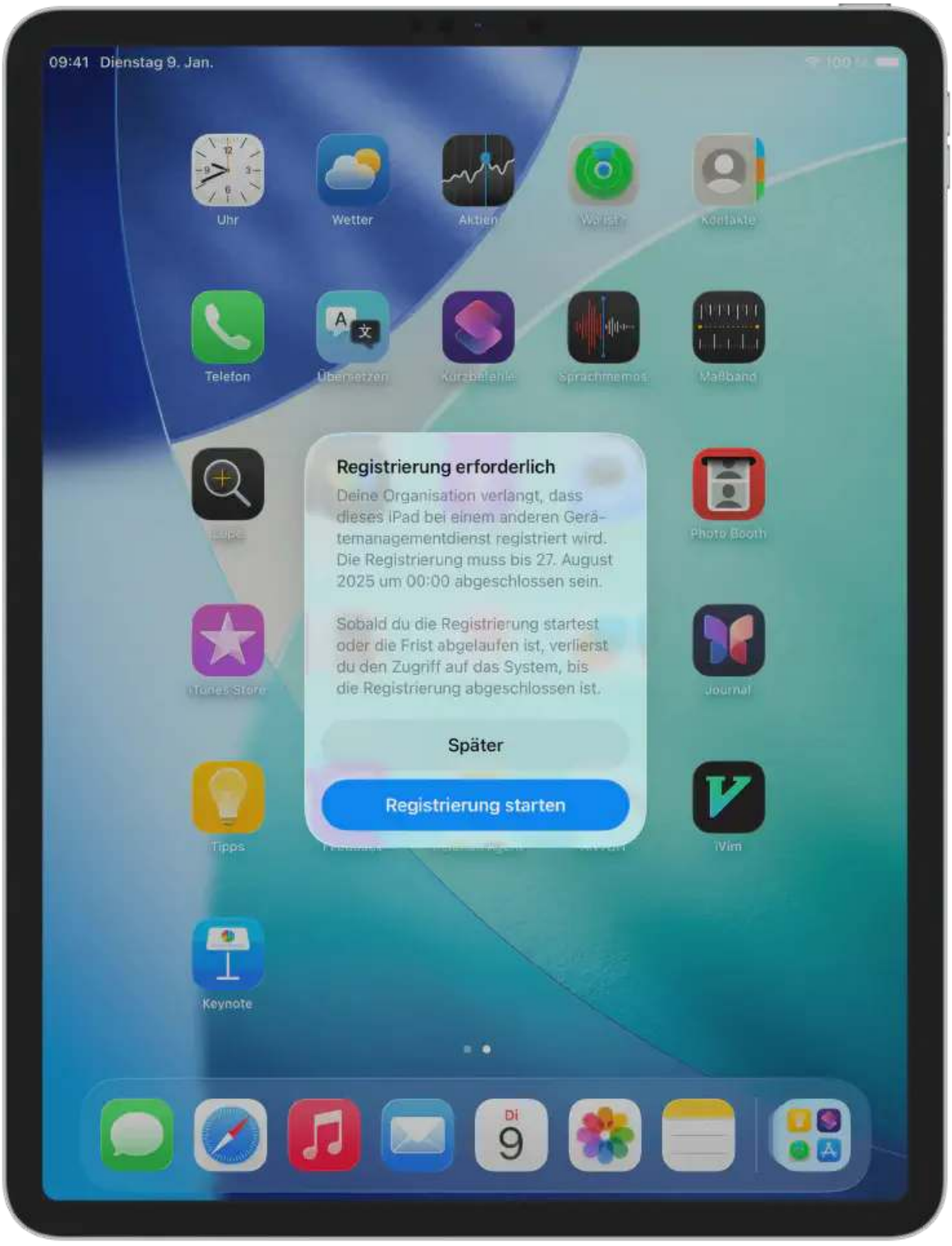
- Pour une migration directe, il est possible de démarrer la migration sur l’appareil via `Réglages` → `Général` → `VPN et gestion de l'appareil` en cliquant sur Démarrer

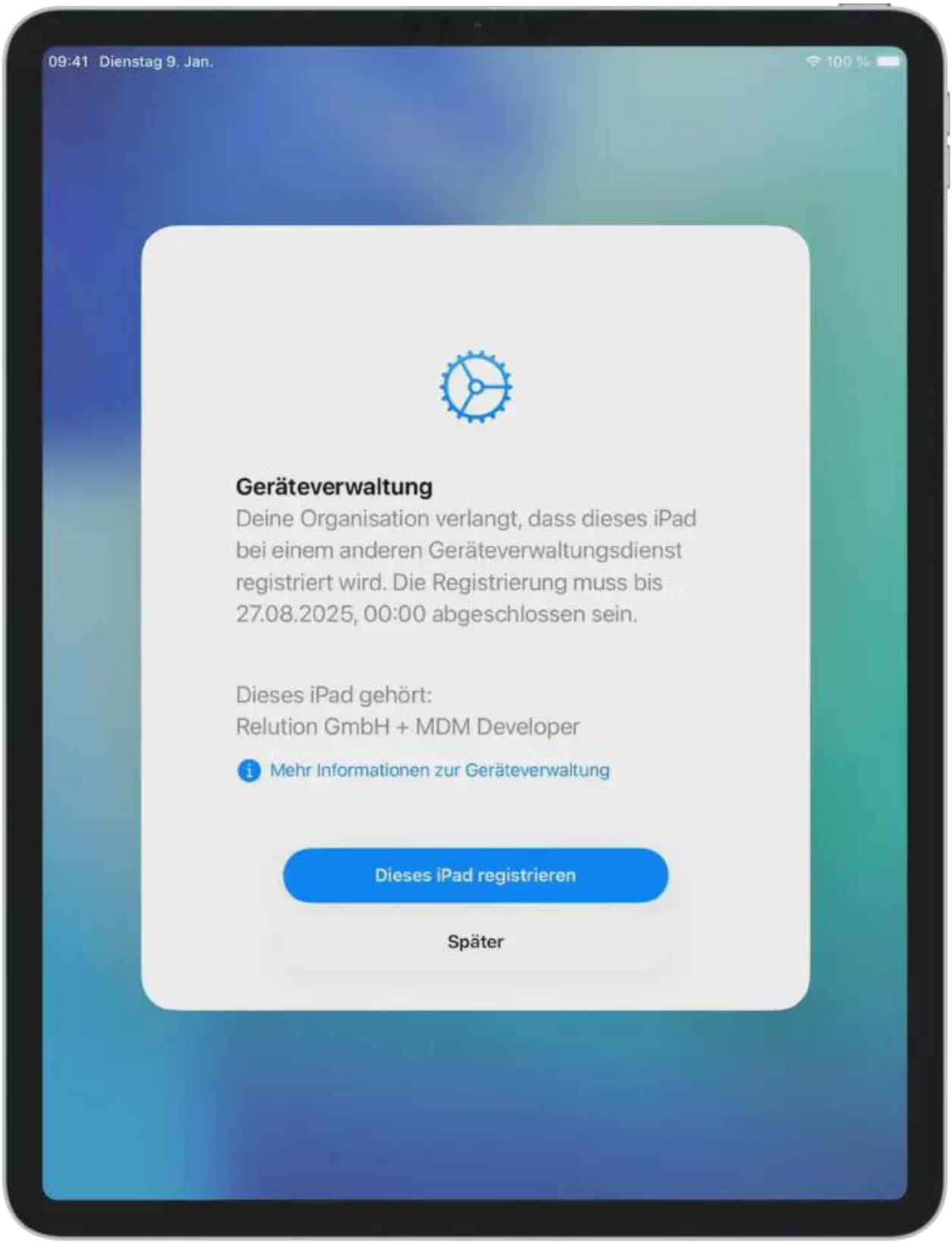
l'inscription.

- Lorsque la procédure est lancée, l'appareil est retiré de l'ancien MDM et ajouté à Relution, sans réinitialisation aux réglages d'usine.
- Une fois terminé, l'appareil apparaît comme géré dans Relution.



Pour la version 26.4.0


09:41 Dienstag 9. Jan.
Uhr
Wetter
Aktien
Telefon
Übersetzen
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

Limites et remarques

- Les appareils qui ne sont pas supervisés via DEP et ne sont pas gérés dans l’ABM/ASM doivent être réinscrits.
- Pour que la migration fonctionne sous iOS 26, un délai doit être défini dans l’ASM/ABM. Si l’option est grisée, la migration n’est pas disponible.
- L’option de migration dans l’ASM/ABM peut n’apparaître que jusqu’à deux jours après la mise à jour vers iOS 26.

Pour la version 26.4.0

Enregistrer un appareil non supervisé comme supervisé

Un appareil iOS non supervisé peut être rétrospectivement enregistré dans Apple DEP sans que les utilisateurs ne perdent leurs données. Selon la documentation Apple, la restauration d'une sauvegarde sur le même appareil réapplique le statut de gestion à partir de la sauvegarde — un appareil non supervisé ne peut donc pas passer directement de sa propre sauvegarde à l'état supervisé DEP. La solution de contournement suivante achemine la sauvegarde via un second appareil temporaire : la restauration sur un autre appareil applique les paramètres de gestion d'Apple School / Business Manager.

Apple décrit ce comportement comme suit :

- La restauration à partir d'une sauvegarde sur le même iPhone ou iPad restaure le statut de gestion à partir de la sauvegarde.
- La restauration à partir d'une sauvegarde sur un autre iPhone ou iPad applique le statut de gestion d'Apple School / Business Manager.

Pour la version 26.4.0

Exemple

Si un appareil est configuré pour être supervisé et inscrit automatiquement dans l'accès MDM, mais qu'il est restauré à partir d'une sauvegarde créée lorsqu'il n'était pas supervisé, l'appareil devient non supervisé. Un appareil non supervisé ne peut pas être directement restauré à partir de sa propre sauvegarde si le mode supervisé et l'inscription DEP sont souhaités — c'est pourquoi un passage par un second appareil est nécessaire.

Préparer le profil de récupération DEP

Créer un profil DEP temporaire dans Relution pour cette procédure avec les paramètres suivants :

- Activer `Autoriser l'association avec des Macs ou PC et la configuration via Apple Configurator`.
- Ne pas ignorer l'étape de configuration `Autoriser la localisation de l'appareil`.
- Ne pas ignorer l'étape de configuration `Restaurer à partir d'une sauvegarde`.
- Ne pas ignorer l'étape de configuration `Se connecter avec un identifiant Apple`.

En savoir plus sur la configuration d'un profil DEP dans Relution : Profil pour l'ADE →

Procédure

L'Appareil-01 et l'Appareil-02 doivent utiliser exactement la même version du système d'exploitation. Il faut également s'assurer que `Localiser mon iPhone` est désactivé sur les deux appareils, car une recherche d'appareil active peut empêcher la création ou la restauration d'une sauvegarde.

1. Sauvegarde

Créer une sauvegarde de l'Appareil-01 non supervisé via iCloud ou localement sur un Mac ou un PC. Restaurer cette sauvegarde sur un second appareil, Appareil-02. Créer ensuite une nouvelle sauvegarde de l'Appareil-02 — cette seconde sauvegarde sera ultérieurement restaurée sur l'Appareil-01 et considérée comme provenant d'un "autre appareil".

2. Préparation

Réinitialiser l'Appareil-01 aux paramètres d'usine. Ajouter l'Appareil-01 à Apple School / Business Manager via Apple Configurator 2. En savoir plus dans Ajouter des appareils Apple à DEP rétrospectivement →. Attribuer le profil de récupération DEP temporaire à l'Appareil-01.

Pour la version 26.4.0

3. Intégration dans Relution

Attribuer l'Appareil-01 via Apple School / Business Manager au serveur Relution correspondant avec le profil de récupération DEP temporaire. Configurer l'appareil en suivant l'assistant de configuration.

4. Restaurer la sauvegarde

Sur l'Appareil-01 dans l'assistant de configuration, sélectionner `Restaurer les applications et les données` et choisir la sauvegarde créée à partir de l'Appareil-02. Pour les sauvegardes iCloud, utiliser le même identifiant Apple.

Comme la sauvegarde provient de l'Appareil-02, la restauration compte comme une restauration sur un autre appareil : les paramètres de gestion sont issus du profil DEP configuré dans Relution — l'Appareil-01 devient ainsi supervisé et inscrit au DEP.

Après une restauration réussie, revenir au profil DEP par défaut.

Désinscrire des appareils

La désinscription met fin à la gestion d'un appareil par Relution. La désinscription s'effectue en supprimant l'appareil : l'action Supprimer est disponible dans l'inventaire des appareils ainsi que dans les détails de l'appareil. Après confirmation de la suppression, le profil MDM — y compris toutes les configurations, tous les certificats et toutes les applications gérées distribués via Relution — est retiré de l'appareil et l'appareil est supprimé de l'inventaire. L'appareil lui-même n'est pas réinitialisé ; les données personnelles restent sur l'appareil.

La désinscription est consignée dans le journal d'audit ; une nouvelle inscription de l'appareil est possible à tout moment. Cela s'applique aux appareils inscrits via l'Inscription manuelle → ou l'Inscription des utilisateurs →.

Appareils inscrits via Automated Device Enrollment (DEP)

La suppression d'un appareil dans Relution ne le retire pas de l'Apple School Manager ni de l'Apple Business Manager. Si un appareil doit quitter définitivement l'organisation — par exemple pour un usage privé ultérieur —, il doit en outre être retiré de l'Apple DEP. La procédure complète est décrite sous Supprimer des appareils →.

Pour la version 26.4.0

Corbeille

Les appareils supprimés sont d'abord déplacés dans la corbeille de l'inventaire des appareils. Ce n'est qu'en supprimant à nouveau un appareil depuis la corbeille qu'il est définitivement retiré de Relution.

Mode supervisé / Supervision

Le `Mode supervisé`, également appelé `Supervision`, est une stratégie de déploiement introduite par Apple pour que les organisations puissent gérer les appareils iOS, macOS et tvOS. Depuis son introduction avec iOS 5, `Supervision` a été mis à la disposition des organisations en tant que méthode efficace de gestion des appareils Apple. La supervision signifie qu'une organisation possède et contrôle entièrement les appareils. Les utilisateurs finaux peuvent accéder aux appareils supervisés et les utiliser, mais l'organisation dispose d'un contrôle administratif total. Ainsi, le propriétaire peut décider quelles fonctions peuvent être utilisées sur les appareils en appliquant des restrictions avancées ou en ajustant les paramètres de l'appareil via le système MDM.

Relution prend en charge le type d'inscription via Apple DEP pour mettre les appareils en "mode surveillé".

Enrôlement automatique →

Mettre les appareils en mode supervisé / Mode supervisé

Pour la version 26.4.0

Pour pouvoir accéder à toutes les fonctions des appareils Apple via un système MDM, ceux-ci doivent être surveillés ou supervisés. Cet état est obtenu en inscrivant les appareils dans le programme d'inscription des appareils Apple (DEP). Pour ce faire, il est nécessaire d'ajouter les appareils à l'Apple School/Business Manager. Si les appareils sont déjà inscrits, il est possible de continuer directement à la section suivante.

Inscription automatique →

Ajouter des appareils iOS et tvOS à Apple School / Business Manager

Un Mac et le logiciel Apple Configurator 2 sont nécessaires.

Apple Configurator 2 est une application gratuite disponible sur le Mac App Store. L'application peut être utilisée pour configurer manuellement les appareils Apple connectés par USB à un ordinateur Mac avant que les appareils ne soient distribués aux utilisateurs. Pour ce faire, des profils peuvent être créés et appliqués aux appareils. En outre, `Apple Configurator 2` permet d'ajouter ultérieurement au DEP des appareils Apple qui n'ont pas encore été ajoutés au DEP par

un revendeur agréé. Cette option n’est disponible que pour les iPhones, les iPads et les Apple TV. Les appareils macOS doivent être achetés auprès d’un revendeur agréé pour bénéficier de l’inscription automatique via Apple DEP. D’une manière générale, il est recommandé d’acheter directement les appareils DEP, car leur ajout a posteriori implique un effort manuel.

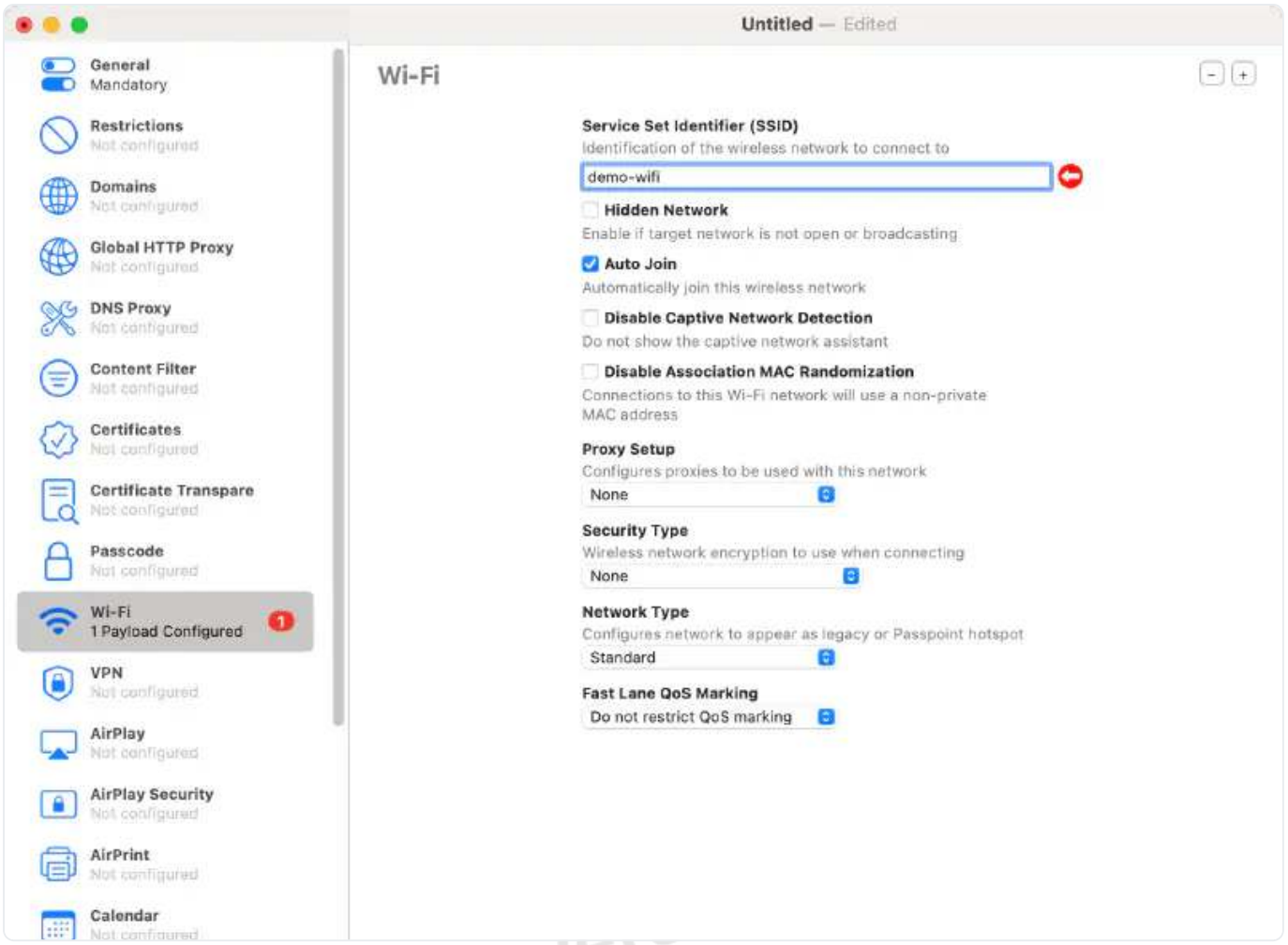
Les appareils Apple qui sont ensuite inscrits via `Apple Configurator 2` dans Apple School/Business Manager ne fonctionneront pas pendant les 30 premiers jours après le provisionnement comme des appareils inscrits directement dans DEP lorsqu’ils ont été achetés auprès d’un revendeur agréé. Même si la suppression manuelle de la gestion MDM sur les appareils a été bloquée via le profil DEP associé dans le système MDM, les utilisateurs peuvent supprimer la gestion MDM sous `Préférences` > Général > `Profils`.

A l’expiration de la période de 30 jours à compter de l’enregistrement, l’utilisateur ne pourra plus supprimer la gestion MDM sur les appareils.

Préparation

Pour que les appareils Apple se connectent automatiquement à Internet et que l’enregistrement ultérieur à DEP soit le plus pratique possible, il est recommandé de créer un `profil Wi-Fi` à l’avance. Ce profil peut être créé sur un Mac via l’option de menu `File` → `New Profile` → `WiFi` et ensuite sauvegardé en tant que fichier.

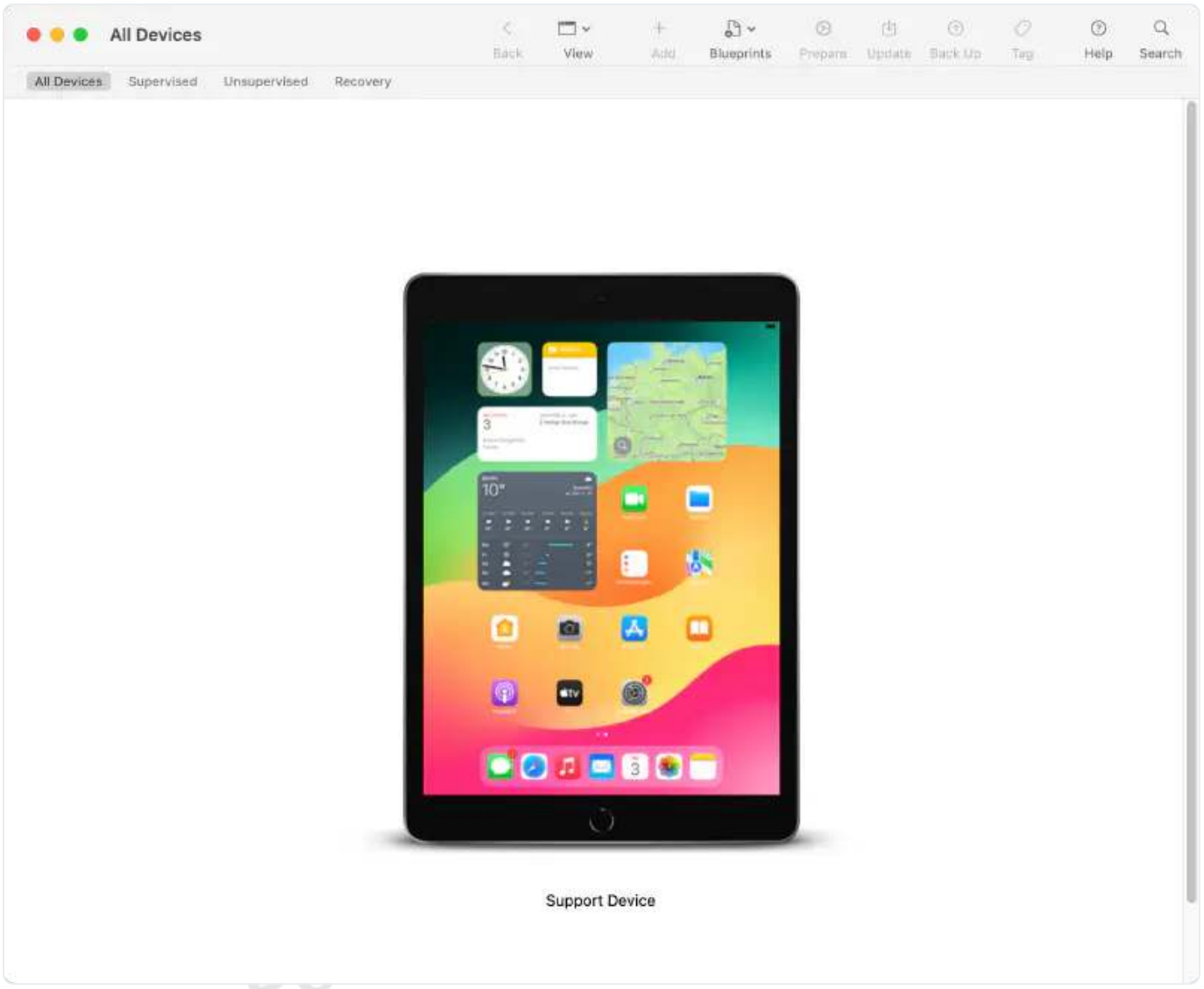
Pour la version 26.4.0



Pour la ver

Ajouter des appareils à DEP

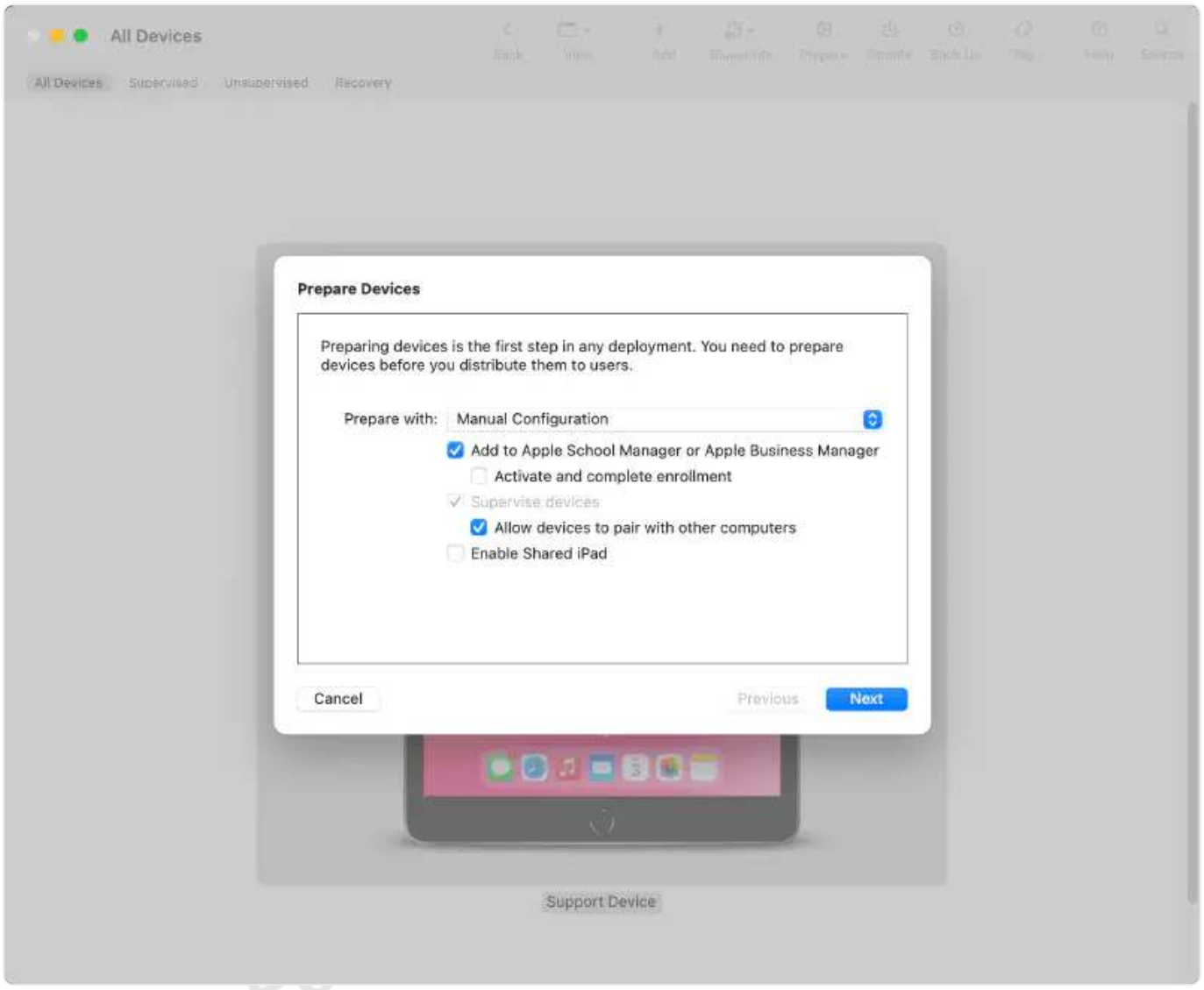
Les appareils Apple doivent être connectés avec un câble USB à un ordinateur Mac, sur lequel le `Apple Configurator 2` est ensuite lancé. La boîte de dialogue suivante apparaît :



Sélectionner l’appareil affiché avec le bouton droit de la souris et cliquer sur `Prepare...`. Dans l’étape suivante, les options suivantes doivent être sélectionnées :

- Ajouter à Apple School Manager ou Apple Business Manager (éducation/entreprise).
- Autoriser les appareils à s’associer à d’autres ordinateurs.

> L'option d'activation et d'inscription complète ne doit pas être sélectionnée, sinon l'appareil essaiera directement de s'inscrire. Toutefois, cela nécessite une configuration supplémentaire dans Apple School/Business Manager et Relution après l'ajout au DEP.

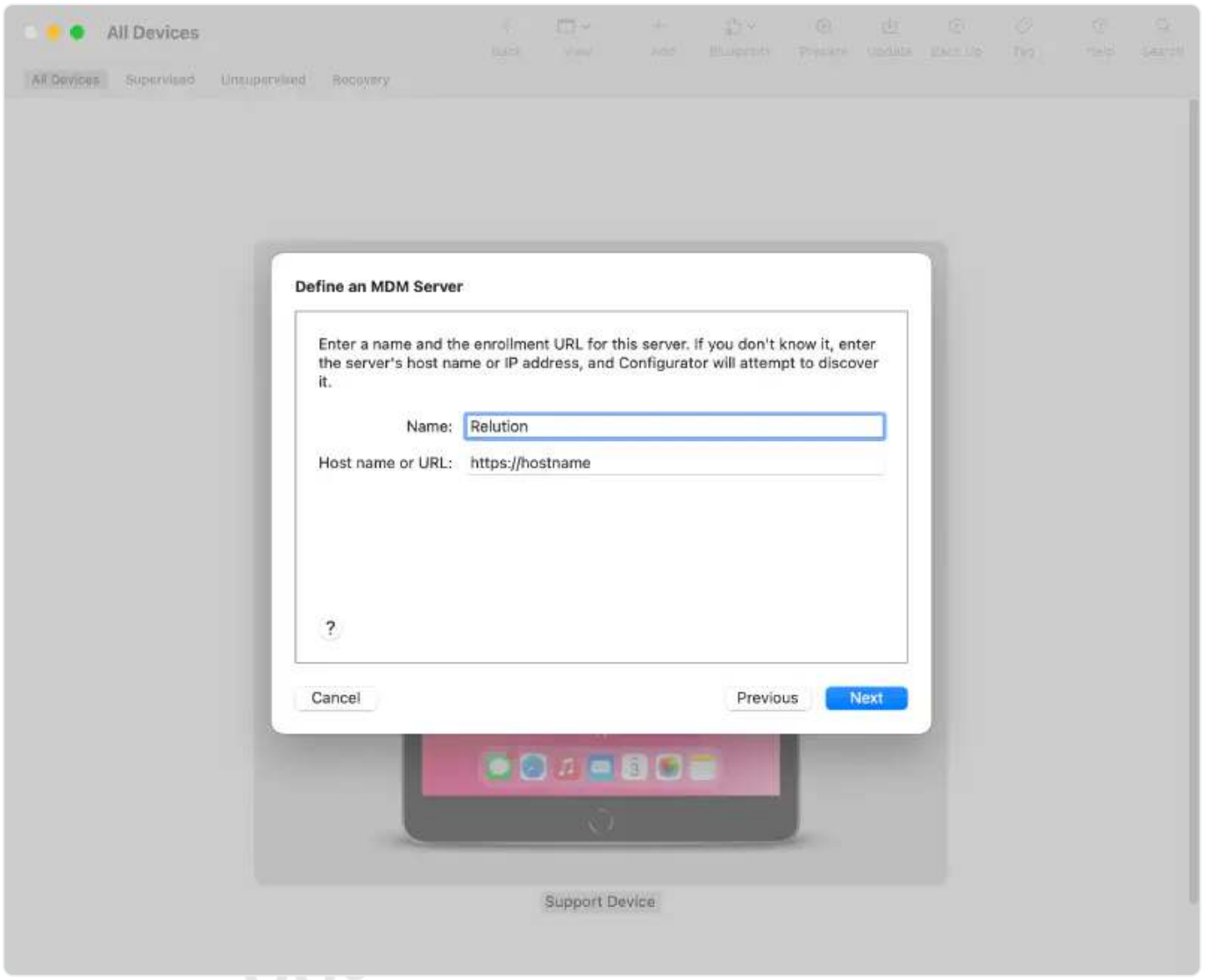


Dans l'étape suivante, sélectionner "Nouveau serveur…" et cliquer sur "Suivant".

Spécifier maintenant le nom et l'URL du serveur Relution correspondant. Le nom peut être choisi arbitrairement. L'URL commence par `https://` et correspond par exemple au système Relution live :

- Pour les appareils iOS `https://live.relution.io/`
- Pour les appareils tvOS `https://live.relution.io/api/enrollment/v1/appleMdm/depenroll`.

Cela ne fonctionne que si les appareils doivent être gérés dans le système de test Relution.

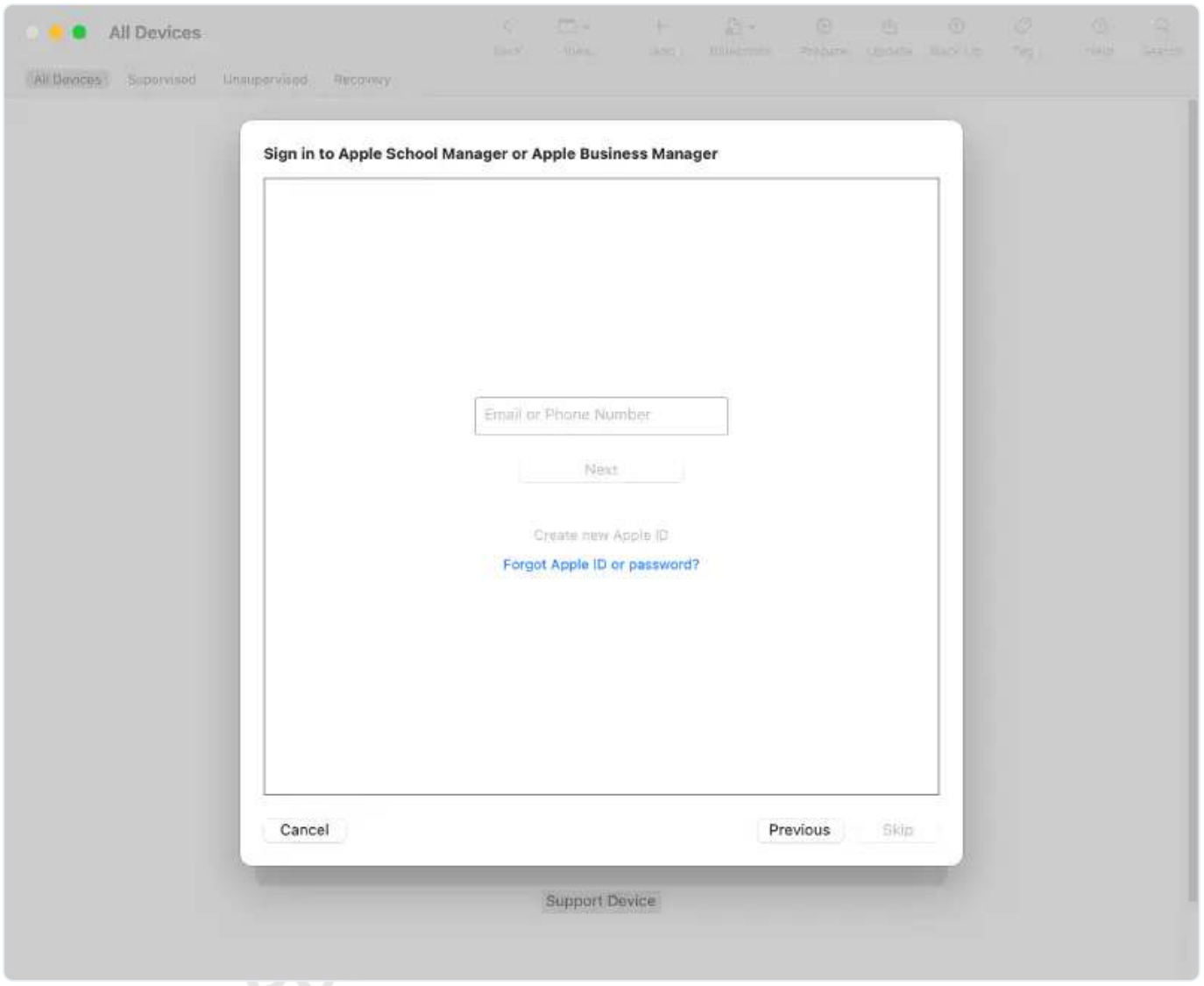


L’étape suivante consiste à sélectionner le certificat affiché. S’il y a plusieurs certificats, le premier est sélectionné.

Le serveur est alors défini et stocké dans le `Apple Configurator 2`. L’information est à nouveau disponible pour ajouter ultérieurement d’autres appareils au `Programme d'inscription d'appareils`.

Maintenant, dans le dialogue suivant, `New Organization...` est sélectionné et confirmé avec `Next`.

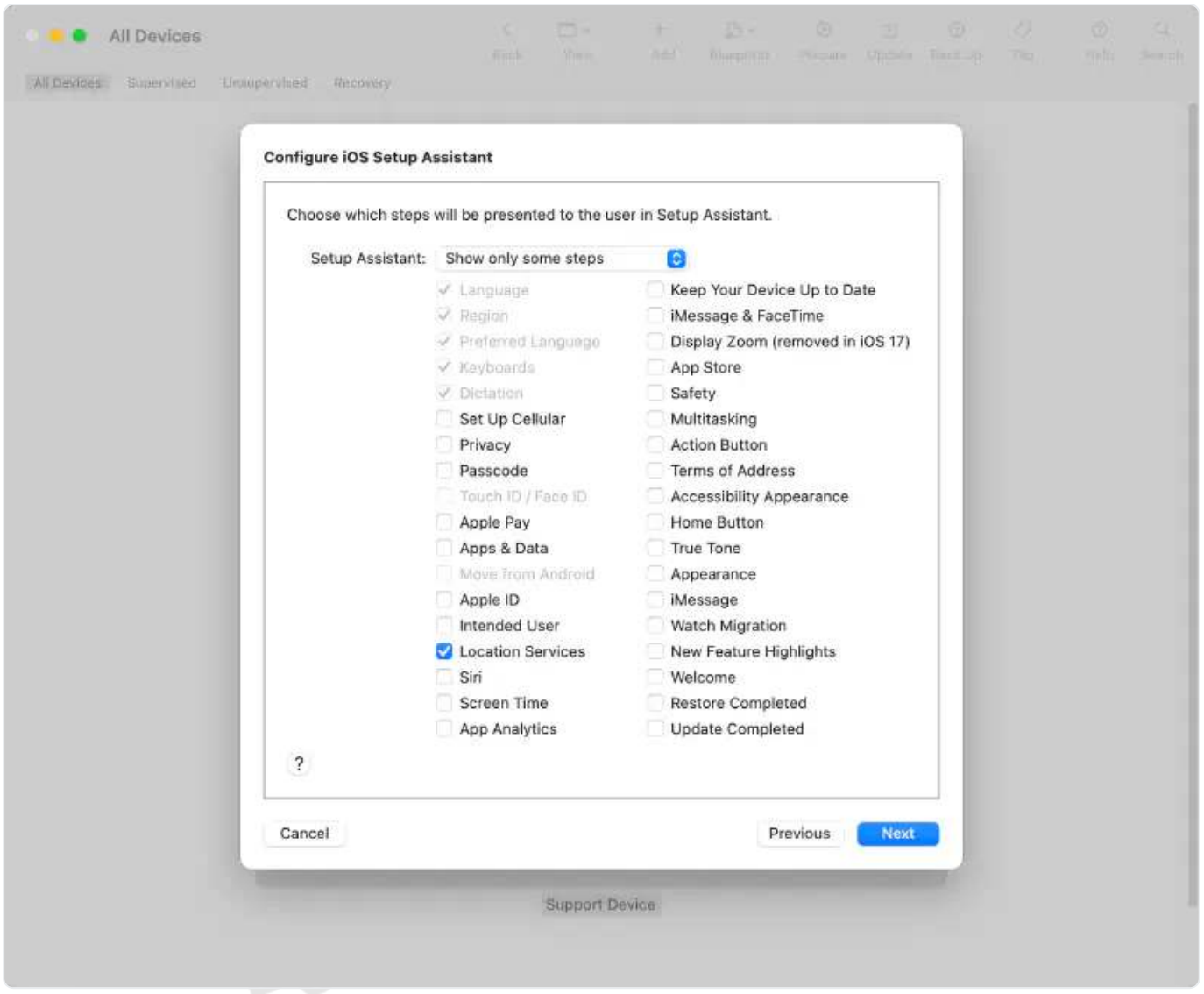
L’étape suivante consiste à se connecter au serveur Apple DEP. Pour ce faire, l’Apple ID et le mot de passe du compte Apple School / Business Manager correspondant sont saisis.



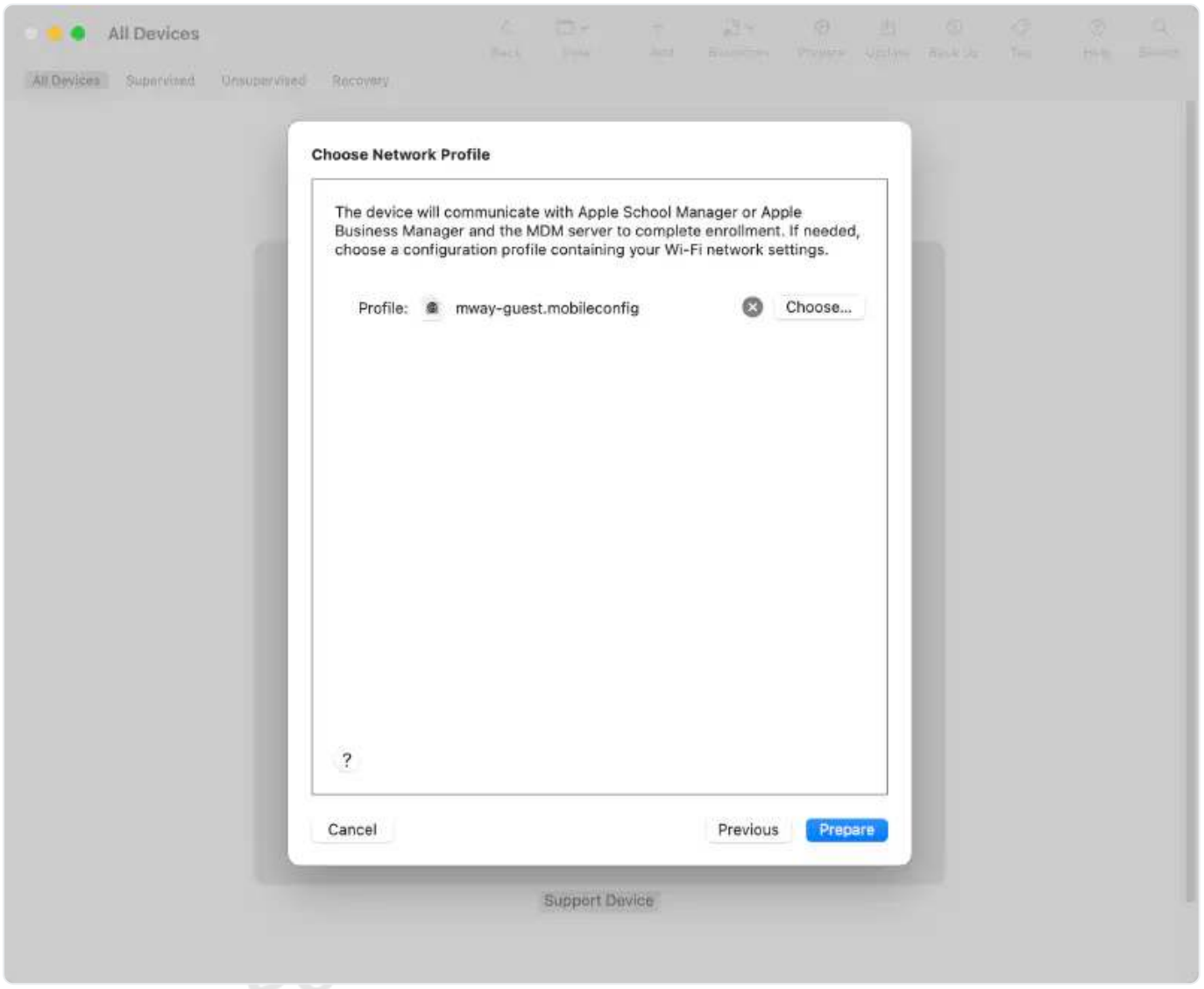
Si nécessaire, cette connexion doit être confirmée par une authentification à deux facteurs (saisie d'un code à quatre chiffres envoyé par SMS).

Sélectionner ensuite `Créer une nouvelle identité d'aidant` et confirmer avec `Suivant`. Les données de l'organisation sont également sauvegardées par `Apple Configurator 2`, de sorte qu'elles peuvent être réutilisées plus tard et qu'il n'est pas nécessaire de créer une nouvelle organisation.

Ensuite, les étapes de configuration qui ne doivent pas être sautées lors de la configuration des appareils sont sélectionnées dans le dialogue suivant. L'option `Services de localisation` doit être sélectionnée, sinon l'appareil Apple ne sera pas assigné au bon fuseau horaire.

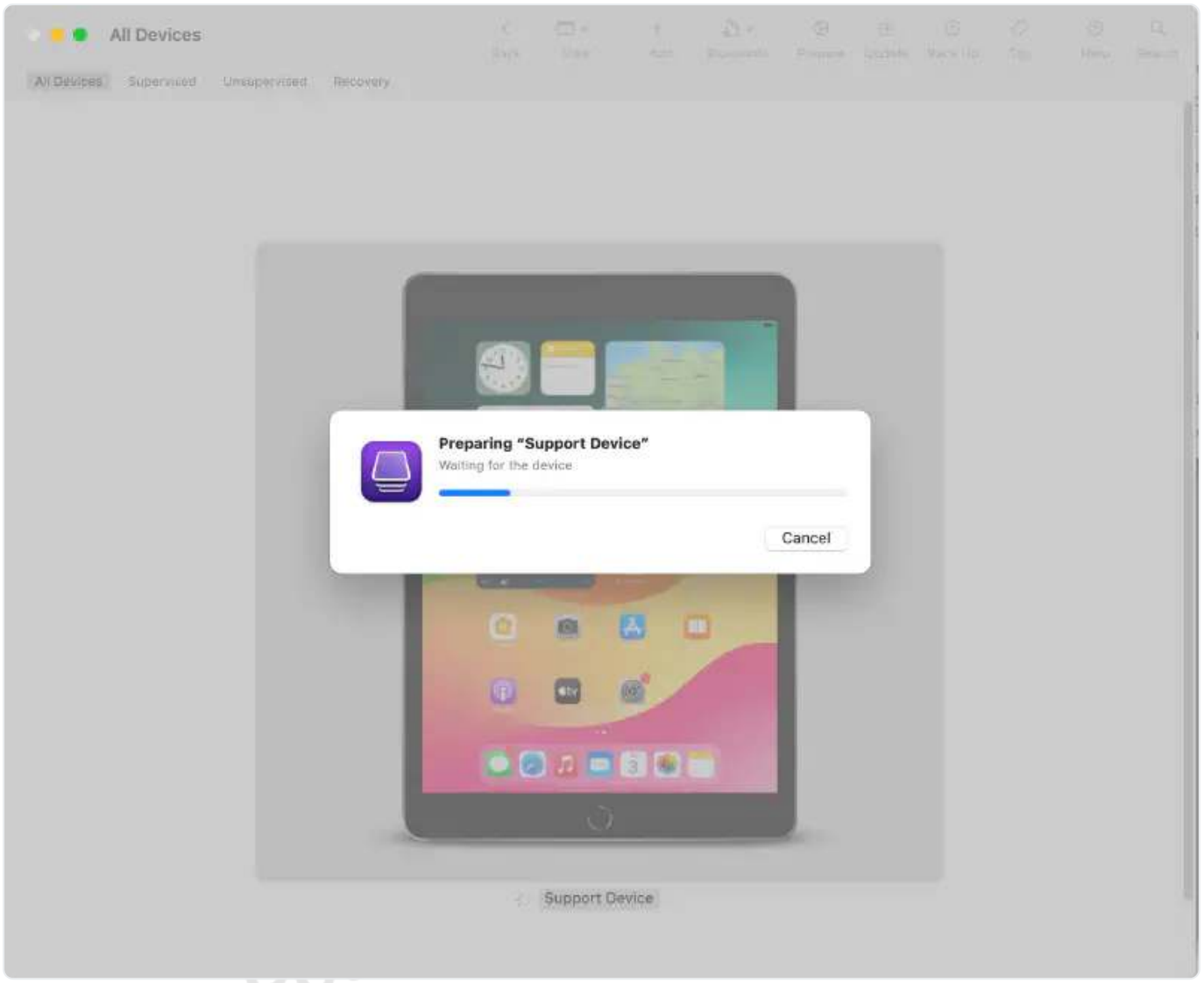


Un profil de configuration WiFi préalablement créé dans `Apple Configurator 2` via `Fichier` → `Nouveau Profil` doit ensuite être sélectionné. Ce profil sera automatiquement adopté par l'appareil après le redémarrage et établira directement une connexion Internet.



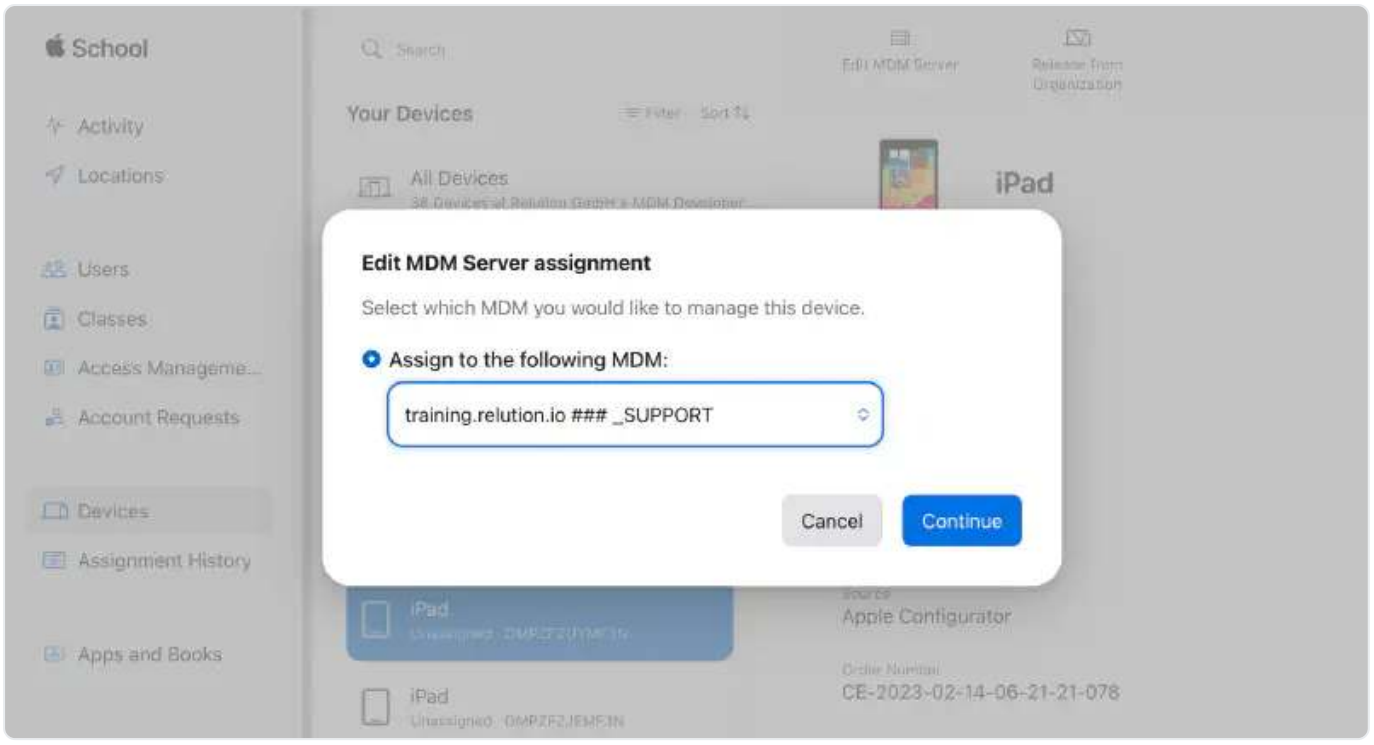
Cela permet à l'appareil Apple de transférer l'enregistrement ultérieur du DEP aux serveurs Apple. Comme alternative au profil WiFi, la connexion Internet de l'ordinateur Mac peut également être partagée avec l'appareil connecté via la connexion USB. Si aucun profil n'est sélectionné, les réglages WiFi sont entrés manuellement lors du redémarrage des appareils. Cliquer sur "Préparer" pour redémarrer l'appareil. Il est automatiquement enrôlé dans le DEP et ensuite assigné manuellement au serveur Relution MDM approprié dans Apple School/Business Manager.

Par défaut, les appareils sont affectés à Apple Configurator 2 via ce chemin.



Réglages dans Apple School and Business Manager

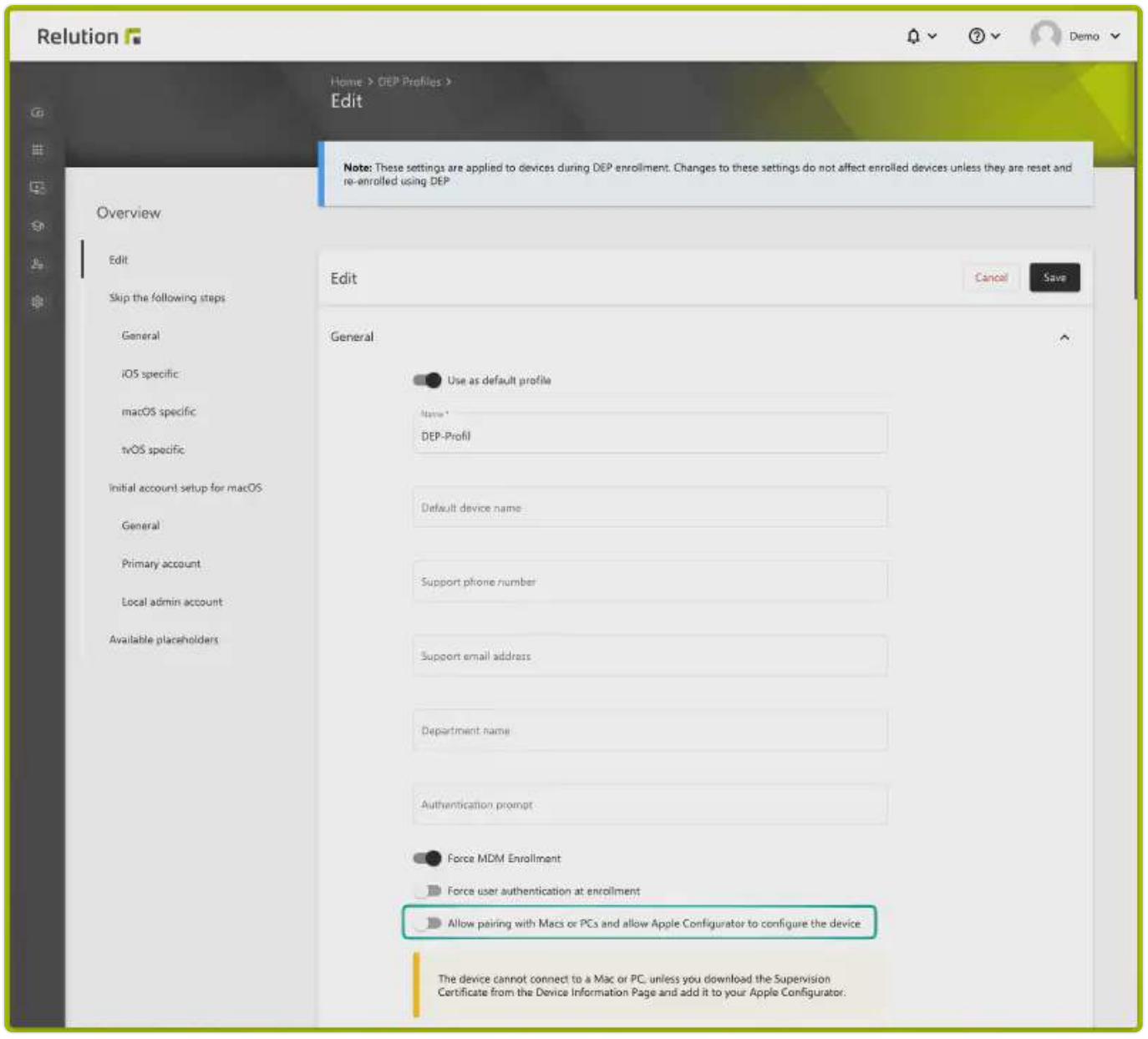
Après avoir ajouté manuellement des appareils Apple dans DEP, il faut les affecter au serveur MDM souhaité dans Apple School / Business Manager. Il est également possible de configurer un paramètre dans Apple School / Business Manager, de sorte que les nouveaux appareils soient automatiquement affectés à un serveur MDM défini. Toutes les options de configuration sont décrites dans la documentation en ligne d'Apple.



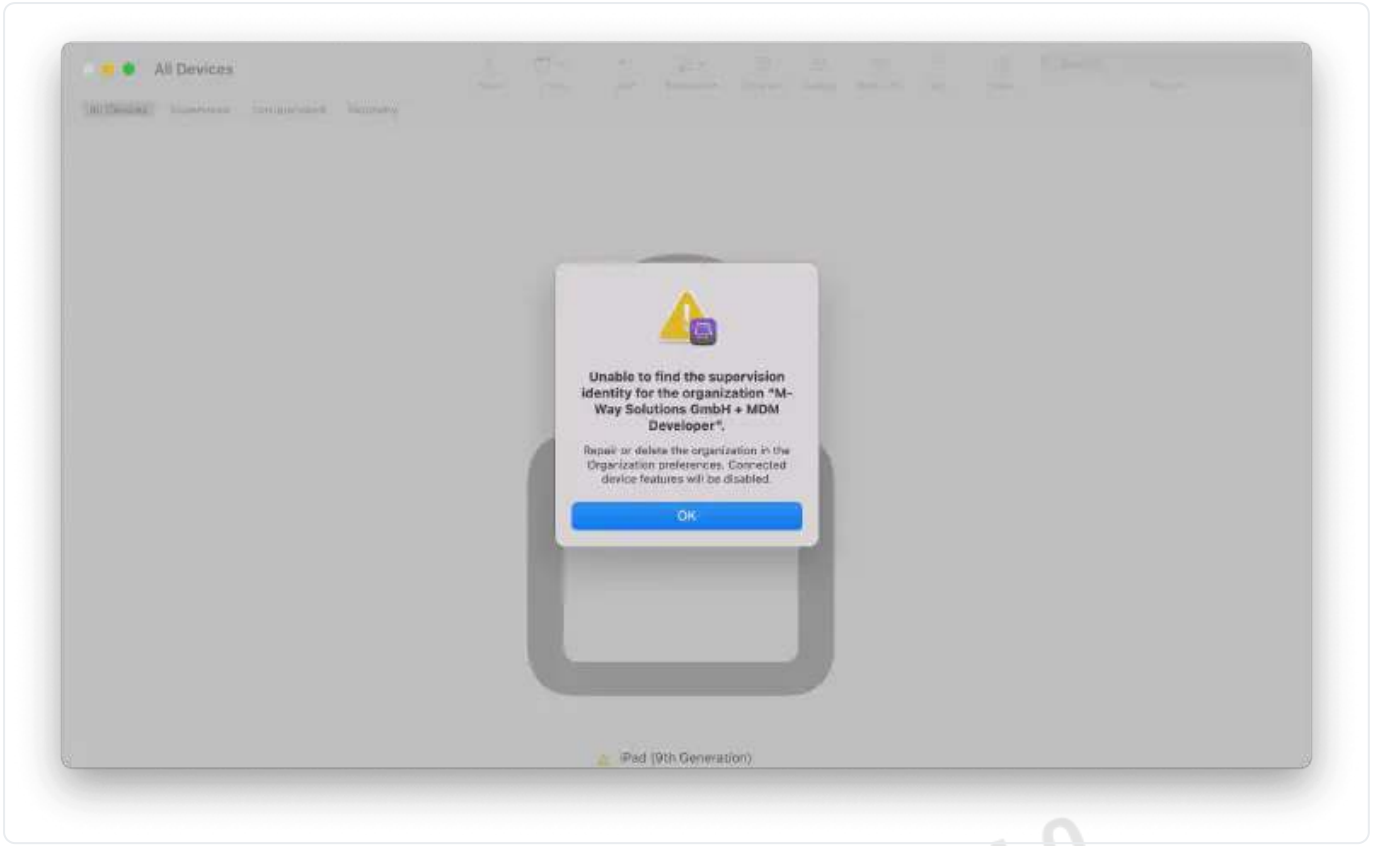
Certificat de supervision

Pour protéger les appareils DEP et empêcher tout accès non autorisé, Relution permet de désactiver l'option Autoriser la connexion aux Mac ou PC et la configuration avec Apple Configurator dans le profil DEP. Ceci empêche l'appareil Apple de se connecter à un Mac ou un PC et d'être configuré ultérieurement à l'aide d'Apple Configurator. Par exemple, cela empêche les utilisateurs de supprimer le profil MDM. Cette configuration ne peut être modifiée qu'après une réinitialisation de l'appareil.

Pour la version 26.4.0



À quoi faut-il faire attention lors de l'utilisation de ce paramètre ? Dans certains cas, le blocage de l'accès via un Mac ou un PC peut empêcher l'administrateur de réinitialiser manuellement un appareil depuis un ordinateur. Cela peut se produire, par exemple, si les paramètres Wi-Fi sont mal configurés ou si le serveur MDM dysfonctionne. L'appareil n'est alors plus accessible via Relution et ne peut plus être géré ni réinitialisé. On parle alors d'effet de verrouillage.



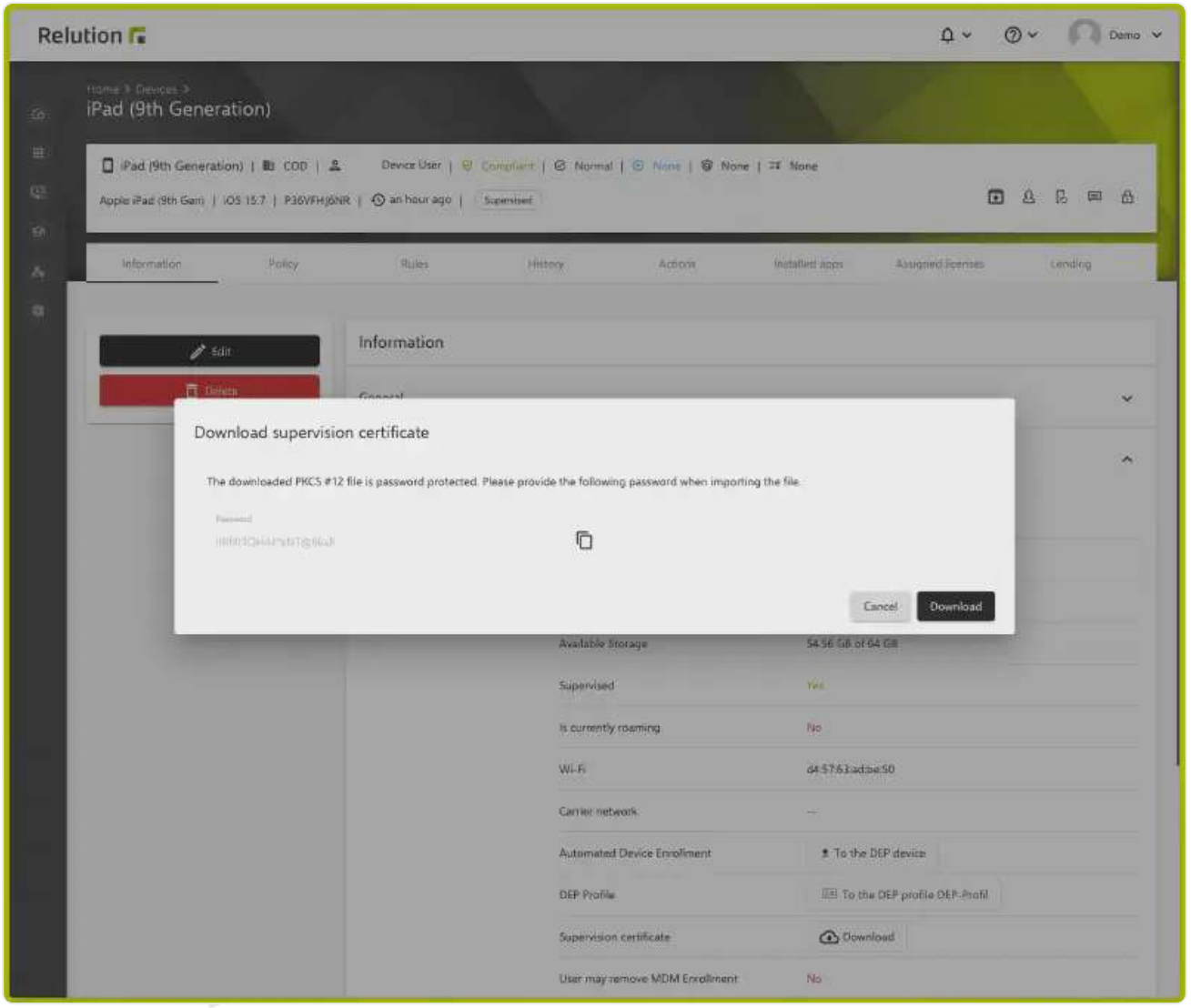
Pour la version 26.4.0

Comment garantir un accès autorisé avec Relution? Avec la version serveur 5.13, Relution autorise les connexions aux Mac et PC, même si le profil DEP les interdit. Lors de l'inscription d'appareils DEP dans Relution, un certificat de supervision est généré automatiquement. Grâce à ce certificat, l'administrateur peut connecter l'appareil à un Mac ou un PC malgré la restriction. Pour ce faire, le certificat est téléchargé depuis Relution et spécifié une seule fois lors de la connexion via Apple Configurator. Le certificat est ensuite disponible au téléchargement dans les détails de l'appareil. L'appareil est alors de nouveau accessible.

Avec Relution, l'appareil est de nouveau accessible. Que faut-il prendre en compte lors du déverrouillage de l'appareil ?

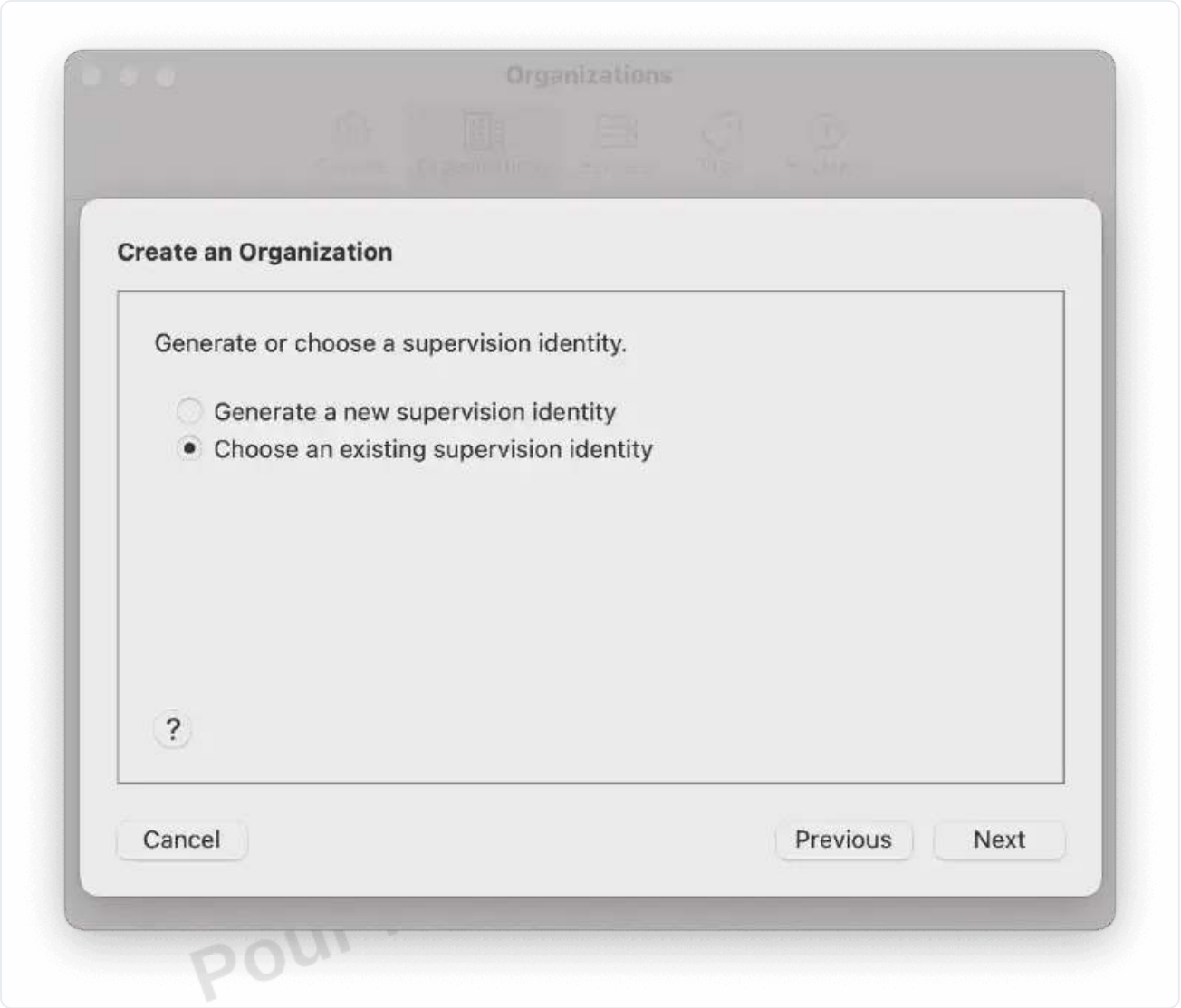
Voici la procédure de déverrouillage via Apple Configurator:

1. Télécharger le certificat de supervision et copier le mot de passe.

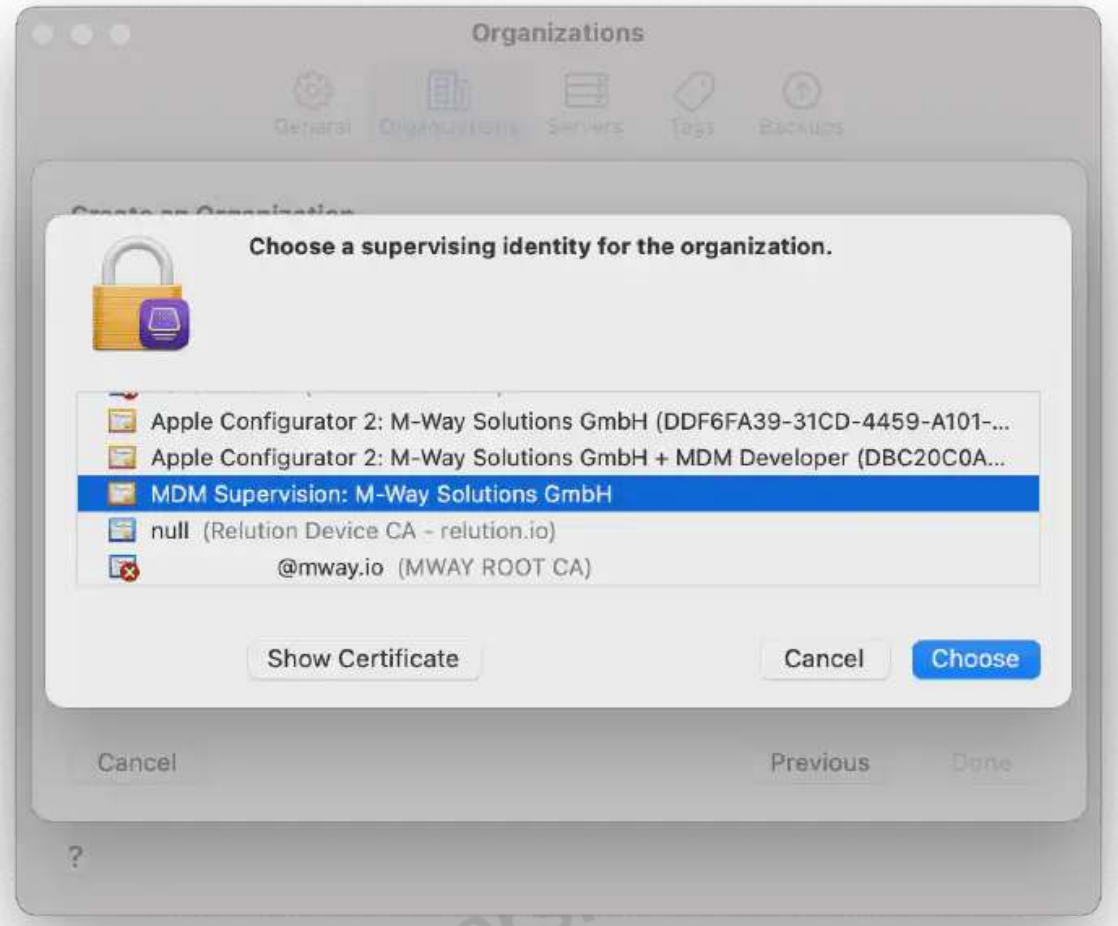


2. Créer une nouvelle organisation dans les réglages d’Apple Configurator et saisir l’identifiant Apple et le code de vérification.

3. Sélectionner l’identité de superviseur existante et cliquer sur Suivant.

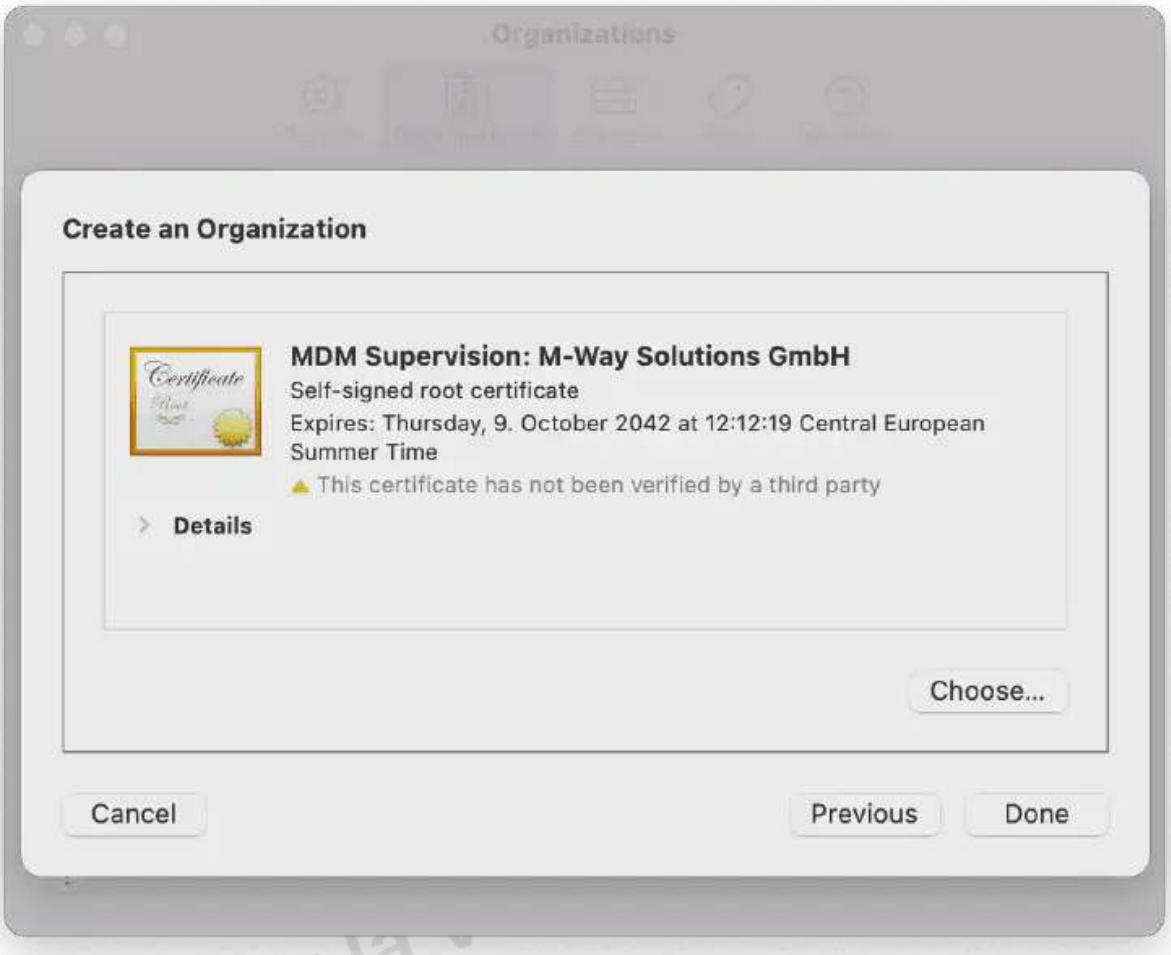


4. Ouvrir ensuite le certificat de supervision téléchargé sur l’ordinateur à l’aide du mot de passe fourni par Relution. Le Trousseau contenant le certificat s’ouvre.
5. Le certificat apparaît alors dans la boîte de dialogue Apple Configurator, sous Identités de superviseur, pour sélection.



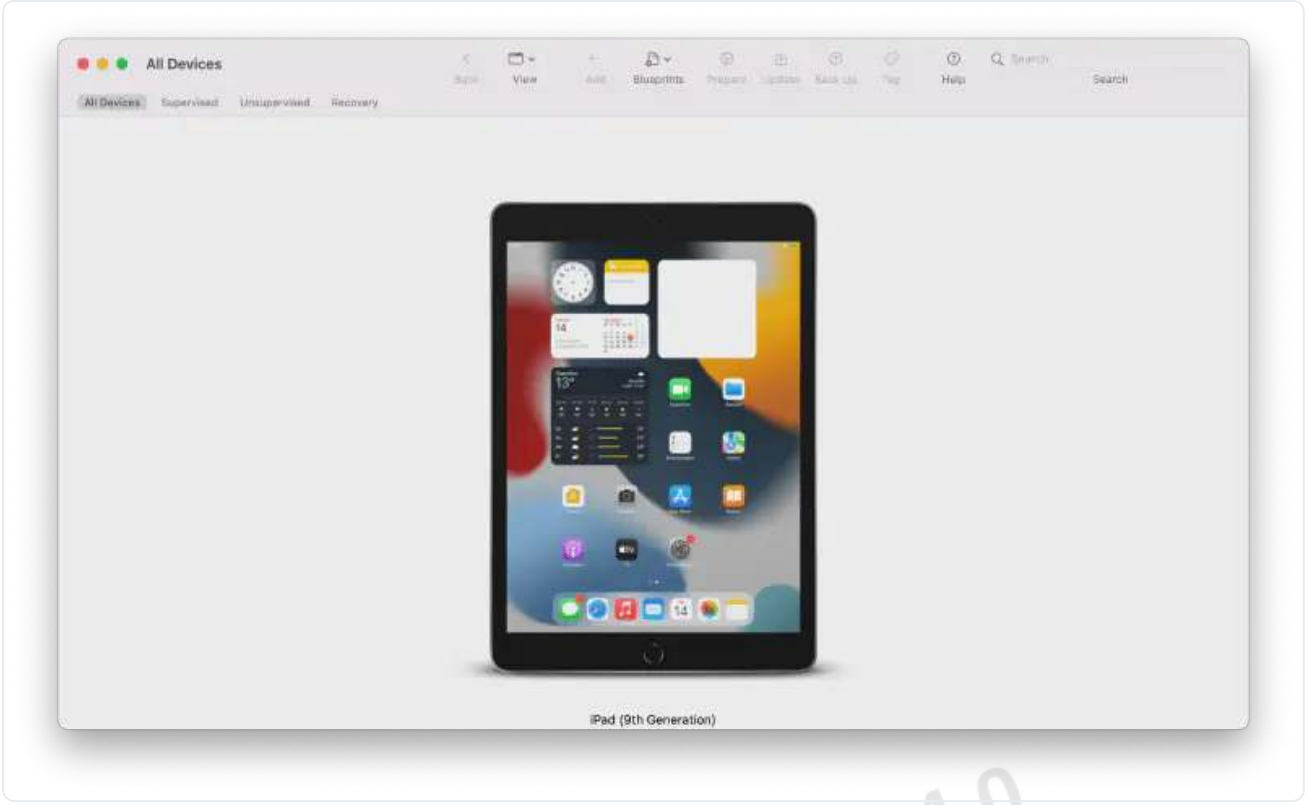
Pour la version

6. Créer une organisation.



Pour la

7. L’appareil est maintenant déverrouillé et peut être géré via Apple Configurator.



Que faut-il prendre en compte lors de l’utilisation du certificat de supervision?

Le certificat est généré uniquement lors de l’inscription de nouveaux appareils au programme DEP. Durant cette inscription, il est automatiquement créé et installé sur l’appareil. Cette fonctionnalité ne s’applique pas aux appareils déjà inscrits, et aucun certificat n’est généré pour ces derniers.

Pour la version 26.4.0

Supprimer le mode supervisé

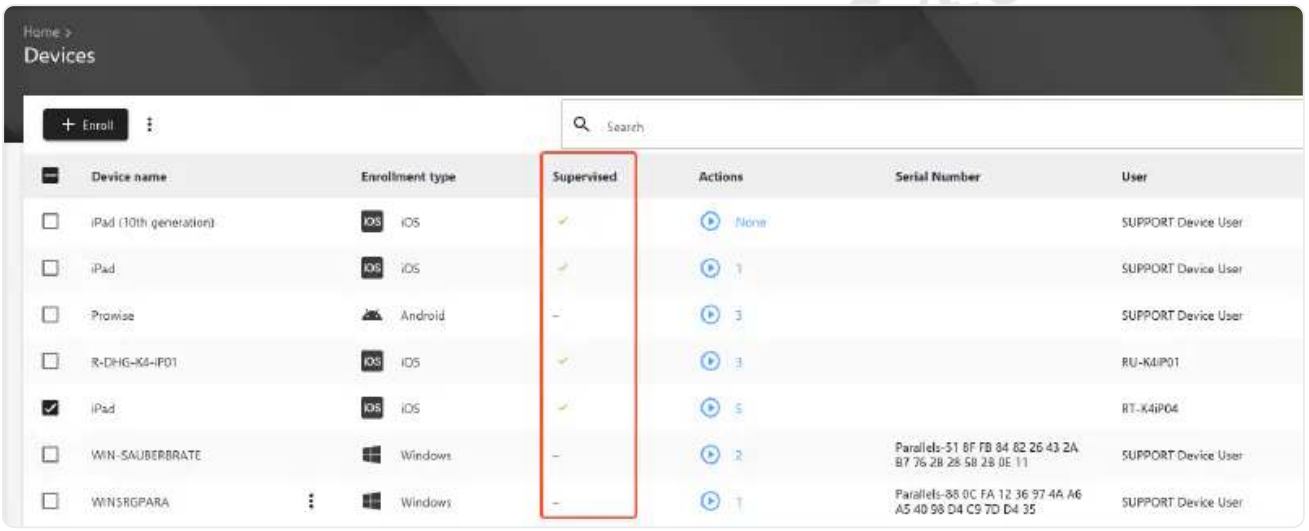
De temps en temps, il peut être nécessaire de révoquer ce mode sur les appareils Apple qui fonctionnent en mode supervisé.

> Pour les appareils iOS et tvOS, cet état peut être inversé. Les appareils macOS, en revanche, ne peuvent être exploités en `Mode supervisé` qu'à partir de la version 11.

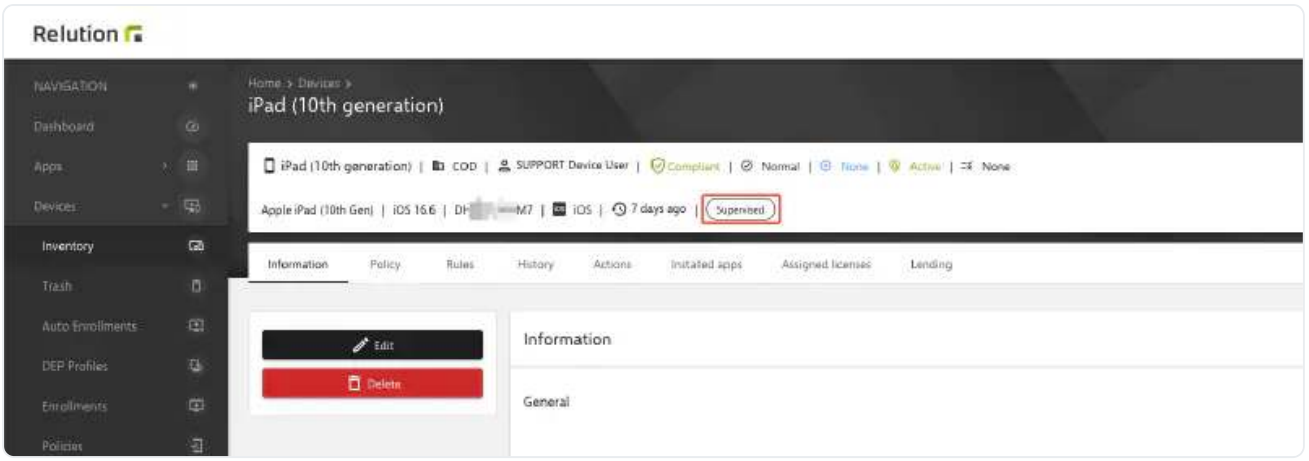
Identifier les appareils surveillés

Les appareils surveillés peuvent être localisés comme suit :

1. Afficher la colonne `Sera surveillé` dans l'inventaire. Les appareils correspondants sont marqués d'une coche.



2. Dans les détails de l'appareil, le statut peut être vu par le badge correspondant `Will be supervised` dans l'infobox.



Appareils enrôlés via Apple Configurator

> Cette opération supprime également le profil MDM des appareils, qui ne pourront plus être gérés par la suite sans être réinscrits. En outre, toutes les applications et les données seront supprimées des appareils.

Réinitialiser les appareils en utilisant l'une des options suivantes :

1. Envoyer une action "réinitialisation d'usine" aux appareils.
2. Aller dans les réglages de l'appareil sous `Général` → `Transférer/Réinitialiser l'iPad` → `Effacer tout le contenu et les réglages`.
3. Connecter les appareils à l'ordinateur Mac et ouvrir l'application `Apple Configurator 2`. Faire un clic droit sur les appareils et sélectionner "Avancé", puis sélectionner "Effacer tout le contenu et les réglages".

Il est possible que les utilisateurs finaux ne soient pas autorisés à effectuer une `Réinitialisation d'usine` sur les appareils car cela a été interdit dans les restrictions.

Appareils DEP inscrits via Apple School/ Business Manager par l'intermédiaire d'un revendeur agréé

Si des appareils ont été ajoutés au système MDM via Apple School / Business Manager, le lien doit être annulé à cet endroit, sinon les appareils se rapporteront toujours automatiquement au système MDM après une `Réinitialisation d'usine` et obtiendront le `Mode supervisé`.

1. Se connecter à Apple School / Business Manager et cliquer sur "Appareils".

2. Sélectionner l’appareil approprié et cliquer sur “Modifier l’affectation de l’appareil” sur le côté droit.
3. Cliquer sur “Désassigner”.
4. Réinitialiser l’appareil aux paramètres d’usine.

Appareils DEP ajoutés ultérieurement via Apple Configurator

La suppression du “mode supervisé” des appareils ajoutés à Apple School / Business Manager via `Apple Configurator` fonctionne de la même manière que les appareils DEP inscrits via un revendeur agréé.

Toutefois, les utilisateurs finaux peuvent supprimer manuellement le profil MDM sur les appareils dans les 30 premiers jours suivant l’ajout des appareils au DEP. Cela entraînera la perte de l’inscription MDM ainsi que du mode surveillé.

Pour la version 26.4.0

Vue d'ensemble

Optimisez la gestion de vos appareils iOS avec les actions polyvalentes de Relution.

Relution propose une variété d’actions pouvant être exécutées sur les appareils iOS pour optimiser leur gestion. Ces actions permettent de contrôler efficacement les appareils, d’améliorer la sécurité et de simplifier les flux de travail. L’aperçu suivant décrit les actions disponibles et fournit des exemples pour illustrer leur utilité.

Les actions suivantes peuvent être effectuées sur les appareils iOS

Action	Description
Ajouter un raccourci	Ajoute un raccourci vers un site web.
Alert	Fait retentir une alerte sonore sur l’appareil, même en mode silencieux.
Effacer le mot de passe des restrictions	Efface le mot de passe de restriction et les restrictions.
Continue in device setup assistent	Informe l’appareil que la pré-configuration est terminée et qu’il peut passer à l’assistant de configuration.
Supprimer les utilisateurs locaux	Supprime les comptes d’utilisateurs locaux.
Déployer une application à partir de l’Apple App Store →	Installe des applications directement à partir de l’Apple App Store.
Déployer une application du Relution Store →	Installe une application à partir de l’App Store de Relution.
Enable Lost Mode →	Active le ‘Mode Perdu’ avec l’écran de verrouillage et la localisation.
Activer ou désactiver Bluetooth	Active ou désactive la fonction Bluetooth.

Action	Description
Activer ou désactiver le hotspot personnel	Active le hotspot sur l’appareil.
Plan cellulaire de l’eSIM	Met à jour le plan cellulaire de l’eSIM.
Install Media	Installe un média sur l’appareil.
Installer la mise à jour	Installe une mise à jour du système d’exploitation si elle est disponible.
Localiser l’appareil	Recherche l’emplacement actuel de l’appareil.
Verrouiller l’appareil	Verrouille l’appareil avec le mot de passe actuel.
Déconnecter l’utilisateur	Force l’utilisateur actuel à se déconnecter.
Reboot device	Redémarre l’appareil iOS.
Refresh device info	Synchronise les informations de l’appareil avec Relution.
Remove app	Désinstalle une application sélectionnée sur l’appareil.
Remove Media →	Supprime les médias déployés (PDF, ePub).
Remove: cut →	Supprime un raccourci de l’écran d’accueil de l’appareil.
Request mirroring	Active la transmission sans fil de l’écran aux dispositifs d’affichage compatibles.
Réinitialisation du code de verrouillage	Réinitialise le mot de passe de l’utilisateur.
Retour au service →	L’appareil est réinitialisé aux paramètres d’usine, puis remis en service automatiquement sans intervention de l’utilisateur.
Envoyer un message	Affiche un message texte sur l’appareil.
Arrêter l’appareil	L’appareil s’éteint.
Arrêter la mise en miroir	Arrête la transmission AirPlay en cours.
Mise à jour du profil MDM	Met à jour le profil MDM sur l’appareil.
Wipe Device	Supprime toutes les données et réinitialise l’appareil.

Action	Description
Accès conditionnel →	Nécessite la configuration de l’accès conditionnel sur l’appareil via l’agent Relution pour pouvoir utiliser les ressources protégées.
Itinérance des données →	Active ou désactive l’itinérance des données.

Pour la version 26.4.0

Installation de l'application

Relution propose plusieurs façons d'installer des applications sur les appareils, en fonction de la plateforme gérée.

1. Installation via `action`.
2. Installation via la configuration de la politique.
3. Installation via `auto-deployments`.

Chacune de ces méthodes possède des caractéristiques qui peuvent être utiles dans certains cas d'utilisation.

Installation par action

Sur les appareils gérés dans Relution, les applications peuvent être installées par `Action`. Pour cela, passer à l'onglet `Actions` dans les détails de l'appareil et cliquer sur le bouton `Appliquer une action`. Ici, en fonction du système d'exploitation, sélectionner les options `Installer l'application depuis le Play Store` (`Android Enterprise`) ou `Installer l'application` (toutes les autres plateformes).

Pour la version 26.4.0

Sélectionner ensuite l'application à installer et cliquer sur `Suivant`.

Une nouvelle `Action` sera créée dans l'aperçu des actions et l'installation sera lancée dès qu'elle aura été livrée à l'appareil correspondant.

Installation via la configuration de la politique

L'installation d'applications via la configuration de la politique est une approche plus raisonnable pour un grand nombre d'applications et d'appareils que de le faire via des actions individuelles.

Se référer aux chapitres individuels des politiques de la plateforme pour apprendre comment cela fonctionne.

Conformité des applications iOS →
Conformité des applications tvOS →
Gérer les applications Android Enterprise →

Installation via l’auto-déploiement

Les “auto-déploiements” sont des installations d’applications spécifiques à l’utilisateur qui dépendent des comptes d’utilisateurs et des groupes associés aux appareils. Cela permet à certaines applications d’être installées sur les appareils dès que l’utilisateur correspondant s’y connecte.

Les déploiements automatiques peuvent entrer en conflit avec une conformité d’application. Si une exigence de conformité interdit l’utilisation d’une application spécifique, mais que cette application est incluse dans un déploiement automatique assigné à un utilisateur ou à un groupe, elle ne sera pas accessible pour l’utilisateur concerné.

Les paramètres de `Déploiement Automatique` se trouvent aux endroits suivants dans le portail Relution :

Détails de l’utilisateur ou du groupe

Au bas de la page de détails d’un utilisateur ou d’un groupe, les applications correspondantes peuvent être déployées en fonction de l’utilisateur ou du groupe.

Détails de l’application

Au bas de la page de détail d’une application, l’utilisateur ou le groupe correspondant peut être déposé.

Pour la version 26.4.0

Itinérance des données

Contrôlez l'itinérance des données sur les appareils iOS directement via Relution.

Avec Relution 26.2, les administrateurs ont la possibilité d’activer ou de désactiver l’itinérance des données sur les appareils iOS.
Cette fonctionnalité peut également être exécutée comme une action directe sur l’appareil.

Remarque : Cette configuration peut être désactivée par l’utilisateur sur l’appareil.

Retour au service

Avec iOS 17+ et Relution Server version 5.20, il est possible de déclencher une action `Return to Service` sur les appareils iOS. Cette action réinitialise l'appareil aux paramètres d'usine. L'appareil essaiera de se reconnecter automatiquement après la réinitialisation. Cela permet d'éliminer les étapes répétitives telles que l'entrée dans le réseau local sans fil et les étapes de configuration qui sont activées comme n'étant pas ignorées dans le profil DEP.

> L'utilisateur doit désactiver tous les verrous d'activation pour que cette fonction fonctionne correctement

Prérequis

1. l'appareil cible doit être un appareil iOS 17+ inscrit dans Relution avec un profil DEP.
2. le serveur Relution doit être au moins en version 5.20+.
3. une politique avec une configuration WLAN doit être spécifiée.

Pour la version 26.4.0

Exécuter l'action Retourner au service

Pour ce faire, l'élément de menu 'Appliquer l'action' doit être sélectionné pour le périphérique souhaité dans l'inventaire.

L'action peut être trouvée et sélectionnée via la recherche.

Dans l'étape suivante, la politique avec la configuration WLAN est sélectionnée. Pour l'eSIM, il y a l'option "Conserver le tarif de données existant".

Enfin, il y a un dernier feedback pour exécuter l'action.

Mode perdu et suivi des appareils

Le Mode Perdu permet de verrouiller un iPhone ou un iPad afin de s'assurer que personne ne puisse accéder aux données personnelles. Le mode permet de configurer un message pour l'appareil indiquant qu'il a été perdu, ainsi que les coordonnées pour le contacter. En outre, l'emplacement actuel de l'appareil peut être affiché sur une carte. Il s'agit d'une option supplémentaire pour retrouver l'appareil s'il est perdu.

> Le mode perte et la localisation nécessitent une connexion internet sur l'appareil.

Application unique

Pour verrouiller ou localiser un appareil, celui-ci doit être sélectionné dans l'inventaire des appareils de Relution. Dans l'onglet `Actions`, sélectionner l'option `Mode Perdu`. Il est possible de saisir ici des informations sur le contact ; elles seront affichées sur l'écran de verrouillage.

Pour la version 26.4.0

De plus, il est nécessaire d'avoir préalablement activé la fonction "Localiser l'appareil" afin de pouvoir localiser celui-ci par la suite. Une fois l'action effectuée, la page Web de Relution doit être rechargée en appuyant sur le raccourci clavier `CTRL+R` (Windows) ou `CMD+R` (Mac). Cela affichera l'onglet "Localisation" à côté des "Actions" et montrera la localisation sur une carte.

Application permanente

Il est également possible d'activer de façon permanente le Mode Perdu pour les appareils DEP, en particulier en cas de vol de l'appareil. L'avantage est que les appareils réinitialisés et mis en service sont automatiquement placés en mode Perdu dès qu'ils sont connectés à l'internet. Ce mode peut être activé de manière permanente pour l'appareil via le portail Relution sous `Appareils` > `Auto-Enregistrements` > `Appareil affecté` > `Activer le Mode Perdu` > `Sauvegarder`.

Hint

- Afin de limiter les abus potentiels, Relution à partir de la version 5.31.0 offre la possibilité d'ajuster une autorisation de localisation.

Verrouiller le profil MDM

L'enrôlement automatique des appareils Apple DEP permet aux organisations d'enrôler automatiquement les appareils Apple dans une solution MDM. Le profil de configuration associé aux appareils lors de l'enrôlement DEP permet de déployer des configurations directement au démarrage. La gestion continue des appareils n'est donc possible que tant que le profil MDM reste verrouillé sur les appareils. Si les utilisateurs retirent manuellement le profil MDM des appareils, les administrateurs ne peuvent plus gérer ces appareils. Par conséquent, il est possible de verrouiller le profil MDM sur les appareils afin que les utilisateurs finaux ne puissent pas le retirer des appareils.

Verrouiller le profil MDM

Modifier ou créer un profil DEP dans le portail Relution sous `Home` → `Devices` → `DEP profiles` > `Create / edit`.

Il est ici possible de désactiver l'option `Les utilisateurs peuvent supprimer l'inscription MDM`.

Pour la version 26.4.0

Définir le profil DEP par défaut

Les profils DEP peuvent être définis par défaut pour tous les futurs appareils. Les nouvelles inscriptions se verront alors automatiquement attribuer le profil DEP sélectionné.

Attribuer un profil DEP à des appareils déjà enrôlés

Un profil DEP peut être attribué et synchronisé ultérieurement pour des appareils déjà existants.

> Les modifications apportées au profil DEP n'affectent pas automatiquement les appareils déjà inscrits. Pour cela, les appareils concernés doivent être réinitialisés et réinscrits.

SFTP Upload (téléchargement SFTP)

Relution peut être utilisé pour créer des Apple ID gérés en grand nombre. Cela est possible via le portail Relution dans les paramètres et facilite la configuration automatique de ces identifiants par les écoles et les autorités scolaires afin qu'ils puissent être mis à la disposition des étudiants et des enseignants.
Ce processus permet également de migrer automatiquement les classes créées dans Relution vers des classes dans Apple School Manager.

Exigences

- Autoriser le port 22 en sortie vers les serveurs Apple, en particulier pour l'URL : `upload.appleschoolcontent.com`.
- Un Apple School Manager
- Une licence Education dans Relution
- Au moins un domaine vérifié dans Apple School Manager (les adresses de réserve d'Apple ne sont pas possibles)
- Une classe dans Relution avec au moins un enseignant et un étudiant utilisateur
- Les enseignants doivent faire partie du groupe système `Teacher` et les étudiants doivent faire partie du groupe système `Student`.

Pour la version 26.4.0

Configuration

- Ouvrir le portail Relution et Apple School Manager.
- Naviguer jusqu'au point suivant dans Relution : `Paramètres` → `Education` → `Apple School Manager SFTP Upload`
- Continuer dans l'assistant de configuration jusqu'à la saisie de l'URL du serveur, de l'utilisateur et du mot de passe.
- Dans School Manager, naviguer jusqu'au point suivant : dans le coin inférieur gauche, cliquer sur `Utilisateur` → `Paramètres` → `Comptes Apple gérés` → `Démarrer les premières étapes de la synchronisation des répertoires de liaison`.
- Cliquer sur `Créer de nouveaux comptes`
- Cliquer sur `Utiliser un fichier CSV au format Apple`
- A l'étape 1, `Set up SFTP`
- Copier les valeurs, les saisir dans les champs de Relution, puis cliquer sur `Suivant`.
- Entrer le domaine vérifié dans Apple School Manager et continuer à naviguer.

- Cliquer sur `Synchroniser les données`
- Cliquer sur `Suivant` dans Apple School Manager et attendre l'importation.

Les IDs seront maintenant affichés et peuvent être vérifiés pour des erreurs ici. Dans l'étape suivante, il est possible de spécifier la structure des identifiants Apple.

Par exemple

- Étudiants: `(Prénom + Nom)@relution.io`
- Enseignants: `(Première lettre du Prénom + Nom)@relution.io`

Emplacement

Le téléchargement SFTP crée un nouvel emplacement dans Apple School Manager pour chaque organisation Relution qui utilise le téléchargement SFTP. Le nom de cet emplacement est le même que le nom unique de l'organisation Relution concernée.

Par exemple :

- Nom de l'organisation: `Utilisateur-Import-Test`
- Nom unique de l'organisation: `UIT`
- Nouvel emplacement dans ASM: `UIT`

Si l'emplacement dans Apple School Manager utilisé pour l'achat d'applications et qui existe déjà porte le même nom, cela peut causer des problèmes. Il est recommandé d'en discuter au préalable avec l'opérateur de serveur ou le partenaire concerné.

Pour la version 26.4.0

Déconnexion

Ne jamais déconnecter la connexion de téléchargement SFTP si les identifiants sont encore activement utilisés et si d'autres identifiants doivent être créés à l'avenir. En cas de déconnexion, tous les identifiants créés via le téléchargement SFTP seront remplacés par la source Manuellement à partir de SFTP. Une reconnexion ultérieure risque de créer des identifiants Apple en double. Étant donné que la version 5.26 de Relution a également introduit l'importation d'utilisateurs, cela peut créer un cercle vicieux.

Vue d'ensemble

Une politique est un ensemble d’une ou plusieurs configurations. Chaque politique peut être appliquée à un ou plusieurs appareils en même temps. En outre, une ou plusieurs politiques peuvent être associées à chaque appareil.

Configurations disponibles

Configuration	Description
Domaines gérés →	Définir les domaines de messagerie ou web gérés
AirPlay	Gestion de la transmission sans fil de contenu vers des appareils récepteurs compatibles AirPlay
AirPrint	Gestion des paramètres d’impression AirPrint
Conformité des applications	Gestion des restrictions spécifiques aux applications
Association application-VPN	Configuration du VPN utilisé par des applications individuelles
Configuration Apple Configurator 2	Appliquer un profil de configuration (mobileconfig) créé à l’aide d’Apple Configurator 2 aux appareils.
Proxy DNS	Configuration du proxy DNS
Paramètres de chiffrement DNS	Configurer les paramètres de chiffrement DNS
E-mail	Ajouter des configurations d’e-mail pour plusieurs utilisateurs
Paramètres iPad partagé	Configurer les paramètres pour les appareils iPad partagés
Mode application unique	Limiter les appareils à une seule application

Configuration	Description
Exchange	Gestion des comptes Exchange
Filtre de contenu	Autoriser ou interdire des URL spécifiques
Délai de verrouillage de l’appareil	Configuration d’un verrouillage d’appareil limité dans le temps
Paramètres de l’appareil	Configurer les paramètres généraux de l’appareil
Nom de l’appareil	Configurer le nom de l’appareil
Proxy HTTP global	Configurer les paramètres de proxy globaux
Compte Google	Gestion des comptes Google
Fond d’écran	Gérer le fond d’écran
Disposition de l’écran d’accueil	Grouper les applications sur l’écran d’accueil par catégorie
Calendrier	Gestion des calendriers CalDAV
Abonnements de calendrier	Gérer les abonnements de calendrier
Contact	Gestion des comptes CardDAV
Application gérée	Envoyer les configurations d’application pour les applications gérées
Réseau cellulaire	Configure les paramètres du réseau cellulaire
Message sur l’écran de verrouillage	Configurer un texte personnalisé sur l’écran de verrouillage
Mot de passe →	Politique de mot de passe pour les appareils Apple
Partages de fichiers Relution	Configuration des partages de fichiers pour l’application cliente Relution
Appareil partagé Relution	Mettre les appareils en mode appareil partagé
Restrictions	Gestion des restrictions d’appareils

Configuration	Description
SCEP	Gestion des paramètres SCEP
Assistant d’installation →	Masquer les étapes de configuration affichées après la configuration initiale (appareils supervisés uniquement)
Mises à jour système	Gérer les mises à jour des appareils Apple (iOS/tvOS)
Mises à jour logicielles gérées →	Imposer les mises à jour du système en ciblant une version précise avant une échéance (successeur de Mises à jour système)
VPN	Gestion des paramètres VPN
Lien web →	Ajouter un lien web aux appareils
WLAN	Gestion des paramètres WLAN
Fuseau horaire	Configuration du fuseau horaire
Certificat	Sélectionner un certificat à installer par défaut sur l’appareil

Pour la version 26.4.0

Mot de passe

La politique de mot de passe Apple définit les exigences de sécurité pour les codes d'accès des appareils iOS. Lors de l'enregistrement d'un utilisateur sur iOS, une restriction système s'applique : si une politique de code est définie, iOS impose automatiquement un code complexe d'au moins six caractères – indépendamment des autres paramètres. Certains paramètres de configuration peuvent ainsi être ignorés.

La politique propose néanmoins de nombreuses options pour adapter les exigences de sécurité du mot de passe. Cela inclut la complexité, la longueur, la durée de validité et le nombre de tentatives échouées autorisées.

Options de configuration

- ☐ Autoriser les mots de passe simples
- ☐ Exiger des mots de passe alphanumériques
- Longueur minimale du mot de passe
- Nombre de caractères spéciaux requis
- Âge maximal du mot de passe (en jours)
- Inactivité (en minutes) : Valeur maximale sélectionnable par l'utilisateur final
- Historique des mots de passe
- Délai maximal avant verrouillage automatique (en minutes)
    - Immédiatement
    - 1 minute
    - 5 minutes
    - 15 minutes
    - 60 minutes
    - 4 heures
- Nombre maximal de tentatives échouées

> Si la limite est dépassée, une action d'effacement est déclenchée

Pour la version 26.4.0

iPad partagé : Modes de fonctionnement et gestion des codes d’accès

Apple propose deux modes de fonctionnement pour l’iPad partagé :

Utilisation avec des identifiants Apple gérés (Managed Apple IDs) Dans ce mode, l’appareil est configuré avec des comptes utilisateurs gérés. Les codes d’accès sont définis et administrés de manière centralisée via ces identifiants. À ce jour, il n’est pas possible pour les utilisateurs de modifier individuellement la durée de verrouillage automatique.

Utilisation en mode invité Dans ce mode, l’utilisateur se connecte en tant qu’invité, sans compte personnel ni code d’accès. Ce mode convient particulièrement aux environnements où les utilisateurs changent fréquemment et où aucune personnalisation des données n’est requise.

À noter : pour une utilisation flexible sans code d’accès, le mode invité est généralement recommandé.

Nom de l'appareil

Pour la version 26.4.0

Avec Relution, il est possible de définir le nom de l’appareil pour iOS, iPadOS et macOS. Une règle avec la configuration `Nom de l'appareil` peut être créée et attribuée à des groupes d’appareils.

Le nom peut être défini de manière statique, par exemple `Valise iPad`, ce qui signifie que tous les appareils du groupe auront ce même nom.

Pour plusieurs appareils dans un groupe, il peut être plus judicieux d’utiliser des variables.

Par exemple : `Valise ${device.model} ${user.name}` Ce qui donnera un nom tel que : `Valise iPad12,1 Max.Mustermann` Cela facilite la gestion et la vue d’ensemble de l’inventaire.

Conformité de l'application

La configuration de la politique “App Conformance” détermine quelles applications doivent être présentes sur un appareil iOS et lesquelles doivent en être exclues. Dans Relution, il est possible de configurer `App Conformance` de deux manières différentes.

Toutes les applications de la liste suivante ne sont pas autorisées

Il s’agit d’une `blocklist` classique. Toutes les applications de cette liste seront cachées sur les appareils iOS et les utilisateurs ne pourront pas y accéder. Les applications ne sont pas désinstallées. Par exemple, les applications système individuelles ou les applications de l’App Store public qui ne sont pas autorisées à être utilisées sur les appareils peuvent être stockées ici.

> Ce type de liste n'est pas compatible avec Relution Shared Device. Toujours utiliser la liste positive (Allowlist) en combinaison avec Relution Shared Device.

Pour la version 26.4.0

Autoriser toutes les applications de la liste suivante

Il s’agit de la “liste positive (Allowlist)” classique. Toutes les applications, qui sont stockées ici, peuvent être installées sur les appareils iOS, sont ensuite visibles par les utilisateurs et peuvent être utilisées.

Trois autres options peuvent être configurées :

Ajouter toutes les applications requises

Toutes les applications stockées dans la liste des “applications requises” sont automatiquement ajoutées à la “liste positive”. Cela permet d’économiser de l’effort et d’éviter les erreurs.

Ajouter tous les déploiements automatiques

Toutes les applications qui sont stockées dans la liste `Auto Deployments` pour les comptes utilisateurs ou groupes correspondants sont automatiquement ajoutées à la `Liste Positive`.

Cela permet d’économiser de l’effort et d’éviter les erreurs.

Liens web

- Bloquer les liens web
  Tous les liens web sont bloqués, qu’ils aient été introduits sur les appareils iOS par le biais d’une politique ou d’une action.
- Autoriser les liens web en plein écran.
  Seuls les liens web configurés pour le mode plein écran seront affichés.
- Autoriser tous les liens web.
  Tous les liens web seront autorisés. Le navigateur Safari est automatiquement activé ici.

Applications requises

Toutes les applications figurant dans cette liste sont automatiquement installées et les utilisateurs ne peuvent pas les supprimer des appareils iOS. Si une application de cette liste n’a pas été installée, l’appareil correspondant sera affiché comme “non conforme” dans l’inventaire de l’appareil. L’agent de résolution ne peut pas être ajouté à cette liste. Il est automatiquement installé sur les appareils lors de l’inscription.

En outre, les applications système ne doivent pas être incluses dans la liste des applications requises. Elles n’ont pas besoin d’être installées car elles se trouvent déjà sur les appareils. Il suffit de les ajouter à la liste positive.

Pour la version 26.4.0

Configurer la connexion SSO pour iOS

La technologie d'authentification unique (Single Sign-On, SSO) permet aux utilisateurs de se connecter une seule fois et d'accéder ensuite de manière fluide à différentes applications. Pour les appareils iOS en particulier, l'intégration de Microsoft SSO constitue une solution efficace pour combiner facilité d'utilisation et sécurité. Elle simplifie non seulement le quotidien grâce à des connexions simplifiées, mais réduit également les risques de sécurité et la charge de travail informatique. Ce guide constitue la base d'une configuration SSO avec iOS et Microsoft SSO.

Prérequis

Deux configurations et une application sont nécessaires dans Relution.

- `Conformité de l'application`
- `Authentification unique extensible`
- `Application VPP Microsoft Authenticator`

Pour la version 26.4.0

Configuration de la conformité de l'application

Il faut ici ajouter l'application Microsoft Authenticator → à la liste des applications requises. Celle-ci contient l'extension `com.microsoft.azureauthenticator.ssoextension` nécessaire pour Microsoft SSO.

Configuration de l'authentification unique extensible

Les points de configuration suivants peuvent servir de modèle minimal fonctionnel pour Microsoft SSO. Les points non mentionnés peuvent être laissés à leur valeur par défaut. La configuration finale doit être adaptée à l'environnement concerné.

- Identifiant de l'extension
  - `com.microsoft.azureauthenticator.ssoextension`
- Type
  - `Redirection`
- 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`

Interaction utilisateur

Une fois la configuration terminée et attribuée aux appareils, les utilisateurs peuvent désormais se connecter à un service Microsoft dans le navigateur, par exemple Outlook, ou à une application Microsoft, par exemple Teams, et sont ainsi automatiquement connectés dans toutes les autres applications compatibles.

Pour la version 26.4.0

App to VPN assignment

Lors de la mise en place d'un VPN inter-appareils, toutes les données des appareils sont acheminées via le réseau privé. Il peut arriver qu'une entreprise souhaite configurer un VPN uniquement pour ses applications d'entreprise. Apple permet de configurer des connexions VPN pour les iPhones, les iPads et les MacBooks, application par application. Dans ce cas, les administrateurs peuvent contrôler exactement les données qui transitent par le VPN. La configuration d'une politique de mappage entre applications et VPN aide les entreprises à séparer le trafic au niveau des applications, ce qui permet de séparer les données personnelles de celles de l'entreprise.

Prérequis

Une association app-to-VPN peut être mise en place directement par Relution. Cela ne fonctionne que pour les applications qui sont installées et gérées par le MDM sur les appareils. En outre, les administrateurs peuvent également configurer les connexions VPN pour établir automatiquement des connexions VPN pour des domaines spécifiques lorsqu'une application correspondante demande une connexion réseau.

Pour la version 26.4.0

Relution prend en charge les types de connexion suivants pour établir une connexion VPN sur les appareils iOS et macOS :

- IPSec
- JuniperSSL
- SonicWALL
- AnyConnect Legacy
- AnyConnect
- IKEv2
- SSL personnalisé.

Comment configurer l'app-to-VPN pour les appareils iOS et macOS.

1. Deux configurations de politique sont nécessaires pour mettre en place un VPN utilisé pour des applications individuelles :
    - VPN

    - mappage App-to-VPN.
2. Dans la configuration du VPN, l'option `Connexion VPN pour les applications et les comptes` doit être activée et selon le type de VPN, tous les champs nécessaires doivent être remplis.

3. Dans la configuration 'app-to-VPN-association', les applications peuvent être définies pour la connexion VPN stockée.

4. Des paramètres supplémentaires de domaine et d'email sont possibles dans la configuration VPN sous `Per-Account-VPN`.

Pour la version 26.4.0

Polices

Avec Relution, il est possible de distribuer des polices de caractères aux appareils iOS et macOS par le biais d'une politique. Cette police est ensuite disponible dans les applications prises en charge telles que Keynote. La police ne peut pas être définie comme police système et n'est sélectionnable que dans les applications.

Exigences

- Une police au format `otf` ou `ttf` (les autres formats comme `ttc` ou `woff` ne sont pas pris en charge)
- Une politique avec la configuration de la police
- Des applications qui permettent la sélection d'une police installée, par exemple `Keynote`

Gérer les polices

Les polices sont gérées de manière centralisée sous `Paramètres` → `Polices` avant de pouvoir être assignées à une politique.

Pour la version 26.4.0

Téléverser une police

Utiliser Ajouter pour téléverser une nouvelle police. Un nom (255 caractères max.) et le fichier de police au format `otf` ou `ttf` sont requis.

Visibilité (portée)

La visibilité d'une police est déterminée automatiquement par l'organisation dans laquelle elle a été créée — elle ne peut pas être sélectionnée manuellement :

- Globale : Créée dans l'organisation globale → disponible dans toutes les organisations.
- Locale : Créée dans une organisation classique → disponible uniquement là.

La liste d'aperçu affiche également la portée, la date de création/modification, ainsi que l'auteur de la modification, et peut être exportée en CSV.

Remarque : Seules les polices appartenant à l'organisation concernée peuvent être téléchargées — les polices héritées d'autres organisations via une portée globale ne peuvent pas être

téléchargées.

Suppression

Les polices peuvent être supprimées individuellement ou via une sélection multiple ; la modification d’une police existante n’est pas possible.

> La suppression ne vérifie pas si la police est encore utilisée par une politique. Supprimer une police encore utilisée entraîne une violation de conformité sur les appareils concernés lors du prochain transfert de configuration.

Utilisation

La police souhaitée peut être téléchargée dans Relution sous `Home` → `Settings` → `Fonts` → `Add`.
En outre, un nom doit être donné à la police.
Ensuite, elle doit être ajoutée à une politique iOS ou macOS dans la configuration `Font`.

Pour la version 26.4.0

Disposition de l'écran d'accueil

La disposition de l’écran d’accueil permet aux administrateurs de contrôler l’agencement des applications et des dossiers sur les appareils iOS et iPadOS. Il existe deux types de disposition :

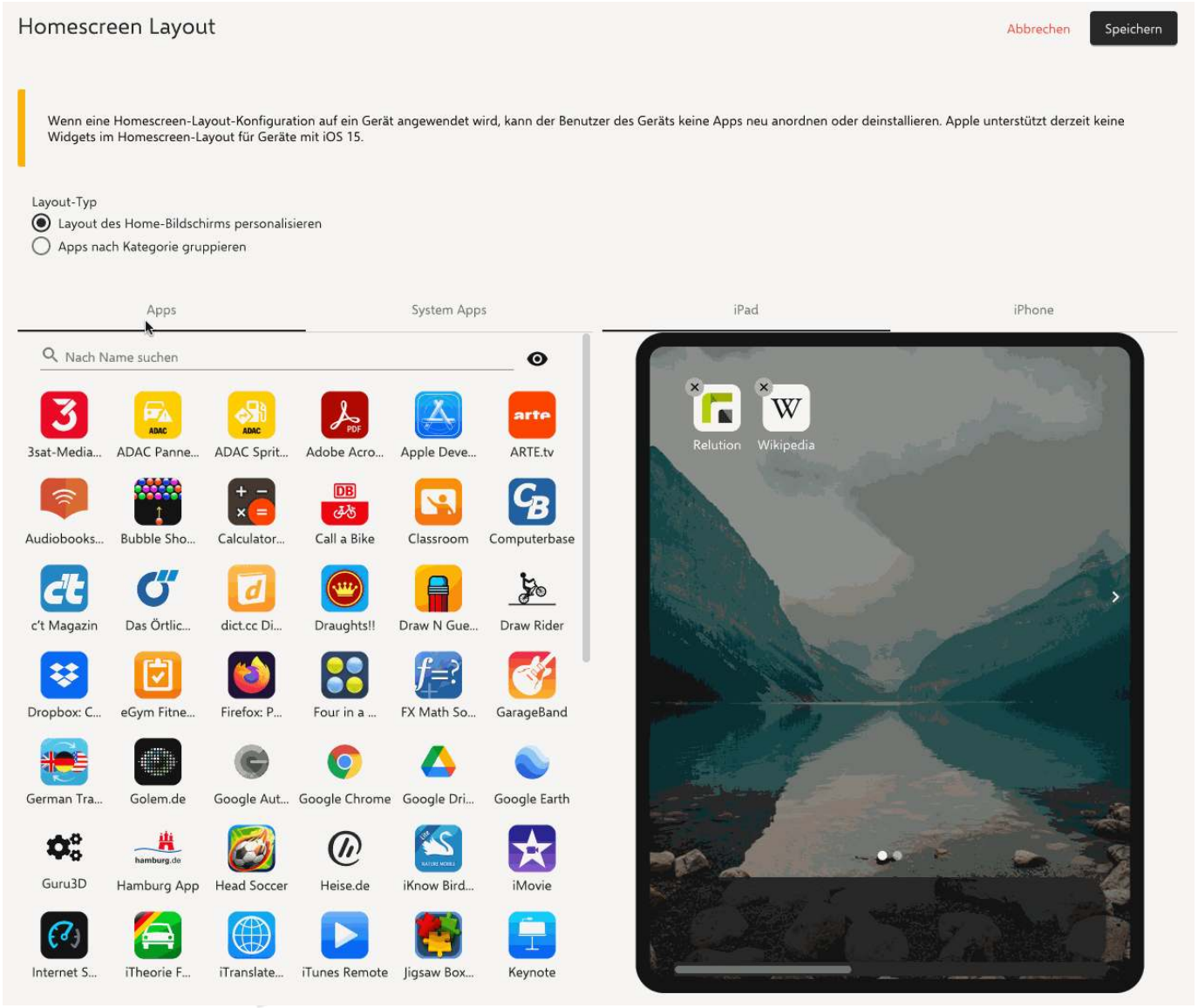
1. Personnaliser la présentation de l’écran d’accueil.
2. Regrouper les apps par catégorie.

> Lorsqu'une configuration Homescreen Layout est appliquée à des appareils, les utilisateurs ne peuvent pas réorganiser ou désinstaller manuellement les apps sur les appareils. Apple ne prend actuellement pas en charge les widgets Homescreen Layout pour les appareils fonctionnant sous iOS 15.

Personnaliser l’écran d’accueil

Il est possible de personnaliser la présentation en classant les applications individuellement. Des dossiers peuvent être créés pour catégoriser les applications.

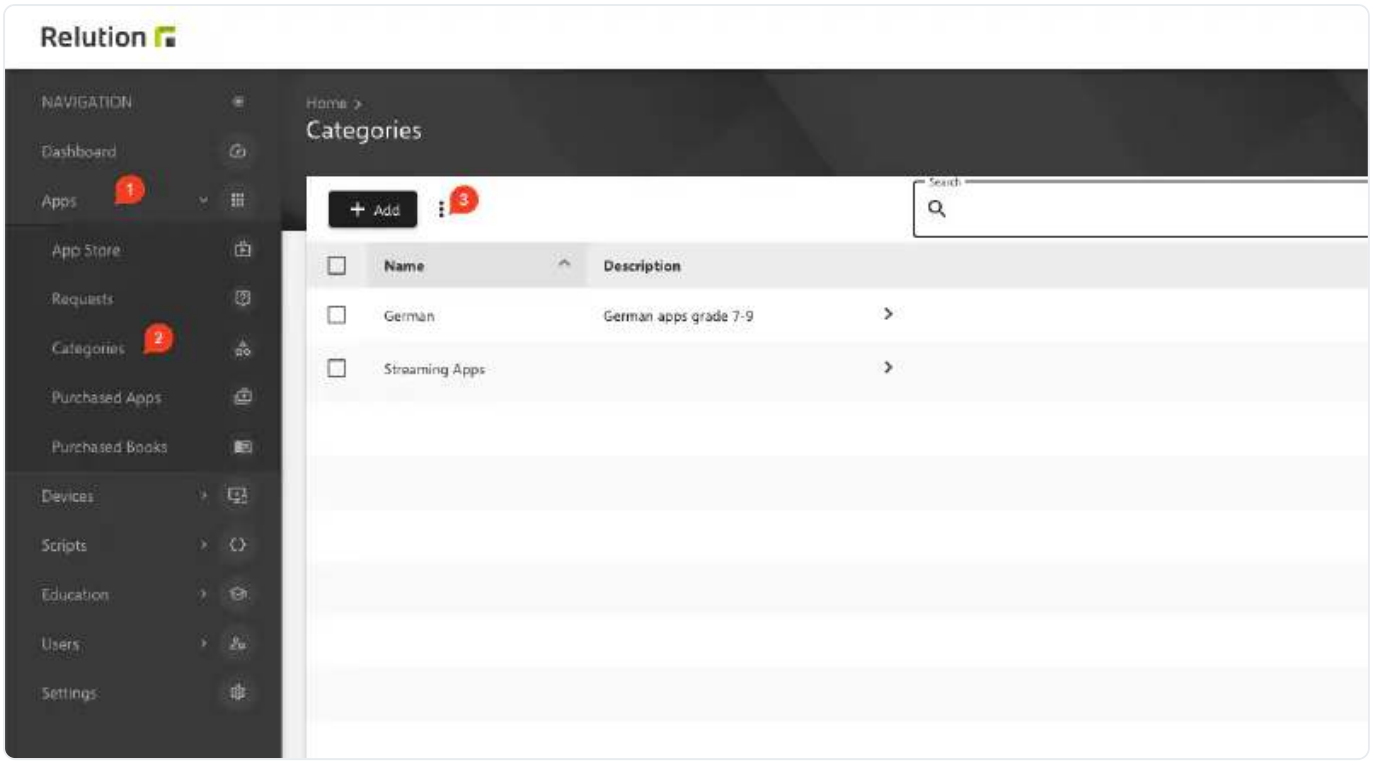
Pour la version 26.4.0



Maintenir la souris immobile tout en glissant-déposant sur une autre application créera automatiquement un dossier. Homescreen Layout est limité à 20 applications par page.

Regrouper les applications par catégorie

Cette présentation regroupe les applications installées en fonction des catégories créées dans le portail Relution. Les applications système sont regroupées automatiquement.



Pour la version 26.4.0

Relution Decon (filtre)

À partir de la version 5.27, Relution pour iOS permet la configuration d'un filtre de contenu basé sur DNS. Cette fonctionnalité assure un accès Internet sécurisé et ciblé en restreignant l'accès à certains sites web et applications. Grâce à la catégorisation des contenus basée sur l'IA, Relution Decon fournit également un contrôle parental complet avec des options avancées de configuration.

Qu'est-ce que Relution Decon ?

Relution Decon est un module complémentaire basé sur l'IA pour iOS et iPadOS qui filtre le contenu en temps réel, créant un environnement numérique sécurisé. Grâce au contrôle de contenu basé sur DNS, Decon bloque les sites web et applications indésirables, permettant aux utilisateurs de travailler et d'apprendre dans un espace protégé et sans distraction.

Relution Decon utilise un proxy DNS pour transmettre toutes les requêtes au serveur Decon. Les sites web sont classés et soit autorisés, soit bloqués selon les règles définies par les politiques. Toutes les communications sont chiffrées SSL, garantissant la sécurité des activités des utilisateurs.

Pour la version 26.4.0

Application Decon

L'application Decon est automatiquement déployée sur les appareils iOS lors de l'installation de la politique. Elle surveille les requêtes DNS de l'appareil et garantit que seuls les contenus autorisés sont accessibles.

Fonctionnalités de l'application :

- Active un proxy DNS global, qui ne peut pas être désactivé par l'utilisateur
- Affiche le statut actuel de Relution Decon
- Fournit des informations sur les sites bloqués et les catégories de filtrage appliquées

Recommandation : disposer d'un nombre suffisant de licences VPP avant le déploiement.

Configuration VPP dans Relution →
Relution Decon sur l'Apple App Store →

Politique Decon

Dans la politique des appareils, cliquer sur `Ajouter` → `Relution Decon`. Cette politique installe automatiquement l'application Decon sur les appareils iOS associés et agit comme proxy pour toutes les requêtes DNS.

La configuration est complétée lors de la publication de la politique.

Hiérarchie de configuration des politiques (de la plus haute à la plus basse priorité)

1. Applications autorisées (Allow Apps)
2. Applications bloquées (Block Apps)
3. Sites web autorisés (Allow Websites)
4. Sites web bloqués (Block Websites)
5. Catégories bloquées

Decon dans Relution Teacher

Decon peut être sélectionné et géré dans les profils de classe avec Relution Server 5.32.0 et Relution Agent 5.19.0. Les appareils des élèves doivent avoir une politique Decon assignée.

En savoir plus sur Relution Teacher →

Pour la version 26.4.0

Classification par catégorie

Relution Decon attribue automatiquement chaque site web à une catégorie. Les administrateurs peuvent définir quelles catégories doivent être bloquées :

Catégorie	Description	Exemples
Non adapté aux jeunes	Sites inappropriés pour les jeunes	Pornographie, Violence, Armes, Drogues, Jeux d'argent, Divertissement adulte, Shopping adulte, Rencontres, Google Safe Search
Publicité	Sites publicitaires	Fournisseurs de publicité

Catégorie	Description	Exemples
Communication	Services de communication	Email, Messenger, Appels (vidéo)
Réseaux sociaux	Contenus de réseaux sociaux	Facebook, Instagram, TikTok, etc.
Divertissement	Sites de divertissement comme streaming ou jeux	Films, Jeux, Vidéos
Musique	Services de streaming musical	Spotify, Tidal, etc.
Actualités	Sites d’information et magazines	News, Météo
Shopping	Boutiques en ligne (hors contenus adultes)	Amazon, eBay, etc.
Travail	Sites liés au travail	Office, Partage de fichiers, Intranet
Éducation	Sites éducatifs pour l’apprentissage	Wikipedia, Google Scholar
IA générative	Sites liés à l’intelligence artificielle	ChatGPT, Perplexity.ai, etc.
Phishing	Sites potentiellement frauduleux	Escroqueries potentielles, Vol de données
Autres	Tous les autres sites	Restants

Listes Allow et Block

- Sites autorisés / Sites bloqués : Permet de spécifier des domaines autorisés ou bloqués indépendamment des catégories. Seul le domaine doit être indiqué, pas le chemin.
- Applications autorisées / Applications bloquées : Permet de contrôler l’accès Internet des applications ; les fonctions de base restent accessibles si aucune connexion Internet n’est

nécessaire.

Configuration DNS avancée

Serveurs DNS sur l’appareil : Des serveurs DNS alternatifs peuvent être configurés si le DNS Relution Decon n’est pas disponible. Fallback : Cloudflare Families DNS (1.1.1.3).

Serveur DNS Relution Decon : Un serveur DNS alternatif peut remplacer le DNS standard sur le serveur Decon. Les adresses IP (UDP) ou DNS-over-HTTPS (DoH) comme Zero ou Quad9 sont configurables.

Limitations

- Mise en cache : Les sites bloqués et les modifications de politique peuvent être mis en cache jusqu’à 1 minute ; les changements peuvent ne pas être appliqués immédiatement.
- Indépendance du chemin : Le DNS fonctionne au niveau du domaine, il est impossible de définir des règles différentes pour des chemins différents d’un même domaine.
- Blocage des applications : Seul l’accès Internet est bloqué ; les fonctions de base et le contenu mis en cache restent accessibles.

Pour la version 26.4.0

Appareil partagé Relution

Relution propose son propre mode multi-utilisateurs pour les appareils iOS. Pour cela, les utilisateurs se connectent aux appareils via l'agent Relution avec un utilisateur (compte) Relution existant. Un Apple ID (géré) n'est pas nécessaire. Avec Relution, il est également possible de se connecter avec un compte utilisateur LDAP. Contrairement au mode multi-utilisateur d'Apple, `Shared iPad`, le mode `Relution Shared Device` peut être commodément activé et désactivé via la configuration de la politique appropriée.

> La condition préalable à l'utilisation de cette configuration est que les appareils cibles soient en mode supervisé.

Notes

Le mode `Relution Shared Device` installe toutes les applications requises à la connexion de l'utilisateur et les désinstalle automatiquement à la déconnexion de l'utilisateur. Cela supprime automatiquement tout le contenu créé temporairement dans les applications des appareils. De cette manière, Relution garantit une utilisation des appareils conforme à la vie privée lorsqu'ils sont utilisés par plusieurs utilisateurs via le mode `Relution Shared Device`.

Pour la version 26.4.0

> Les applications système, telles que le navigateur Safari ou l'application Photos, ne peuvent pas être désinstallées du côté d'Apple. Cela signifie qu'aucune donnée créée temporairement ne peut être supprimée pour ces apps. Dans ce cas, il est recommandé de passer à des applications alternatives telles que le navigateur Firefox ou la fonction photo de Relution.

La réinstallation des applications peut provoquer des pics de charge importants sur le réseau. Par conséquent, la configuration `App Conformance` doit être maintenue aussi légère que possible. Dans ce cas, la "liste positive (Allowlist)" ne devrait contenir que très peu d'applications de petite taille. Les utilisateurs peuvent facilement installer des applications à partir du Relution App Store via l'agent Relution, ou les faire installer dans le contexte de l'école par un enseignant en utilisant l'application Relution Teacher App et un profil d'enseignant.

En termes de volume de données réseau, il n'est pas conseillé d'avoir toutes les applications installées sur un dispositif partagé Relution à tout moment.

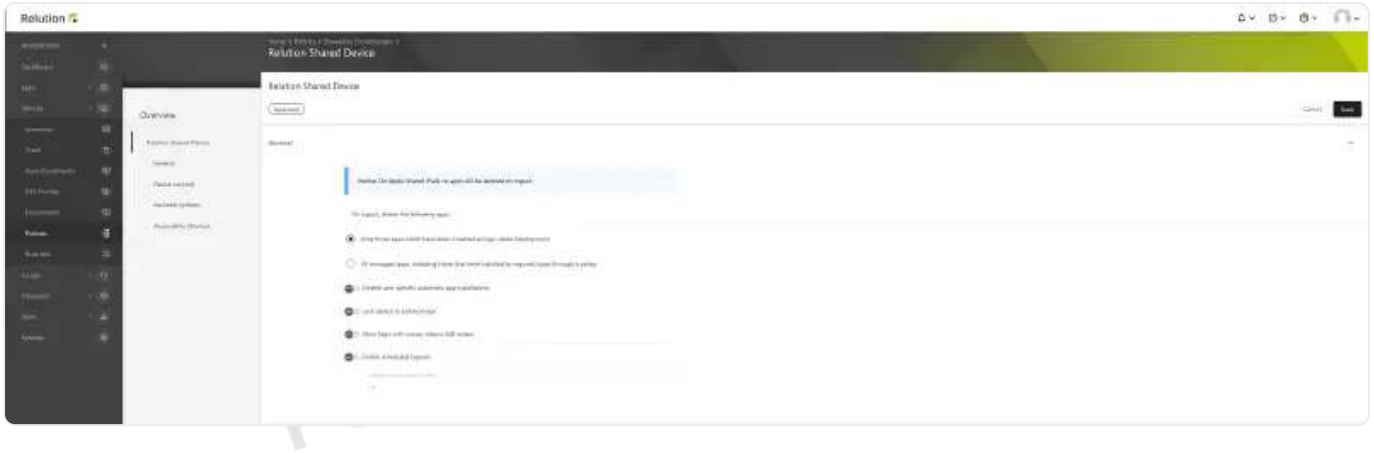
Si le mode `Relution Shared Device` est utilisé en combinaison avec la fonctionnalité Apple `Shared iPad`, aucune désinstallation des applications installées n'a lieu. Dans ce cas d'utilisation, le travail conforme à la protection des données n'est possible que si les utilisateurs

se connectent en tant qu'invités en mode Apple `Shared iPad`. En mode `Guest`, toutes les données temporaires sur les appareils sont automatiquement supprimées par la fonctionnalité Apple `Shared iPad` après la déconnexion de l'invité.

Le mode invité de l'iPad partagé d'Apple n'est pas compatible avec l'application Apple Classroom. Dans le contexte scolaire, cela signifie que les iPad des élèves dans la configuration ci-dessus n'apparaîtront pas comme étant en ligne dans l'application Apple Classroom de l'enseignant.

La conformité des applications ne fonctionne que sous la forme d'une liste positive en combinaison avec le mode Périphérique partagé de Relution. Les listes de blocage n'ont aucun effet.

Paramètres de Relution Shared Device



Avec iOS 17.x, l'utilisation de la configuration de restriction allowCloudKeychainSync false entraîne un ralentissement de la connexion sur les appareils partagés Apple

- Les quatre premières options de la configuration `Relution Shared Device` sont les plus importantes. Il faut tout d'abord décider si seules les applications spécifiques à l'utilisateur installées via `Auto-Deployments` doivent être supprimées lorsque l'utilisateur se déconnecte, ou si toutes les applications installées via Relution doivent être supprimées. Selon la configuration, la deuxième configuration garantit que plus d'applications sont désinstallées.
- La case à cocher pour désactiver `User specific auto app installment` désactive les déploiements automatiques.
- La case à cocher pour l'option `User specific auto app install` désactive les déploiements automatiques existants au niveau de l'utilisateur ou du groupe.

- La case à cocher de l'option `Lock device and force login` met l'Agent de Relution en `Single App Mode` avant la connexion de l'utilisateur. Les utilisateurs doivent donc d'abord effectuer une connexion réussie pour quitter l'Agent de Relution et ensuite accéder à l'appareil. Cette option ne fonctionne pas sur les Apple Shared iPads.

> Il n'est pas recommandé d'utiliser la dernière option, car dans ce mode, il n'y a pas d'accès aux paramètres de l'appareil et, entre autres, aucune connexion WiFi ne peut être établie manuellement si aucune configuration réseau n'est appliquée. Si l'option est désactivée, les utilisateurs pourront ouvrir les paramètres de l'appareil sans se connecter.

Les données qui doivent être sauvegardées doivent être soit stockées sur un serveur externe via `Relution Files`, soit stockées sur un système externe via des services comme Own- ou Nextcloud.

Pour cette configuration, consulter également notre
Aide à la décision pour le mode multi-utilisateur →

Pour la version 26.4.0

Relution Files

Pour iOS, Relution offre la possibilité d'intégrer des partages de fichiers locaux, également appelés lecteurs réseau, via SMB et WebDAV. En se connectant à des solutions de serveurs scolaires ou d'entreprise, par exemple, il est possible d'accéder à des documents et contenus pertinents et de stocker des données et des résultats de travail en toute sécurité sur un serveur central.

Avantages de Relution Files

Les données ne doivent pas être stockées dans un Cloud non sécurisé avec des serveurs situés en dehors de l'UE si un travail conforme au RGPD est nécessaire. De même, il est conseillé de ne pas stocker les données directement sur les appareils si ceux-ci sont utilisés par plusieurs utilisateurs. L'enregistrement et le stockage de documents sur des serveurs locaux propres via `Relution Files` garantit la sécurité et la souveraineté des données pour tous les utilisateurs.

Pour la version 26.4.0

Configurer les lecteurs du réseau local pour Relution Files

Les partages de fichiers locaux peuvent être configurés dans Relution de deux manières :

Configurer manuellement les Relution Files dans l'Agent de Relution

Sous File Shares dans l'application `Relution Agent` pour iOS, les lecteurs réseau peuvent être configurés sous `Add Share`. Pour ce faire, il faut configurer les champs de saisie suivants :

- URL du serveur
- Nom d'utilisateur (ou ID utilisateur)
- Mot de passe
- Facultatif : Single Sign On (connexion unique) (utilise l'utilisateur Relution actuel des appareils).

Les URL du serveur doivent être saisies dans un sous-menu comme suit :

- Pour SMB au format `server/share`.
- Pour WebDAV au format `server/path/`.

En outre, les paramètres suivants sont importants :

- `https://` pour WebDAV.
- Pour SMB, après le `server`, un `share` doit être spécifié.
- Selon les spécifications du protocole, les sous-chemins ne sont pas autorisés ni pris en charge par SMB `(//server/path/subpath/subpath)`.

Cela masque les champs déjà configurés par Relution du côté du serveur. Une exception est le nom d'utilisateur, qui est affiché à des fins de contrôle mais ne peut pas être modifié. De cette manière, les utilisateurs ne peuvent pas voir les URL du serveur.

En appuyant sur le bouton "Ajouter", il est possible de configurer un maximum de cinq URL de serveur supplémentaires. Ceci n'est possible que s'il n'y a pas de configuration de politique avec des partages de fichiers sur les appareils.

Après avoir ajouté ou modifié une entrée, la validité des entrées est automatiquement vérifiée (la connexion aux serveurs est établie). Dès que la connexion est établie, une coche verte apparaît à côté de l'URL en guise de confirmation. Dans le cas contraire, l'URL, le nom d'utilisateur ou le mot de passe n'est pas correct.

Configuration automatique des Relution Files via les politiques

Pour la version 26.4.0

Pour éviter aux utilisateurs d'entrer manuellement les noms des serveurs et des partages, les paramètres attendus par l'Agent de Relution peuvent être transmis via la configuration de la politique. Cela se fait en ajoutant la configuration `Relution Files` à une politique iOS. La configuration doit contenir les paramètres suivants :

- server/share URL au format `server/share`.
  - Pour WebDAV, `https://` doit être spécifié.
  - Pour SMB, un `share` doit être spécifié après le `server`.
- Nom d'utilisateur (il est également possible d'utiliser les caractères génériques connus de Relution comme `${user.name}`).
- mot de passe.
- Ou encore Single Sign On :
  - Avec les données d'accès actuellement utilisées par les utilisateurs avec saisie d'un mot de passe unique dans Relution (également possible en mode Relution Shared Device sans saisie de mot de passe).
  - Les partages configurés sont disponibles immédiatement.
  - Lorsqu'un nouvel utilisateur se connecte en mode Relution Shared Device, les partages sont reconfigurés, de sorte que la connexion au partage de l'utilisateur précédent n'est plus disponible pour les nouveaux utilisateurs.

Apple Configurator 2

Cette configuration de politique peut être utilisée pour transférer des fichiers `.mobileconfig` vers des appareils Apple. Ces fichiers peuvent contenir, par exemple, une connexion WiFi et le certificat correspondant.

Configuration

Pour pouvoir transférer un fichier `.mobileconfig` vers des appareils, les informations correspondantes doivent être stockées et nommées directement dans la configuration de Relution.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/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>
```

Il n'est pas possible d'utiliser un fichier mobileconfig dans lequel un grand nombre de configurations sont stockées.

Pour la version 26.4.0

Configuration gérée (iOS)

Il est possible de préconfigurer certaines apps avec la configuration de politique `Application gérée (Managed App)`. Cette configuration n'est disponible que pour les appareils iOS à partir de la version 7 et les appareils macOS à partir de la version 11+.

Configuration

Spécifier l'ID du bundle de l'application à configurer et joindre un payload de configuration d'application valide. Dans la charge utile, il est possible d'utiliser les espaces réservés qui apparaissent au bas de la page. Par exemple, une application client de messagerie peut être configurée en utilisant le caractère générique `${user.email}`. De cette façon, la configuration peut être rendue utilisable pour différents utilisateurs. Les espaces réservés seront remplis lorsque la configuration sera poussée vers les appareils.

> L'application à configurer doit déjà être installée sur les appareils avant que la configuration de l'application ne soit appliquée. Si l'app est installée sur les appareils dans la même politique, veiller à exécuter la configuration de l'app après l'avoir installée en l'ajoutant ultérieurement à la liste des configurations.

Pour la version 26.4.0

En principe, le fabricant de chaque application est responsable des options de configuration. Nous avons listé ici quelques exemples qui fonctionnaient avec les applications au moment de la rédaction de ce document. Nous ne garantissons pas que ce sera toujours le cas.

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/DTD
<plist version="1.0">
<dict>
    <key>ManagedAppConfigurationVersion</key>
```

```
    <string>1</string>
    <key>LicenseKey</key>
    <string>AAAA-BBBBBB-CCCCCC-DDDDDD-123456-V3</string>
</dict>
</plist>
```

Des informations supplémentaires peuvent être trouvées sur le site web de Goodnotes →

Microsoft Outlook pour 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/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>${user.email}</string>
  <key>com.microsoft.outlook.EmailProfile.AccountDomain</key>
  <string></string>
  <key>com.microsoft.outlook.EmailProfile.ServerAuthentication</key>
  <string>Nom d'utilisateur et mot de passe</string>
  <key>IntuneMAMAllowedAccountsOnly</key>
  <string>Activé</string>
  <key>IntuneMAMUPN</key>
  <string>${user.email}</string>
</dict>
</plist>
```

Microsoft Outlook pour un serveur Exchange sur site

```
com.microsoft.Office.Outlook
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTD
<plist version="1.0">
<dict>
  <key>com.microsoft.outlook.EmailProfile.AccountType</key>
  <string>BasicAuth</string>
  <key>com.microsoft.outlook.EmailProfile.EmailAccountName</key>
  <string>${user.fullname}</string>
  <key>com.microsoft.outlook.EmailProfile.ServerHostName</key>
  <string>exchange.server.name</string>
  <key>com.microsoft.outlook.EmailProfile.AccountDomain</key>
  <string>nomdedomaine</string>
  <key>com.microsoft.outlook.EmailProfile.EmailAddress</key>
  <string>${user.email}</string>
  <key>com.microsoft.outlook.EmailProfile.EmailUPN</key>
  <string>${user.email}</string>
  <key>com.microsoft.outlook.EmailProfile.ServerAuthentication</key>
  <string>Nom d'utilisateur et mot de passe</string>
  <key>IntuneMAMAllowedAccountsOnly</key>
  <string>Désactivé</string>
  <key>IntuneMAMUPN</key>
  <string>${user.email}</string>
</dict>
</plist>
```

SecurePIM pour Office365

```
com.virtual-solution.securepim-enterprise
```

```
<?xml version="1.0" ?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://www.apple.com
<plist version="1.0">
 <dict>
  <key>license</key>
    <string>votre-clé-de-licence</string>
    <key>activeSyncServer</key>
    <string>outlook.office365.com</string>
    <key>userEmail</key>
    <string>${utilisateur.email}</string>
    <key>activeSyncUser</key>
    <string>${user.email}</string>
    <key>deviceSerialNumber</key>
    <string>${device.serialnumber}</string>
    <key>recipientCertificateEmail</key>
    <string>${utilisateur.email}</string>
    <key>allowTouchIDAuthentication</key>
    <string>true</string>
    <key>callKitEnabled</key>
    <string>true</string>
  </dict>
 </plist>
```

Pour la ve

Configuration incomplète

Lorsqu'une configuration existante est exportée depuis un autre système MDM au format XML puis convertie en fichier `plist`, une valeur marquée comme optionnelle et laissée vide peut devenir une valeur `<string></string>` vide dans le `plist`. La clé `subscriptionWebServiceEndPointURL` est notamment concernée par ce comportement.

Dans ce cas, SecurePIM affiche en permanence le message « Configuration incomplète » au démarrage de l'application, bien que la clé fonctionnait sans valeur dans le système d'origine. Le fait de saisir une valeur non vide dans la clé concernée, ou de supprimer entièrement la clé du `plist`, résout le problème.

FileBrowser for Education

```
com.stratospherix.filebrowsereducation
```

Configuration d’un partage SMB

```
<?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>Mon NAS</string>
  <key>1domaine</key>
  <string>office.mwaysolutions.com</string>
  <key>1flags</key>
  <integer>1746</integer>
  <key>1machinename</key>
  <string>smb://yoursmbservershare/</string>
  <key>1username</key>
  <string>${utilisateur.email}</string>
  <key>1vpntype</key>
  <integer>0</integer>
  <key>waitForSearchButton</key>
  <integer>0</integer>
</dict>
</plist>
```

IBM Verse client

```
com.ibm.lotus.traveler
```

Show full configuration example

Pour la version 26.4.0

Mode d'application unique

Cette configuration de politique peut être utilisée pour définir les applications qui s’exécutent sur les appareils en mode “application unique”. Les utilisateurs ne peuvent alors pas quitter l’application.

Configuration

Sélectionner d’abord l’application à afficher en “Single App Mode”. Sélectionner ensuite les options souhaitées pour ce mode afin d’obtenir des restrictions supplémentaires lors de l’affichage de l’application sélectionnée.

Contrôle des appareils

- `Désactiver l'entrée tactile` désactivé, si défini.
- Désactiver la rotation automatique de l’écran, si elle est activée.
- `Désactiver les touches de volume` désactivé, si défini.
- `Disable side switches` (désactiver les commutateurs latéraux) Les commutateurs de sonnerie situés sur le côté des appareils sont désactivés lorsqu’ils sont réglés en position “silencieux”. S’ils sont désactivés, le comportement de la sonnerie dépend de la position dans laquelle se trouvait le commutateur lorsqu’il a été désactivé pour la première fois.
- `Désactivation de l'interrupteur marche/arrêt` désactivé, s’il est activé.
- `Disable auto lock` Les appareils ne se mettent pas automatiquement en veille après une période d’inactivité, si cette option est activée.

Pour la version 26.4.0

Aides au fonctionnement

- `VoiceOver` Autoriser la personnalisation, si elle est définie.
- `Zoom` Permet la personnalisation, si défini.
- `Inverser les couleurs` Permet la personnalisation, si elle est définie.
- `AssistiveTouch` Permet l’ajustement, si défini.
- `Sélection de lecture` Sélection de parole activée, si définie.
- `Mono Audio` activé, si défini.

Raccourci pour l’assistance à l’opérateur

- `VoiceOver` activé, si défini. La valeur par défaut est désactivée.
- `Zoom` activé, si défini. La valeur par défaut est désactivée.
- `Invert colors` (Inverser les couleurs) activé, si défini. La valeur par défaut est désactivée.
- `AssistiveTouch` activé, si défini. La valeur par défaut est désactivée.

Filtre pour le contenu

Il s’agit d’un filtre de contrôle parental qui peut être activé ou désactivé sur les appareils iOS et macOS.

> Relution n'a aucun contrôle sur le contenu filtré. Apple est responsable de la gestion du filtre. En outre, il n'est pas possible de déterminer si le contenu répond ou non à une classification d'âge spécifique.

Pour la version 26.4.0

Configuration

Néanmoins, les sites web peuvent être ajoutés à une `liste bloquée (Blocked URLs)` ou à une `liste positive (Allowed URLs)`. Dans la configuration, le filtre est en principe actif si la case à cocher `Enable Auto-Filter` est activée :

Dans certaines circonstances, le filtre n’atteint pas toujours le résultat souhaité, car les URL qui ne contiennent pas de contenu préjudiciable aux mineurs sont parfois filtrées.

Pour filtrer une URL qui n’est pas bloquée par le filtre automatique, la placer dans la liste des “URL bloqués”. Pour débloquer une URL filtrée, la placer dans la liste des “URL autorisées”.

Il convient d’accorder une attention particulière à la liste des “signets déterminés”. Si des entrées sont faites dans cette liste, seules ces URL sont autorisées. Indépendamment de ce qui a été configuré dans la liste `Allowed URLs`. De plus, ces “Signets déterminés” sont créés en tant que signets dans Safari.

Si le filtre de contenu est actif, la fonction Supprimer ne peut plus être exécutée sur les appareils dans les réglages de l’historique de Safari et des données des pages web.

Temps de verrouillage

En définissant des délais de verrouillage pour les appareils iOS, il est possible d'empêcher l'utilisation active. Si la configuration de la politique est active, toutes les applications seront masquées et seront à nouveau disponibles après l'expiration du délai.

Notifications

A partir de la version 5.25, Relution pour iOS permet de préconfigurer les paramètres des notifications pour les applications individuelles. La configuration de la politique `Notifications` peut être sélectionnée à cette fin.

Configuration

Pour configurer les paramètres de notification, une application à laquelle le paramètre doit être appliqué doit être sélectionnée. Les options de sélection habituelles 'Relution App Store`,` Apple App Store`,` iOS System Apps`et` Manual entry` sont disponibles à cet effet. Une fois qu'une application a été sélectionnée, elle peut être configurée en conséquence.

Pour la version 26.4.0

À ce stade, des notifications peuvent être activées sur l'appareil pour l'application correspondante. Cela comprend l'affichage dans CarPlay, sur l'écran de verrouillage ou dans le centre de messages. Le type de notification peut être défini comme une bannière temporaire ou permanente.

Des messages d'avertissement critiques peuvent également être activés et des sons peuvent être activés.

Le type de prévisualisation peut également être défini. Le choix se fait entre `Toujours`, `Déverrouillé` et `Jamais`.

Il est également possible de regrouper les applications.

Exchange

Avec Relution, une configuration Microsoft Exchange pour les appareils iOS peut être transférée vers l'application Mail native. Cela évite à l'utilisateur final une configuration complexe. Selon l'authentification → choisie, l'appareil ne nécessite que le mot de passe de l'utilisateur, une connexion via OAuth ou aucune saisie.

Général

- Utiliser la passerelle de messagerie sécurisée (Secure Mail Gateway) : Si cette fonction est activée, l'URL et le domaine de la passerelle de messagerie sécurisée sont distribués aux appareils à la place de l'URL et du domaine Exchange. Ainsi, les appareils communiquent avec le serveur Exchange via la passerelle de messagerie sécurisée.
- Hôte Exchange
- Domaine Exchange
- Le serveur Exchange utilise SSL pour l'authentification

Pour la version 26.4.0

Paramètres du compte

- Nom du compte
- Utiliser l'adresse e-mail de l'utilisateur `${user.email}`
- Adresse e-mail

Nom d'utilisateur

- Manuel
- Utiliser le nom d'utilisateur de l'utilisateur `${user.name}`
- Utiliser l'adresse e-mail de l'utilisateur `${user.email}`

Les champs OAuth, Mot de passe et Certificat déterminent la manière dont l'appareil se connecte au serveur Exchange. Ils sont décrits dans la section Authentification →.

Services activés

- Activer le calendrier
  - L'utilisateur peut activer et désactiver le calendrier
- Activer la messagerie
  - L'utilisateur peut activer et désactiver les e-mails

- Activer les notes
  - L’utilisateur peut activer et désactiver les notes
- Activer les rappels
  - L’utilisateur peut activer et désactiver les rappels
- Activer les contacts
  - L’utilisateur peut activer et désactiver les contacts

Paramètres de synchronisation

- Autoriser le déplacement
- Empêcher l’envoi de mails via la feuille de partage
- Synchroniser les adresses e-mail récentes
- Activer la signature S/MIME
- La signature S/MIME peut être remplacée par l’utilisateur
- Activer le chiffrement S/MIME par défaut
- Activer l’option de chiffrement par message
- Le chiffrement S/MIME peut être remplacé par l’utilisateur
- Période de synchronisation
  - Aucune limite
  - 1 jour
  - 3 jours
  - 1 semaine
  - 2 semaines
  - 1 mois

Pour la version 26.4.0

Authentification

Trois méthodes sont disponibles pour la connexion au serveur Exchange : un mot de passe, OAuth ou un certificat. Relution ne connaît pas les mots de passe des utilisateurs et ne peut donc pas les transférer par utilisateur.

Mot de passe

Une valeur saisie dans le champ Mot de passe est transférée telle quelle à tous les appareils auxquels la politique est attribuée. Il n’existe pas d’espace réservé pour le mot de passe de l’utilisateur concerné. Pour les comptes personnels, le champ reste donc généralement vide et le mot de passe est saisi sur l’appareil.

C’est le système d’exploitation qui détermine si iOS demande lui-même le mot de passe. Relution ne peut pas déclencher de demande de mot de passe dans l’application Mail.

OAuth

Si OAuth est activé, l'utilisateur se connecte via la page de connexion du fournisseur d'identité, p. ex. Microsoft Entra ID pour Exchange Online ou Exchange Server avec Hybrid Modern Authentication. Dans ce cas, le champ Mot de passe est verrouillé.

Certificat

Avec un certificat, l'appareil se connecte au serveur Exchange sans mot de passe. Le serveur Exchange doit accepter la connexion par certificat. Deux variantes sont disponibles :

- Sélectionnez un certificat : un certificat précis ou un modèle de certificat de la Gestion des certificats → est utilisé.
- Utiliser un certificat utilisateur : le certificat de l'utilisateur concerné est utilisé. Si un utilisateur possède plusieurs certificats de ce type, le champ Nom du certificat en sélectionne un. S'il reste vide, le certificat ayant la plus longue validité est utilisé.

Pour une connexion directe par certificat au serveur Exchange, OAuth reste désactivé.

> Relution n'empêche pas de configurer OAuth et un certificat en même temps. Dans ce cas, le certificat est tout de même transféré à l'appareil.

Pour la version 26.4.0

Mode de mise à jour

> Si ce paramètre est réglé sur Seulement lors de la publication de nouvelles versions de politiques, les mises à jour de cette configuration ne seront envoyées que si la version de la politique publiée a changé. Les mises à jour déclenchées pour d'autres raisons, comme un changement d'utilisateur de l'appareil ou d'espace réservé, ne seront pas appliquées aux appareils.
>
> Cela réduit le nombre de synchronisations pour cette configuration, ce qui peut diminuer l'utilisation des ressources sur l'appareil, tout en présentant un risque de manquer des mises à jour.

Mode de mise à jour

- Standard
- Seulement lors de la publication de nouvelles versions de politiques

Mise à jour logicielle

Avec Relution 26.1.0, la nouvelle configuration Apple Mise à jour logicielle a été introduite pour les appareils fonctionnant sous iOS 18 ou ultérieur. Cette configuration peut être utilisée en parallèle avec la configuration existante Mises à jour système. Elle remplace, entre autres, les restrictions Report de mise à jour et le comportement de mise à jour de l'ancienne configuration Mises à jour système, qui est marquée comme obsolète dans Relution.

Pour garantir les mises à jour sur l'ensemble du parc d'appareils, les configurations Mise à jour logicielle et Mises à jour système peuvent être configurées en parallèle et déployées sur tous les appareils iOS.

> La configuration Mises à jour système obsolète sera progressivement supprimée par Apple à moyen terme.

Pour la version 26.4.0

Général

Inscription au programme bêta

- Autorisé
- Toujours désactivé

Notifications de mise à jour logicielle

- Afficher toutes les notifications
- Mises à jour affichées à l'utilisateur :
  - Toutes
  - Dernière
  - Plus ancienne

Actions automatiques de mise à jour logicielle

Télécharger automatiquement les mises à jour disponibles du système d'exploitation

- Choix de l'utilisateur
- Toujours désactivé
- Toujours activé

Installer automatiquement les mises à jour disponibles du système d'exploitation

- Choix de l'utilisateur
- Toujours désactivé
- Toujours activé

Installer automatiquement les mises à jour de sécurité disponibles

- Choix de l'utilisateur
- Toujours désactivé
- Toujours activé

Report des mises à jour du système d'exploitation

- Nombre de jours : Nombre de jours pour reporter une mise à jour majeure ou mineure du système d'exploitation sur l'appareil

---

Réponse rapide pour les mises à jour de sécurité

- Permet à l'utilisateur d'installer les améliorations de sécurité en arrière-plan
- Permet à l'utilisateur de revenir sur les mises à jour de sécurité en arrière-plan

Pour la version 26.4.0

Mises à jour logicielles gérées

Nouveau dans 26.4

La configuration Mises à jour logicielles gérées impose les mises à jour du système d'exploitation en ciblant une version précise avant une échéance. Elle succède à la configuration obsolète Mises à jour système et complète les réglages Mise à jour logicielle décrits ci-dessus : ceux-ci pilotent le *comportement* de mise à jour (téléchargement automatique, report, notifications), tandis que Mises à jour logicielles gérées définit de manière contraignante *quelle* version doit être installée et *pour quand*.

iOS 17 ou une version ultérieure en mode supervisé est requis. La configuration est également disponible pour tvOS à partir de 18.4 et visionOS à partir de 26.

Version cible

- Version à imposer
  - Dernière version majeure — l'appareil est porté à la version majeure la plus récente disponible.
  - Dernière version mineure — la mise à jour s'effectue au sein de la version majeure installée.
  - Version minimale spécifique — une version concrète est définie comme niveau minimal.
- URL de la page de détails — lien facultatif que iOS affiche aux utilisateurs dans l'annonce de mise à jour.

Mise en application

- Calendrier de mise en application
  - Par rapport à la date de sortie — l'échéance découle des champs Jours après la sortie et Heure de la journée. La même règle s'applique alors automatiquement à chaque version future.
  - Date et heure spécifiques — l'Échéance est définie comme un moment fixe.
- Délai de grâce après l'inscription — facultatif. Reporte l'échéance à ce nombre de jours après l'inscription d'un appareil, afin que les appareils récemment inscrits ne soient pas forcés de se mettre à jour immédiatement. Ce réglage s'applique aux deux calendriers et ne fait que prolonger une échéance, jamais la raccourcir. Si le champ reste vide, la fonction est désactivée.

Pour la version 26.4.0

> Si les versions disponibles du système d'exploitation ne peuvent pas être chargées dans le portail, la configuration le signale à l'ouverture. La sélection d'une version minimale spécifique n'est alors pas possible, les deux autres modes restent utilisables.

Déclenchement des mises à jour

Il existe deux manières d'effectuer les mises à jour iOS :

Configuration de la politique La politique Mises à jour système peut être utilisée pour définir la plage horaire des mises à jour système.

Action sur l'appareil Grâce aux actions dans l'inventaire des appareils, les appareils peuvent être mis à jour immédiatement vers la dernière version disponible.

Pour que les appareils iOS puissent effectuer une mise à jour avec succès, les conditions suivantes doivent être remplies :

- Les appareils doivent être suffisamment chargés ou connectés à une source d'alimentation.
- Les appareils doivent être déverrouillés ; sinon, les utilisateurs doivent saisir le code d'accès de leur appareil.
- La mise à jour installée sera toujours la dernière version publique d'iOS disponible.
- Les appareils iOS compatibles vérifient les mises à jour indépendamment de cette configuration de politique une fois par jour.
- Cette configuration remplace toute restriction sur le report des mises à jour.
- Aucun utilisateur ne doit être connecté sur des appareils partagés.

Fond d'écran

La configuration "Fond d'écran" pour les appareils iOS permet de stocker une image pour l'écran d'accueil et/ou l'écran de verrouillage qui s'affiche sur les appareils après l'application de la politique. Par exemple, les appareils des élèves d'une école ou ceux d'une entreprise peuvent être dotés d'une image d'arrière-plan uniforme et/ou d'une image sur l'écran de verrouillage.

> Si l'image d'arrière-plan est définie via la politique, l'image d'arrière-plan originale du périphérique est supprimée et ne peut pas être restaurée avec Relution.

Pour la version 26.4.0

Quelles vues peuvent être configurées sur les appareils ?

Il est possible de définir si le fond d'écran doit être affiché uniquement sur l'écran de verrouillage ou sur l'écran d'accueil après la connexion, ou s'il doit être utilisé pour les deux affichages.

Calendrier (CalDAV)

La stratégie Calendrier transmet un compte CalDAV à l'application Calendrier native d'iOS et d'iPadOS via un profil de configuration, ce qui évite toute configuration manuelle par l'utilisateur final. Sur les versions récentes d'iOS, les chemins de calendrier associés au compte sont déterminés automatiquement selon la RFC 6764, via une redirection sous `/.well-known/caldav`. Une redirection `/.well-known/caldav` correctement configurée côté serveur est donc obligatoire sur les versions récentes d'iOS ; la seule indication d'une URL de principal n'y suffit plus.

Options de configuration

Les champs suivants sont disponibles pour le compte CalDAV. Ils correspondent aux clés de la charge utile CalDAV d'Apple (`com.apple.caldav.account`).

Paramètres du compte

- Description du compte — nom affiché du compte sur l'appareil.
- Hôte — adresse du serveur sans schéma et sans chemin (par exemple `calendrier.example.com`).
- Port — en règle générale `443`.
- Utiliser SSL — obligatoire lorsque le serveur est accessible via HTTPS. Sans SSL actif, une connexion non chiffrée est tentée sur le port `443`, ce qui échoue.
- Nom d'utilisateur — saisi manuellement ou via les espaces réservés `${user.name}` ou `${user.email}`.
- Mot de passe — s'il n'est pas renseigné, il est demandé sur l'appareil lors de l'installation du profil.
- URL de principal *(facultatif)* — le chemin vers le principal de l'utilisateur (par exemple `/remote.php/dav/principals/users/${user.name}/`).

> L'URL de principal doit être indiquée sous forme de chemin simple, et non d'URL complète avec schéma et hôte (pas `https://hote/...`). L'hôte, le port et le chiffrement découlent des champs Hôte, Port et Utiliser SSL. Sur les versions récentes d'iOS, une URL de principal renseignée ne remplace toutefois plus la détection automatique — c'est une redirection `/.well-known/caldav` correctement configurée qui est déterminante. Le champ peut donc rester vide.

Pour la version 26.4.0

Détection automatique via .well-known

Les versions récentes d'iOS configurent les comptes CalDAV selon la RFC 6764. Le déroulement est le suivant :

1. Requête `PROPFIND /.well-known/caldav` vers le serveur indiqué sous Hôte.
2. Le serveur répond par une redirection (`301`) vers son point de terminaison DAV (`/remote.php/dav` pour ownCloud/Nextcloud).
3. Le point de terminaison DAV permet de déterminer le `current-user-principal` et, à partir de là, l'espace calendrier de l'utilisateur.

La fiabilité de la configuration dépend donc entièrement d'une redirection `/.well-known` correcte. Sur les versions récentes d'iOS, la détection automatique ne peut plus être contournée par l'indication d'une URL de principal — sans redirection `/.well-known` fonctionnelle, la configuration échoue, même si une URL de principal est renseignée.

> Les versions récentes d'iOS évaluent la redirection plus strictement qu'iOS 17. Une redirection erronée (par exemple vers `http://` au lieu de `https://`), encore tolérée sous iOS 17, provoque l'interruption de la détection sur les versions actuelles. Les comptes déjà configurés sous iOS 17 sur d'anciens appareils peuvent continuer de fonctionner alors que les nouvelles configurations échouent.

Pour la version 26.4.0

Configuration de la redirection côté serveur

`/.well-known/caldav` et `/.well-known/carddav` doivent rediriger par `301` vers le point de terminaison DAV du serveur. L'adresse cible doit impérativement commencer par **`https://`** et ne doit pas contenir de port interne.

Pour nginx :

```
location = /.well-known/caldav  { return 301 https://$host/remote.php/dav; }
location = /.well-known/carddav { return 301 https://$host/remote.php/dav; }
```

Pour Apache (dans le vHost) :

```
Redirect 301 /.well-known/caldav  https://calendrier.example.com/remote.php/da
Redirect 301 /.well-known/carddav https://calendrier.example.com/remote.php/da
```

Exploitation derrière un reverse proxy / terminaison TLS : si un proxy en amont termine la connexion TLS et transmet en interne par HTTP vers un autre port (par exemple `8080`), le serveur web ne connaît souvent son adresse publique que comme `http` sur le port interne. La redirection générée est alors erronée, par exemple `http://calendrier.example.com:8080/remote.php/dav`. Les versions récentes d'iOS ne suivant pas un passage de `https` à `http`, la détection échoue. Dans ce cas, la redirection doit être définie avec une adresse cible **`https://`** complète — soit directement sur le proxy qui termine le TLS, soit comme URL cible absolue, comme dans l'exemple Apache.

Vérification

La redirection peut être vérifiée avec `curl` :

version 26.4.0

```
curl -sI https://calendrier.example.com/.well-known/caldav
```

La réponse doit contenir une redirection avec un en-tête `location` correct :

```
HTTP/2 301
location: https://calendrier.example.com/remote.php/dav
```

L'en-tête `location` doit commencer par `https://` et ne doit pas contenir de port interne (par exemple `:8080`).

Résolution des problèmes

Symptôme	Cause	Solution
La configuration échoue uniquement sur les versions récentes d'iOS ; les anciens appareils continuent de fonctionner	La redirection pointe vers `http://` (rétrogradation) ; les anciennes versions d'iOS le toléraient	Corriger la redirection vers `https://`
Le `301` pointe vers un port interne (par exemple `:8080`)	Reverse proxy/terminaison TLS, le serveur web ne connaît pas son adresse publique	Définir la redirection avec l'adresse `https://` complète sur le proxy ou le serveur web
`405 Method Not Allowed` sur des chemins tels que `/` ou `/principals/`	La détection automatique n'aboutit pas et teste des chemins par défaut qui n'existent pas sur le serveur	Configurer correctement la redirection `/.well-known` (obligatoire sur les versions récentes d'iOS)
Le chemin déterminé est manifestement incorrect	URL de principal renseignée comme URL complète au lieu d'un chemin simple, ou Utiliser SSL non activé	Indiquer l'URL de principal sous forme de chemin simple et activer Utiliser SSL

Délimitation du problème sur l'appareil

Pour délimiter le problème, un compte CalDAV peut être configuré à titre de test directement sur l'appareil sous `Réglages` → `Calendrier` → `Comptes`. Si le compte configuré manuellement se connecte alors que le compte distribué par profil échoue, la cause se situe dans la détection automatique (`/.well-known`) ou dans l'URL de principal distribuée via le profil — et non dans le serveur lui-même.

Utilisation sous macOS

La configuration CalDAV et le prérequis `/.well-known` côté serveur s’appliquent de manière identique à macOS :

- Calendrier (CalDAV) pour macOS →

Pour la version 26.4.0

Domaines gérés

La configuration Domaines gérés détermine quels domaines de messagerie et web iOS traite comme domaines de l'entreprise. Elle est disponible pour les appareils avec inscription de l'appareil (Device Enrollment), mais pas pour les appareils avec inscription utilisateur (User Enrollment/BYOD).

Domaines de messagerie

Les domaines de l'entreprise sont saisis dans la liste Domaines de messagerie, p. ex. `relution.io`. Lors de la rédaction d'un message, l'application Mail marque en rouge toutes les adresses de destinataires dont le domaine ne figure pas dans la liste. Il est ainsi immédiatement visible lorsqu'un message quitte l'entreprise.

L'envoi à ces adresses n'est pas bloqué. Le marquage est purement indicatif.

Domaines web

iOS traite comme gérées les URL des domaines de la liste Domaines Web. Les contenus téléchargés depuis ces pages dans Safari sont donc considérés comme des données de l'entreprise, p. ex. un PDF de l'intranet.

Cette liste n'a d'effet visible qu'en combinaison avec les restrictions relatives à l'ouverture de documents dans la configuration Restrictions → :

- Autoriser l'ouverture de documents gérés dans des applications non gérées
- Autoriser l'ouverture de documents non gérés dans des applications gérées

Si l'ouverture de documents gérés dans des applications non gérées est interdite, un PDF de l'intranet ne peut ensuite être ouvert que dans des applications gérées. Plus d'informations sur la séparation des données gérées et non gérées figurent dans l'article Séparation des données →.

Pour la version 26.4.0

Paramètres Intelligence

Avec Relution, la configuration Paramètres Intelligence peut être gérée de manière centralisée afin de contrôler les fonctions d'Apple Intelligence sur les appareils iOS gérés. Cette politique permet d'autoriser ou de bloquer des fonctions individuelles pilotées par l'IA, telles que le rapport Apple Intelligence, Genmoji, Image Playground, Image Wand, les résultats d'écriture manuscrite personnalisée, le résumé Visual Intelligence et les outils d'écriture. Elle permet en outre de contrôler les fonctions Intelligence spécifiques aux applications dans Mail, Notes et Safari, ainsi que d'imposer un traitement de la dictée et de la traduction exclusivement local sur l'appareil, sans connexion aux serveurs d'Apple.

La configuration est disponible pour les appareils iOS à partir de la version 26.4 et ne peut être appliquée que dans le cadre de l'inscription des appareils, et non lors de l'inscription des utilisateurs (BYOD). Elle est disponible sous la même forme pour macOS et visionOS à partir de la version 26.4.

Pour la version 26.4.0

Toutes les options ne sont pas prises en charge par chaque plateforme. Le formulaire les affiche néanmoins pour toutes les plateformes.

- visionOS : Autoriser les résultats d'écriture manuscrite personnalisée, Autoriser le résumé Visual Intelligence, Forcer la traduction uniquement sur l'appareil ainsi que, dans la section Notes, Autoriser la transcription et Autoriser le résumé de transcription ne sont pas pris en charge.
- macOS : Autoriser Image Wand, Autoriser les résultats d'écriture manuscrite personnalisée, Autoriser le résumé Visual Intelligence et Forcer la traduction uniquement sur l'appareil ne sont pas pris en charge.

Paramètres

- Autoriser le rapport Apple Intelligence
  - Si désactivé, le rapport Apple Intelligence est désactivé sur l'appareil. Activé par défaut.
- Autoriser Genmoji
  - Si désactivé, la fonction Genmoji est désactivée. Activé par défaut.
- Autoriser Image Playground
  - Si désactivé, Image Playground est désactivé. Activé par défaut.
- Autoriser Image Wand
  - Si désactivé, Image Wand est désactivé. Activé par défaut.

- Autoriser les résultats d’écriture manuscrite personnalisée
  - Si désactivé, les résultats d’écriture manuscrite personnalisée sont désactivés. Activé par défaut.
- Autoriser le résumé Visual Intelligence
  - Si désactivé, le résumé Visual Intelligence est désactivé. Activé par défaut.
- Autoriser les outils d’écriture
  - Si désactivé, les outils d’écriture (Writing Tools) sont désactivés. Activé par défaut.
- Forcer la dictée uniquement sur l’appareil
  - Si activé, la dictée est traitée exclusivement en local sur l’appareil, sans connexion aux serveurs d’Apple. Désactivé par défaut.
- Forcer la traduction uniquement sur l’appareil
  - Si activé, la traduction est traitée exclusivement en local sur l’appareil, sans connexion aux serveurs d’Apple. Désactivé par défaut.

Mail

- Autoriser les réponses intelligentes
  - Si désactivé, les réponses intelligentes (Smart Replies) dans Mail sont désactivées. Activé par défaut.
- Autoriser le résumé
  - Si désactivé, la fonction de résumé dans Mail est désactivée. Activé par défaut.

Pour la version 26.4.0

Notes

- Autoriser la transcription
  - Si désactivé, la transcription dans Notes est désactivée. Activé par défaut.
- Autoriser le résumé de transcription
  - Si désactivé, le résumé des transcriptions dans Notes est désactivé. Activé par défaut.

Safari

- Autoriser le résumé
  - Si désactivé, la fonction de résumé dans Safari est désactivée. Activé par défaut.

Paramètres d'intelligence externe

La configuration Paramètres d’intelligence externe permet de contrôler de manière centralisée si et comment des services d’IA externes basés sur le cloud (par ex. ChatGPT) peuvent être utilisés via Siri et Apple Intelligence sur les appareils iOS. La politique est disponible à partir d’iOS 26.4 — exclusivement pour les appareils avec une inscription complète des appareils, pas en mode User Enrollment/BYOD — et est transmise à l’appareil via la gestion déclarative des appareils (DDM). La même configuration est disponible sous une forme identique pour les appareils macOS et visionOS à partir de leur version 26.4 respective.

> Remarque : cette configuration est une politique autonome basée sur le DDM et complète les champs déjà existants relatifs aux intégrations d’intelligence externe au sein des restrictions iOS →. Les deux types de configuration peuvent être affichés en parallèle dans le portail, mais couvrent les trois mêmes fonctions.

Intégrations d’IA externes

- Autoriser les intégrations d’IA externes
  - Si désactivé, les intégrations d’IA externes sont entièrement bloquées. Activé par défaut.
- Autoriser la connexion pour les intégrations d’IA externes
  - Si désactivé, la connexion (Sign-In) aux intégrations d’IA externes n’est pas possible. Activé par défaut.
- Identifiant d’espace de travail autorisé
  - Définit l’identifiant de l’espace de travail auquel l’intégration d’IA externe est restreinte. Actuellement limité à un seul identifiant d’espace de travail.

Pour la version 26.4.0

Paramètres du clavier

À partir d'iOS 26.4 et de Relution 26.3, la configuration Paramètres du clavier est disponible ; elle est mise en œuvre via la gestion déclarative des appareils (DDM). Cette politique permet d'activer ou de désactiver de manière centralisée des fonctions du clavier telles que la correction automatique, la dictée, la vérification orthographique, la reconnaissance de texte, le remplacement de texte, la saisie par glissement et les suggestions mathématiques du clavier – utile par exemple pour les établissements d'enseignement ou les entreprises souhaitant garantir une saisie de texte uniforme et contrôlée sur les appareils gérés.

> Remarque : cette configuration nécessite iOS 26.4 ou une version ultérieure et n'est disponible que pour les appareils gérés via l'inscription des appareils (Device Enrollment). Tous les paramètres sont activés par défaut ; leur désactivation restreint la fonction de clavier correspondante.

Paramètres pour le clavier

Pour la version 26.4.0

- Autoriser la recherche de définitions
  - Si désactivé, la recherche de définitions de mots (Look Up) sur le clavier n'est plus disponible.
- Autoriser la dictée
  - Si désactivé, la fonction de dictée du clavier ne peut plus être utilisée.
- Autoriser les suggestions mathématiques du clavier
  - Si désactivé, le clavier n'affiche plus de suggestions de résolution automatiques pour les expressions mathématiques.
- Autoriser la correction automatique
  - Si désactivé, le clavier ne corrige plus automatiquement les fautes de frappe.
- Autoriser la reconnaissance de texte
  - Si désactivé, aucune suggestion de mot prédictive (Predictive Text) n'est plus affichée au-dessus du clavier pendant la saisie.
- Autoriser la saisie par glissement
  - Si désactivé, il n'est plus possible de saisir du texte en glissant sur le clavier (Slide to Type / saisie gestuelle continue).
- Autoriser la vérification orthographique
  - Si désactivé, le clavier ne souligne plus les mots mal orthographiés.
- Autoriser le remplacement de texte

- Si désactivé, les remplacements/raccourcis de texte configurés ne sont plus insérés automatiquement pendant la saisie.

Paramètres Siri

À partir d'iOS 26.4 et de Relution 26.3, la configuration Paramètres Siri est disponible ; elle est mise en œuvre via la gestion déclarative des appareils (DDM). Cette politique permet de contrôler de manière centralisée la disponibilité générale de Siri, le filtre d'obscénités ainsi que — exclusivement sous iOS — le traitement du contenu généré par l'utilisateur et l'accès à Siri en état verrouillé.

> Remarque : la configuration nécessite iOS 26.4 ou une version ultérieure et n'est disponible que pour les appareils gérés via l'inscription des appareils (Device Enrollment) ; elle n'est pas disponible pour les appareils avec inscription des utilisateurs (User Enrollment/BYOD).

Remarque : des commutateurs Siri comparables existent déjà dans les Restrictions iOS →. Les Paramètres Siri constituent une configuration distincte et supplémentaire qui ne remplace pas les restrictions.

Pour la version 26.4.0

Paramètres pour Siri

- Activer Siri
  - Active ou désactive Siri sur l'appareil. Activé par défaut.
- Appliquer le filtre d'obscénités
  - Impose le filtre d'obscénités de Siri. Désactivé par défaut.
- Autoriser le contenu généré par l'utilisateur
  - Autorise Siri à accéder au contenu généré par l'utilisateur. Activé par défaut.
- Autoriser Siri en état verrouillé
  - Autorise l'utilisation de Siri lorsque l'appareil est verrouillé. Activé par défaut.

Paramètres Safari

Avec la configuration Paramètres Safari, le comportement du navigateur Safari peut être géré de manière centralisée sur les appareils iOS gérés. Cela comprend notamment la gestion des cookies, l'avertissement de fraude, JavaScript et les fenêtres pop-up, ainsi que la suppression de l'historique, la navigation privée, le résumé de contenu et la page de démarrage affichée à l'ouverture d'un nouvel onglet. Sur les appareils macOS, seules les quatre dernières options citées sont disponibles – les cookies, l'avertissement de fraude, JavaScript et les pop-up ne peuvent pas y être configurés.

> Remarque : la configuration n'est disponible que pour les appareils disposant d'un profil d'inscription des appareils (pas d'inscription des utilisateurs/BYOD) et nécessite au moins iOS 26.

Paramètres pour le navigateur Safari

Pour la version 26.4.0

- Autoriser les cookies
  - Définit la manière dont Safari gère les cookies.
    - Toujours – Safari autorise toujours les cookies. *(valeur par défaut)*
    - Des sites déjà visités – Safari n'autorise que les cookies des sites web déjà visités.
    - Du site web actuel – Safari n'autorise que les cookies du site web actuellement ouvert.
    - Jamais – Safari bloque systématiquement les cookies.
- Autoriser la désactivation de l'avertissement de fraude
  - Si désactivé, le système impose l'avertissement de fraude dans Safari ; les utilisateurs ne peuvent pas le désactiver. Activé par défaut.
- Autoriser JavaScript
  - Si désactivé, JavaScript est désactivé dans Safari à l'échelle du système. Activé par défaut.
- Autoriser les pop-up
  - Si désactivé, les fenêtres pop-up sont désactivées dans Safari à l'échelle du système. Activé par défaut.
- Autoriser la suppression de l'historique

    - Si désactivé, l'historique de navigation dans Safari ne peut pas être supprimé. Activé par défaut.
- Autoriser la navigation privée
    - Si désactivé, le mode de navigation privée n'est pas disponible dans Safari. Activé par défaut.
- Autoriser le résumé de contenu
    - Si désactivé, le résumé automatique de contenu dans Safari est désactivé. Activé par défaut.
- Page de démarrage *(champ obligatoire)*
    - Détermine quelle page est affichée à l'ouverture d'un nouvel onglet dans Safari.
        - Démarrage – Safari utilise sa page de démarrage par défaut ; la page d'accueil est désactivée. *(valeur par défaut)*
        - Extension – Safari utilise comme page de démarrage l'extension Safari référencée par l'identifiant indiqué ; la page d'accueil est désactivée. Nécessite d'indiquer un identifiant d'extension au format `Identifiant (IdentifiantEquipe)`, par ex. `com.example.app (ABCD1234)`.
        - Accueil – Safari utilise l'URL indiquée à la fois comme page de démarrage pour les nouveaux onglets et comme page d'accueil. Nécessite d'indiquer une URL de page d'accueil qui doit commencer par `https://` ou `http://`.

Pour la version 26.4.0

Extensions Safari

Avec la configuration Extensions Safari, le comportement des extensions Safari individuelles peut être géré de manière centralisée sur les appareils iOS gérés. Pour chaque extension, son identifiant unique permet de définir si elle est autorisée de manière générale, toujours activée ou toujours désactivée, si elle peut également être utilisée en navigation privée, et à quels domaines elle peut ou ne peut pas accéder. Plusieurs extensions peuvent être configurées par politique.

> Remarque : cette configuration n'est disponible que pour les appareils iOS supervisés à partir d'iOS 18 qui ont été intégrés via l'inscription des appareils (Device Enrollment) ; elle ne peut pas être utilisée pour les appareils en inscription des utilisateurs (User Enrollment/BYOD).

Paramètres par extension Safari

- Identifiant de l'extension
  - L'identifiant de l'extension Safari, ou `*` pour appliquer les réglages à toutes les extensions. Pour gérer l'extension, l'application à laquelle elle appartient doit être installée sur l'appareil. Cet identifiant peut être déterminé via `codesign -dv <chemin vers l'extension (dans le répertoire PlugIns de l'application)>` sur un appareil macOS, si l'extension est disponible sur macOS. Sinon, cette information doit être fournie par le développeur de l'extension.
- Statut
  - Détermine si l'extension est autorisée. Options : Autorisée / Toujours activée / Toujours désactivée.
- Navigation privée
  - Autoriser également l'extension en mode Navigation privée. Options : Autorisée / Toujours activée / Toujours désactivée.
- Domaines autorisés
  - Détermine les (sous-)domaines auxquels l'extension Safari a accès. Les domaines sans préfixe ont priorité sur ceux avec préfixe ; les domaines refusés ont priorité sur les domaines autorisés. Tous les domaines non configurés via les deux listes peuvent être configurés par les utilisateurs sur l'appareil.
- Domaines refusés
  - Détermine les (sous-)domaines auxquels l'extension Safari n'a pas accès. Les domaines sans préfixe ont priorité sur ceux avec préfixe ; les domaines refusés ont

Pour la version 26.4.0

priorité sur les domaines autorisés. Tous les domaines non configurés via les deux listes peuvent être configurés par les utilisateurs sur l’appareil.

Pour la version 26.4.0

Paramètres des accessoires audio

À partir de la version 26.1.0 de Relution, la nouvelle configuration Paramètres des accessoires audio a été introduite pour les appareils à partir d'iOS 26+.

Cette fonction permet le jumelage temporaire d'accessoires audio (par ex. écouteurs ou enceintes) avec des appareils gérés. Un accessoire audio peut ainsi être jumelé pour une durée limitée, puis découplé automatiquement ou manuellement.

Désactiver le jumelage temporaire d'accessoires audio **Marche/Arrêt**

Ce commutateur permet d'activer ou de désactiver le jumelage temporaire d'accessoires audio.

- Activé : le jumelage temporaire est autorisé.
- Désactivé : aucun jumelage temporaire d'accessoires audio n'est possible.

Pour la version 26.4.0

Politique de découplage

Ce paramètre définit comment et quand un accessoire audio jumelé temporairement est à nouveau déconnecté :

- Aucun découplage automatique L'appareil ne supprime pas automatiquement le jumelage.

  Remarque : cette option ne doit être utilisée que lorsqu'un appareil est supprimé et réenregistré (par ex. *Return to Service*) ou lors d'un changement d'utilisateur.

- Découplage automatique à une heure précise L'appareil supprime automatiquement le jumelage des accessoires audio connectés temporairement à un moment défini.

Heure de découplage

- Définir une heure (par ex. 16 h 30) Définit le moment à partir duquel l'appareil met automatiquement fin au jumelage des accessoires audio connectés temporairement.

  Remarque : à l'heure définie, seul le jumelage des accessoires audio préalablement connectés de manière temporaire est supprimé.

Accès conditionnel

En complément de l'article suivant Microsoft Conditional Access →, Relution 5.33 introduit une politique Accès conditionnel pour iOS.

Il y a les 2 options suivantes :

- L'appareil est marqué comme non conforme si l'utilisateur ne l'a pas encore enregistré via l'agent Relution
- Informe l'utilisateur via une notification push pour qu'il enregistre son appareil

Pour la version 26.4.0

Paramètres mathématiques

À partir de la version 26.1.0 de Relution, la nouvelle configuration Paramètres mathématiques est disponible pour les appareils à partir d'iOS 18+.

Cette politique permet de gérer de manière centralisée les fonctions et modes de l'application Calculatrice Apple et de les adapter aux exigences pédagogiques ou organisationnelles.

Paramètres pour l'application Calculatrice Apple

Mode de base

- Ajouter la racine carrée : ajoute au calculateur de base une touche racine carrée, en remplaçant la touche +/-. Par défaut, la fonction racine carrée n'est disponible qu'en mode scientifique. Cette option permet d'accéder à la racine carrée même lorsque le mode scientifique est restreint.

Mode Notes mathématiques

- Activer / Désactiver : définit si le mode Notes mathématiques peut être utilisé dans l'application Calculatrice.

Pour la version 26.4.0

Mode scientifique

- Activer / Désactiver : détermine si le mode scientifique de l'application Calculatrice est disponible.

Options de saisie globales de la calculatrice

- Activer la conversion d'unités : permet d'utiliser la fonction de conversion d'unités intégrée dans l'application.

Comportement du système

Activer les suggestions du clavier

- Activer / Désactiver : définit si des solutions mathématiques sont affichées automatiquement dans les suggestions du clavier.

Activer les notes mathématiques dans d'autres applications

- Activer / Désactiver : définit si la fonction Math Notes peut également être utilisée dans d’autres applications (par ex. Notes).

Pour la version 26.4.0

AirPrint

La configuration de politique AirPrint transmet des imprimantes compatibles AirPrint aux appareils iOS et iPadOS au moyen d'un profil de configuration. Les imprimantes définies apparaissent ensuite dans la boîte de dialogue d'impression de l'appareil, sans devoir être détectées sur le réseau local via Bonjour.

Cas d'utilisation

Par défaut, les imprimantes AirPrint sont détectées via Bonjour (mDNS). Les annonces Bonjour ne franchissent toutefois pas les limites de sous-réseau ou de VLAN — dans les réseaux scolaires et d'entreprise dotés de segments distincts pour les appareils et les imprimantes, celles-ci ne sont donc souvent pas visibles dans la boîte de dialogue d'impression. La configuration AirPrint indique directement l'adresse de l'imprimante, de sorte que l'appareil peut la joindre de manière ciblée.

La configuration est également disponible pour les appareils en User Enrollment et est proposée, outre dans les politiques iOS et iPadOS, dans les politiques macOS (voir AirPrint pour macOS →).

Pour la version 26.4.0

Prérequis

- Une imprimante ou un serveur d'impression (p. ex. CUPS) compatible AirPrint, joignable via IPP ou IPPS.
- Une connexion réseau entre l'appareil et l'imprimante sur le port utilisé (port IPP par défaut : `631`) ; les pare-feu entre les segments réseau doivent autoriser ce port.
- Le nom d'hôte ou l'adresse IP ainsi que le chemin d'accès aux ressources de l'imprimante.

Configuration

La configuration est créée sous `Appareils` → `Politiques` dans une politique iOS via Ajouter une configuration → AirPrint. La section Général répertorie les imprimantes dans un tableau ; Ajouter ouvre la boîte de dialogue Ajouter une imprimante. Une configuration peut contenir un nombre quelconque d'imprimantes ; elle ne peut être enregistrée qu'à partir du moment où au moins une imprimante a été saisie.

Les champs suivants sont disponibles pour chaque imprimante :

Champ	Obligatoire	Description
Nom d’hôte ou adresse IP	oui	Adresse de l’imprimante ou du serveur d’impression, p. ex. `192.168.10.25` ou `imprimante01.example.com`.
Port	non	Port du service IPP (`0` – `65535`). Sans indication, le port par défaut est utilisé.
Chemin d’accès aux ressources	oui	Chemin de la file d’impression, p. ex. `ipp/print` pour de nombreuses imprimantes réseau ou `printers/<file>` pour les serveurs CUPS.
Utiliser TLS	non	Impose une connexion chiffrée TLS (IPPS) vers l’imprimante. Désactivé par défaut.

Les imprimantes déjà saisies peuvent être modifiées via Éditer ou retirées via Supprimer dans le menu contextuel du tableau ; plusieurs imprimantes peuvent être supprimées en une fois grâce à la sélection multiple.

> L’imprimante annonce son chemin d’accès aux ressources dans l’enregistrement TXT Bonjour `rp`. Sur un Mac situé dans le même réseau que l’imprimante, il peut être lu avec `dns-sd -B _ipp._tcp` (recherche des imprimantes), puis `dns-sd -L "<nom de l'imprimante>" _ipp._tcp`. Il figure aussi souvent dans l’interface web de l’imprimante.

Pour la version 26.4.0

Restrictions associées

En complément de la configuration AirPrint, la configuration de politique Restrictions contient, dans la section Restrictions des réglages, d’autres options liées à AirPrint, notamment Autoriser AirPrint, Autoriser le stockage des identifiants AirPrint, Autoriser la découverte par iBeacon des imprimantes AirPrint et Exiger un protocole TLS fiable pour AirPrint. Si Autoriser AirPrint est désactivé, l’impression n’est pas disponible sur l’appareil, même avec des imprimantes configurées.

- Restrictions pour iOS →

Si Exiger un protocole TLS fiable pour AirPrint est actif, l’appareil n’accepte que des imprimantes disposant d’un certificat de confiance. Les imprimantes utilisant des certificats auto-signés ne sont alors plus utilisables, à moins que le certificat émetteur ne soit en outre installé sur l’appareil via une politique.

Pour la version 26.4.0

Assistant d'installation

La configuration Assistant d’installation permet de masquer les étapes de configuration qu’iOS affiche sur un appareil déjà configuré, p. ex. après une mise à jour logicielle. Elle est disponible à partir d’iOS 14 et ne s’applique qu’aux appareils supervisés. Elle n’est pas disponible pour les appareils avec inscription utilisateur (User Enrollment/BYOD).

Différence avec le profil DEP

Les étapes de l’assistant d’installation peuvent être ignorées à deux endroits, qui s’appliquent à des moments différents :

	Profil DEP	Configuration Assistant d’installation
Moment	Configuration initiale de l’appareil	Après l’inscription, p. ex. après une mise à jour logicielle
Configuré dans	profil → de l’Inscription automatisée des appareils (ADE, DEP dans le portail)	Politique avec la configuration Assistant d’installation

Les étapes sélectionnées dans le profil DEP ne s’appliquent qu’à la configuration initiale. Si iOS affiche à nouveau des étapes de configuration par la suite, p. ex. pour l’apparence, Siri ou Temps d’écran après une mise à jour, celles-ci ne peuvent être masquées que via la configuration Assistant d’installation. Sans cette configuration, ces étapes s’affichent comme prévu par Apple.

La configuration n’est donc pas une condition préalable à l’inscription. Elle n’est nécessaire que si aucune étape de configuration supplémentaire ne doit être affichée après la configuration initiale.

Paramètres

Dans la section Ignorez les étapes suivantes, les étapes à masquer sont activées. La sélection correspond aux étapes de configuration du profil DEP.

Les interrupteurs de la section Général, p. ex. Sauter l’accessibilité ou Ignorer la configuration Siri, ne s’appliquent qu’à macOS et n’ont aucun effet sur les appareils iOS. Voir Assistant d’installation (macOS) →.

> Apple n’autorise qu’une seule configuration Assistant d’installation par appareil. Il convient donc de ne pas attribuer simultanément à un appareil plusieurs politiques contenant cette configuration.

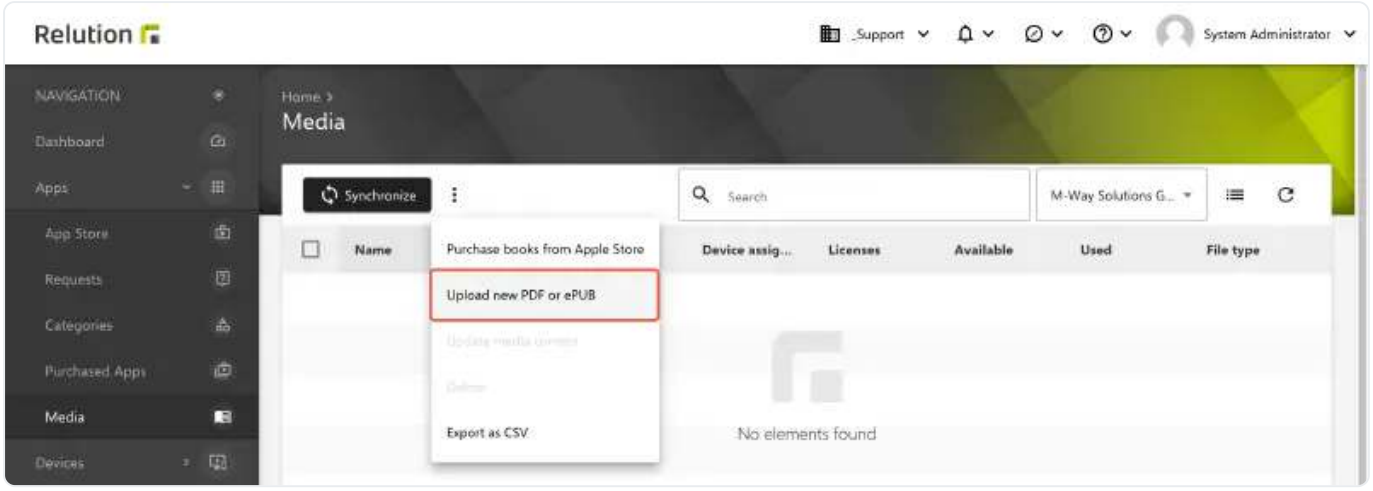
Pour la version 26.4.0

Médias gérés

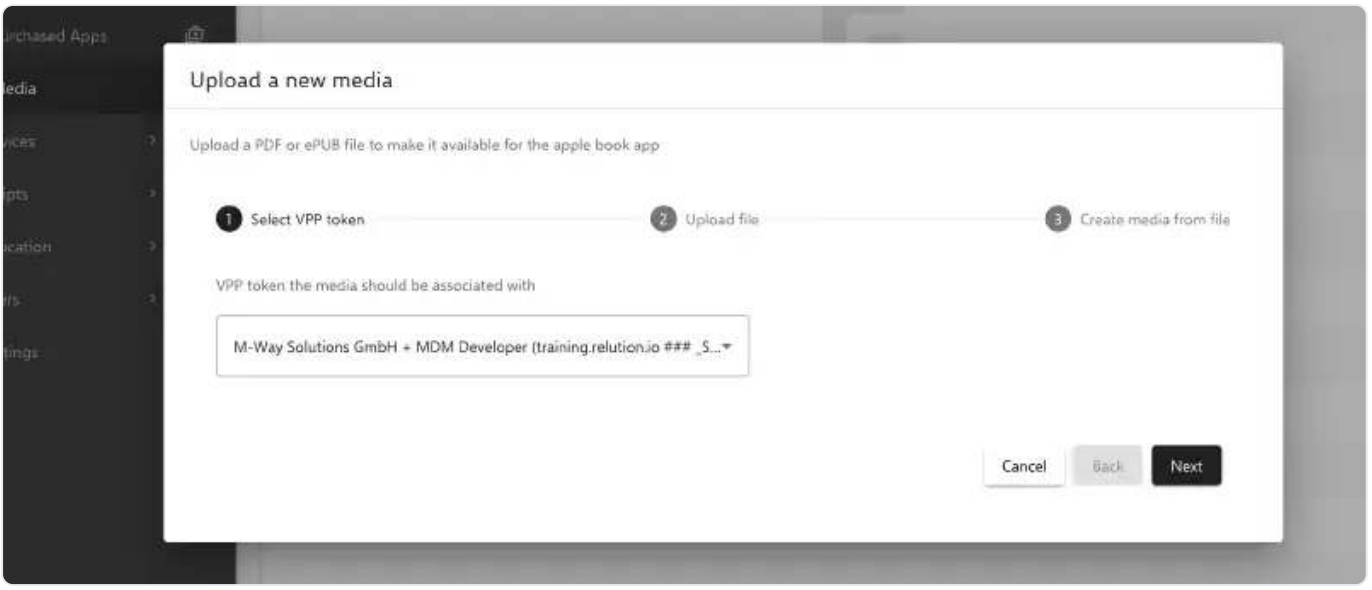
Depuis Relution 5.20, il est possible de distribuer des fichiers PDF ou ePUB directement sur les appareils iOS via la configuration de la politique Managed Media et de les afficher dans l'application Books sur l'iPad. Les livres VPP ne peuvent être liés qu'à des utilisateurs VPP et non à des appareils.

Préparation et téléchargement des médias

Pour pouvoir distribuer des fichiers PDF et ePUB, ceux-ci doivent d'abord être téléchargés dans Relution. Cela se fait via l'aperçu des livres. Pour ce faire, allez à la section correspondante dans le menu latéral.

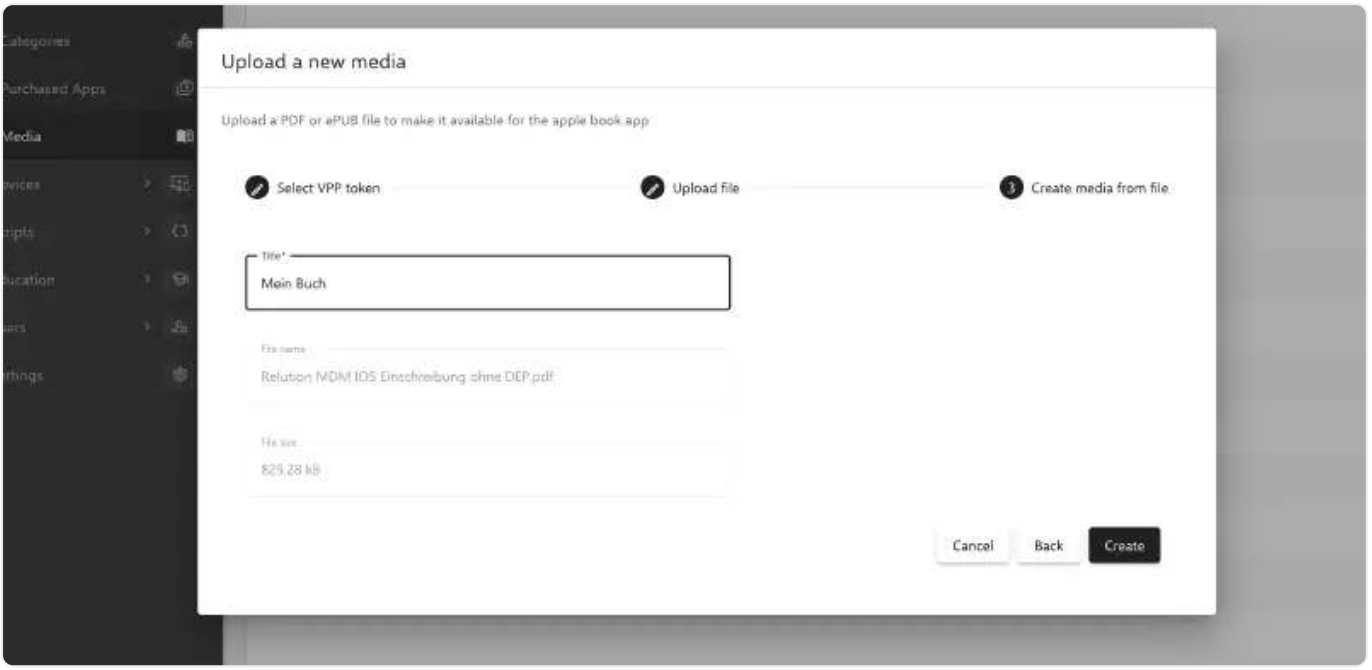


Le menu situé derrière les trois points permet de sélectionner "Télécharger un nouveau livre".



Dans cette étape, le jeton VPP à associer au fichier média doit être sélectionné.

Ensuite, le fichier (pdf ou epub) doit être sélectionné et téléchargé.



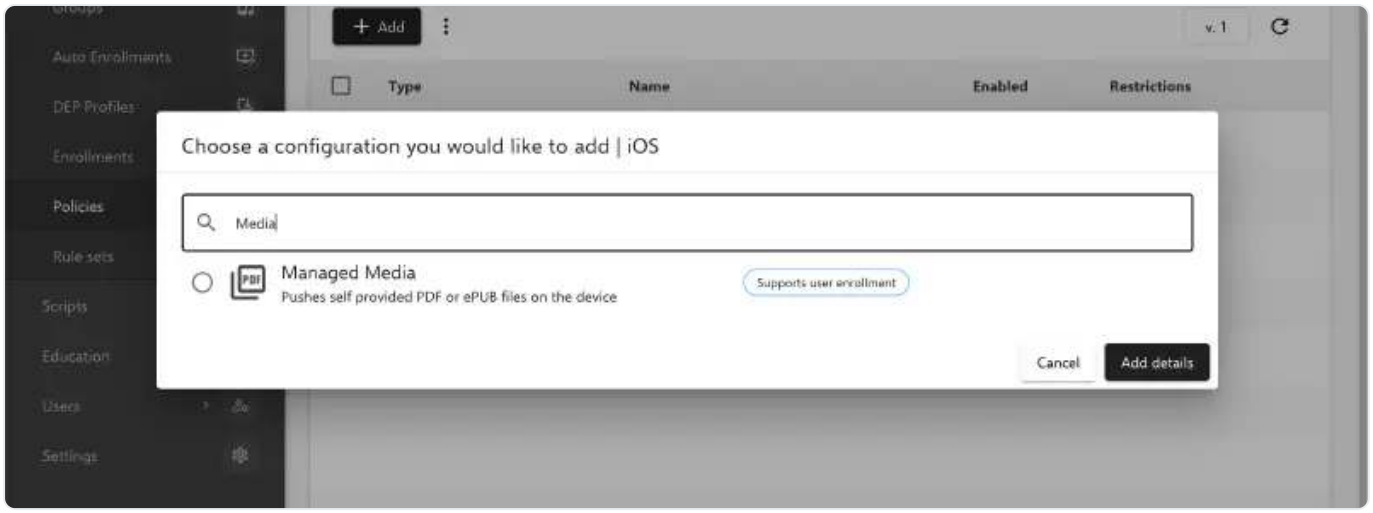
La dernière étape consiste à donner un titre au livre.

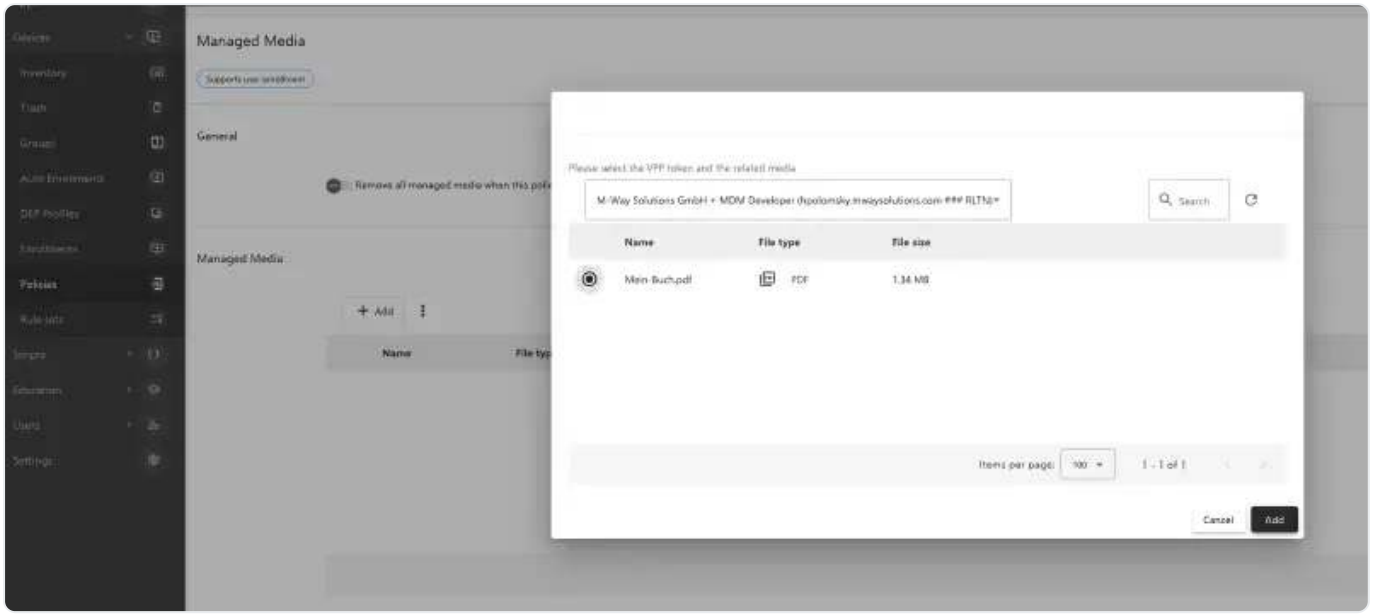
Le fichier PDF est maintenant visible dans l'aperçu des livres.

Configuration de la politique

Comme déjà décrit, cette configuration de politique est disponible à partir de Relution Server 5.20 et peut donc être sélectionnée dans une politique iOS.

Dans la configuration Managed Media, les fichiers précédemment ajoutés peuvent être liés et apportés à l'appareil via la politique.





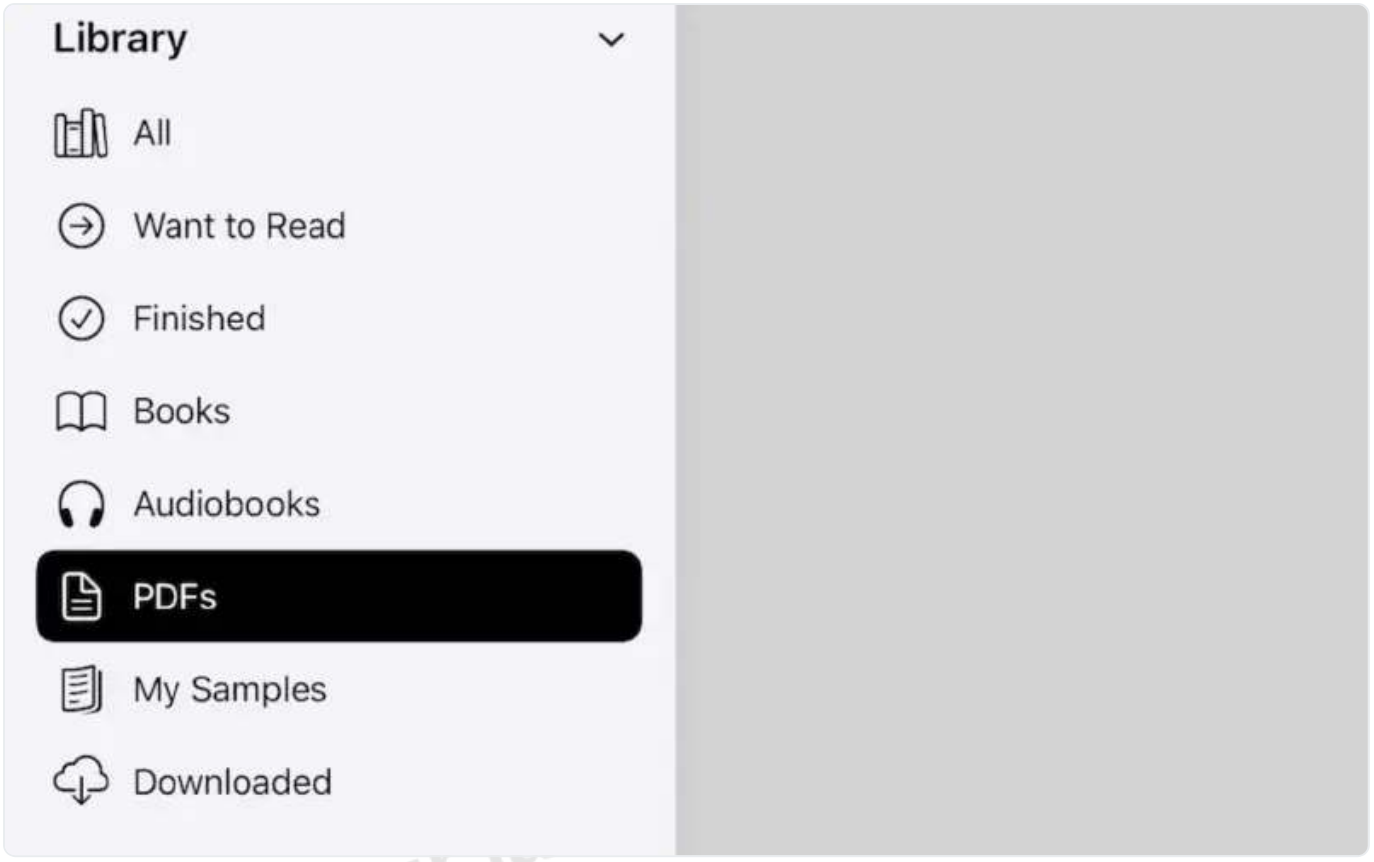
Un paramètre de configuration est également disponible pour forcer ou empêcher la suppression automatique des fichiers après avoir retiré la politique du périphérique.

Exécuter en tant qu'action

En complément de la configuration de la politique, les médias précédemment téléchargés peuvent également être installés ou supprimés directement sur un appareil via une action. Les actions correspondantes sont appelées Installer les médias et Supprimer les médias.

Sur l’iPad

Sur l’iPad, le PDF lié est alors disponible dans la catégorie correspondante.



Restrictions

Ce qui suit est une vue d'ensemble des restrictions iOS/iPadOS disponibles dans Relution `5.28.3`. Noter les informations supplémentaires aux points de configuration individuels dans Relution, tels que `supervised`, `User Enreollment`, `deprecated`, `deprecated on non-supervised Devices`, ainsi que la version minimale du système d'exploitation, telle que `iOS 16+`. OS comme `iOS 16+`

Restrictions recommandées →

Appareil

> Afficher toutes les restrictions

Safari

> Afficher toutes les restrictions

Pour la version 26.4.0

SIRI

> Afficher toutes les restrictions

Autres applications

> Afficher toutes les restrictions

Restrictions pour les applications et documents gérés

> Afficher toutes les restrictions

Restrictions des réglages

Afficher toutes les restrictions

Restrictions relatives à la salle de classe

Afficher toutes les restrictions

Restrictions pour les médias

Afficher toutes les restrictions

Restrictions sur les modifications

Afficher toutes les restrictions

Pour la version 26.4.0

Restrictions iCloud

Afficher toutes les restrictions

Restrictions de l’écran de verrouillage

Afficher toutes les restrictions

Restrictions pour les sauvegardes et la synchronisation

Afficher toutes les restrictions

Général

Afficher toutes les restrictions

Pour la version 26.4.0

Distribution d'applications

Les entreprises choisissent de plus en plus souvent de soutenir des processus de travail spécifiques à l'aide d'une application mobile. Outre de nombreuses autres questions conceptuelles, la question se pose rapidement de savoir comment cette application doit être distribuée aux utilisateurs. Souvent, le cas d'utilisation se présente comme suit : l'application doit être mise à la disposition non seulement des employés, mais aussi des personnes externes - il peut s'agir, par exemple, de prestataires de services, de partenaires ou de clients. Dans la plupart des cas, l'application n'est explicitement pas destinée à un large éventail de clients, mais à des utilisateurs professionnels sélectionnés. Les sections suivantes de cet Insight ont pour but d'aider à décider de la meilleure méthode de distribution.

Distribution via les magasins d'applications publics

Apple et Google fournissent chacun une infrastructure pour la distribution des applications. Apple fournit des applications aux utilisateurs finaux par l'intermédiaire de l'Apple App Store. L'App Store est préinstallé sur chaque appareil iOS.

Les applications sont gérées et publiées via le portail des développeurs et le portail iTunesConnect. Google fournit des applications aux utilisateurs finaux par l'intermédiaire du Play Store. Sur chaque appareil Android, l'App Play Store est préinstallé.

L'administration et la publication des applications se font par l'intermédiaire du portail des développeurs. Apple et Google définissent le cadre de publication des applications par l'intermédiaire de leurs systèmes.

Si un appareil est géré par un système MDM, l'application du magasin peut également être bloquée pour l'utilisateur et peut donc être bloquée et probablement non disponible pour l'utilisateur final.

Distribution via l'App Store d'Apple - Avantages

- Les applications sont disponibles pour les utilisateurs finaux par le biais du mécanisme standard d'Apple.
- Les applications n'ont pas besoin d'être re-signées et déployées après un an avec un profil de provisionnement mis à jour.

Pour la version 26.4.0

- Les applications n’ont pas besoin d’être re-signées et re-provisionnées avec un profil de provisionnement mis à jour après un an.
- Les applications peuvent, si nécessaire, être activées ou désactivées de manière sélective pour certains pays.
- Les applications peuvent être proposées à titre onéreux dans des structures définies - si souhaité - (Apple exige une commission de 15 %).
- Apple fournit l’infrastructure de distribution et de facturation.

Distribution via l’Apple App Store - Inconvénients

- Les utilisateurs ont besoin d’un identifiant Apple sur leurs appareils pour installer les applications de l’Apple App Store.
- Pour les entreprises disposant d’appareils gérés, l’Apple App Store peut être bloqué par le MDM.
- Il doit être conforme à toutes les exigences d’Apple, comme la prise en charge des nouvelles classes d’appareils telles que l’iPhone X.
- Apple se réserve le droit de publier un examen avant l’application ou de la supprimer par la suite.
- L’examen peut entraîner des retards allant jusqu’à 10 jours (actuellement, le délai moyen d’examen est d’environ 3 jours ouvrables).
- Les applications ne peuvent être mises à la disposition de certains groupes d’utilisateurs que dans une mesure limitée.

Pour la version 26.4.0

Distribution via Google Play Store - Avantages

- Les applications sont mises à la disposition des utilisateurs finaux par le biais du mécanisme standard de Google.
- Les applications peuvent - si nécessaire - être activées ou désactivées de manière sélective pour certains pays.
- Les applications peuvent - si on le souhaite - être proposées à titre onéreux dans des structures définies (Google exige une commission de 15 % à cet effet).
- Google fournit l’infrastructure pour la distribution et la facturation.

Distribution via Google Play Store - Inconvénients

- Les utilisateurs ont besoin d’un compte Google pour installer des applications à partir du Play Store.

- Pour les entreprises disposant d'appareils gérés, le Play Store peut être bloqué par le MDM.
- L'application doit être conforme à toutes les exigences de Google, notamment en ce qui concerne la version Cordova.
- Google se réserve le droit de retirer l'application du magasin après des analyses automatisées.
- Les analyses techniques peuvent retarder la publication de l'application de quelques heures.
- Les applications ne peuvent être mises à la disposition de certains groupes d'utilisateurs que dans une mesure limitée.

Distribution via les programmes bêta des magasins d'applications publics

Apple et Google proposent également un programme de test bêta en plus de la distribution d'applications publiques. Chez Apple, les applications destinées aux tests bêta des utilisateurs finaux sont fournies par l'intermédiaire de l'application TestFlight. Sur les appareils iOS, cette application peut être installée à partir de l'application Apple Store.
Pour gérer et publier des applications, utilisez le portail des développeurs et le portail iTunesConnect dans la section TestFlight. Google propose des applications pour les tests alpha ou bêta via le Play Store.

Pour la version 26.4.0

Le Play Store est préinstallé sur tous les appareils Android. La gestion et la publication des applications s'effectuent via le portail des développeurs pour les tests alpha et bêta. Apple et Google définissent le cadre de publication des applications par l'intermédiaire de leurs systèmes.

Distribution via Apple Testflight - Avantages

- Les applications sont mises à la disposition des utilisateurs par le biais d'un mécanisme fourni par Apple.
- Les applications peuvent être activées de manière sélective pour des utilisateurs individuels.
- Apple fournit l'infrastructure de distribution et de facturation.

Distribution via Apple Testflight - Inconvénients

- Les utilisateurs ont besoin d'un identifiant Apple pour installer les applications de l'Apple App Store.
- L'installation de l'application nécessite une installation unique de l'application TestFlight.

- Apple se réserve le droit de ne pas publier l'application dans le cadre d'une évaluation "réduite".
- L'examen peut entraîner des retards allant jusqu'à 10 jours (actuellement, le délai moyen d'examen est d'environ deux jours ouvrables).
- La signature des applications expire après 90 jours.

Le service TestFlight est principalement destiné à une courte période d'essai avant la sortie d'une application iOS. Pour une opération permanente, la solution n'est pas adaptée en raison de la courte durée de validité de la signature.

Distribution via Google Alpha et Beta Testing - Avantages

- Les applications sont mises à la disposition des utilisateurs par le biais d'un mécanisme fourni par Google.
- Les applications peuvent être activées de manière sélective pour des utilisateurs individuels.
- Google fournit l'infrastructure de distribution et de facturation.

Distribution via Google Alpha et Beta Testing - Inconvénients

Pour la version 26.4.0

- Les utilisateurs ont besoin d'un identifiant Google pour installer des applications à partir du Play Store.
- Pour les entreprises disposant d'appareils gérés, le Play Store peut être bloqué par le MDM.

Distribution via l'App Store interne de l'entreprise

Apple et Google proposent non seulement la distribution d'applications via leurs magasins publics respectifs, mais aussi des mécanismes de distribution interne d'applications, principalement pour les entreprises. Apple a besoin de l'Apple Enterprise Program et d'un App Store d'entreprise tel que Relution.

Les applications sont mises à la disposition des utilisateurs finaux par le biais d'une application App Store distincte ou d'une page web mobile. Les applications sont gérées via le portail des développeurs.
La distribution des applications se fait par l'intermédiaire du fournisseur respectif de l'App Store d'entreprise. Chez Google, les applications peuvent être mises à disposition via un service web

pour le téléchargement et l'installation.
Pour les appareils spéciaux tels que Samsung, des mécanismes d'installation et de distribution optimisés peuvent être utilisés. Apple et Google sont en train de définir des moyens de distribuer des applications parallèlement à leurs systèmes.

Distribution d'applications iOS via l'App Store d'entreprise - Avantages

- Les applications peuvent être distribuées à des groupes d'utilisateurs sélectionnés, par exemple sous la forme d'un lien profond ou après connexion à l'aide d'un nom d'utilisateur et d'un mot de passe préalablement configurés.
- Les utilisateurs n'ont pas besoin d'un identifiant Apple pour installer des applications à partir d'un magasin d'applications d'entreprise interne.
- Il n'est pas nécessaire de satisfaire à toutes les exigences d'Apple.
- La publication des mises à jour d'applications n'est pas retardée par un examen d'Apple.
- Certains magasins d'applications d'entreprise (tels que Relution) peuvent également être utilisés sans gestion des appareils (MDM).
- Un système de gestion des utilisateurs existant (ActiveDirectory / LDAP) peut être connecté de sorte que les utilisateurs n'aient pas besoin de nouvelles données d'accès.

Pour la version 26.4.0

Distribution d'applications iOS via l'App Store d'entreprise - Inconvénients

- Les applications sont disponibles pour les utilisateurs finaux par le biais d'un mécanisme spécial approuvé par Apple mais nécessitant une configuration initiale par l'utilisateur (voir ici →).
- Les applications doivent être re-signées et déployées après un an avec un profil de provisionnement mis à jour. Ce n'est pas un inconvénient dans ce cas, car Relution peut automatiser ces tâches.
- L'infrastructure de distribution peut être fournie, par exemple, sous la forme d'un service en nuage ou sur site.
- Selon les directives d'Apple, la distribution d'applications ne peut se faire qu'aux employés, aux prospects et aux partenaires, mais surtout à un groupe d'utilisateurs connus.

Distribution d’applications Android via l’App Store d’entreprise - Avantages

- Les applications peuvent être distribuées à des groupes d’utilisateurs sélectionnés, par exemple sous la forme d’un lien profond ou après connexion à l’aide d’un nom d’utilisateur et d’un mot de passe préalablement configurés.
- Les utilisateurs n’ont pas besoin d’un identifiant Google pour installer des applications à partir d’une boutique d’applications interne à l’entreprise.
- Il n’est pas nécessaire de satisfaire à toutes les exigences de Google.
- La publication des mises à jour d’applications n’est pas retardée par les analyses techniques de Google.
- Certains magasins d’applications d’entreprise (tels que Relution) peuvent également être utilisés sans gestion des appareils (MDM).
- Un système de gestion des utilisateurs existant (ActiveDirectory / LDAP) peut être connecté, de sorte que les utilisateurs n’ont pas besoin de nouvelles données d’accès.

Distribution d’applications Android via l’App Store d’entreprise - Inconvénients

Pour la version 26.4.0

- Les applications sont accessibles aux utilisateurs finaux par le biais d’un mécanisme spécial approuvé par Google, mais nécessitant une configuration initiale par l’utilisateur.
- L’infrastructure de distribution doit être fournie, par exemple sous la forme d’un service en nuage.

Certificat d'identité

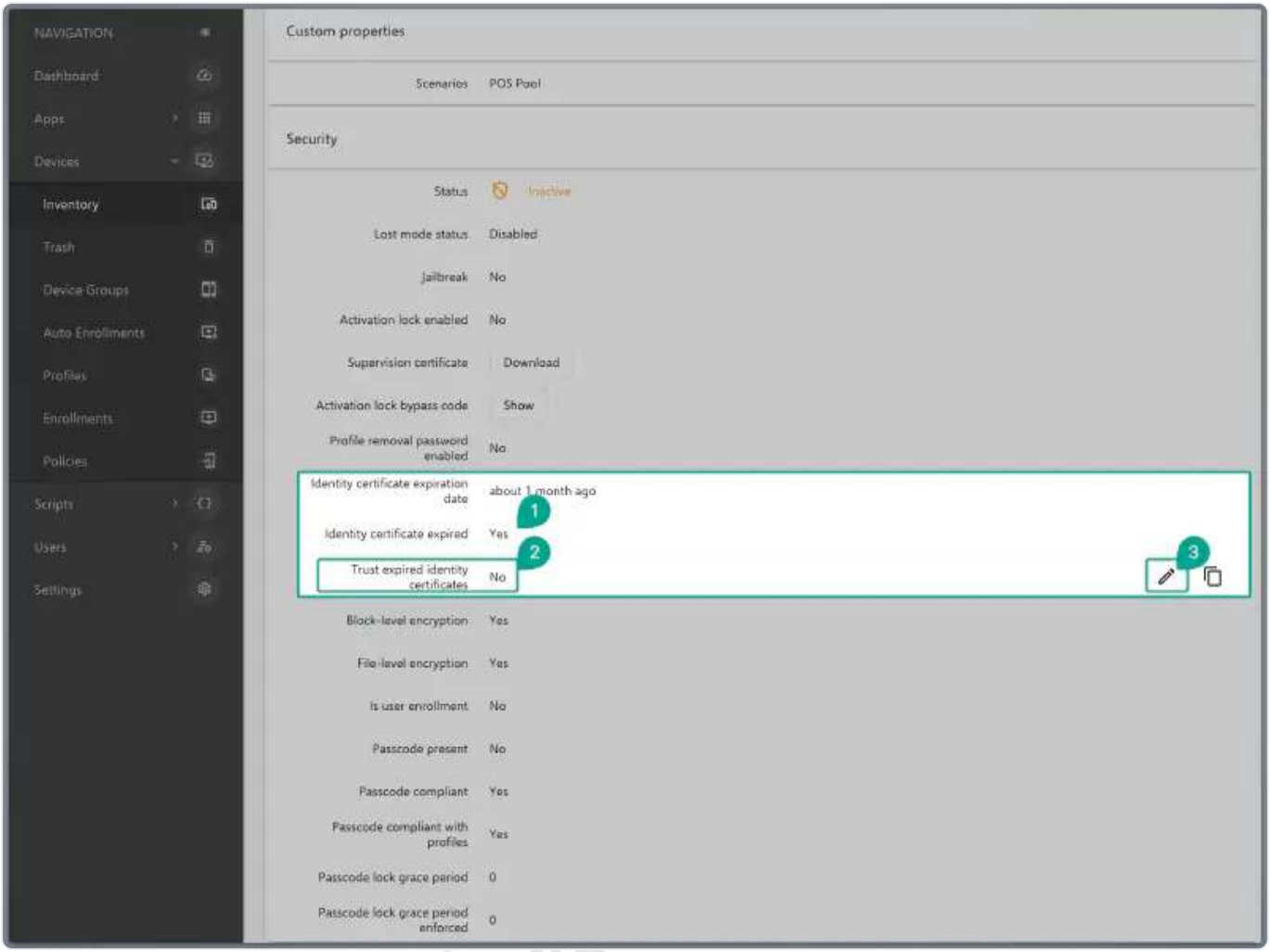
Les appareils Apple et Windows enrôlés dans Relution reçoivent un certificat d’identité. Celui-ci est valable 1 an et est automatiquement renouvelé tant qu’il y a une communication avec l’appareil. Il peut arriver que des appareils soient stockés ou inactifs, et que le certificat d’identité ne puisse pas être renouvelé en conséquence. Pour des raisons de sécurité, Relution refuse toute communication avec un appareil si le certificat d’identité a expiré.

Vérifier et renouveler le certificat d’identité

Les appareils concernés peuvent être vérifiés sous `Navigation` → `Appareils` → `Inventaire` → `[Appareil]` dans l’onglet Informations du bloc Sécurité. Il y a 3 champs pertinents ici :

- Date d’expiration du certificat d’identité
- Le certificat d’identité a expiré
- Faire confiance aux certificats d’identité expirés

Pour la version 26.4.0



Si un certificat d'identité a expiré, le mode d'édition peut être activé en survolant l'option Faire confiance aux certificats d'identité expirés avec la souris, et le certificat peut être renouvelé. La communication avec l'appareil redevient ainsi digne de confiance et les commandes MDM peuvent être traitées.

Places de marché alternatives

La version 17.4 d'iOS prend en charge les places de marché d'applications tierces pour les appareils situés dans l'Union européenne (UE). Grâce à l'introduction d'une autorisation spéciale, les développeurs tiers peuvent désormais créer leurs propres places de marché d'applications alternatives qui peuvent être téléchargées et installées sur les appareils fonctionnant sous iOS 17.4 ou une version ultérieure. Les places de marché d'applications alternatives offrent une nouvelle méthode de distribution des applications qui permet aux utilisateurs de l'UE de télécharger des applications en dehors de l'App Store d'Apple.

Configuration via la restriction Relution

La configuration `Allow installation of alternative app marketplaces` a été ajoutée aux restrictions. Cela permet d'ajuster facilement la valeur dans Relution.

Configuration via Apple Configurator 2 Configuration dans Relution

Pour la version 26.4.0

1. Créer une nouvelle politique avec le nom `Restrict Marketplace` (Restriction sur les places de marché)
2. Ajouter une configuration `Apple Configurator 2` dans cette politique
3. Créer un fichier texte vide avec le contenu suivant et l'enregistrer sous `restrictMarket.mobileconfig`

> Show full configuration example

1. Attribuer un nom dans la configuration `Apple Configurator 2` et télécharger le fichier mobileconfig créé.
2. Publier la politique et l'assigner aux appareils avec iOS 17.4 ou plus.

> Important ! Si la politique est affectée à des appareils sous iOS 17.4, elle doit être supprimée et réaffectée.

Séparation des données

Lors de l'utilisation d'appareils mobiles, on accède à des données de toutes sortes. La conformité de la protection des données doit être garantie. On distingue les appareils appartenant à l'entreprise, appelés "Corporate Owned devices" (COD), et les appareils appartenant à l'utilisateur, appelés "Bring Your Own Devices" (BYOD). Pour les deux types d'utilisation, les fabricants des systèmes d'exploitation d'appareils mobiles iOS et Android proposent désormais leurs propres technologies de séparation des données. Ces "moyens embarqués" et leur mise en œuvre dans Relution sont décrits en détail ci-après.

iOS - Appareils appartenant à l'entreprise

Différenciation géré / non géré

Depuis iOS12, Apple fait fondamentalement la distinction entre "managed" et "unmanaged" pour les objets suivants :

Pour la version 26.4.0

Appareils gérés

1. Apps- poussées par Relution ou installées via l'Appstore de Relution Enterprise, configurables par le serveur.
2. Comptes de messagerie - configurés par Relution via une stratégie.
3. Contacts - chargés depuis le compte de messagerie géré vers l'appareil (synchronisés).
4. Documents - chargés depuis le compte de messagerie géré vers l'appareil (synchronisés).

Appareils non gérés

1. Apps - installées par l'utilisateur à partir de l'AppStore d'Apple, non configurables par le serveur.
2. Comptes de messagerie - configurés sur l'appareil par l'utilisateur.
3. Contacts - créés par l'utilisateur.
4. Documents - générés par l'utilisateur dans des applications non gérées ou reçus dans des comptes de messagerie non gérés.

Une application non gérée peut être convertie en une application gérée en étant à nouveau poussée par Relution. Elle remplace l'application non gérée du même nom sur l'appareil. Cependant, les comptes de messagerie, les contacts et les documents non gérés ne peuvent pas être transférés vers des applications gérées.

Restrictions d’accès

Dans iOS, les données sont séparées du côté du système au moyen d’une politique qui permet de définir si l’accès aux données gérées à partir d’applications non gérées doit être autorisé ou non. À cette fin, la configuration Restrictions en tant que partie d’une politique dans Relution offre les options de restriction suivantes :

- Interdire l’ouverture de documents gérés dans des applications non gérées.
- Autoriser l’ouverture de documents non gérés dans les applications gérées.
- Interdire aux applications non gérées l’accès aux contacts gérés.
- Autoriser les applications gérées à écrire des contacts non gérés.
- Considérer généralement les cibles AirDrop comme non gérées.
- Interdire le déplacement de messages vers des comptes de messagerie non gérés.

Par exemple, les éléments suivants peuvent être empêchés :

- Une application privée (par exemple WhatsApp) qui voit des contacts professionnels (Exchange).
- Un courrier professionnel est transféré à volonté.
- Une pièce jointe d’un courrier professionnel est ouverte dans n’importe quelle application (par exemple Dropbox).

Les contenus web qu’iOS traite comme gérés, p. ex. les téléchargements depuis l’intranet, sont définis via la configuration Domaines gérés →. Il est également possible d’y indiquer des domaines de messagerie afin que l’application Mail signale les destinataires externes.

Pour la version 26.4.0

Restrictions iCloud

Pour prévenir toute fuite incontrôlée de données, Relution permet de bloquer ou, à minima, de restreindre strictement l’utilisation des comptes cloud. Les fonctionnalités suivantes peuvent ainsi être désactivées :

- Sauvegardes iCloud
- synchronisation du trousseau iCloud
- Autoriser les applications gérées à stocker des données dans iCloud
- Enregistrement de photos dans iCloud
- Synchronisation des documents iCloud.

Restrictions fonctionnelles

Enfin, certaines fonctions du système iOS peuvent être considérées comme des critères de sécurité des données et peuvent également être désactivées par restriction :

- Blocage/autorisation de l’application
- Blocage/autorisation des URL Web
- AirDrop (peut être complètement désactivé)
- Partage du mot de passe
- Accès à l’AppStore d’Apple
- Captures d’écran et enregistrements
- Appareil photo (peut être complètement désactivé, y compris pour les fonctions in-app)
- Création et modification de comptes (Mail, Apple ID)
- Bluetooth
- Installation de profils VPN
- Connexions USB.

Via l’application VPN

En tant que mesure importante de protection des données, iOS offre la possibilité de coupler en permanence la connexion de données des applications à une connexion VPN, qui peut à son tour être reconfigurée par le serveur Relution. Cela permet de s’assurer que certaines applications ne fonctionnent que sur le réseau de l’entreprise et que l’accès externe est empêché (intranet uniquement).

Pour la version 26.4.0

iOS - Appareils personnels (BYOD)

Jusqu’à iOS 12, il était courant d’utiliser une application conteneur sur les appareils iOS BYOD qui pouvait être configurée du côté du serveur et garantissait ainsi la séparation des données professionnelles et privées.

Entre-temps, iOS propose une “solution de conteneur” intégrée pour séparer les applications et les données professionnelles des données privées. À cette fin, un appareil iOS est ajouté à Relution par le biais d’une inscription (BYOD) dans l’inventaire. Un profil MDM est ainsi installé sur l’appareil, ce qui permet de le gérer via Relution. Techniquement, une distinction est alors faite entre les applications et le contenu “gérés” et “non gérés”. Cela transforme l’appareil iOS en un appareil à “double personnalité” et sépare complètement les données. Des restrictions peuvent également être utilisées pour contrôler si les données peuvent être partagées entre les applications “gérées” et “non gérées”.

Différentes configurations peuvent être chargées sur les appareils et gérées par Relution :

- Apps
- Configuration VPN
- Notes (d’autres applications système suivront dans les prochaines versions d’iOS)

- Compte iCloud
- Trousseau
- Comptes de messagerie / pièces jointes
- Comptes de calendrier / pièces jointes.

Si le profil MDM est supprimé, toutes les applications et tous les contenus gérés sont supprimés. Cette action peut être effectuée via Relution ou sur l’appareil lui-même.

Pour la version 26.4.0

Listes de classes (iPad partagé)

Grâce à la fonction des listes de classes pour les iPad partagés dans Relution, la connexion avec des comptes Apple gérés est optimisée pour les élèves. Plutôt que de devoir saisir manuellement l'identifiant Apple géré (Managed Apple ID) complet, souvent long, les élèves peuvent simplement sélectionner leur classe puis leur nom ou leurs initiales.

Conditions préalables

Pour pouvoir utiliser cette fonction, les conditions suivantes doivent être remplies :

- Jeton DEP : au moins un jeton DEP valide pour le site concerné.
- Identifiants Apple gérés : disposer de comptes Apple gérés.
- Appareil compatible : un iPad partagé Apple configuré via le même jeton DEP que celui utilisé pour gérer les comptes Apple gérés.

Pour la version 26.4.0

Configuration

Les étapes suivantes permettent d'activer les listes de classes :

1. Ouvrir les politiques : accéder dans Relution à la section Politiques.
2. Créer une politique : créer une nouvelle politique iOS ou modifier une politique existante.
3. Ajouter une configuration : ajouter la configuration iPad partagé.
4. Sélectionner les classes : choisir les classes à autoriser pour la connexion sur l'iPad partagé.
5. Finalisation : une fois la politique attribuée, les classes disponibles sont proposées à la sélection sur l'écran de verrouillage de l'iPad.

Remarques importantes pour le dépannage

Si des problèmes de connexion surviennent, cela provient souvent d'une discordance dans les données de compte :

- Comparaison des comptes : vérifier le compte Apple de l'utilisateur enregistré dans Relution.
- Exemple de discordance :
  - Compte dans Relution : `Eleve@relution.io`

    - Compte dans Apple School Manager : `Eleve@appleid.relution.io`
- Solution : les comptes doivent correspondre exactement pour que la connexion via la liste de classes fonctionne.

Astuce : tester la connexion manuellement via la méthode classique Se connecter à l'iPad. Si les identifiants fonctionnent ainsi mais pas via la liste de classes, il y a fort probablement une discordance dans les données utilisateur enregistrées.

Pour la version 26.4.0

Restrictions recommandées

Un grand nombre de restrictions peuvent être configurées pour les appareils iOS. Chaque réglage n'est pas toujours utile ou ne conduit pas toujours au résultat souhaité. Parfois, les réglages entraînent également des problèmes si l'on ne sait pas exactement comment ils agissent. Dans cet article, nous nous limiterons à quelques problèmes potentiels que l'on peut rencontrer en tant qu'utilisateur et nous nommerons les réglages recommandés.

> De nombreuses restrictions ne peuvent être configurées que sur des appareils en mode supervisé. Elles sont indiquées par la note En mode supervisé

Autoriser la connexion aux Macs ou aux PCs

Ce paramètre n'a d'effet que si la connexion aux Macs ou aux PCs a été autorisée dans le DEP profile. Si ce n'est pas le cas, le paramètre correspondant dans les restrictions n'a aucun effet.

Activer le délai des mises à jour du système d'exploitation

Une valeur comprise entre 1 et 90 jours peut être définie ici. Pendant cette période, les nouvelles mises à jour du système ne sont pas affichées pour les utilisateurs et ne sont donc pas installées. Cela concerne également les mises à jour de sécurité.

Autoriser la connexion USB en mode verrouillé

profile mway-chat-max Today at 16:03 Si les appareils ne sont plus connectés à Internet, ils peuvent être reconnectés, par exemple à l'aide d'une carte réseau externe (adaptateur Lightning/Ethernet). Toutefois, si les appareils sont verrouillés, par exemple en mode perdu, les accessoires externes ne peuvent pas être débloqués par les utilisateurs et ne fonctionnent donc pas. Ce réglage permet d'éviter cela.

Pour la version 26.4.0

Autoriser la suppression de tous les contenus et paramètres

Il s’agit de la réinitialisation d’usine. Si cette option ne doit pas être proposée, elle doit être décochée.

Interdire la désactivation du WiFi

Si cette option est activée, les utilisateurs ne pourront pas éteindre le WiFi, même en mode vol. Le passage d’un réseau WiFi à l’autre reste autorisé.

Forcer le réglage automatique de la date et de l’heure

Ce paramètre ne fonctionne que si les services de localisation ont été activés sur les appareils. Les appareils règlent automatiquement la date et l’heure. Cela se fait également en fonction du fuseau horaire dans lequel il se trouve. Ceci ne peut pas être déterminé si les services de localisation sont désactivés.

Pour la version 26.4.0

Forcer la liste blanche WiFi

Si cette option est activée, les appareils ne pourront se connecter qu’aux réseaux qui leur ont été apportés par le biais d’une politique. Avant d’activer cette fonction, s’assurer que les réseaux transférés fonctionnent sur les appareils. Il n’est pas possible d’ajouter manuellement des connexions WiFi par la suite.

Installation silencieuse

Pour installer des applications “silencieusement” sur les appareils iOS, il est nécessaire que les appareils soient en “mode supervisé” et que des licences VPP soient disponibles pour l’application, ou que les utilisateurs soient connectés aux appareils avec un identifiant Apple.

Si ces conditions sont remplies, les applications peuvent être installées sur les appareils via Relution sans que les utilisateurs n’aient à le confirmer sur les appareils finaux. S’assurer que suffisamment de licences VPP sont disponibles.

S’il n’y a pas assez de licences VPP, une invite à se connecter à l’App Store peut apparaître sur les appareils. Cela peut également se produire si Relution et le serveur VPP d’Apple ne sont pas synchronisés. Dans ce cas, passer à la section Apps achetées et effectuer une synchronisation à cet endroit.

Pour la version 26.4.0

Gérer les apps natives

Avec Relution, il est possible de distribuer des applications iOS natives et de gérer les versions. Cela signifie que différentes versions peuvent être fournies à différents groupes de personnes. Par exemple, les utilisateurs peuvent avoir la version 1.0 d'une application en usage productif, tandis qu'un groupe d'utilisateurs clés teste la version 1.1 sans que les utilisateurs s'en aperçoivent. Pour cela, la version 1.0 doit être téléchargée sur Relution au début et avoir le statut "productif".

La distribution et l'installation automatiques d'applications natives ne sont pas possibles avec Android Enterprise.

Créer une nouvelle application.

Pour ce faire, cliquer sur `Apps` → `App Store` dans le menu. Un `Type d'application` peut ici être sélectionné via le bouton `Ajouter`. Cliquer sur `Native App`.

Sélectionner maintenant le fichier approprié de l'application à télécharger.

> Faire attention à la taille du fichier. Pour les applications volumineuses, des problèmes peuvent survenir si la base de données ou le reverse proxy ne le permet pas. Dans ce cas, la configuration devra être ajustée.S

Pour la version 26.4.0

Spécifier le statut de la version appropriée et cliquer sur `Save`.

Cette application peut maintenant être vue et installée dans le `Relution Agent` de la plateforme correspondante par les membres des groupes `Appstore User` et `Device Manager`. Les permissions peuvent également être ajustées à ce stade. Indépendamment de cette permission, les administrateurs peuvent également distribuer cette application aux appareils via le portail Relution.

Mettre à jour l'application

Si une nouvelle version doit être testée pour l'application, elle peut être mise à l'état 'Développement' ou 'Test' à l'avance. Avant cela, la nouvelle version doit être sélectionnée et téléchargée via le bouton 'Nouvelle version'.

Dans l’exemple, l’application est dans le statut `testing`. Elle passera automatiquement au statut `Productive` le 31/5/2022. La `date de sortie` peut être utilisée de manière optionnelle.

Les deux versions peuvent être visualisées dans les propriétés de l’application.

Les utilisateurs ayant les permissions adéquates (groupe inside, par exemple) peuvent consulter, installer et tester l’application sur les points de terminaison correspondants.

Mise en service manuelle de la nouvelle version

Dans le portail Relution, les différentes versions peuvent être visualisées et configurées. En cliquant sur le bouton ‘Productif’, la nouvelle version passe à ce statut. Si une version est déjà dans le statut productif, elle sera automatiquement déplacée vers l’“Archive”.

L’application n’est pas automatiquement mise à jour sur les terminaux. Cela doit être fait manuellement par les utilisateurs via l’Agent de Relution ou déclenché par les administrateurs via une action manuelle Install App.

Pour la version 26.4.0

Gérer les apps de l'App Store

Les applications de l’App Store d’Apple peuvent être distribuées aux appareils gérés via Relution. Une licence d’application est requise dans tous les cas — y compris pour les applications gratuites.

Obtenir une licence

Une licence d’application peut être obtenue de deux manières :

- via le `Volume Purchase Program` (VPP) d’Apple,
- ou via un identifiant Apple connecté sur l’appareil.

Le choix dépend du scénario d’utilisation. Sur les appareils utilisés sans identifiant Apple, une licence VPP est indispensable.

Configurer le VPP →

Pour la version 26.4.0

Applications issues d’Apple School Manager et Business Manager

Les applications achetées dans Apple School Manager ou Apple Business Manager sont synchronisées automatiquement avec Relution (à partir de la version 5.10). Elles y apparaissent avec le statut de publication productif et sont immédiatement prêtes à être distribuées.

Si une application ne doit pas être accessible à tous les utilisateurs, le statut de publication peut être modifié manuellement.

Ajouter une application manuellement

Une application peut être ajoutée manuellement à l’App Store de Relution à tout moment. Deux restrictions s’appliquent :

- Aucune licence VPP n’est disponible automatiquement pour les applications ajoutées manuellement.

- L’installation n’aboutit que sur les appareils où un utilisateur est connecté avec un identifiant Apple.

Des licences VPP peuvent être obtenues ultérieurement pour ces applications.

Forcer une mise à jour

Les applications de l’App Store sont mises à jour automatiquement par le système d’exploitation. Dans de rares cas, cela n’a pas lieu. L’action d’appareil Installer l’application déclenche une mise à jour : l’appareil relance l’installation et compare la version de l’application avec celle de l’App Store. Si une version plus récente y est disponible, l’application existante est mise à jour.

Pour la version 26.4.0

Les actions ne sont pas traitées

Dans les environnements scolaires et autres scénarios où les appareils iOS sont gérés de manière centralisée à l'aide de la gestion des appareils mobiles (MDM), des perturbations peuvent occasionnellement se produire. L'un des problèmes les plus courants est l'incapacité des appareils à traiter les actions MDM, ce qui peut entraîner des problèmes importants, que ce soit pendant les cours ou dans le fonctionnement général des appareils. Cet article décrit les schémas d'erreur potentiels, analyse leurs causes sous-jacentes et propose des solutions pour remédier à ces situations.

Certificats expirés

Error Pattern: Les actions MDM restent en attente et ne sont pas exécutées par l'appareil.

Cause: Le certificat d'identité de l'appareil iOS a expiré. Cela se produit souvent avec des appareils qui ont été stockés pendant une longue période et qui n'étaient pas en communication avec le serveur MDM peu de temps avant le renouvellement automatique du certificat.

Voir aussi : Certificat d'identité → — cette page décrit la durée de validité, le renouvellement automatique ainsi que le renouvellement manuel d'un certificat expiré.

Pour la version 26.4.0

VPN Apps

Modèle d'erreur: Les appareils iOS se bloquent pendant les leçons, ou les configurations basées sur le temps, comme le démarrage ou la fin d'une leçon, ne sont pas exécutées.

Cause: Souvent, les utilisateurs finaux, en particulier dans les contextes éducatifs, installent des applications VPN de leur propre chef, ce qui bloque la communication avec le serveur MDM. Certaines applications VPN offrent également une fonction "Kill-Switch", qui permet aux utilisateurs de déconnecter intentionnellement toute communication internet. Cela interrompt les actions de MDM, telles que le démarrage ou la fin des cours. Sur les appareils concernés, les applications VPN peuvent être identifiées dans Relution sous "Apps installées".

Solution: Dans Relution, il est possible de restreindre l'installation ou l'utilisation des VPN. Pour ce faire, aller dans les Restrictions et activer l'option `Désactiver la configuration VPN`. Avec ce paramètre, il ne sera plus possible de créer des configurations VPN non gérées sur les appareils.

DNS

Error Pattern: Les appareils iOS restent bloqués pendant les leçons, ou les configurations basées sur le temps - telles que le début ou la fin d'une leçon - ne sont pas exécutées.

Cause: Une raison fréquente est que les utilisateurs finaux, en particulier dans les écoles, configurent manuellement un DNS alternatif. Cela peut bloquer la communication avec le serveur MDM, entraînant l'échec des actions MDM. Sur les appareils concernés, naviguer vers "Paramètres > WiFi > DNS" pour vérifier les configurations DNS personnalisées.

Solution: Pour éviter de tels problèmes, une configuration pour `Paramètres DNS cryptés` peut être appliquée dans Relution. Cela garantit que les modifications apportées au DNS par les utilisateurs finaux ne seront pas prises en compte (même si la configuration reste possible), en donnant la priorité à la communication via le serveur DNS géré.

Fournisseurs fiables et guides de configuration

- Google DNS](https://developers.google.com/speed/public-dns/docs/dns-over-tls?hl=en)
- Cloudflare DNS →

Pour la version 26.4.0

Optimiser l'appareil partagé

Lorsqu'un utilisateur change de mode de fonctionnement en `Relution Shared Device Mode`, selon la configuration, de nombreuses applications, voire plusieurs gigaoctets de données, sont téléchargées. Cela peut entraîner des retards dans l'enseignement en raison du volume élevé de données et du grand nombre de téléchargements et d'installations.

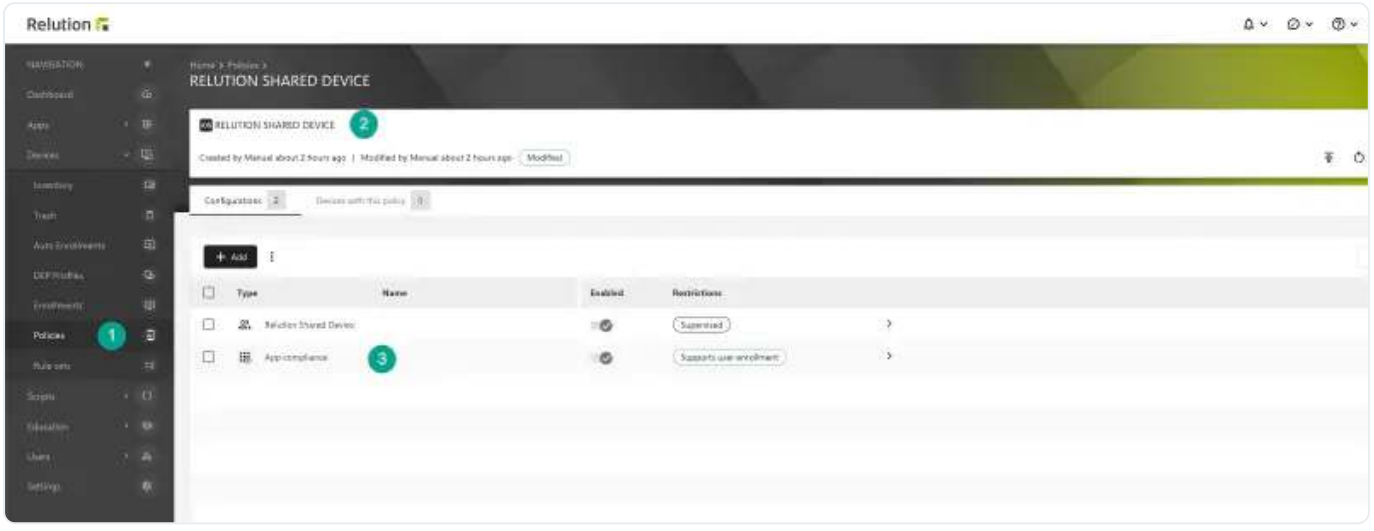
Afin de pouvoir supprimer le contenu temporaire des applications utilisées lorsque les appareils sont utilisés par plusieurs utilisateurs, Relution doit supprimer les applications des appareils lors de la déconnexion de l'utilisateur. Pour en savoir plus, consulter les liens suivants
. Mode multi-utilisateurs →

Optimisations

Les mesures suivantes sont recommandées pour réduire au minimum les retards des classes :

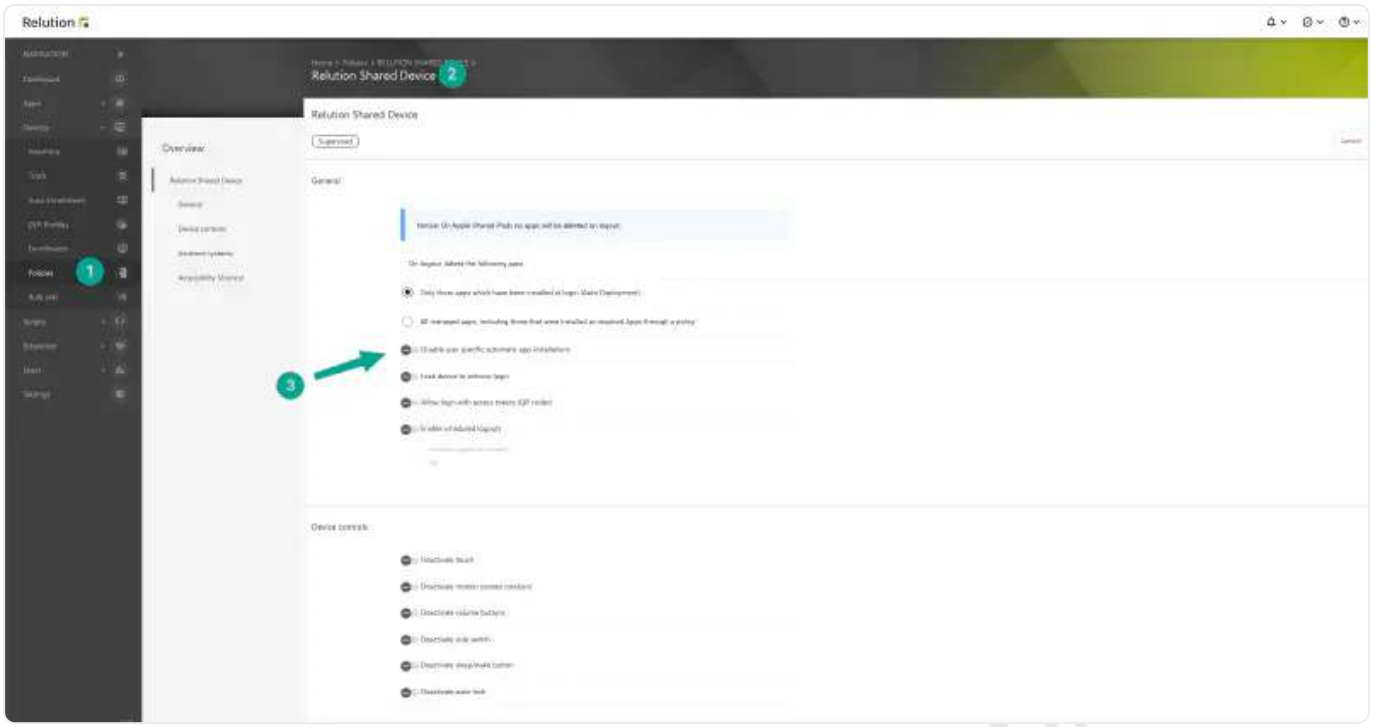
Minimiser la conformité des applications et les déploiements automatiques.

Garder la liste des "Applications Requises" dans la configuration de la politique de "Conformité des Applications" relativement petite. Un petit ensemble d'applications de base pour tous les appareils est généralement suffisant. Chaque application doit être transférée à travers le réseau plusieurs fois, une fois pour chaque appareil sur lequel la politique s'applique. Ainsi, 50 Mo se transforment rapidement en 5 Go lorsque les cours commencent.



Pour la version 26.4.0

En outre, il est possible de désactiver les “déploiements automatiques” pour les applications spécifiques à l’utilisateur afin de réduire au maximum l’empreinte de la connexion de l’utilisateur.



Alternativement, les applications requises peuvent être rétrofitées sur les appareils des utilisateurs à tout moment via l’agent Relution.

Pour la version 26.4.0

Profils d’enseignement via Relution Teacher.

Si la mesure ci-dessus a été suivie et qu’il n’y a pas ou peu d’applications stockées dans `App Conformance` et `Auto Deployments`, les enseignants peuvent utiliser l’application Relution Teacher et l’utilisation de `Teaching Profiles` pour prédéfinir toutes les applications requises pour les leçons. De cette manière, seules les applications nécessaires à la leçon en question seront chargées.

Pas maintenant

Les actions pour les appareils iOS sont en attente et ne sont pas traitées.

Les actions sont des opérations exécutées et des modifications effectuées via Relution sur des appareils enrôlés. Elles peuvent être déclenchées soit par une configuration de politique, soit par une action. L'aperçu de toutes les actions se trouve dans les détails de l'appareil sous l'onglet Actions.

Cause

Les appareils iOS ne sont pas en mesure d'accepter et d'exécuter des actions. Celles-ci s'accumulent dans la file d'attente des actions. Cela peut être dû à plusieurs raisons :

- Les appareils ont un code de déverrouillage. Cela empêche le traitement de certaines actions. Il s'agit par exemple de l'application de restrictions. L'écran affiche alors `Pas maintenant`.
- L'appareil a été redémarré et n'a pas été déverrouillé. Le trousseau numérique est alors verrouillé. Par conséquent, les appareils ne peuvent pas se connecter à un réseau WiFi crypté et ne peuvent donc pas recevoir et traiter des actions.

Pour la version 26.4.0

Ceci est une limitation par Apple et se produit indépendamment de Relution.

Solution

Déverrouiller les appareils et s'assurer d'une connexion WiFi pour résoudre l'état `Pas maintenant`.

Plus d'informations

Le statut `Pas maintenant` a été introduit avec la version 5.8.1 de Relution. Depuis Relution 5.9, les actions `Mode perdu` et `Réinitialisation du mot de passe` déclenchent un saut des actions en attente. Une fois qu'une connexion Internet est établie, ces deux actions sont prioritaires et toutes les autres actions en attente sont ignorées.

Apple Dev-Doku Not Now Status →

Noms des appareils

- Les appareils DEP perdent le nom de l'appareil précédemment assigné dans l'inventaire de l'appareil après une réinitialisation.
- L'exportation d'un fichier CSV depuis `Appareils` → `Inventaire` ne peut pas être importé dans `Appareils` → `Auto-enrôlement` et vice versa.

Cause

- Le nom de `Auto enrollment` écrase le nom de l'appareil modifié ultérieurement dans l'inventaire.
- Le format du fichier `CSV` exporté est différent du format du fichier `CSV` importé et contient des champs différents.

Solution.

Exporter le fichier `CSV` avec les noms d'appareils souhaités à partir de l'inventaire et transférer les données dans le format modèle du fichier `CSV` de `auto enrollment` à importer.

Pour la version 26.4.0

Des modèles de fichiers CSV peuvent être téléchargés pour `Auto enrollment` et `Inventory`. Le format correct pour les changements de nom est ainsi obtenu dans chaque cas.

> La première ligne du modèle de format est obligatoire et ne doit pas être modifiée.S

Copier le numéro de série et le nom de l'appareil à partir des données exportées, puis les importer dans `Auto Enrollments`. Si les appareils sont nouvellement enrôlés, le nom correct de l'appareil sera maintenant entré dans les `Enrôlements Automatiques`.

Instruction

1. Exporter la liste d'inventaire.
2. Télécharger le modèle de format pour l'importation dans `Auto enrollments`.
3. Importer les données correspondantes de l'exportation dans le modèle de format pour l'importation. Importer le modèle de format rempli dans `Auto-enrollments`.

Mode multi-utilisateurs

Relution et Apple proposent chacun leur propre mode multi-utilisateurs.

Dispositif partagé par Relution et iPad partagé par Apple.

Les deux modes apportent des fonctionnalités différentes. Une description détaillée à ce sujet est disponible dans nos Insights :

Dispositif partagé Relution →

> Avec iOS 17.x, l'utilisation de la configuration de restriction allowCloudKeychainSync false entraîne un ralentissement de la connexion sur les appareils partagés Apple

Exigences définies comme aide à la décision

Pour la version 26.4.0

Définir les exigences pour les appareils en mode multi-utilisateurs afin de mieux choisir l'une des deux solutions. Les points suivants fournissent des indications :

- Travail conforme au GDPR
- Disponibilité de `Apple Classroom` pour les enseignants
- Connexion simple sans nom d'utilisateur ni mot de passe
- Faible bande passante disponible
- Pas d'utilisateurs et/ou de classes créés dans Relution
- Temps de connexion le plus court possible
- Utilisation d'applications système nécessaire
- Utilisation de lecteurs personnels
- Utilisation de `Relution Teacher`

Comparaison des exigences

Les exigences ne sont que partiellement satisfaites par les deux modes :

Fonction	Relution Shared Device	Apple Shared iPad
Conformité RGPD	Oui	Uniquement en mode invité
Les élèves sont-ils visibles en ligne dans l’app Classroom ?	Oui	Pas en mode invité
Connexion sans nom d’utilisateur et mot de passe	Non	Oui
Bande passante disponible faible	Dépend de la configuration	Oui
Aucun utilisateur et/ou classe créé dans Relution	Non	Oui
Temps de connexion aussi courts que possible	Dépend de la configuration	Oui
Utilisation des applications système nécessaire	Non	Oui
Utilisation des lecteurs personnels	Oui	Non
Utilisation de la console enseignant Relution	Oui	Uniquement avec Relution Shared Device

Mode invité

Si le temps de connexion le plus rapide possible est requis et que la bande passante disponible est faible, l’Apple ‘Split iPad’ est tout indiqué. Il permet de se connecter en mode “invité”, ce qui garantit une utilisation anonyme. En tant qu’invité, cependant, les appareils ne sont pas affichés comme étant “en ligne” dans `Apple Classroom`. Pour travailler dans le respect du GDPR et utiliser `Apple Classroom`, le mode multi-utilisateurs d’Apple est hors de question. Avec le mode `Relution Shared Device`, cette combinaison est possible.

Applications système

Étant donné que Relution ne peut supprimer les données temporaires et le contenu des applications qu'en les désinstallant des appareils, il n'est pas recommandé d'utiliser les applications système qui stockent des données. Par exemple, le navigateur Safari est l'une de ces applications système. Elle ne peut pas être désinstallée, ce qui signifie que le contenu et les onglets ouverts par les utilisateurs précédents sont toujours disponibles et peuvent être consultés lorsqu'un utilisateur change. Pour contourner ce problème, d'autres applications peuvent être utilisées, comme le navigateur Firefox, qui peut être supprimé de l'appareil.

Photos

En ce qui concerne les photos, l'appareil photo natif doit également être désactivé sur les appareils iOS. Sinon, les photos créées sont automatiquement enregistrées dans l'application système `Photos`, qui ne peut pas non plus être supprimée. Ainsi, les photos créées ne peuvent pas être supprimées par Relution. Relution Camera offre également la possibilité d'enregistrer les photos créées non pas sur les appareils, mais sur un lecteur réseau configuré.

Applications Microsoft

Lors de l'utilisation d'applications Microsoft telles que `Teams` ou `Excel`, la caractéristique spéciale suivante doit être prise en compte :

Si les appareils sont utilisés en mode `Relution Shared Device` et que les utilisateurs ne se déconnectent pas de ces applications, les connexions sont stockées dans le trousseau numérique des appareils et ne peuvent pas être supprimées en les désinstallant. Les utilisateurs doivent être informés qu'il est obligatoire de se déconnecter de ces applications. Une autre solution consiste à utiliser l'"iPad partagé" d'Apple.

Pour la version 26.4.0

Combinaison des deux modes multi-utilisateurs

Il est possible d'activer simultanément `Relution Shared Device` et `Apple Shared iPad`. Cette combinaison permet de bénéficier des avantages des deux solutions. Grâce au système Apple `Guest Mode`, les applications peuvent être utilisées sans laisser de données sur les appareils. En même temps, grâce à `Relution Agent`, les enseignants peuvent appliquer des `Profils d'enseignement` avec des applications et des fonctionnalités pertinentes sur les appareils des étudiants.

Lorsque le mode invité est utilisé sur les appareils des élèves, Apple Classroom ne peut pas être utilisé par les enseignants.

Disposition écran d'accueil

Avec Relution Homescreen Layout, il est possible d’organiser les applications et de les placer clairement dans différents dossiers.

Problème

Lors de la configuration de la politique `Homescreen Layout`, aucun dossier n’est créé dans le simulateur.

Solution

Afin de créer un dossier lors de l’utilisation de la fonctionnalité `drag & drop` du simulateur, veiller à positionner l’application absolument immobile au-dessus d’une autre icône d’application pendant une courte période de temps afin qu’un dossier soit automatiquement créé.

La disposition de l’écran d’accueil est actuellement limitée à 20 applications par page.

Pour la version 26.4.0

Créer un Apple Case

Après des mises à jour du système d'exploitation sur des appareils Apple, des dysfonctionnements ou des problèmes inattendus peuvent parfois survenir. Dans de telles situations, nous recommandons d'ouvrir directement un Case chez Apple afin d'accélérer l'analyse et la résolution du problème.

Transmettre ensuite l'ID du Case du ticket Apple via notre support. Nous le transmettons également à nos contacts Apple pour soutenir et accélérer davantage le traitement.

Créer un Apple Case

1. Ouvrir le site web : Feedback Assistant d'Apple →
2. Se connecter avec l'ID ASM/ABM.
3. Lors de la première visite, un choix s'affiche entre :
    - Beta Program
    - Developer Program

   Sélectionner ici Beta Program.

Pour la version 26.4.0

Quels sujets peuvent être signalés ?

Il est possible de soumettre des cases pour les plateformes Apple suivantes :

- iOS / iPadOS
- watchOS
- tvOS
- macOS
- HomePod
- visionOS

Pour nous, iOS / iPadOS ainsi que macOS sont particulièrement pertinents.

Informations importantes lors de la soumission d’un case

Pour l’exemple d’*iOS / iPadOS*, les champs suivants doivent être remplis :

- Titre du problème
- Catégorie : `Something Else Not on the List`
- Type de problème : `Incorrect / Unexpected Behaviour`
- Description du problème (en anglais) → aussi détaillée et précise que possible

Informations nécessaires dans la description du problème

S’assurer que les points suivants sont inclus :

- Version du système d’exploitation des appareils concernés
- Moment/circonstances d’apparition du problème
- Reproductibilité : comment le problème peut-il être reproduit exactement ?
- Joindre un diagnostic système → la manière de le créer est expliquée via le symbole ? dans le formulaire.

Pour la version 26.4.0

Filtre pour le contenu (intégré)

Les résultats de recherche Google contiennent des résultats inappropriés malgré l'activation du filtre automatique. Les pages web au contenu inapproprié sont bloquées comme prévu. Cependant, le contenu inapproprié est toujours affiché dans les résultats de recherche de la catégorie `Photos et Vidéos`.

Problème

Le filtre de contenu d'Apple n'offre pas la possibilité de restreindre la recherche de Google (par exemple Safe-Search). Le filtre automatique d'Apple filtre les pages web en fonction du "langage adulte" et non du contenu multimédia comme les images ou les vidéos. La recherche d'images de Google n'est pas limitée par ce filtre.

Solution

Pour restreindre davantage les résultats de la recherche, des applications tierces appropriées ou un filtre de contenu au niveau du réseau (proxy/VPN) sont nécessaires.

Pour la version 26.4.0

Collection de liens

Les sites web suivants donnent un aperçu des applications qui peuvent être utilisées pour filtrer les contenus inappropriés. De la part de Relution, les applications recommandées sur les sites externes n'ont pas été testées - par conséquent, aucune déclaration contraignante ne peut être faite sur la qualité et/ou l'adéquation de ces applications.

wondershare →

WithSecure →

Code QR non scannable

Sur les appareils iOS, il peut arriver qu'au cours d'une configuration de politique appliquée avec "app compliance", le scanner de code QR de l'appareil photo soit désactivé. L'appareil photo reconnaît un code QR existant, mais n'offre pas le lien pour l'ouvrir dans le navigateur. Le problème ne se produit qu'en conjonction avec une "liste positive" dans la configuration "conformité des applications".

Comment faire

L'application ou le plugin doit être ajouté manuellement à la `liste positive` de `conformité d'application`.

1. Aller dans la configuration de la politique correspondante.
2. Créer une nouvelle entrée `positive list` pour `add app manually`.
3. Le nom peut être choisi librement. Comme `nom interne`, entrer `com.apple.barcodesupport`.
4. Sauvegarder et publier la politique.

Pour la version 26.4.0

Appareil verrouillé

Si les appareils iOS sont protégés par un code PIN et redémarrés, ils ne peuvent pas être connectés à un WI-FI protégé par un mot de passe tant qu'ils ne sont pas déverrouillés, car le système d'exploitation ne peut pas accéder au trousseau. Une situation similaire peut être provoquée par l'activation du mode perdu. Par conséquent, sans connexion réseau, aucune action telle que la réinitialisation du mot de passe ou la désactivation du mode perdu n'est effectuée.

LAN vers adaptateur Lightning / USB-C

Cela peut être utilisé pour établir une connexion LAN à l'appareil final via un adaptateur RJ45 afin que l'appareil puisse établir une connexion Internet et traiter les actions MDM. Cependant, la condition préalable est que l'option `Autoriser les accessoires USB dans l'état verrouillé` a été définie dans les restrictions avant de verrouiller l'appareil.

Pour la version 26.4.0

WI-FI ouvert connu

Si un WI_FI ouvert / non protégé était connu de l'appareil avant qu'il ne soit verrouillé, la connexion à ce WI_FI peut être établie automatiquement par l'appareil sans déverrouillage et les actions MDM peuvent être traitées à nouveau.

> Obsolète pour iOS 18.x

Réinitialiser l'appareil

La réinitialisation des appareils concernés aux paramètres d'usine est toujours une option valable. Il est toujours possible de réinitialiser complètement les appareils iOS via DFU mode → pour les réinitialiser complètement.

Liens web

Weblink peut être déployé comme une application dans Relution. Ceci est utile si, par exemple, un lien web doit être déployé de manière spécifique à l'utilisateur ou au groupe (auto-déploiements) ou placé dans la configuration de la politique "Disposition de l'écran d'accueil".

1. Créer un lien web

1. Cliquer sur "Ajouter" dans Relution sous "App Store".
2. Sélectionner `Web Link`.
3. Cliquer sur `Suivant`.
4. Entrer l'URL du lien.
5. Cliquer sur `Add details`.
6. Activer le statut de partage `Productif`
7. Attribuer un nom
8. Activer éventuellement l'option Ouvrir en plein écran pour que le lien web démarre comme web app (voir Ouvrir un lien web comme web app →)
9. Cliquer sur "Enregistrer" dans le coin supérieur droit.

Pour la version 26.4.0

2. Distribuer le lien Web via des déploiements automatiques

Weblink ne peut pas être déployé en tant qu'"Application Requise" dans la configuration de la politique de "Conformité des Applications". Cependant, il est possible de déployer automatiquement Weblink vers des utilisateurs ou des groupes d'utilisateurs spécifiques via les `Déploiements Automatiques`.

1. Ouvrir le compte utilisateur ou le groupe correspondant.
2. Cliquer sur le bouton "Ajouter" en bas de la section "Auto Deployments".
3. Sélectionner les liens web créés et cliquer sur "Ajouter".
4. Cliquer sur "Sauvegarder" en haut.

Les liens web ajoutés seront immédiatement affichés sur les appareils où l'utilisateur correspondant ou un membre du groupe d'utilisateurs correspondant s'est connecté.

3. Fournir un lien web via la politique

Les liens web peuvent également être fournis avec la configuration `Lien web`, pour cela, une configuration via les politiques doit être créée comme suit :

1. Dans la navigation de la page, aller à `Devices` > `Policies` > `Add` ou ouvrir une politique existante.
2. Cliquer sur le bouton `Add` > `Weblink` > `Add Details` pour créer une configuration de lien web.
3. Label et URL (p. ex. `https://relution.io`) sont des champs obligatoires.
4. Application pour ouvrir un lien Web avec : une application de navigateur tierce peut être sélectionnée ici, p. ex. Firefox. Sans saisie, Safari est utilisé. Pour l'affichage comme web app, le champ reste vide.
5. amovible : le lien web peut être supprimé par l'utilisateur.
6. Icône précomposée : si l'option est activée, iOS n'ajoute aucun effet visuel à l'icône téléchargée. L'option date d'anciennes versions d'iOS qui ajoutaient un effet de brillance aux icônes.
7. Plein écran : le lien web démarre comme web app au lieu de s'ouvrir dans Safari (voir Ouvrir un lien web comme web app →).

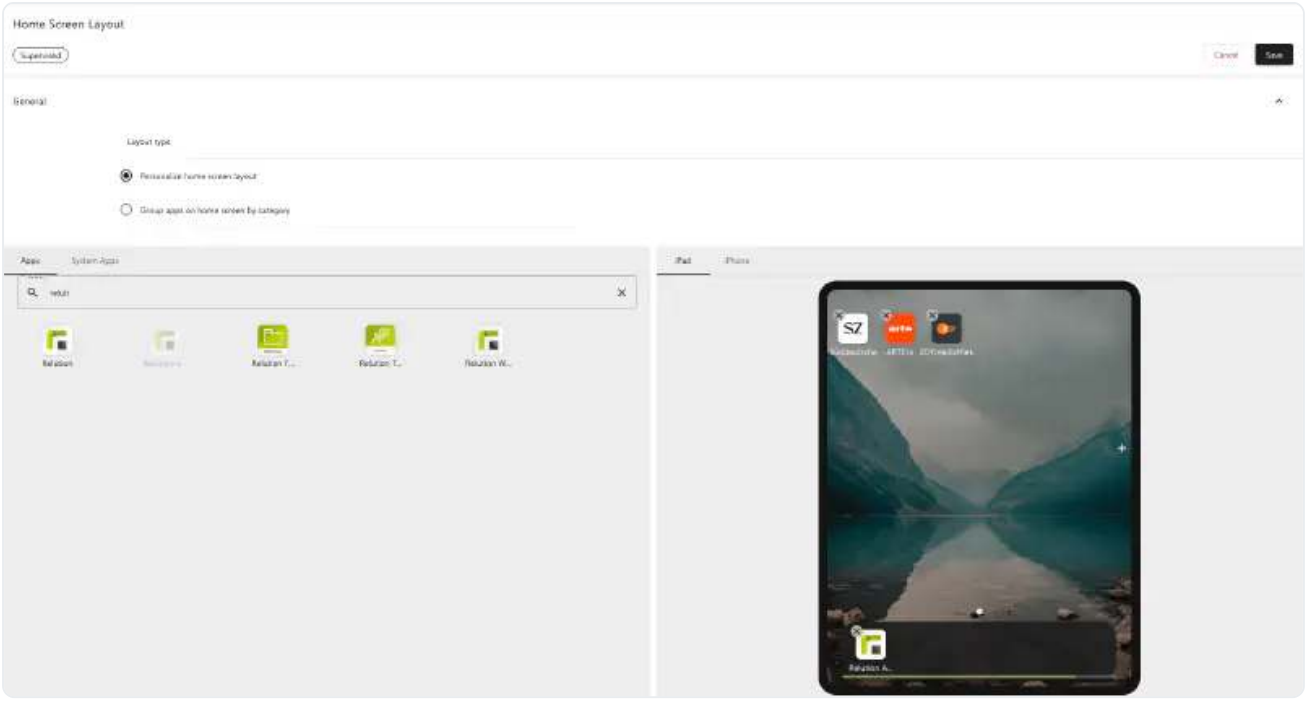
Avec RELUTION 5.32.0, l'espace réservé peut être utilisé sur les liens Web pour inclure un nom d'utilisateur.

Pour la version 26.4.0

4. Optionnel : Disposer le lien Web dans la disposition de l'écran d'accueil

La configuration de la politique `Homescreen Layout` peut être utilisée pour placer des applications et des liens web spécifiquement sur l'écran d'accueil des appareils iOS.

1. Naviguer vers l'élément de menu `Devices` → `Policies` dans le portail Relution et cliquer sur `Add`.
2. Créer une politique iOS et attribuer un `nom`. Cliquer sur `Save`.
3. Après avoir cliqué sur `Add`, sélectionner l'option `Homescreen Layout` et passer à `Add Details`.
4. Si des liens web existants ont été précédemment assignés à une catégorie, ils peuvent être automatiquement placés dans des dossiers créés sur l'écran d'accueil. Pour les arranger manuellement, décocher l'option `Grouper les icônes par catégorie`.
5. Placer ensuite les applications et les liens Web pertinents dans l'ordre souhaité en utilisant la fonction glisser-déposer.



6. Cliquer sur “Enregistrer” et publier la version actuelle de la politique.
7. Pour appliquer la politique aux appareils iOS, ajouter les appareils souhaités en utilisant l’onglet “Appareils avec cette stratégie”. Les paramètres sélectionnés seront alors automatiquement appliqués aux appareils.

> Pour afficher un lien web dans la disposition de l’écran d’accueil, les étapes 1+2 ou 1+3 sont nécessaires. L’URL du lien web doit être identique lors de sa création dans le magasin Relution et dans la configuration du lien web.

Pour la version 26.4.0

Ouvrir un lien web comme web app

Sur l’appareil, un lien web démarre soit comme signet dans Safari, soit comme web app autonome. Ce comportement est contrôlé par l’option Ouvrir en plein écran (lien web dans l’App Store) ou Plein écran (configuration `Lien web` dans une politique) :

- Option désactivée : le lien web ouvre la page dans Safari, avec barre d’adresse et onglets.
- Option activée : iOS démarre la page comme web app dans une fenêtre dédiée, sans l’interface de Safari. Dans le sélecteur d’applications, elle apparaît comme une application distincte.

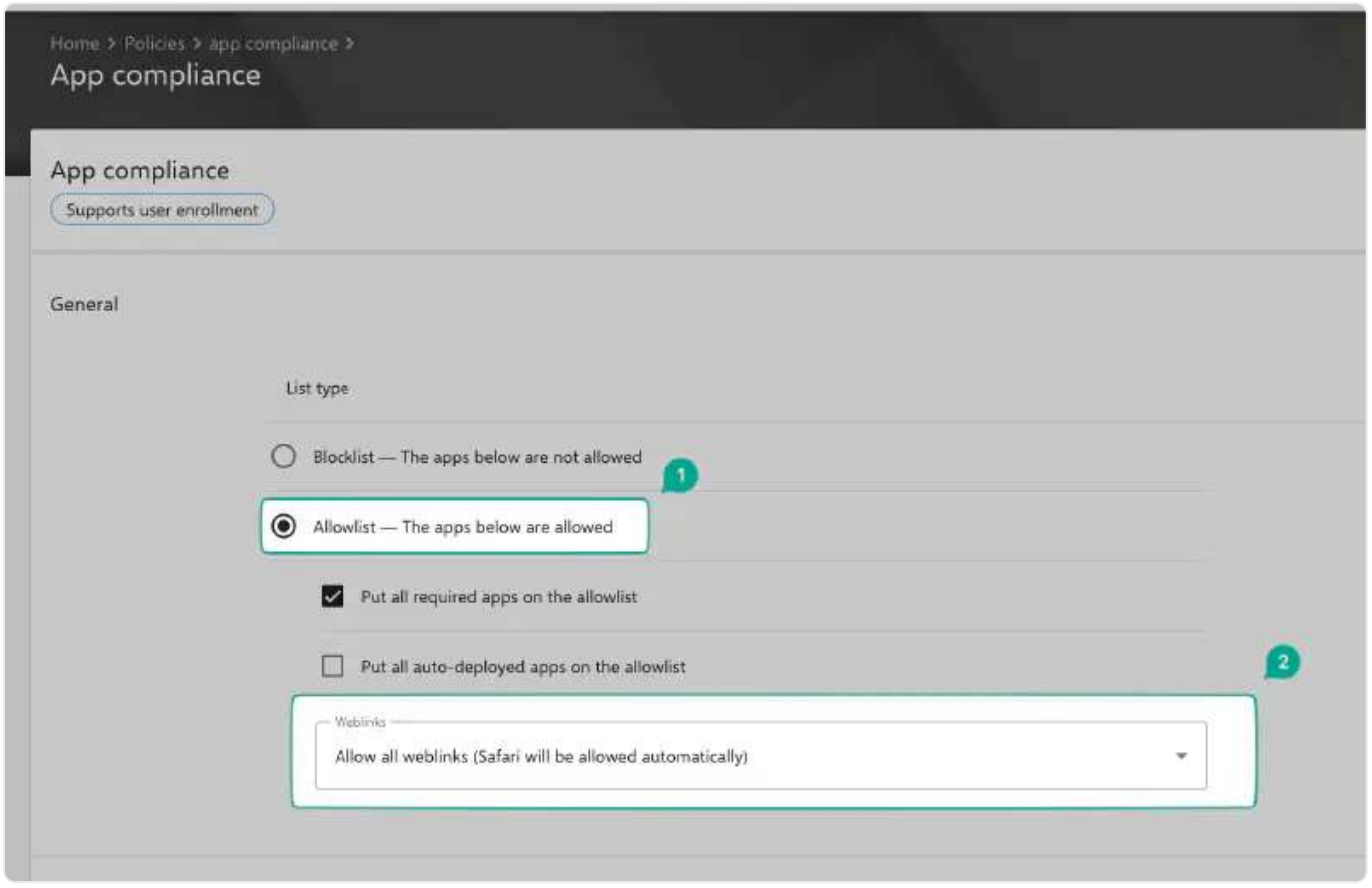
L’affichage effectif comme web app dépend aussi du site web lui-même. Celui-ci doit prendre en charge le mode web app, p. ex. via un manifeste d’application web avec `"display": "standalone"` ou la balise meta `apple-mobile-web-app-capable`. Sans cette prise en charge, iOS affiche la page comme dans Safari, même si l’option est activée.

Dans la configuration de la politique, Application pour ouvrir un lien Web avec reste vide pour l'affichage comme web app. Si une application y est sélectionnée, le lien web s'ouvre dans cette application.

Liens Web sur les dispositifs partagés de Relution

Pour afficher et utiliser des liens Web sur les périphériques partagés de Relution, une politique de conformité d'application doit être attribuée aux périphériques. Cette politique doit être configurée comme suit :

- Définir List Type sur `Allowed` (Autorisé)
- Régler Liens Web sur `Autoriser tous les liens Web (Safari sera automatiquement autorisé)`



Sauvegarde

Les sauvegardes Apple iOS permettent aux utilisateurs de sauvegarder leurs données importantes telles que les contacts, les photos, les messages et les paramètres, et de les restaurer en cas de besoin. Ces sauvegardes peuvent être créées via iCloud ou iTunes et servent de protection contre la perte de données en cas de remplacement, d'endommagement ou de vol de l'appareil.

Restauration standard via l'assistant de configuration

Un appareil DEP enregistré est restauré à partir d'une sauvegarde dans le même état, avec l'état de surveillance de l'appareil et le profil MDM qu'il avait au moment de la création de la sauvegarde. La procédure générale pour restaurer un appareil à partir d'une sauvegarde est décrite par Apple sur le lien suivant : Apple Backup→.

Pour la version 26.4.0

Transfert de données Quick Start

Le transfert de données via Quick Start permet de déplacer directement le contenu d'un ancien iPhone ou iPad vers un nouvel appareil en plaçant les deux appareils l'un à côté de l'autre. La condition préalable est que le Bluetooth et le Wi-Fi soient activés sur les deux appareils et qu'iOS/iPadOS 12.4 ou une version ultérieure soit installé.

Pendant l'assistant de configuration du nouvel appareil, une invitation à continuer apparaît sur l'ancien appareil. En scannant le motif animé affiché sur le nouvel écran avec l'appareil photo de l'ancien appareil, les deux appareils sont jumelés. Après avoir saisi le code d'accès et l'identifiant Apple, sélectionner l'option Transférer depuis l'iPhone ou l'iPad, puis les données sont migrées directement et de manière chiffrée via une connexion sans fil.

Apple Quick Start →

Pour qu'un appareil enregistré via Apple School/ Business Manager (DEP) se voie proposer l'option Quick Start lors de la configuration initiale, les étapes de configuration suivantes ne doivent pas être ignorées dans le profil DEP attribué (laisser les cases décochées) :

- `Configuration rapide de l'iPad`
- `Restauration depuis une sauvegarde`

Si l'une de ces deux options est activée, l'étape correspondante de l'assistant de configuration est masquée et le nouvel appareil ne pourra plus recevoir de données via Quick Start depuis l'ancien appareil.

> Sur l'appareil existant, l'option Autoriser la configuration de proximité doit être activée dans les restrictions.

Sauvegarde

Créer une sauvegarde sur l'appareil à l'aide de l'Apple ID via iCloud ou localement sur un Mac ou un PC.

Préparation

Configurer un nouveau profil de récupération DEP avec les paramètres suivants :

- Activer `Autoriser la connexion aux Macs ou PCs et la configuration avec Apple Configurator`.
- Ne pas activer `Autoriser la localisation de l'appareil`.
- Ne pas activer l'option "Importer une sauvegarde".
- Ne pas activer l'option `Log in with Apple ID`.

Pour la version 26.4.0

Intégration dans Relution

Attribuer l'appareil via Apple School/ Business Manager au serveur Relution correspondant avec le profil de récupération DEP créé précédemment. Après l'affectation, cliquer sur `Synchroniser les périphériques DEP`.

Restaurer la sauvegarde

Démarrer l'appareil de réinitialisation et suivre l'assistant de configuration. Dans l'assistant de configuration, sélectionner `Restaurer les applications et les données`. Pour une sauvegarde iCloud, le même identifiant Apple doit être utilisé pour la restauration que celui utilisé pour la sauvegarde.

Pendant la configuration, l'appareil passe automatiquement par le processus d'enregistrement DEP. Les paramètres liés à la gestion de l'appareil ne sont pas appliqués à partir de la sauvegarde, mais à partir du profil DEP configuré dans Relution. Après une sauvegarde réussie, revenir au profil DEP original par défaut. L'étape de configuration visant à restaurer la sauvegarde sur l'appareil ne s'affichera plus.

Enregistrement d'un appareil non géré avec Apple DEP et restauration par sauvegarde

Un appareil iOS non géré peut être enregistré ultérieurement dans Apple DEP sans que ses utilisateurs perdent leurs données et leur contenu. Or, selon la documentation d'Apple, une restauration conserve l'état de gestion de l'appareil issu de la sauvegarde lorsqu'elle est effectuée sur le même appareil (voir l'exemple ci-dessous) - un appareil non géré ne peut donc pas passer directement à un état DEP supervisé à partir de sa propre sauvegarde. La méthode ci-dessous fait donc transiter la sauvegarde par un second appareil temporaire : la restauration étant alors considérée comme une restauration vers un appareil différent, Apple applique l'état de gestion provenant d'Apple School/ Business Manager.

Pour la version 26.4.0

La documentation d'Apple indique ce qui suit :

- Lorsqu'un iPhone ou un iPad est restauré à partir d'une sauvegarde, l'état de gestion de l'appareil est restauré à partir de la sauvegarde.
- Si la restauration s'effectue à partir d'une sauvegarde vers un autre iPhone ou iPad, l'état de gestion de l'appareil proviendra d'Apple School/ Business Manager.

Exemple

Si un appareil est configuré pour être supervisé et automatiquement enregistré dans le système MDM, mais qu'il est ensuite restauré à partir d'une sauvegarde créée lorsque le même appareil n'était pas supervisé, l'appareil n'est pas supervisé. Autrement dit, un appareil non géré ne peut pas être restauré directement à partir de sa propre sauvegarde pour activer le mode supervisé et enregistrer l'appareil avec Apple DEP à cette occasion - c'est précisément pour cela que le détour par un second appareil est nécessaire.

Sauvegarde

Créer une sauvegarde sur l'appareil-01 non géré via iCloud ou localement sur un Mac ou un PC. Restaurer cette sauvegarde sur un second appareil, l'appareil-02. Puis sauvegarder à nouveau l'appareil-02 via iCloud ou localement - cette seconde sauvegarde sera ensuite restaurée sur

l’appareil-01 et, étant techniquement celle de l’appareil-02, comptera comme une sauvegarde « d’un autre appareil ».

Préparation

Réinitialiser l’appareil-01 aux paramètres d’usine. Ajouter l’appareil-01 à l’Apple School/ Business Manager via Apple Configurator 2. Pour en savoir plus, consulter notre Insight Add Apple devices to DEP afterwards →. Configurer également un profil de récupération DEP pour l’appareil-01, comme décrit dans la section Préparation précédente.

Intégration dans Relution

Attribuer l’appareil-01 via Apple School/ Business Manager au serveur Relution approprié avec le profil de récupération DEP créé précédemment. Configurer l’appareil en suivant l’assistant de configuration sur l’appareil.

Restauration de la sauvegarde

Sur l’appareil-01, sélectionner “Restaurer les applications et les données” dans l’assistant de configuration et choisir la sauvegarde créée précédemment depuis l’appareil-02. Pour la sauvegarde iCloud, le même identifiant Apple doit être utilisé pour la restauration que celui utilisé pour la sauvegarde.

Pour la version 26.4.0

Comme la sauvegarde provient techniquement de l’appareil-02, la restauration est considérée comme une restauration vers un appareil différent : les paramètres relatifs à la gestion de l’appareil ne proviennent pas de la sauvegarde, mais du profil DEP configuré dans Relution - c’est ce qui supervise et enregistre l’appareil-01 dans DEP.

Après une restauration réussie, revenir au profil DEP original par défaut. L’étape de configuration visant à restaurer la sauvegarde sur l’appareil ne sera alors plus affichée.

Teamviewer Support invite

Avec TeamViewer, des sessions de support à distance peuvent être créées et partagées avec les destinataires. Via Relution, un lien de session peut être envoyé à un appareil par message. Conditions préalables : L'application TeamViewer QuickSupport est installée sur l'appareil.

Ce guide décrit comment créer une session, partager le lien et faire en sorte que le destinataire se connecte.

Exigences

- TeamViewer
- TeamViewer QuickSupport App sur l'appareil cible (par exemple, iPhone ou iPad)
- Accès à Relution pour envoyer le message
- Permission d'utiliser l'assistance à distance

Pour la version 26.4.0

Étapes de la création d'une session à distance

1. Créer un message avec un lien:
    - Se connecter à Relution.
    - Sous Devices > Inventory > Select device > Select action > Send message, un message peut être envoyé.
    - Un lien vers la session TeamViewer est inséré dans le message.
    - Le message est envoyé à l'appareil souhaité.
2. Ouvrir le lien sur l'appareil : Le destinataire reçoit le message sur son ordinateur.
    - Le destinataire reçoit le message sur son appareil.
    - Le destinataire ouvre le message et clique sur le lien.
    - L'application TeamViewer QuickSupport s'ouvre automatiquement.
3. Démarrer la session:
    - L'expéditeur du message peut maintenant démarrer la session sur son ordinateur.
    - Le destinataire doit confirmer la connexion sur son appareil.

Notes

- S'assurer que l'application TeamViewer QuickSupport est à jour.

- Le lien vers la session TeamViewer n’est valable que pour une durée limitée.
- Le destinataire doit disposer d’une connexion internet stable.

Divers

- De plus amples informations sur TeamViewer sont disponibles sur le site officiel : teamviewer.com →

Conseils de sécurité

- Les liens vers les sessions TeamViewer ne doivent être partagés qu’avec des personnes de confiance.
- Les connexions provenant d’expéditeurs inconnus ne doivent pas être confirmées.

Pour la version 26.4.0

Airdrop

Depuis la mise à jour vers iOS 26.2 (ainsi qu'iPadOS 26.2 et macOS 26.2), Apple a renforcé les exigences de sécurité pour l'échange de données via AirDrop. De nombreux utilisateurs, en particulier dans les écoles et les entreprises, constatent que l'envoi de fichiers requiert désormais soudainement la saisie d'un code – un comportement qui n'existait pas encore sous iOS 18.x.

Si un fichier est envoyé à une personne qui n'est pas enregistrée dans les contacts, le transfert est bloqué jusqu'à ce qu'un code numérique soit saisi. Cela complique considérablement l'échange rapide de données en classe ou au sein de groupes de travail.

Cause

Selon la documentation officielle d'Apple, il s'agit d'une fonction de sécurité délibérée visant à protéger la vie privée :

- Vérification d'identité : les personnes qui ne sont pas enregistrées dans les contacts doivent désormais obligatoirement utiliser un code AirDrop pour envoyer des objets.
- Déroulement : le destinataire doit sélectionner Continuer, ce qui affiche un code sur son écran. Ce code doit être saisi par l'expéditeur pour autoriser le transfert.
- Limitation MDM : les administrateurs n'ont actuellement aucun moyen de désactiver globalement cette demande via la gestion des appareils mobiles (MDM). Apple n'offre ici aux fournisseurs de MDM aucune option supplémentaire par rapport à l'utilisateur final.

Pour la version 26.4.0

Condition préalable : compte Apple et iCloud

> Important : l'utilisation d'AirDrop en mode Contacts uniquement ainsi que la connexion permanente sans code aux contacts connus nécessitent un compte Apple (iCloud) connecté sur l'appareil. Plus d'informations dans la documentation Apple →

Sur les iPad sans compte Apple, une fenêtre de confirmation apparaît lors du passage d'AirDrop en mode Contacts uniquement, indiquant qu'iCloud est requis à cet effet. Sans connexion, ce réglage n'est pas utilisable.

Pour qu'AirDrop fonctionne de manière fiable en mode Contacts uniquement, l'adresse e-mail ou le numéro de téléphone mobile du compte Apple de la personne qui envoie doit en outre être

enregistré dans sa fiche de contact chez le destinataire.

Solution de contournement

Pour éviter la saisie constante d'un code, voici les approches possibles :

Solution temporaire : régler AirDrop sur **Tout le monde pendant 10 minutes**

La solution la plus simple à court terme consiste à régler temporairement AirDrop sur Tout le monde pendant 10 minutes. Dans ce mode, aucune relation de contact ni saisie de code n'est requise. Le réglage revient automatiquement à la valeur précédente après 10 minutes.

Utiliser la règle des 30 jours

Une fois qu'un code a été saisi avec succès, le système mémorise la connexion. D'autres objets peuvent alors être échangés avec cette personne pendant 30 jours, sans qu'un code soit à nouveau demandé.

Pour la version 26.4.0

Solution permanente : ajouter aux contacts

La demande de code est définitivement supprimée si l'expéditeur et le destinataire s'enregistrent mutuellement dans leurs contacts.

- Après une réception, sélectionner l'option Créer un nouveau contact ou Ajouter au contact.
- Une fois la personne enregistrée comme contact connu, l'échange se déroule normalement, sans vérification supplémentaire.

Gérer ou ignorer les contacts connus

Pour interrompre une connexion avant l'expiration des 30 jours :

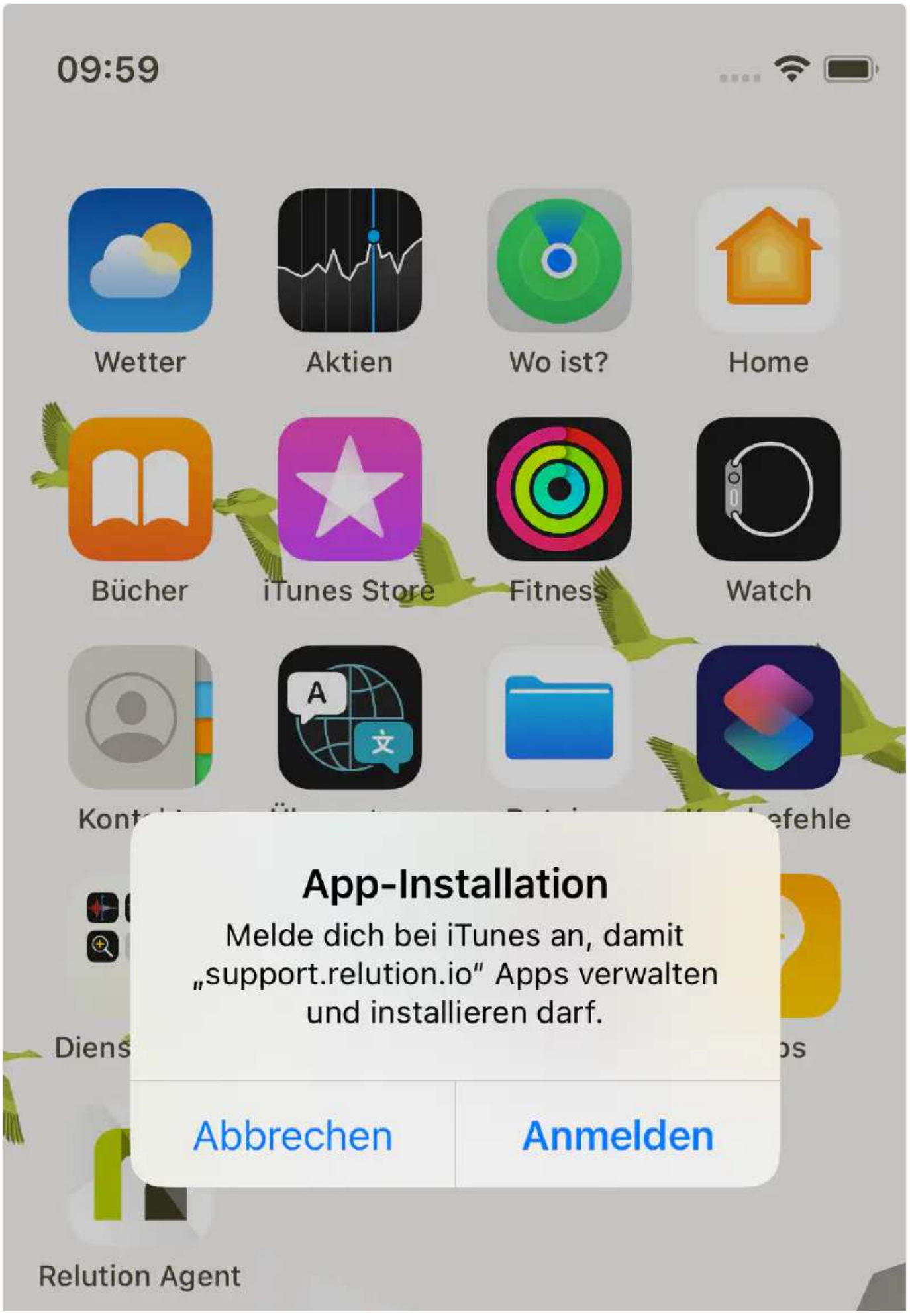
- Ouvrir l'application Contacts.
- Rechercher la personne concernée dans la liste sous Autres contacts connus.
- Sélectionner Ignorer cette personne pour mettre fin à l'échange automatisé.

Se connecter à iTunes

Si les applications Apple Appstore sont distribuées via un MDM (en relation avec une action d’installation d’application, via une politique ou via un déploiement automatique), le message suivant peut apparaître sur l’appareil final.

> Installation d'applications - Connectez-vous à iTunes pour que votre organisation puisse gérer et installer des applications.

Pour la 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



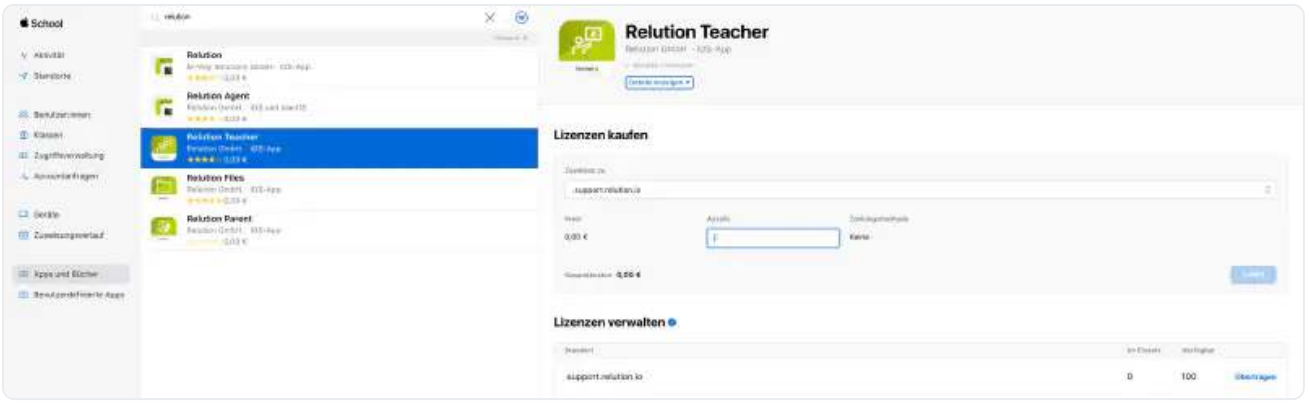
Pour la version

Cause

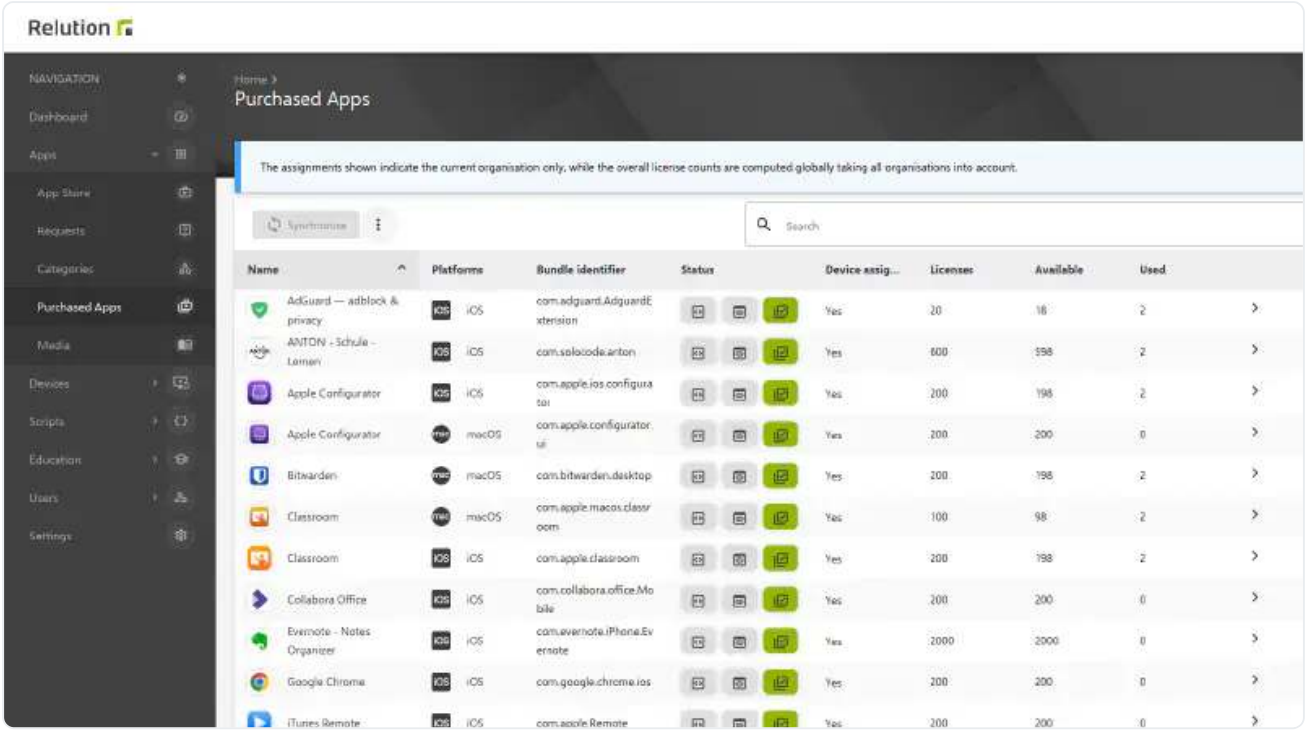
Les applications Appstore (même celles qui sont gratuites) nécessitent toujours une licence. Dans l'environnement privé, cela se fait via l'AppleID et se fait automatiquement lorsqu'une application est téléchargée depuis la boutique. Pour les fournisseurs de MDM, cela se fait via l'Apple VPP (Volume Purchase Program). Pour ce faire, des licences doivent être achetées à l'avance dans ASM / ABM (Apple School / Business Manager) pour chaque application à distribuer.

Solution

1. Pour ce faire, se connecter au portail ASM / ABM et acheter un nombre suffisant de licences pour l'application souhaitée pour l'organisation (distributrice) sous Apps & Books.



2. Après un court laps de temps, l'application est également visible en relation sous "Applications achetées" dans le menu latéral.



3. Toutes les fenêtres pop-up (un message par application sans licence) doivent être annulées sur les appareils finaux contenant le message. L'action ou la politique peut ensuite être exécutée à nouveau et les applications sont installées sans message.

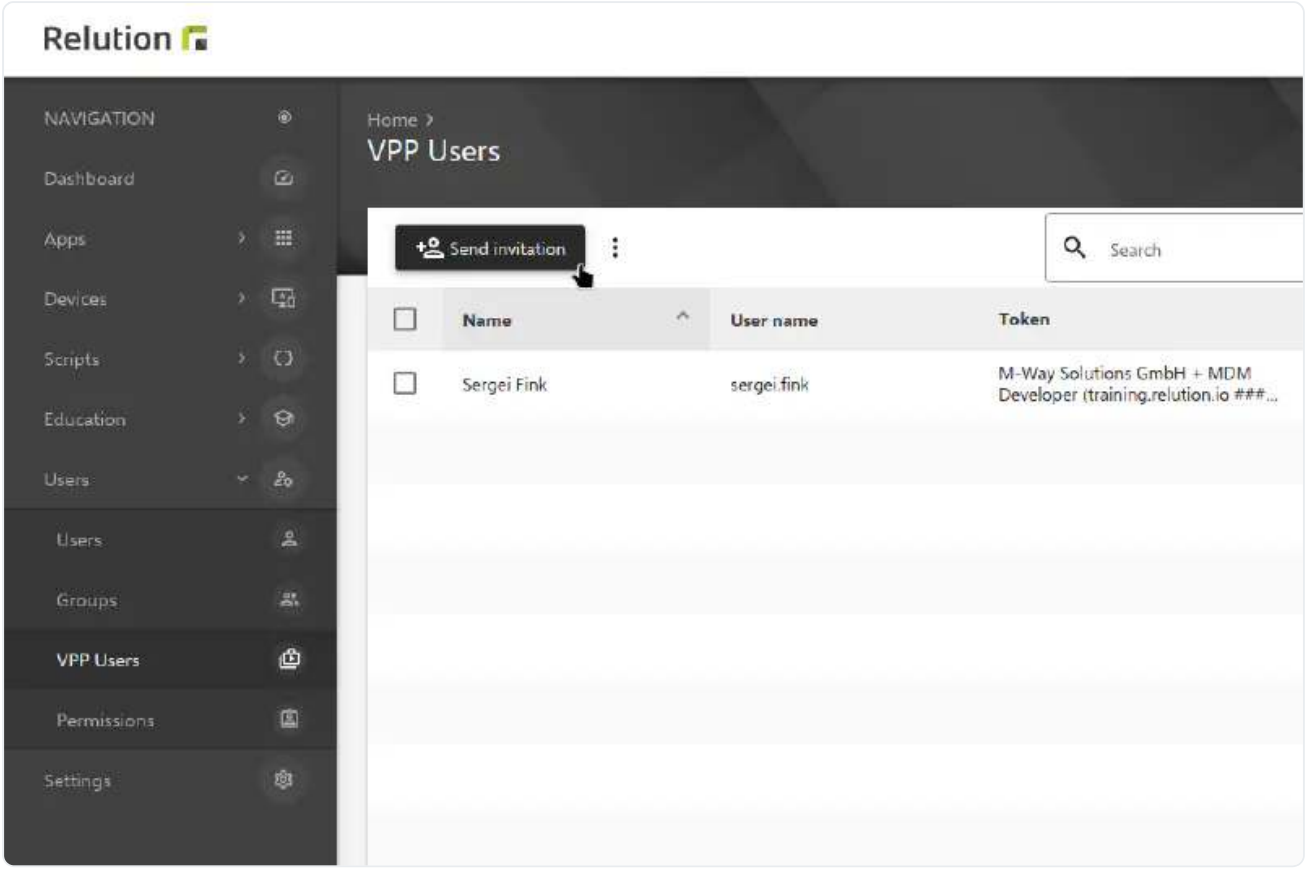
Configurer VPP →

Attribuer des livres achetés

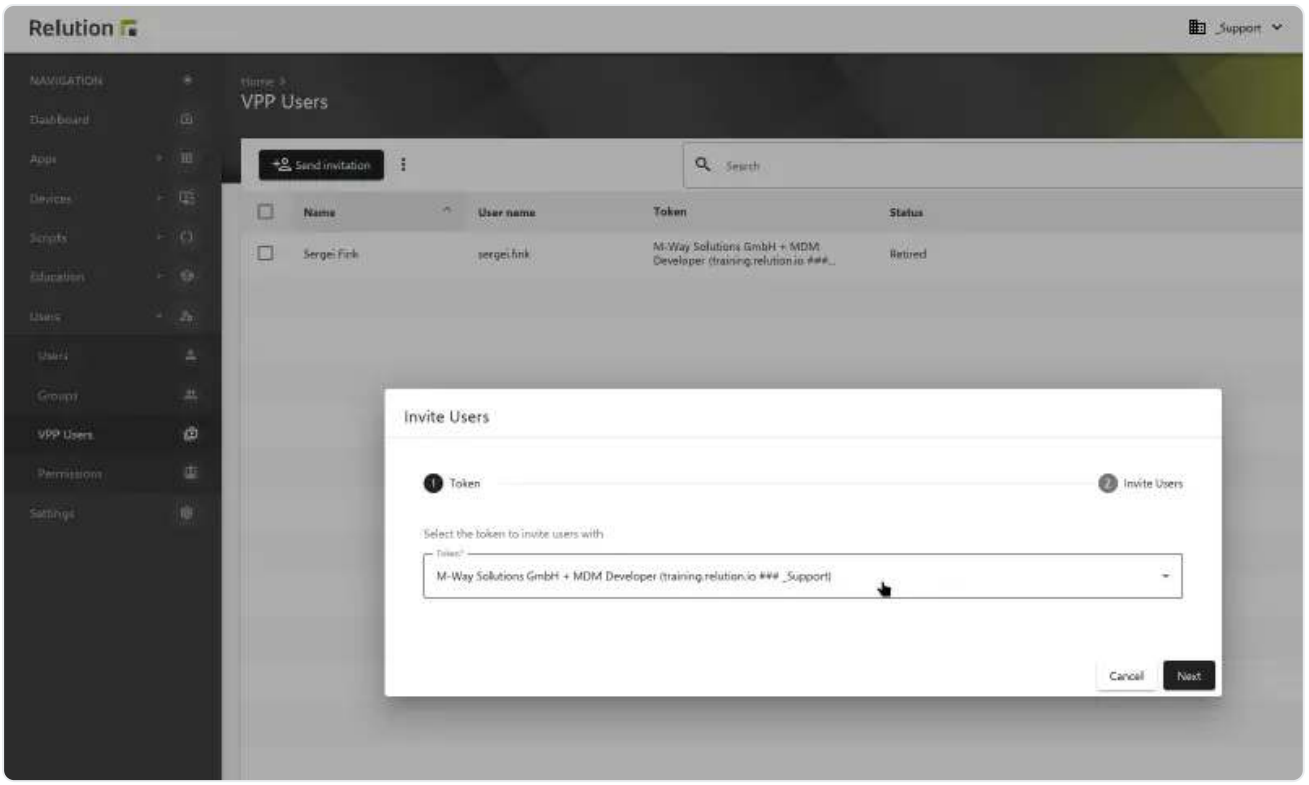
Les livres achetés par l'intermédiaire d'Apple peuvent être attribués à des utilisateurs individuels dans Relution. Il ne suffit pas de créer un Apple ID géré pour ces utilisateurs ; ils doivent recevoir une invitation via Relution et suivre les instructions à l'écran.

Comment faire

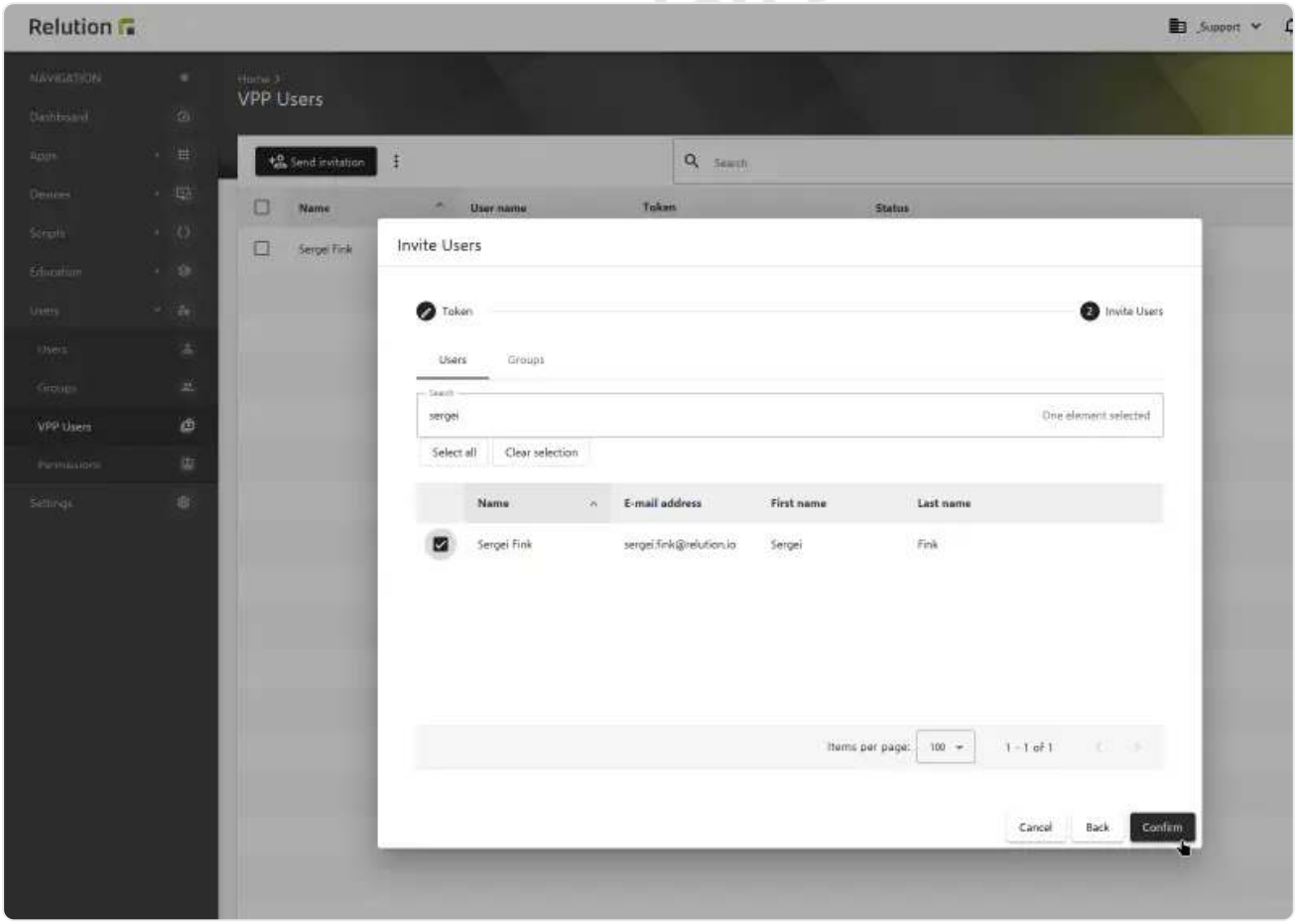
1. Créer les utilisateurs souhaités dans Relution, si cela n'a pas encore été fait.
2. Aller dans la section `Utilisateurs` → `Utilisateurs VPP`.
3. Sélectionner "Envoyer l'invitation".



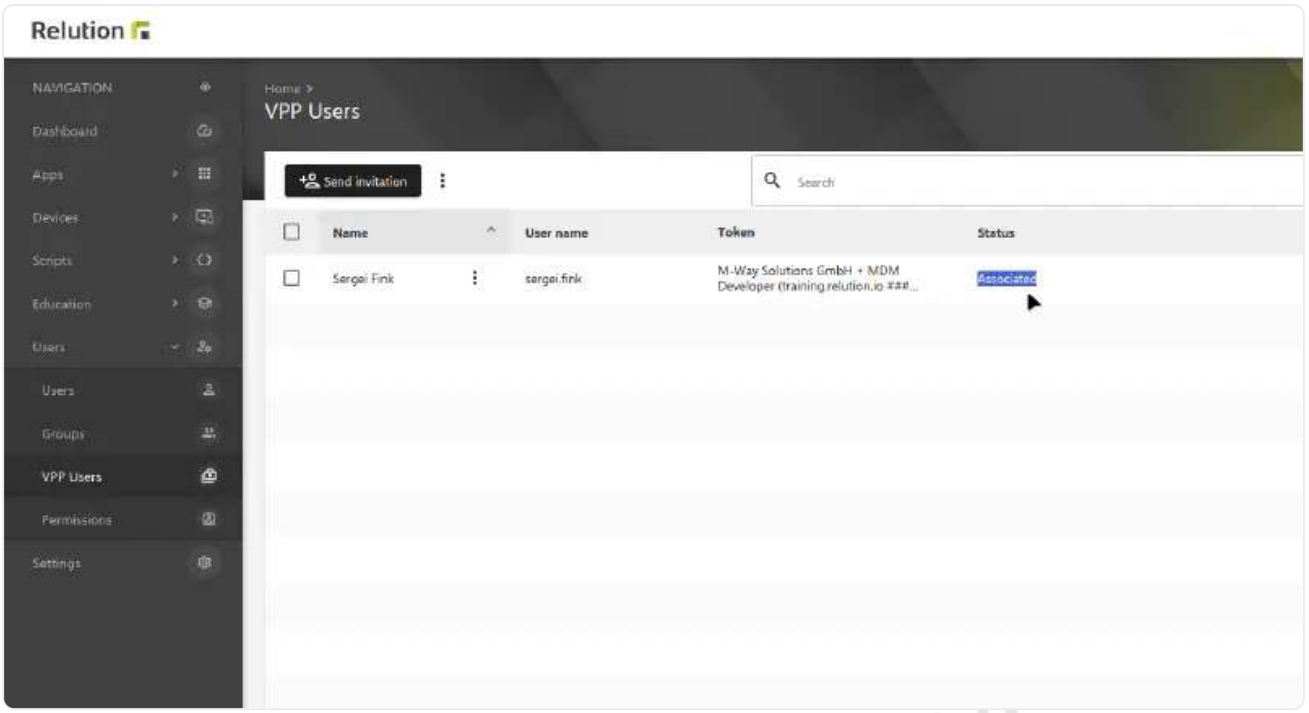
4. Sélectionner le jeton VPP souhaité et cliquer sur `Suivant`.



5. Sélectionner l'utilisateur à inviter et cliquer sur `Confirm`.

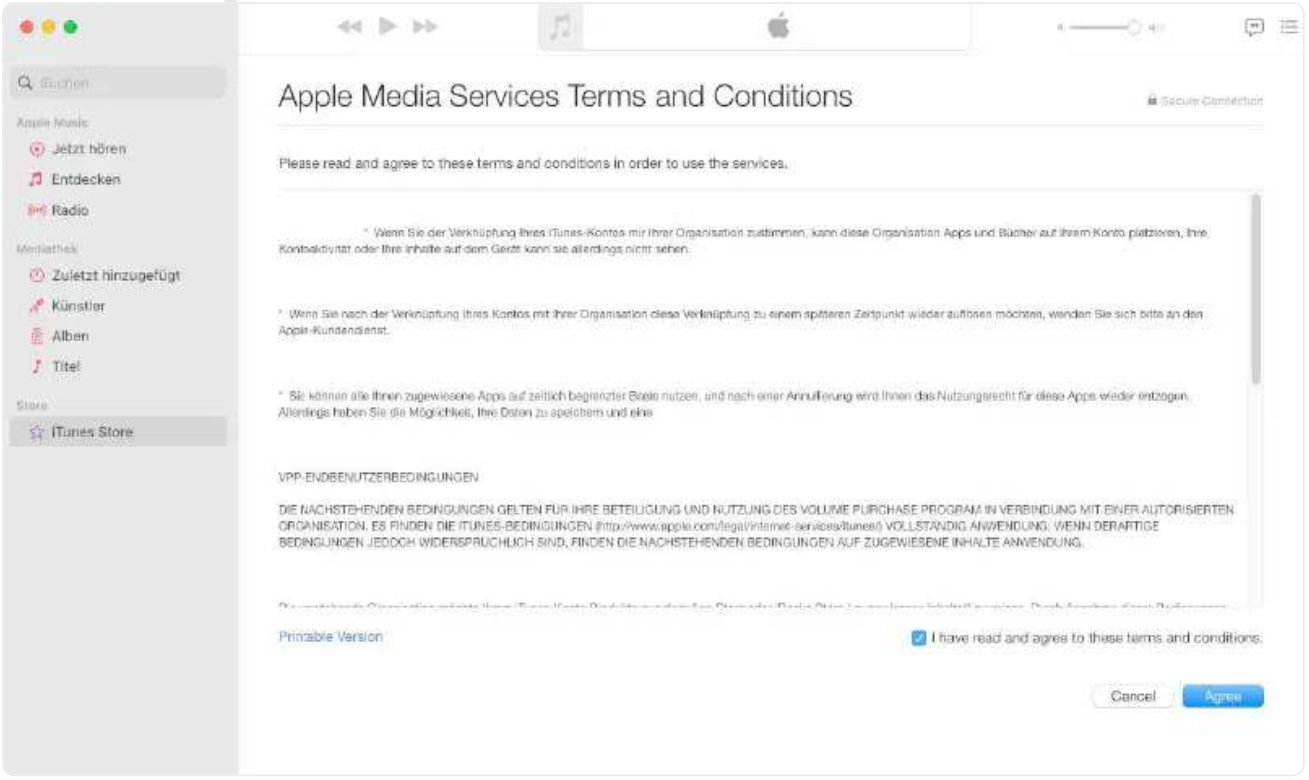


6. L’utilisateur sera ajouté à la liste avec le statut “Enregistré”. L’utilisateur devrait recevoir un courrier électronique.



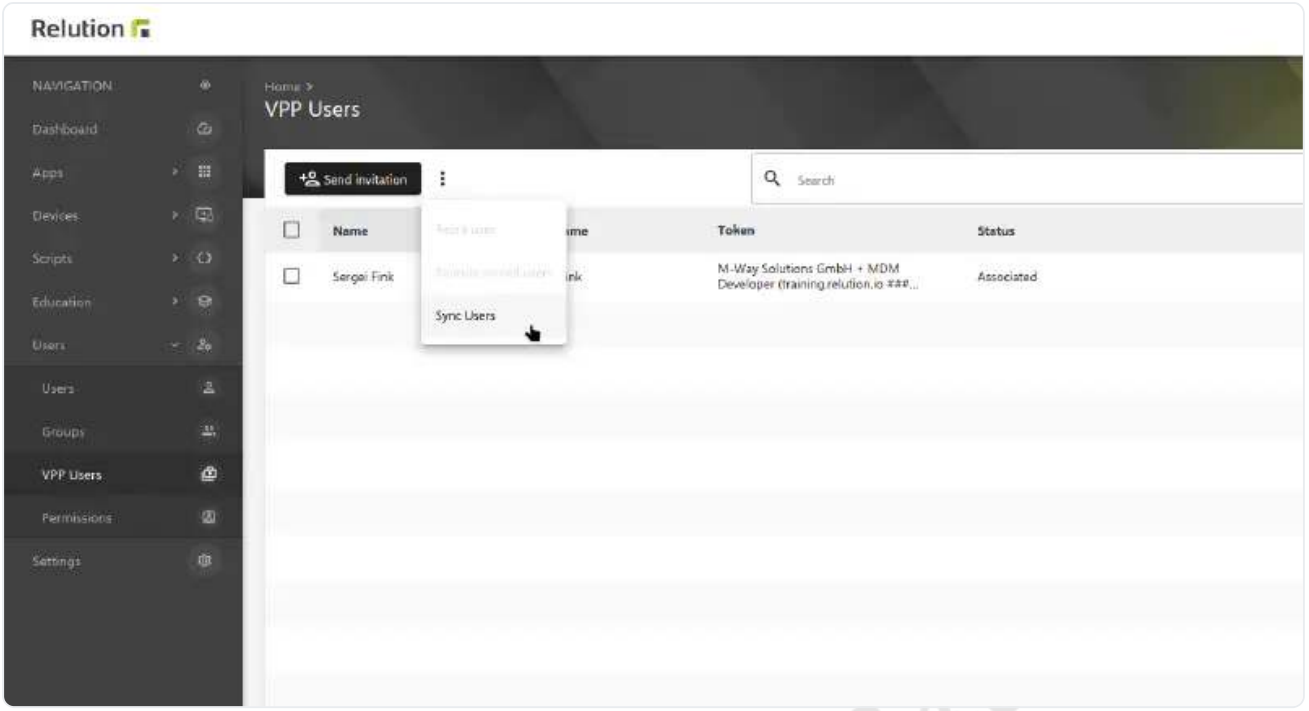
7. Dans l’email, il y a un lien qui doit être ouvert - soit avec `iTunes`, soit avec `Apple Music`. L’utilisateur doit y accepter et confirmer les termes et conditions. Si aucun utilisateur n’est encore connecté sur l’appareil, il peut être nécessaire de saisir un nom d’utilisateur et un mot de passe.

Pour la version 26.4.0



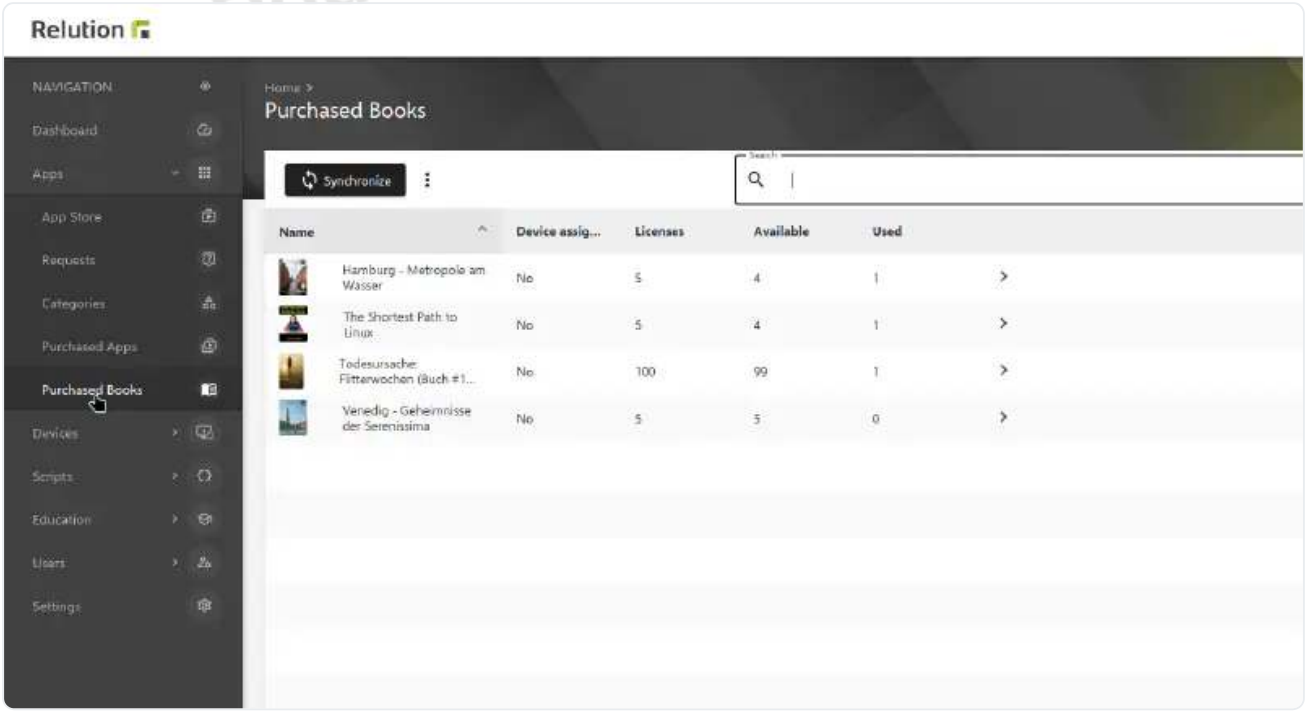
8. Dans Relution, l'attribution d'applications doit être à nouveau autorisée.

9. Dans Relution, les utilisateurs VPP doivent maintenant être synchronisés.

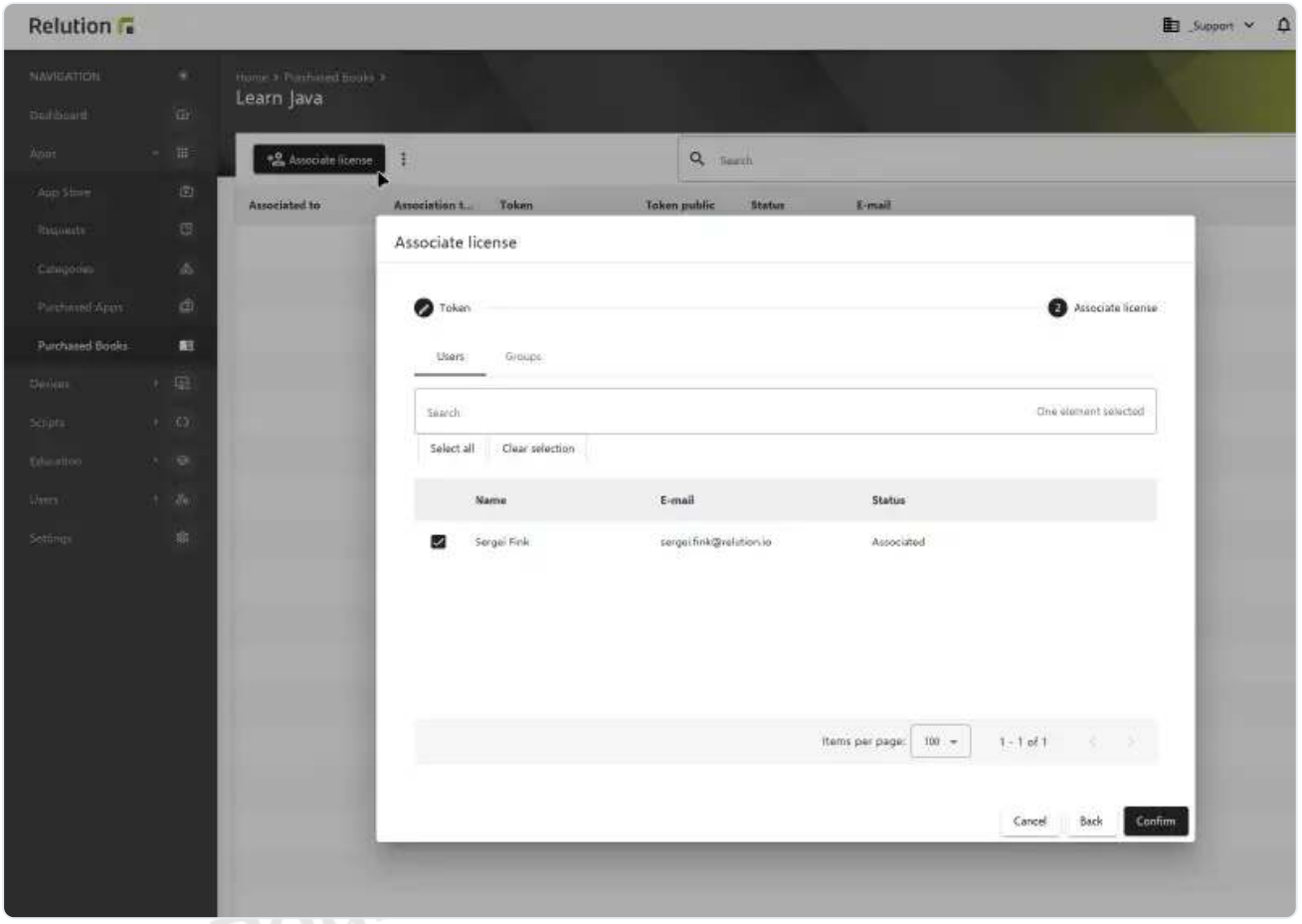


10. Si l'affichage est mis à jour par la suite, l'utilisateur est indiqué comme étant "assigné".

11. Sous `Livres achetés`, cliquer sur le livre à assigner.



12. Dans l'étape suivante, cliquer sur `Assigner une licence`, sélectionner le jeton correspondant et ensuite l'utilisateur désiré. Terminer la sélection en cliquant sur "Confirmer".



Un livre est maintenant attribué à l'utilisateur.

Vue d'ensemble des inscriptions

Les Apple TV sont en train de devenir une entité importante dans les organisations. Ils sont l'un des outils de streaming les plus prometteurs utilisés dans les infrastructures organisationnelles aujourd'hui. Relution prend en charge la gestion des Apple TV avec plusieurs méthodes d'inscription : l'Inscription automatisée des appareils (ADE, DEP dans le portail), l'ajout ultérieur via `Apple Configurator 2` et l'inscription manuelle.

Inscription automatisée des appareils (ADE) via un profil DEP

Apple School ou Business Manager a été introduit par Apple pour aider les organisations et les établissements d'enseignement à déployer des appareils Apple à distance. Grâce à ASM/ABM, de nouveaux appareils Apple peuvent être inscrits dans Relution sans qu'un technicien n'ait à s'en occuper.

Profil pour l'ADE →
DEP Général →

Pour la version 26.4.0

Exigences

- tvOS 10.2 ou version ultérieure.
- L'organisation doit être inscrite à Apple School / Apple Business Manager.
- Les appareils doivent avoir été commandés après le 1er mars 2011, qu'ils aient été achetés directement auprès d'Apple ou d'un revendeur agréé.
- Si les appareils ont été achetés directement auprès d'Apple, le numéro de client Apple attribué à l'organisation est nécessaire pour relier les commandes et les appareils éligibles à Apple School / Apple Business Manager.
- Si les appareils ont été achetés directement auprès d'un revendeur ou d'un opérateur agréé, les appareils doivent être liés à l'ID revendeur (Reseller ID) de ce revendeur. La date réelle d'éligibilité est déterminée par l'historique des ventes du revendeur agréé ou de l'opérateur de réseau.
- Un certificat APNs enregistré dans Relution (Certificats de poussée APNS →).
- Un compte DEP connecté à Relution et un profil DEP attribué aux appareils. Aucune version minimale du système d'exploitation ne peut être définie pour tvOS dans le profil DEP.

Options pour les Apple TV dans le profil DEP

Deux réglages du profil DEP concernent spécifiquement les Apple TV :

- Configuration avancée automatique pour macOS et tvOS : l'assistant de configuration passe automatiquement d'un écran à l'autre. L'Apple TV a besoin pour cela d'une connexion Ethernet. Tant que l'option est activée, les étapes de configuration à ignorer ne peuvent pas être sélectionnées.
- Parmi les étapes de configuration à ignorer, le groupe Spécifique à tvOS regroupe les écrans propres à l'Apple TV : Configuration des économiseurs d'écran aériens et Écran d'options Appuyez pour configurer (à partir de tvOS 10.2) ainsi que Écran de synchronisation de l'écran d'accueil du téléviseur, Écran de connexion du fournisseur de télévision et l'écran « Où est cette Apple TV ? » (à partir de tvOS 11). Les étapes activées sont ignorées lors de la configuration.

Inscription ultérieure via Apple Configurator 2

`Apple Configurator 2` est une application gratuite du Mac App Store qui permet d'ajouter ultérieurement à Apple School / Business Manager des Apple TV qui n'ont pas déjà été enregistrées pour l'ADE par un revendeur agréé. Elles sont ensuite inscrites comme tout autre appareil ADE.

Pour la version 26.4.0

Exigences

- Apple TV avec tvOS 10.2 ou supérieur.
- Appareil macOS avec `Apple Configurator 2.5` ou supérieur.
- L'appareil macOS et l'Apple TV sont connectés au même réseau Wi-Fi ou Ethernet.

Pour les appareils tvOS, le chemin suivant doit être indiqué comme URL du serveur MDM si les appareils doivent être gérés sur le système de production Relution. Pour une instance Relution personnelle, `live.relution.io` est remplacé par le nom d'hôte du serveur utilisé.

```
https://live.relution.io/api/enrollment/v1/appleMdm/depenroll
```

Ajout ultérieur à l'ADE →
Mode supervisé / Supervision →

Inscription manuelle

Les Apple TV peuvent également être ajoutées à Relution sans ADE via une inscription manuelle. Pour cela, une inscription avec la plateforme tvOS est créée sous `Appareils` → `Inscriptions`. La plateforme ne peut être sélectionnée que si un certificat APNs est enregistré dans Relution. Les Apple TV ne disposant pas de navigateur web, le profil MDM de l'inscription est installé sur l'Apple TV à l'aide d'`Apple Configurator 2`.

Inscription manuelle →

Pour la version 26.4.0

Actions disponibles

Relution propose une sélection d'actions permettant de contrôler et de diriger directement les appareils Apple TV. Les actions peuvent être appliquées de manière ciblée à un seul appareil ou, via la sélection multiple dans la liste des appareils, à plusieurs appareils à la fois. Elles peuvent en outre être déclenchées par événement ou de manière planifiée via l'appartenance à des groupes d'appareils : Actions de groupes d'appareils →

La boîte de dialogue des actions s'ouvre sous `Appareils` → `Inventaire` via Appliquer l'action, soit pour les appareils sélectionnés dans la liste, soit dans la vue détaillée d'un appareil. Seules les actions prises en charge par tous les appareils sélectionnés sont proposées.

Aperçu des actions

on 26.4.0

Action	Description
Supprimer l'application	Désinstalle une application de l'appareil.
Effacer l'appareil	Réinitialise l'appareil aux paramètres d'usine et supprime toutes les données de l'appareil.
Redémarrer l'appareil	L'appareil redémarre. Disponible uniquement pour les appareils supervisés.
Actualiser les informations sur l'appareil	Actualise toutes les informations disponibles sur l'appareil, répertoriées sous Détails.
Continuer dans l'Assistant Configuration de l'appareil	Informe l'appareil que la préconfiguration est terminée et qu'il peut poursuivre dans l'assistant de configuration. Disponible uniquement pour les appareils inscrits via l'Inscription automatisée des appareils (ADE, DEP dans le portail). N'a d'effet que si l'option Attendre la configuration est activée dans le Profil du DEP.

Action	Description
Mettre à jour le profil MDM	Réinstalle le profil MDM sur l'appareil. Le certificat d'identité est renouvelé et les paramètres actuels, tels que l'épinglage de certificats, sont appliqués. L'URL du serveur MDM reste inchangée ; une URL externe modifiée n'est donc pas transmise à l'appareil. Relution renouvelle automatiquement le profil MDM avant l'expiration du certificat d'identité. L'action manuelle n'est donc nécessaire que dans des cas particuliers.
Déployer l'application Relution Store	Recherche une application dans le Relution Store et l'installe sur les appareils.
Return to Service	Réinitialise l'appareil aux paramètres d'usine, puis l'appareil tente de se réenregistrer automatiquement. Nécessite tvOS 18 ou une version ultérieure ; sur les versions antérieures, l'action échoue. Une politique comportant une configuration Wi-Fi tvOS doit être sélectionnée dans la boîte de dialogue. L'action n'est disponible que si tous les appareils sélectionnés appartiennent à la même plateforme.
Installer la mise à jour	Installe une mise à jour sélectionnée sur l'appareil sélectionné. Disponible uniquement pour les appareils supervisés. L'action n'est proposée que si Relution a déterminé une mise à jour disponible pour tous les appareils sélectionnés. Les mises à jour disponibles sont à nouveau déterminées à chaque actualisation des informations de l'appareil, par exemple via Actualiser les informations sur l'appareil.

Si au moins un des appareils sélectionnés n'est pas supervisé, Redémarrer l'appareil et Installer la mise à jour ne sont pas affichés dans la boîte de dialogue. Il en va de même pour Continuer dans l'Assistant Configuration de l'appareil dès qu'un appareil sélectionné n'a pas été inscrit via l'Inscription automatisée des appareils.

Vue d'ensemble

Une politique est un ensemble d’une ou plusieurs configurations. Chaque politique peut être appliquée à un ou plusieurs appareils simultanément. De plus, une ou plusieurs politiques peuvent être associées à chaque appareil.

Configurations disponibles

Configuration	Description
Sécurité AirPlay →	Paramètres de sécurité AirPlay pour empêcher la diffusion non autorisée vers les Apple TV via AirPlay
Conformité App →	Gestion des restrictions spécifiques aux applications
Configuration d’Apple Configurator 2 →	Applique aux appareils un profil de configuration (`.mobileconfig`) créé avec Apple Configurator 2
Mode application unique	Limitation des appareils à une seule application
Paramètres de l’appareil	Configuration des paramètres généraux de l’appareil (appareils supervisés uniquement)
Nom de l’appareil	Configuration du nom de l’appareil (appareils supervisés uniquement)
Salle de conférence →	Gestion du mode Salle de conférence
Restrictions	Gestion des restrictions d’appareils
Paramètres de mise à jour du logiciel →	Contrôle du comportement de mise à jour des appareils, p. ex. installation automatique et report des mises à jour (à partir de tvOS 18.4)
Mises à jour système	Gestion des mises à jour des appareils Apple (appareils supervisés uniquement ; obsolète, remplacée par Mises à jour logicielles gérées)

Configuration	Description
Mises à jour logicielles gérées →	Application forcée des mises à jour du système en ciblant une version précise avant une échéance (à partir de tvOS 18.4, appareils supervisés uniquement)
Wi-Fi	Gestion des paramètres Wi-Fi
Fuseau horaire	Configuration du fuseau horaire (à partir de tvOS 14, appareils supervisés uniquement)
Certificat	Sélection d’un certificat à installer par défaut sur l’appareil

Les configurations Wi-Fi, Certificat et Configuration d’Apple Configurator 2 peuvent être ajoutées plusieurs fois à une politique ; toutes les autres une seule fois.

Pour la version 26.4.0

Configuration d'Apple Configurator 2

Cette configuration de politique permet de transférer des fichiers `.mobileconfig` sur les appareils Apple. Un tel fichier peut par exemple contenir une connexion Wi-Fi accompagnée du certificat d'identité correspondant (PKCS#12, `.p12`).

Configuration

Le champ Nom permet d'attribuer un nom à la configuration. Le fichier est importé via le champ de sélection du fichier `.mobileconfig`. Son contenu apparaît ensuite à la place de la sélection de fichier dans le champ Contenu de la charge utile, où il peut être modifié. Le contenu doit être du XML valide. Les profils signés ne sont pas du XML lisible et ne peuvent donc pas être utilisés. Dans Apple Configurator 2, le fichier est par conséquent enregistré sans signature. Si le champ Contenu de la charge utile est vidé, un fichier peut à nouveau être sélectionné.

Des espaces réservés pour l'utilisateur, l'appareil et les certificats peuvent être utilisés dans le champ Contenu de la charge utile. Les espaces réservés disponibles sont affichés sous le formulaire et sont remplacés lors du transfert vers l'appareil, voir Espaces réservés avancés →.

Plusieurs configurations Apple Configurator 2 peuvent être créées par politique. Il est ainsi possible de répartir plusieurs types de configuration sur des configurations distinctes.

Pour la version 26.4.0

Exigences relatives au fichier

Le contenu est vérifié lors de l'enregistrement. Le fichier doit remplir les conditions suivantes :

- Le niveau supérieur contient les clés `PayloadType`, `PayloadVersion` (sous forme de nombre), `PayloadIdentifier`, `PayloadUUID` et `PayloadDisplayName`.
- `PayloadContent` contient exactement un type de configuration. Des charges utiles de certificat peuvent s'y ajouter.

Les fichiers illisibles, ceux auxquels il manque l'une de ces clés ou ceux qui ne contiennent aucune charge utile ou plusieurs types de configuration sont refusés lors de l'enregistrement.

> Seuls les certificats au format PKCS#12 (`com.apple.security.pkcs12`) sont transférés avec la configuration. Les certificats PKCS#1 (`com.apple.security.pkcs1`) sont acceptés lors de la vérification, mais ne sont pas transférés vers l'appareil. Les autres certificats, comme les certificats racine (`com.apple.security.root`), comptent comme

un type de configuration à part entière. Associés à une autre configuration, ils provoquent une erreur lors de l'enregistrement et sont donc déposés dans une configuration distincte.

La configuration proprement dite doit figurer en première position dans `PayloadContent`. Si le fichier contient plusieurs charges utiles du même type, seule la première est transférée vers l'appareil.

Si le fichier contient un type de configuration que Relution propose également sous forme de configuration propre, autorisée une seule fois par politique, cette configuration ne peut plus être ajoutée à la même politique. Sous tvOS, cela concerne :

Type de charge utile dans le fichier	Configuration bloquée
`com.apple.airplay.security`	Sécurité AirPlay →
`com.apple.conferenceroomdisplay`	Salle de conférence →
`com.apple.applicationaccess`	Restrictions
`com.apple.app.lock`	Mode application unique

Pour la ve

À l'inverse, un tel fichier est refusé lors de l'enregistrement si la politique contient déjà la configuration correspondante ou une autre configuration Apple Configurator 2 active avec le même type de charge utile.

Exemple

Le fichier suivant transfère une connexion Wi-Fi (`com.apple.wifi.managed`). Le SSID, le mot de passe, les identifiants et les UUID sont des valeurs d'exemple à remplacer par des valeurs réelles. Chaque `PayloadUUID` doit être unique.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/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>mot-de-passe-WiFi</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>WiFi-Entreprise</string>
   </dict>
  </array>
  <key>PayloadDescription</key>
  <string>Configuration Wi-Fi pour les appareils Apple</string>
  <key>PayloadDisplayName</key>
  <string>Wi-Fi</string>
  <key>PayloadIdentifier</key>
  <string>com.example.wifi</string>
  <key>PayloadOrganization</key>
  <string>Exemple SAS</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>
```

Supprimer le mode supervisé

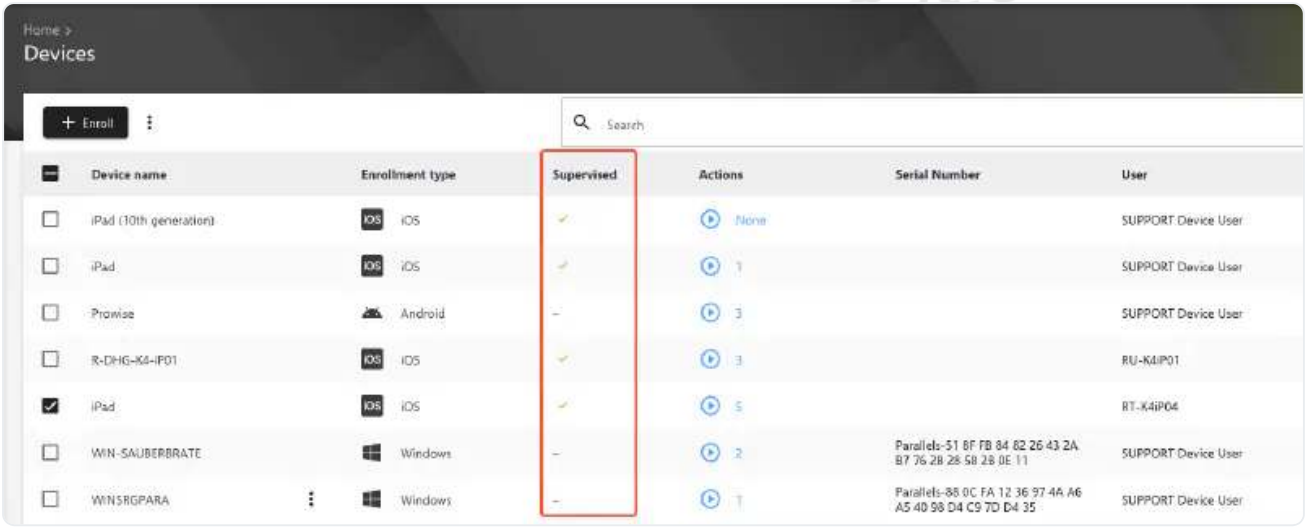
De temps en temps, il peut être nécessaire de révoquer ce mode sur les appareils Apple qui fonctionnent en mode supervisé.

> Pour les appareils iOS et tvOS, cet état peut être annulé. Les appareils macOS, en revanche, ne peuvent plus être exploités qu'en mode supervisé à partir de la version 11.

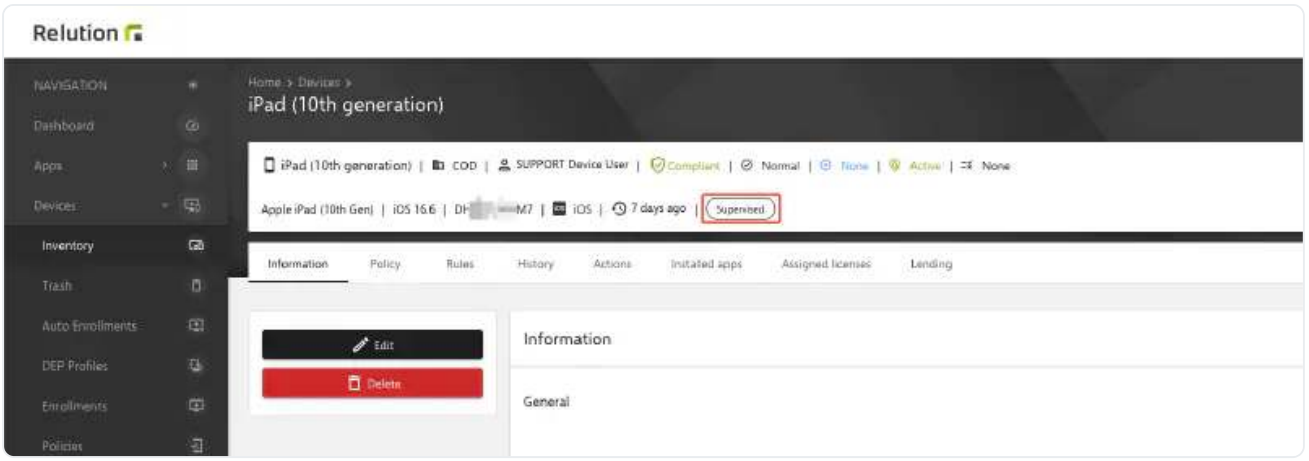
Identifier les appareils supervisés

Les appareils supervisés peuvent être localisés comme suit :

1. Dans l'inventaire, la colonne Supervisé peut être affichée. Les appareils concernés sont marqués d'une coche. La liste peut également être filtrée à l'aide du filtre Supervisé.



2. Dans les détails de l'appareil, le statut est indiqué par le badge Supervisé dans l'encadré d'informations.



Appareils enrôlés via Apple Configurator

> Cette opération supprime également le profil MDM des appareils, qui ne pourront plus être gérés par la suite sans réinscription. Toutes les applications et les données sont également supprimées des appareils.

Les appareils peuvent être réinitialisés en utilisant l'une des options suivantes :

1. Une action Effacer l'appareil est envoyée aux appareils.
2. Les appareils sont réinitialisés directement sur l'appareil : sur iPhone et iPad sous `Réglages` → `Général` → `Transférer ou réinitialiser l'iPhone/iPad` → `Effacer tout le contenu et les réglages`, sur Apple TV sous `Réglages` → `Système` → `Réinitialiser`.
3. Les appareils sont connectés à un ordinateur Mac et l'application Apple Configurator 2 est ouverte. Un clic droit est effectué sur les appareils, puis Avancé → Effacer tout le contenu et les réglages est sélectionné.

L'action Return to Service ne convient pas pour supprimer le mode supervisé : elle réinitialise certes l'appareil, mais le réinscrit ensuite automatiquement (voir Actions disponibles →).

Appareils inscrits par ADE via Apple School/Business Manager

Si les appareils ont été ajoutés au système MDM via l'Inscription automatisée des appareils (ADE, DEP dans le portail) dans Apple School/Business Manager, le lien doit être annulé à cet endroit. Sinon, les appareils se rapporteront toujours automatiquement au système MDM après

une réinitialisation d’usine et repasseront en mode supervisé. Cela vaut également pour les appareils ajoutés par l’intermédiaire d’un revendeur agréé.

1. Après la connexion à Apple School/Business Manager, Appareils est sélectionné.
2. L’appareil concerné est sélectionné, puis Edit Device Assignment est cliqué sur le côté droit.
3. Désassigner est cliqué.
4. L’appareil est réinitialisé aux paramètres d’usine.

Appareils ADE ajoutés ultérieurement via Apple Configurator

La suppression du mode supervisé des appareils ajoutés à Apple School/Business Manager via Apple Configurator fonctionne de la même manière que pour les appareils ADE inscrits par l’intermédiaire d’un revendeur agréé.

> Cependant, les utilisateurs peuvent supprimer manuellement le profil MDM sur les appareils dans les 30 premiers jours suivant l'ajout des appareils à l'Inscription automatisée des appareils (ADE). Cela entraînera la perte de l'inscription MDM ainsi que du mode supervisé.

Pour la version 26.4.0

Mode conférence

Apple TV peut partager l'écran d'un appareil compatible AirPlay sans donner aux utilisateurs l'accès aux autres fonctionnalités d'Apple TV. Lorsque l'écran de la salle de conférence est allumé, il affiche les détails du réseau et les instructions pour se connecter à l'Apple TV via AirPlay, ainsi que le message défini dans la configuration.

La configuration Salle de conférence n'est disponible que dans les politiques tvOS et ne peut être ajoutée qu'une seule fois par politique.

Configurer la salle de conférence pour Apple TV

1. La configuration est créée dans le portail Relution via `Appareils` → `Politiques` → `{politique tvOS}` → `Ajouter` → `Salle de conférence` → `Ajouter des détails`. Les configurations ne peuvent être ajoutées qu'à une version brouillon de la politique.
2. Dans la section Général, le champ obligatoire Votre message contient le texte affiché sur l'écran de salle de conférence de l'Apple TV. Le texte peut contenir des espaces réservés pour l'utilisateur et l'appareil (par ex. `${device.name}`), répertoriés dans la carte Espaces réservés disponibles ; ils sont remplacés par les valeurs correspondantes lors de la transmission à l'appareil. Sans message, la configuration ne peut pas être enregistrée.
3. Ensuite, la politique doit être publiée pour pouvoir l'affecter à des appareils.

Appareils tvOS dans Relution →

Pour la version 26.4.0

Sécurité AirPlay

La Sécurité AirPlay empêche la diffusion en continu non autorisée vers l'Apple TV via AirPlay. Les administrateurs peuvent ainsi contrôler qui peut se connecter à l'Apple TV via la fonctionnalité AirPlay. Il est possible de définir un mot de passe AirPlay ou de restreindre la connexion des appareils d'un autre réseau à la TV. La Sécurité AirPlay peut être utilisée sur les Apple TV fonctionnant avec tvOS 11 ou une version ultérieure.

Ajouter la configuration

La configuration est créée dans le portail Relution via `Appareils` → `Politiques` → `{politique tvOS}` → `Ajouter` → `Sécurité AirPlay` → `Ajouter des détails`. Les configurations ne peuvent être ajoutées qu'à une version brouillon de la politique. La Sécurité AirPlay n'est disponible que dans les politiques tvOS et ne peut être ajoutée qu'une seule fois par politique.

Pour la version 26.4.0

Réglages de sécurité AirPlay disponibles

- Accès (par défaut : Appareils connectés à n'importe quel réseau Wi-Fi) - Définit depuis quel réseau un appareil Apple compatible AirPlay peut se connecter à une Apple TV via AirPlay. Les options suivantes sont disponibles :
  - Appareils connectés à n'importe quel réseau Wi-Fi : Permet à l'Apple TV de se connecter à des appareils Apple compatibles AirPlay sur différents réseaux.
  - Appareils connectés au même réseau Wi-Fi : Permet la connexion entre les appareils Apple compatibles AirPlay et l'Apple TV qui sont sur le même réseau (même Wi-Fi ou Ethernet).
- Sécurité (par défaut : Code d'accès pour la première fois) - Définit comment la connexion est sécurisée. Les options suivantes sont disponibles :
  - Code d'accès pour la première fois : Lorsqu'une Apple TV se connecte à un appareil Apple compatible AirPlay, un code d'accès s'affiche sur l'écran de la TV. Ce code d'accès est saisi sur l'appareil Apple compatible AirPlay pour commencer la diffusion en continu. Le code d'accès n'est plus nécessaire lorsque les mêmes appareils se connectent à nouveau.
  - Code d'accès : Chaque fois que quelqu'un essaie de diffuser du contenu via AirPlay, un code d'accès s'affiche sur l'écran du téléviseur. Ce code d'accès doit être saisi sur l'appareil Apple compatible AirPlay pour démarrer la diffusion.

- Mot de passe : Un mot de passe AirPlay fixe est exigé lorsqu'une connexion est établie entre un appareil Apple compatible AirPlay et une Apple TV. Le mot de passe est saisi dans le champ obligatoire Mot de passe qui apparaît lorsque cette option est sélectionnée ; sans mot de passe, la configuration ne peut pas être enregistrée. Lorsqu'une connexion est établie, l'appareil connecté à l'Apple TV est invité à saisir ce mot de passe ; une fois le mot de passe de la politique saisi, la diffusion démarre. Contrairement à Code d'accès pour la première fois, aucun code n'est affiché sur la TV.

La politique doit ensuite être publiée pour être attribuée aux appareils.

Appareils tvOS dans Relution →

Pour la version 26.4.0

Conformité de l'application

L’installation d’applications issues d’Apps et livres (VPP dans le portail) sur les appareils Apple TV est particulièrement simple grâce à la politique de conformité des applications (Conformité App) de Relution. Cette configuration permet une distribution simple et centralisée des applications sur un grand nombre d’appareils.

Pour commencer la distribution, seuls les éléments suivants sont nécessaires :

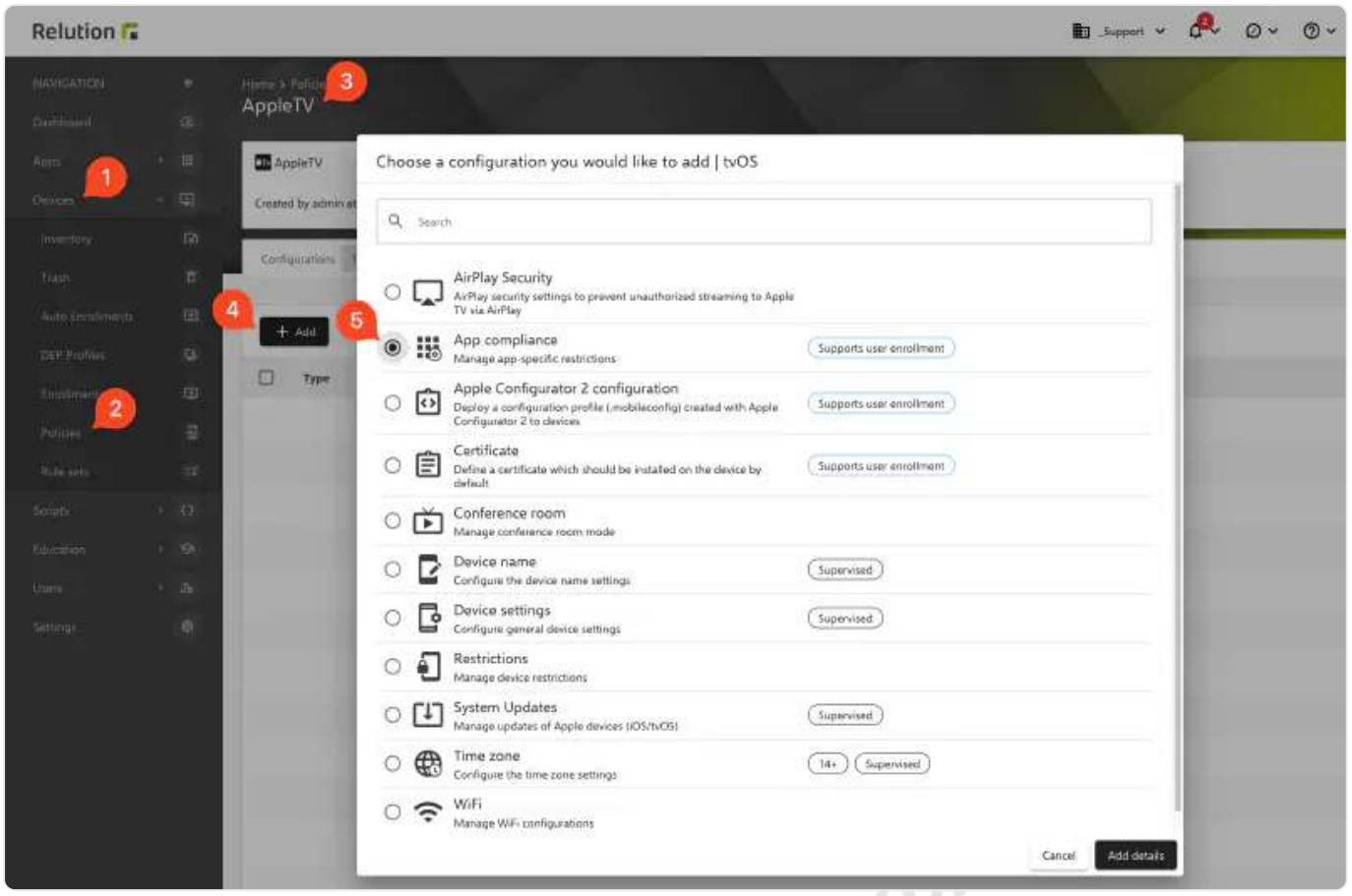
- Un compte Apple School ou Apple Business.
- L’intégration du jeton Apps et livres → de l’organisation dans Relution.
- Des licences acquises pour les applications souhaitées depuis Apple School Manager (ASM) ou Apple Business Manager (ABM).

appareils tvOS dans Relution →

Configuration de la conformité de l’application

La distribution d’applications sur les appareils Apple TV (de manière analogue aux appareils iOS) s’effectue via la configuration de politique Conformité App. Elle est sélectionnée sous `Appareils` → `Politiques` dans une politique tvOS via Ajouter une configuration, puis créée via Ajouter des détails.

Pour la version 26.4.0



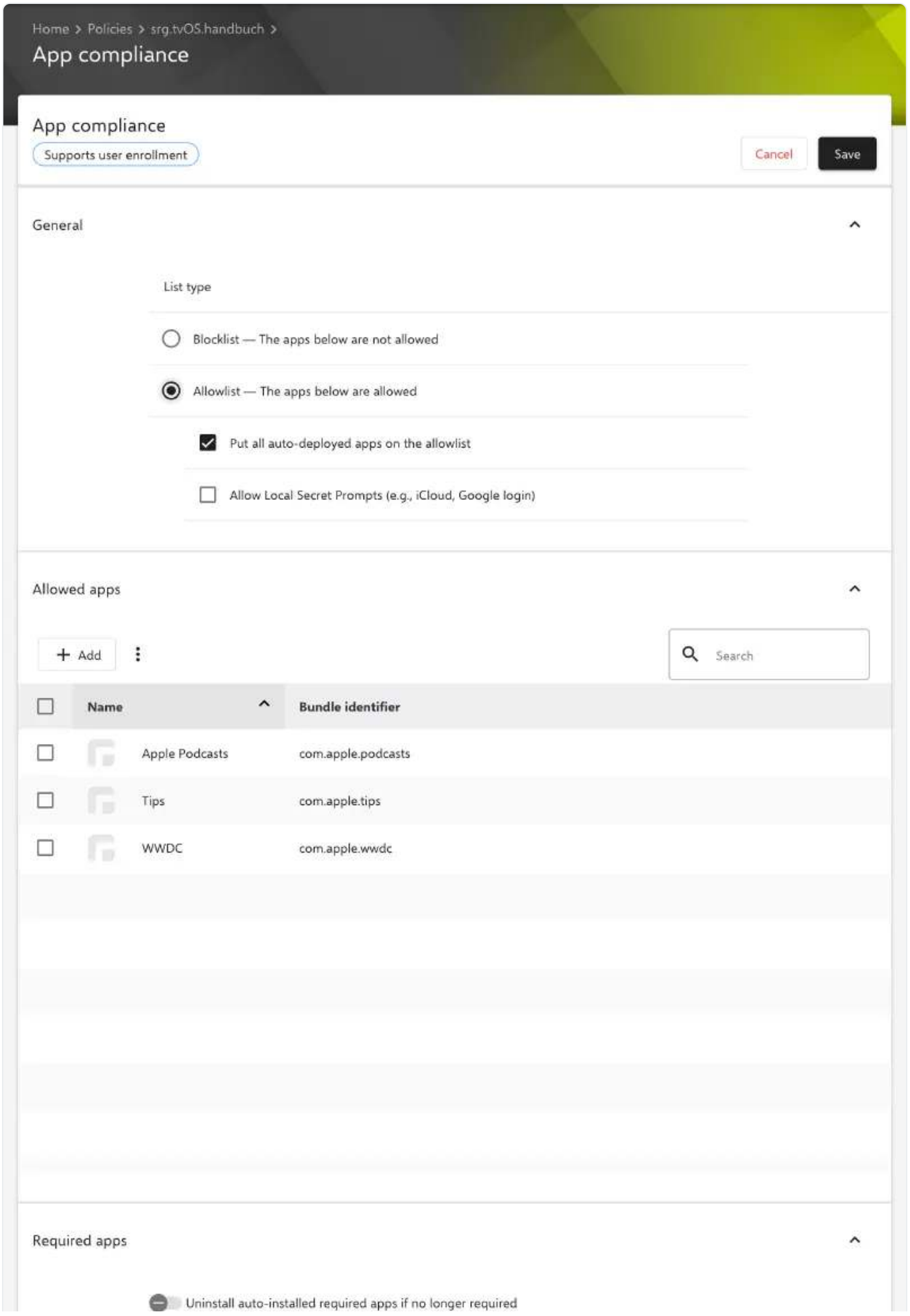
Comme pour les appareils iOS, la disponibilité des applications est contrôlée dans la section Général sous Type de liste : soit sous forme de liste de blocage (Liste de blocage — Les applications ci-dessous ne sont pas autorisées, valeur par défaut des nouvelles configurations), soit sous forme de liste d'autorisation (Liste d'autorisation : les applications ci-dessous sont autorisées). Un seul des deux types de liste est actif par configuration. Les applications sont saisies via Ajouter dans la section Apps bloquées ou Apps autorisées située en dessous.

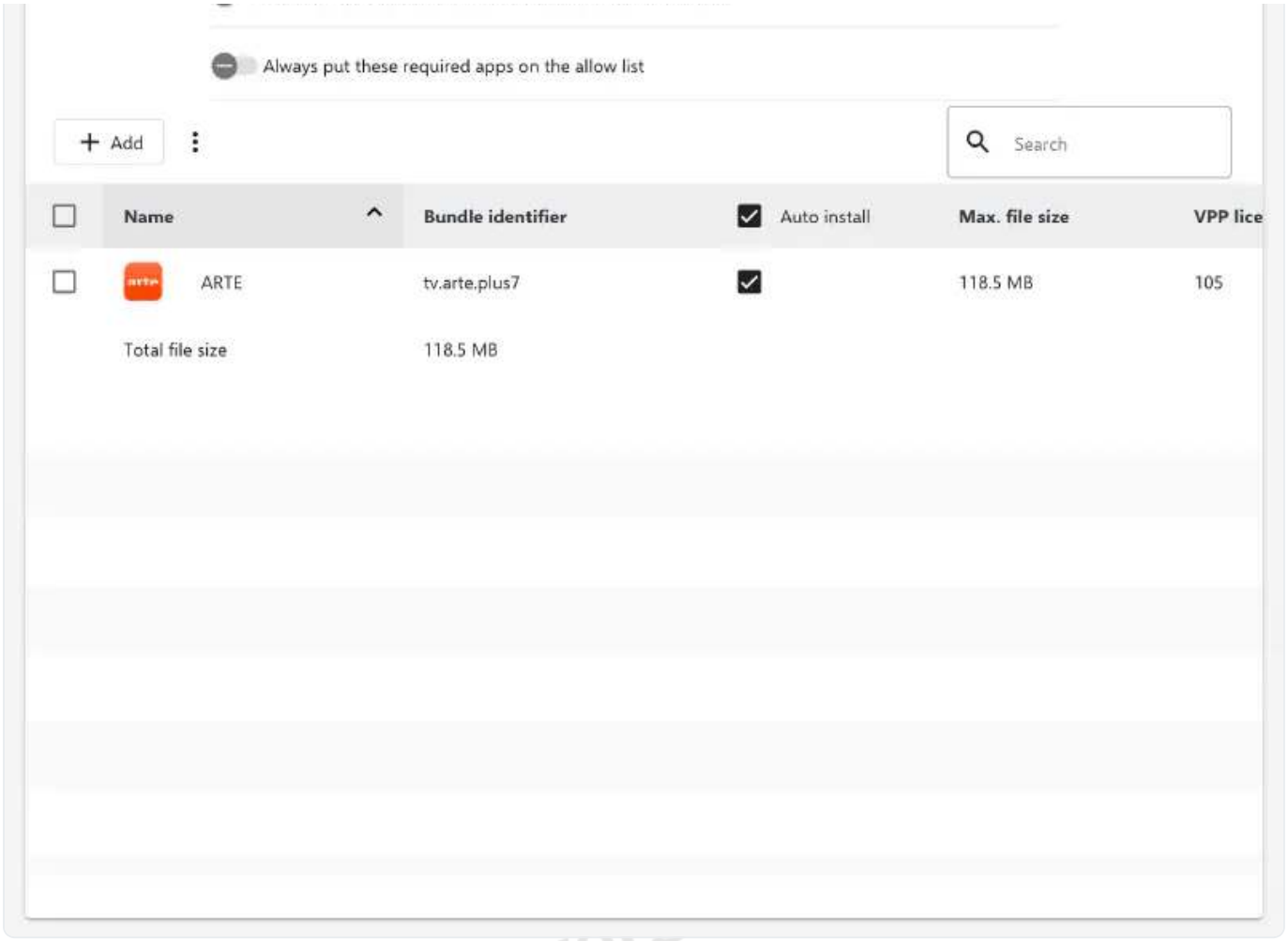
La liste d'autorisation et la liste de blocage ne sont appliquées que sur les appareils supervisés.

Liste d'autorisation (applications autorisées)

La liste d'autorisation permet de définir explicitement les applications autorisées à être disponibles sur les appareils. Deux options supplémentaires sont disponibles :

- Mettre toutes les applications déployées automatiquement sur la liste verte : les applications distribuées aux utilisateurs des appareils via des déploiements automatiques sont automatiquement ajoutées à la liste d'autorisation.
- Autorisation des invites de sécurité locales, par exemple pour la connexion iCloud (dans le portail : Autoriser les invites secrètes locales (par exemple, iCloud, Google login)) : la boîte de dialogue système des invites de sécurité locales est ajoutée à la liste d'autorisation afin que ces invites ne soient pas bloquées.

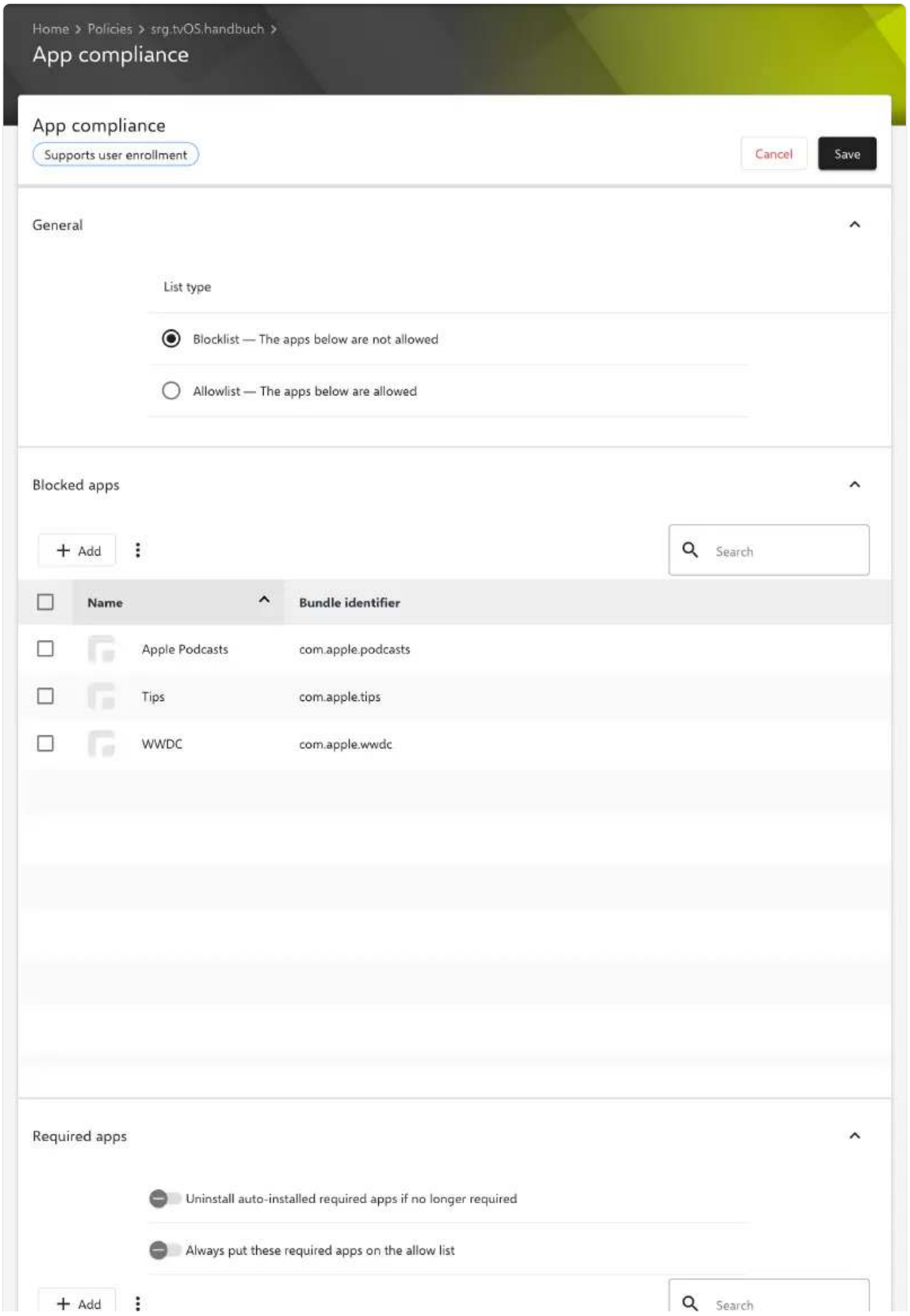

Home > Policies > srg.tvOS.handbuch >
App compliance
App compliance
Supports user enrollment
Cancel
Save
General
List type
Blocklist — The apps below are not allowed
Allowlist — The apps below are allowed
Put all auto-deployed apps on the allowlist
Allow Local Secret Prompts (e.g., iCloud, Google login)
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

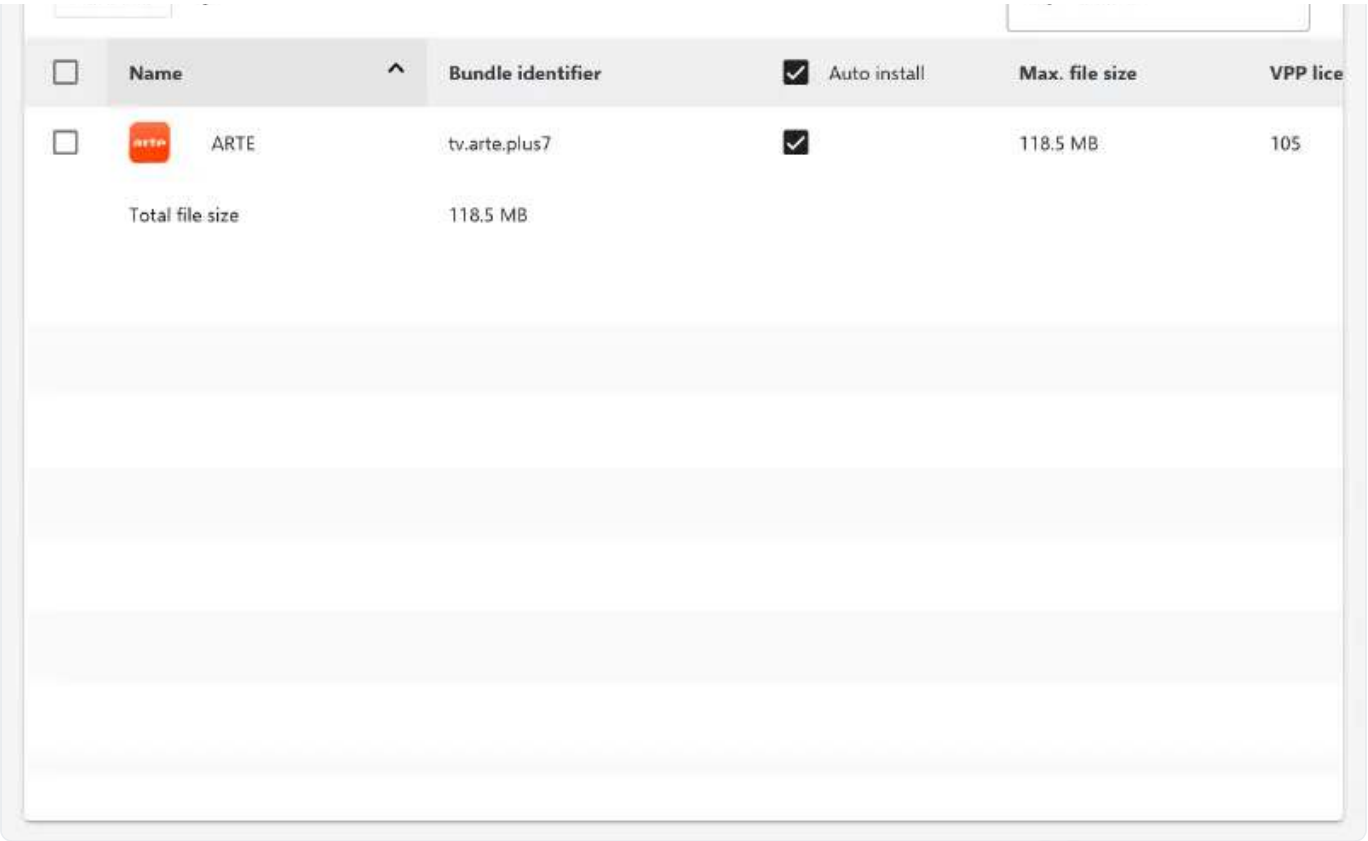


Liste de blocage (applications bloquées)

La liste de blocage permet de masquer ou de bloquer certaines applications sur les appareils tvOS.

Pour la 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

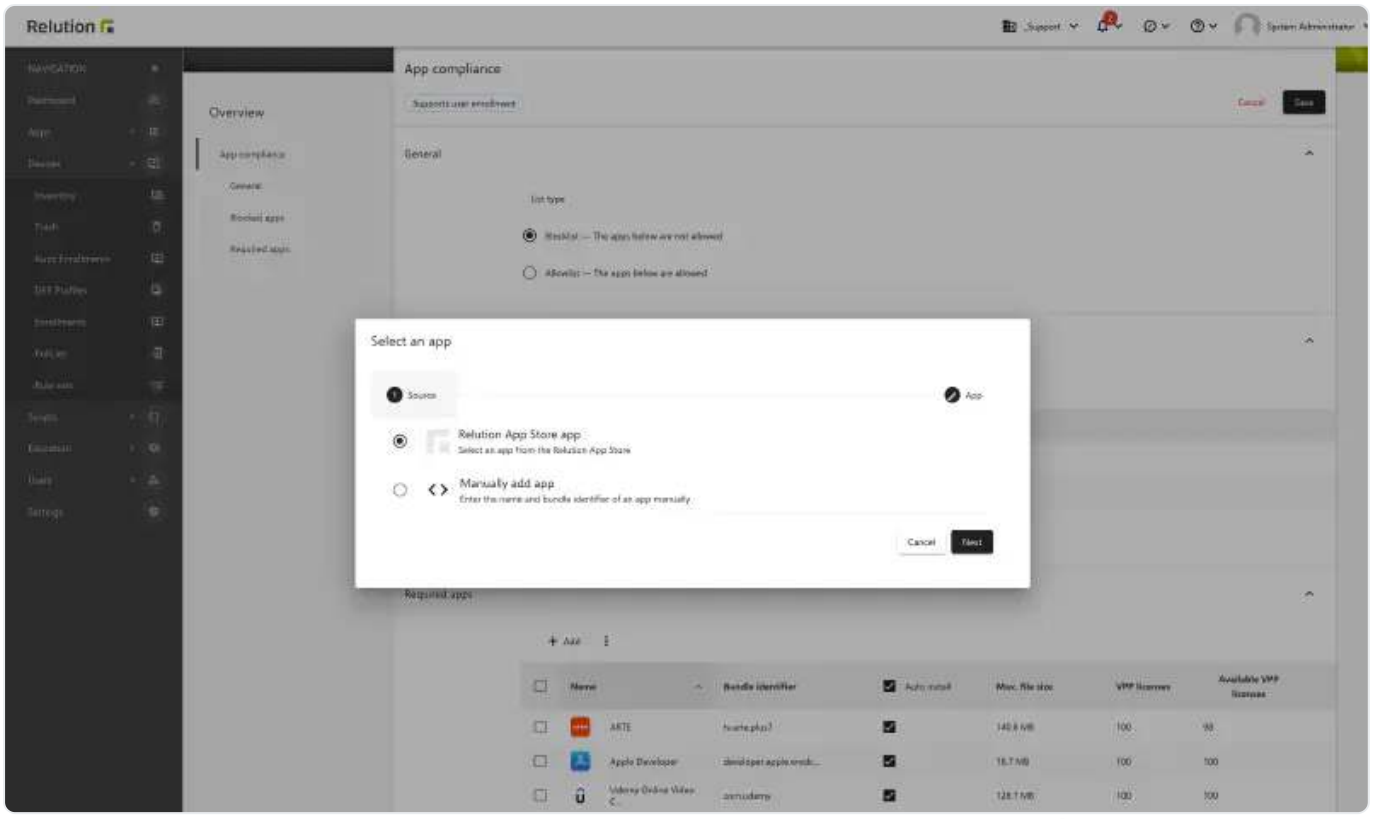


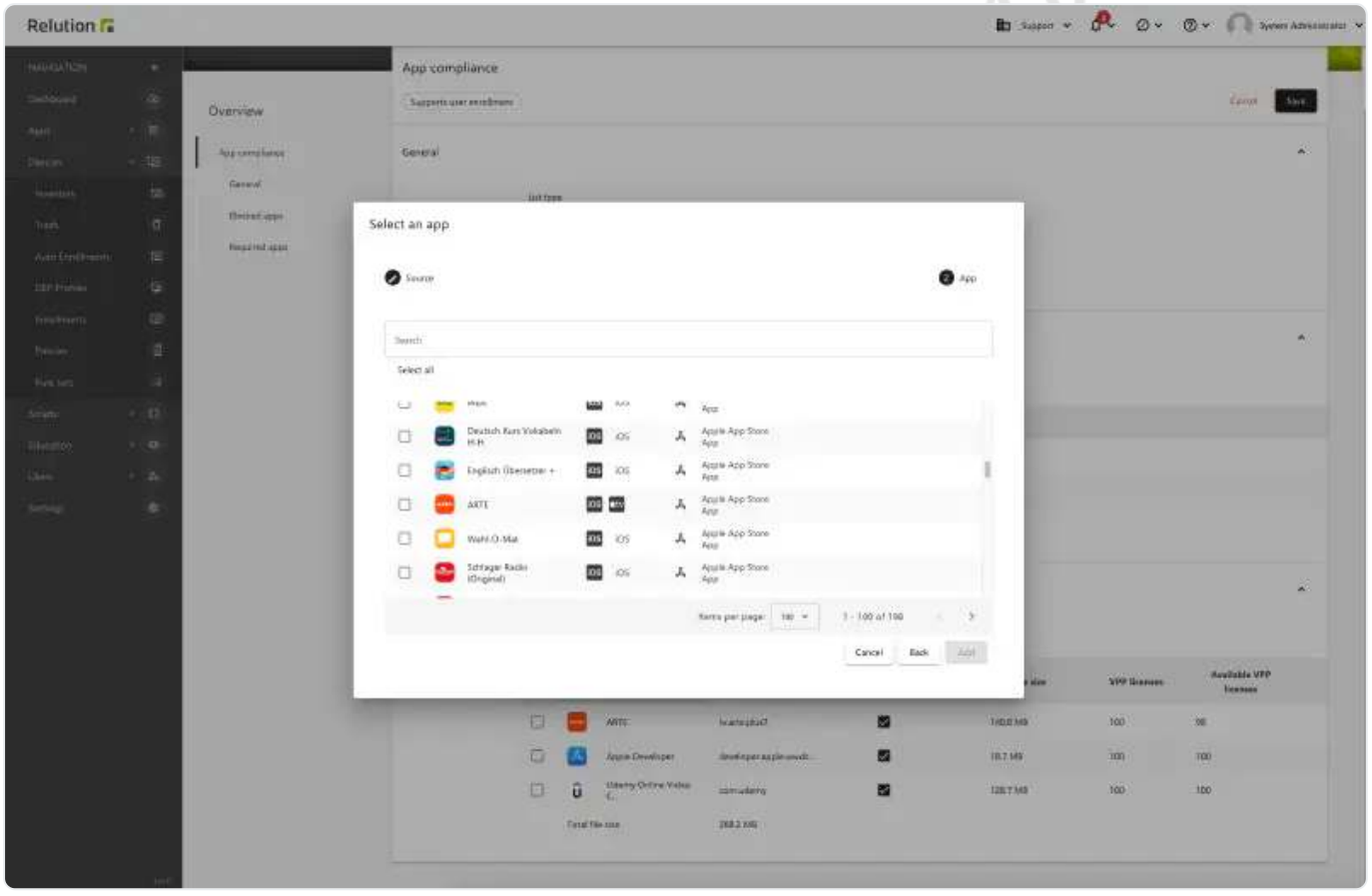
Applications requises

La section Apps requises permet de définir les applications à installer obligatoirement sur les appareils. Ajouter propose les sources suivantes (identiques pour la liste d'autorisation et la liste de blocage) :

- Appli Relution App Store : sélection d'applications des plateformes tvOS et iOS dans le Relution App Store. Pour les applications requises, sont proposées les applications natives (téléversées) ainsi que les applications publiques pour lesquelles l'organisation dispose de licences Apps et livres. Il n'existe pas de recherche directe dans l'App Store public d'Apple pour tvOS.
- Ajouter une application manuellement : saisie d'une application avec son Nom et son Nom interne (identifiant de bundle).

Pour la version 26.4.0





Si une application requise n’est pas installée sur l’appareil, celui-ci est considéré comme non conforme. L’application n’est installée activement que si la case de la colonne Installation automatique est cochée ; elle est cochée par défaut lors de l’ajout d’une application. Les

colonnes Licences VPP et Licences VPP disponibles indiquent, pour chaque application, les licences existantes et celles encore libres.

Deux commutateurs sont disponibles au-dessus de la liste :

- Désinstallation automatique des applications requises qui ne sont plus nécessaires : si une application requise installée automatiquement est retirée de la configuration, ou si la configuration est retirée de l'appareil, l'application est désinstallée. Le commutateur est désactivé pour les nouvelles configurations.
- Ajout systématique des applications requises à la liste des applications autorisées : si cette politique ou une autre configure une liste d'autorisation pour l'appareil, les applications requises y sont ajoutées.

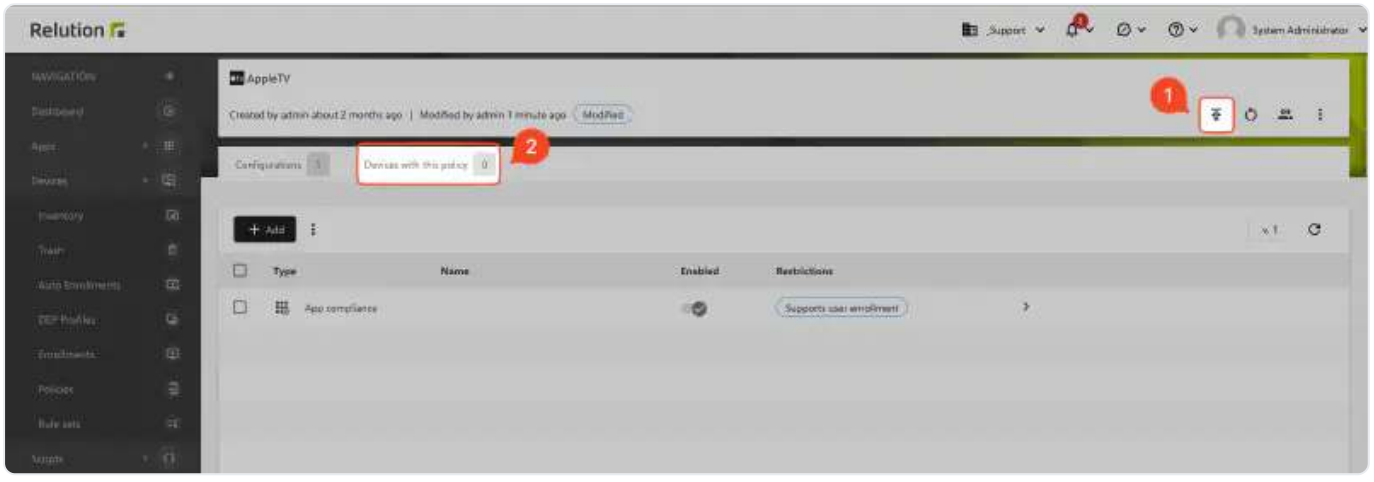
Lors de l'enregistrement, les listes sont vérifiées pour détecter les contradictions : une application requise ne doit pas figurer sur la liste de blocage. Si, pour une liste d'autorisation, le second commutateur est désactivé, toutes les applications requises doivent également figurer sur la liste d'autorisation.

Les applications iOS peuvent également être utilisées sur tvOS, à condition qu'elles soient adaptées à tvOS. Les applications non compatibles sont installées sur l'appareil, mais disparaissent après le processus d'installation et ne sont pas disponibles.

> Les apps publiques sans licence Apps et livres ainsi que les liens web (navigateurs) ne peuvent pas être installés sur les appareils tvOS.

Pour la version 26.4.0

Une fois la configuration terminée, elle peut être enregistrée, publiée et attribuée aux appareils correspondants.



Distribution d'applications

Les entreprises décident de plus en plus souvent de soutenir certains processus de travail à l'aide d'une application mobile. Parmi de nombreux autres problèmes conceptuels, la question de la distribution de cette application aux utilisateurs se pose rapidement. Souvent, le cas d'utilisation est que non seulement les employés, mais aussi les personnes externes doivent obtenir l'application - il peut s'agir de fournisseurs de services, de partenaires ou de clients, par exemple. Dans la plupart des cas, l'application n'est pas destinée à une large clientèle, mais à des utilisateurs professionnels sélectionnés. Les sections suivantes devraient aider à choisir la meilleure méthode de distribution.

> Sur les appareils Apple TV, les applications provenant de Relution sont installées exclusivement via la gestion des appareils (MDM). Une installation par les utilisateurs via un site web, un lien profond ou une application Store n'est pas possible sous tvOS, et les clips web ne sont pas distribués aux appareils tvOS. Dans Relution, les applications tvOS sont classées sous la plateforme iOS (Gérer les apps natives →). Les applications de l'App Store ne peuvent être installées sur Apple TV qu'avec une licence Apps et livres (VPP dans le portail) (Gérer les apps de l'App Store →, Conformité de l'application →). Les sections suivantes décrivent les méthodes de distribution de manière générale pour iOS et Android.

Pour la version 26.4.0

Distribution via les magasins d'applications publics

Apple et Google proposent chacun une infrastructure de distribution d'applications. Pour Apple, les applications sont mises à la disposition des utilisateurs finaux par l'intermédiaire de l'Apple App Store. L'App Store est préinstallé sur chaque appareil iOS.

Les applications sont gérées et publiées via le portail des développeurs et App Store Connect. Sur Google, les applications sont mises à la disposition des utilisateurs finaux via le Play Store. L'application Play Store est préinstallée sur chaque appareil Android.

L'administration et la publication des applications se font via le portail des développeurs. Apple et Google définissent le cadre de publication des applications via leurs systèmes.

Si un appareil est géré par un système MDM, l'application Store peut également être verrouillée pour l'utilisateur et peut donc ne pas être disponible pour l'utilisateur final.

Distribution via l’Apple App Store - Avantages

- Les applications sont disponibles pour les utilisateurs finaux via le mécanisme standard d’Apple.
- Les applications n’ont pas besoin d’être re-signées et re-provisionnées avec un profil de provisionnement mis à jour après un an.
- Les applications peuvent être activées ou bloquées de manière sélective pour certains pays, si nécessaire.
- Les applications peuvent être proposées à titre onéreux - si on le souhaite - dans des structures définies (Apple prélève à cet effet un pourcentage de commission de 15 %).
- Apple fournit l’infrastructure de distribution et de facturation

Distribution via l’Apple App Store - inconvénients

- Les utilisateurs ont besoin d’un identifiant Apple sur les appareils finaux pour installer les applications de l’Apple App Store.
- Pour les entreprises disposant d’appareils gérés, l’Apple App Store peut être bloqué par MDM.
- Toutes les spécifications d’Apple doivent être respectées, comme la prise en charge des nouvelles classes d’appareils telles que l’iPhone X.
- Lors d’un examen, Apple se réserve le droit de ne pas publier l’application ou de la supprimer ultérieurement.
- L’examen peut entraîner des retards allant jusqu’à 10 jours (actuellement, la durée moyenne de l’examen est d’environ 3 jours ouvrables).
- Les applications ne peuvent être mises à la disposition de certains groupes d’utilisateurs que de manière très limitée.

Pour la version 26.4.0

Distribution via Google Play Store - avantages

- Les applications sont disponibles pour les utilisateurs finaux via le mécanisme standard de Google.
- Les applications peuvent - si nécessaire - être activées ou bloquées de manière sélective pour certains pays.
- Les applications peuvent - si on le souhaite - être proposées à titre onéreux dans des structures définies (Google prélève à cet effet un pourcentage de commission de 15 %).
- Google fournit l’infrastructure pour la distribution et la facturation

Distribution via Google Play Store - inconvénients

- Les utilisateurs ont besoin d'un compte Google pour installer des applications à partir du Play Store.
- Pour les entreprises disposant d'appareils gérés, le Play Store peut être verrouillé par MDM.
- Toutes les exigences de Google doivent être satisfaites, comme la version Cordova.
- Après l'analyse automatique des applications, Google se réserve le droit de retirer l'application de la boutique à une date ultérieure.
- En raison des analyses techniques, la publication des applications peut être retardée de quelques heures.
- Les applications ne peuvent être mises à la disposition de certains groupes d'utilisateurs que dans une mesure très limitée.

Distribution via les programmes bêta des magasins d'applications publics

Apple et Google proposent chacun un programme de test bêta en plus de la distribution d'applications publiques. Chez Apple, les applications sont mises à la disposition des utilisateurs finaux pour des tests bêta via l'application TestFlight. Sur les appareils iOS, cette application peut être installée depuis l'App Store.

L'administration et la publication des applications se font via le portail des développeurs et App Store Connect dans la zone TestFlight. Sur Google, les applications sont mises à disposition pour les tests alpha ou bêta via le Play Store. Le Play Store est préinstallé sur tous les appareils Android.

L'administration et la publication des applications se font via le portail des développeurs dans la zone Alpha et Beta Testing. Apple et Google définissent le cadre de publication des applications via leurs systèmes.

Pour la version 26.4.0

Distribution via Apple Testflight - Avantages

- Les applications sont mises à la disposition des utilisateurs par le biais d'un mécanisme fourni par Apple.
- Les applications peuvent être distribuées de manière sélective à des utilisateurs individuels.
- Apple fournit l'infrastructure de distribution et de facturation

Distribution via Apple Testflight - Inconvénients

- Les utilisateurs ont besoin d'un identifiant Apple pour installer les applications de l'Apple App Store.

- L’installation unique de l’application TestFlight est nécessaire pour installer l’application.
- Apple se réserve le droit de ne pas publier l’application dans une évaluation “réduite”.
- L’évaluation peut entraîner des retards pouvant aller jusqu’à 10 jours (actuellement, la durée moyenne d’une évaluation est d’environ deux jours ouvrables).
- La signature de l’application expire après 90 jours

Le service TestFlight est principalement destiné à une courte période de test avant la publication d’une application iOS. Il n’est pas adapté à un fonctionnement permanent en raison de la courte durée de validité de la signature.

Distribution via Google Alpha et Beta Testing - Avantages

- Les applications sont mises à la disposition des utilisateurs par le biais d’un mécanisme fourni par Google.
- Les applications peuvent être activées de manière sélective pour des utilisateurs individuels.
- Google fournit l’infrastructure de distribution et de facturation

---

Distribution via Google Alpha et Beta Testing - Inconvénients

- Les utilisateurs ont besoin d’un identifiant Google pour installer des applications à partir du Play Store.
- Pour les entreprises disposant d’appareils gérés, le Play Store peut être verrouillé par MDM.

Pour la version 26.4.0

Distribution via le magasin d’applications interne de l’entreprise

Outre la distribution d’applications via leurs magasins publics respectifs, Apple et Google proposent également des mécanismes de distribution d’applications en interne, principalement pour les entreprises. Dans le cas d’Apple, le programme Apple Enterprise et un magasin d’applications d’entreprise tel que Relution sont des conditions préalables.

Les applications sont mises à la disposition des utilisateurs finaux par le biais d’une application App Store distincte ou d’un site web mobile. Les applications sont téléversées et gérées dans l’App Store d’entreprise (dans Relution sous `Apps` → `App Store`). Chez Apple, seuls les certificats et les profils de provisionnement sont créés dans le portail des développeurs Apple.

Les applications sont distribuées par l’intermédiaire du fournisseur de la boutique d’applications de l’entreprise concernée. Chez Google, les applications peuvent être mises à disposition pour le téléchargement et l’installation via un service web.

Pour les appareils spéciaux, tels que Samsung, des mécanismes d’installation et de distribution optimisés peuvent être utilisés. Apple et Google définissent les options de distribution des

applications parallèlement à leurs systèmes.

Distribution d'applications iOS via l'App Store d'entreprise - avantages

- Les applications peuvent être distribuées à des groupes d'utilisateurs sélectionnés, par exemple sous la forme d'un lien profond ou après connexion à l'aide de noms d'utilisateurs et de mots de passe préalablement configurés.
- Les utilisateurs n'ont pas besoin d'un identifiant Apple pour installer des applications à partir d'un App Store d'entreprise interne.
- Il n'est pas nécessaire de satisfaire à toutes les exigences d'Apple
- La publication des mises à jour d'applications n'est pas retardée par un examen d'Apple.
- Certains magasins d'applications d'entreprise (par exemple Relution) peuvent être utilisés sans gestion des appareils (MDM).
- Un système de gestion des utilisateurs existant (ActiveDirectory/LDAP) peut être connecté afin que les utilisateurs n'aient pas besoin de nouvelles informations d'identification.

Distribution d'applications iOS par l'intermédiaire d'un magasin d'applications d'entreprise - inconvénients

- Les applications sont disponibles pour les utilisateurs finaux via un mécanisme spécial approuvé par Apple, mais qui nécessite une configuration initiale de la part de l'utilisateur (voir ici →).
- Les applications doivent être re-signées avec un profil de provisionnement mis à jour au bout d'un an, puis téléversées dans Relution en tant que nouvelle version.
- L'infrastructure de distribution peut être fournie sous la forme d'un service en nuage ou sur site, par exemple.
- Selon les directives d'Apple, les applications ne peuvent être distribuées qu'aux employés, aux parties intéressées et aux partenaires, mais surtout à un groupe connu d'utilisateurs.

Distribution d'applications Android via l'App Store d'entreprise - Avantages

- Les applications peuvent être distribuées à des groupes d'utilisateurs sélectionnés, par exemple sous la forme d'un lien profond ou après connexion à l'aide d'un nom d'utilisateur et d'un mot de passe préalablement configurés.
- Les utilisateurs n'ont pas besoin d'un identifiant Google pour installer des applications à partir d'une boutique d'applications interne à l'entreprise.
- Il n'est pas nécessaire de satisfaire à toutes les exigences de Google
- La publication des mises à jour d'applications n'est pas retardée par les analyses techniques de Google.

Pour la version 26.4.0

- Certains magasins d’applications d’entreprise (par exemple Relution) peuvent être utilisés sans gestion des appareils (MDM).
- Un système de gestion des utilisateurs existant (ActiveDirectory/LDAP) peut être connecté afin que les utilisateurs n’aient pas besoin de nouvelles informations d’identification.

Distribution d’applications Android par l’intermédiaire d’un magasin d’applications d’entreprise - inconvénients

- Les applications sont mises à la disposition des utilisateurs finaux par le biais d’un mécanisme spécial approuvé par Google, mais qui nécessite une configuration initiale par l’utilisateur.
- L’infrastructure de distribution doit être fournie, par exemple sous la forme d’un service en nuage.

Pour la version 26.4.0

Gérer les apps natives

Avec Relution, il est également possible de distribuer des applications natives pour tvOS et de les soumettre à une gestion des versions. Il n'existe pas de plateforme tvOS distincte à cet effet : les applications tvOS sont téléchargées sous forme de fichier `.ipa` et gérées dans Relution sous la plateforme iOS. Les appareils Apple TV les reçoivent via cette application iOS. L'application doit avoir été conçue pour tvOS.

Une application peut comporter plusieurs versions dans différents statuts, par exemple une version 1.0 au statut de production (Version dans le portail) et une version 1.1 préparée et vérifiée au statut Développement ou au statut de vérification (Critique dans le portail). Les appareils Apple TV reçoivent toujours la version au statut Version. C'est pourquoi la version 1.0 est d'abord téléchargée sur Relution et placée au statut Version.

Créer une nouvelle application

Pour la version 26.4.0

Les applications natives sont créées dans le menu sous `Apps` → `App Store`. Le bouton Ajouter ouvre la boîte de dialogue Ajouter une nouvelle application. Sous Source, l'option Appli native est sélectionnée.

Après un clic sur Suivant, le fichier de l'application (`.ipa`) est téléchargé via Choisissez un fichier. Ajouter des détails ouvre ensuite le formulaire de l'application.

> Il faut faire attention à la taille du fichier. Pour les applications volumineuses, des problèmes peuvent survenir si la base de données ou le proxy inverse ne le permet pas. Dans ce cas, la configuration doit être adaptée.

Dans le formulaire de l'application, l'État de la version est indiqué et l'application est créée via Enregistrer. À l'exception du statut Archive, chaque statut ne peut contenir qu'une seule version de l'application.

La section Permissions définit qui peut intervenir sur l'application dans le portail Relution :

- Propriétaire : peut appliquer toutes les opérations à l'application, quel que soit le statut.
- Vérificateur (Critique dans le portail) : peut modifier l'application et déplacer des versions vers le statut Version ou Développement.
- Développeur : peut télécharger et modifier des versions au statut Développement et les déplacer vers le statut Critique ou vers l'Archive.
- Utilisateur : peut télécharger, évaluer et commenter les versions au statut Version.

Indépendamment de ces permissions, les administrateurs peuvent distribuer l'application aux appareils via le portail Relution.

Distribuer des applications natives sur Apple TV

Il n'existe pas de Relution Agent pour tvOS, et donc pas de store en libre-service sur l'appareil. Les utilisateurs ne peuvent pas installer eux-mêmes des applications natives sur l'Apple TV. La distribution s'effectue exclusivement via le portail Relution :

- avec l'action Déployer l'application Relution Store (Actions →),
- sous Apps requises dans la configuration Conformité App, à condition que la case de la colonne Installation automatique soit cochée (Conformité App →),
- dans la vue de l'application sous Appareils équipés de cette application, via le bouton de mise à jour de l'application, pour les appareils sur lesquels l'application est déjà installée.

C'est toujours la version au statut Version qui est distribuée. Une version au statut Développement ou Critique ne peut pas être distribuée sur un Apple TV via le portail Relution. Pour tvOS, les déploiements automatiques (Auto-Deployment) ne prennent en compte que les applications publiques, pas les applications natives.

Pour la version 26.4.0

Mettre à jour l'application

Si une nouvelle version de l'application doit être préparée, elle peut être placée au préalable au statut Développement ou Critique. Avant cela, la nouvelle version doit être sélectionnée et téléchargée via le bouton Ajouter une nouvelle version.

Une date peut être indiquée pour la nouvelle version dans le champ Date de mise en ligne. La version ne passe automatiquement au statut Version à cette date que si un processus de validation des applications → est actif et que la version au statut Critique a franchi toutes les étapes de validation. Sans processus de validation actif, la date ne sert que de date souhaitée, et la version est placée manuellement au statut Version (voir ci-dessous).

Les deux versions peuvent être visualisées dans les propriétés de l'application.

Mise en service manuelle de la nouvelle version

Dans le portail Relution, les versions respectives peuvent être visualisées et configurées. Si la nouvelle version se trouve au statut Critique, un clic sur le bouton Version la déplace vers ce

statut. Si elle se trouve encore au statut Développement, le changement s’effectue via `Déplacer vers` → `Version`. Si une version se trouve déjà au statut Version, elle est automatiquement déplacée vers l’Archive.

> L'application n'est pas automatiquement mise à jour sur les appareils. La mise à jour est déclenchée par les administrateurs via l'action Déployer l'application Relution Store ou, dans la vue de l'application sous Appareils équipés de cette application, via le bouton de mise à jour de l'application.

Pour la version 26.4.0

Gérer les apps de l'App Store

Avec Relution, il est possible de distribuer des applications de l’App Store d’Apple à des appareils. Pour ce faire, une licence d’application doit toujours être achetée, que l’application soit payante ou non. Sur les appareils iOS, une licence d’application peut être achetée via Apps et livres (VPP dans le portail) ou obtenue via un identifiant Apple connecté sur l’appareil. Sur les appareils Apple TV, en revanche, les applications de l’App Store ne peuvent être installées qu’avec une licence Apps et livres ; la voie de l’identifiant Apple n’y est pas disponible. La configuration d’Apps et livres est décrite dans le chapitre correspondant →.

Les applications achetées dans Apple School / Business Manager sont automatiquement synchronisées avec Relution (à partir de la version 5.10). Les applications sont publiées dans Relution au statut de production (Version dans le portail) et peuvent être distribuées aux appareils par la suite. Les applications qui ne doivent pas être mises à la disposition de tous les utilisateurs peuvent également être manuellement assignées à un statut de publication différent. Une application peut également être ajoutée manuellement à l’App Store de Relution à tout moment. Cependant, les licences Apps et livres ne sont pas automatiquement disponibles pour ces applications. Sur les appareils Apple TV, elles ne peuvent être installées que lorsque des licences Apps et livres sont disponibles pour elles. Il est possible d’obtenir ces licences ultérieurement.

Pour la version 26.4.0

Distribuer les applications

Les applications de l’App Store sont normalement distribuées aux appareils Apple TV en tant qu’applications requises via la configuration de stratégie Conformité de l’application →.

Une application est attribuée à des appareils individuels via l’action Déployer l’application Relution Store. Outre les applications natives, elle propose également les applications de l’App Store qui sont classées sous la plateforme iOS dans l’App Store de Relution. L’action Déployer une application depuis l’Apple App Store n’est pas disponible pour les appareils tvOS.

Gérer les applications

Les applications de l’App Store sont mises à jour automatiquement par le système d’exploitation. Dans de rares cas, cependant, cela ne fonctionne pas. Il existe alors deux moyens de déclencher une mise à jour :

- Dans la vue détaillée de l’application, les appareils concernés sont sélectionnés dans l’onglet Appareils équipés de cette application, puis mis à jour via le bouton de mise à jour (Mise à jour de dans le portail). Le bouton est désactivé dès que l’un des appareils sélectionnés dispose déjà de la version au statut Version.
- Sinon, l’action Déployer l’application Relution Store est exécutée avec l’application concernée sur les appareils concernés.

Dans les deux cas, une réinstallation est déclenchée et les appareils valident la version de l’application avec l’App Store d’Apple. Si la version disponible est plus récente que la version installée, l’application existante est mise à jour.

Pour la version 26.4.0

Inscription des utilisateurs

L'inscription des utilisateurs permet d'inscrire des Mac privés sans que leur propriétaire n'ait à renoncer à tout contrôle sur ces appareils. Sur la base de l'approche BYOD (Bring Your Own Device), les appareils privés des étudiants ou des employés peuvent être intégrés et utilisés dans le contexte de l'école ou de l'entreprise tout en maintenant la protection des données privées. L'inscription des utilisateurs pour iPhone et iPad est décrite dans l'article Inscription des utilisateurs pour iOS →.

> Les appareils ne doivent pas être en mode supervisé → pour l'inscription des utilisateurs Apple.

Il existe deux variantes d'inscription des utilisateurs : l'inscription utilisateur basée sur le compte, pour laquelle la connexion sur le Mac s'effectue avec un compte Apple géré (Identifiant Apple géré dans le portail), et l'inscription utilisateur basée sur un profil via un lien d'inscription.

> L'inscription utilisateur basée sur un profil n'est plus prise en charge à partir de macOS 15. Pour ces Mac, l'inscription utilisateur basée sur le compte → est utilisée.

Pour la version 26.4.0

Avantages

- Les administrateurs ne peuvent pas voir les applications installées de manière privée.
- Les appareils restent sous le contrôle des utilisateurs.

Inconvénients

- Toutes les actions et configurations de politique ne sont pas possibles.
- Des comptes Apple gérés sont nécessaires.
- Le macOS Companion n'est pas déployé sur les Mac avec inscription des utilisateurs. Les apps de type DMG ne peuvent donc pas être installées sur ces Mac.

Inscription utilisateur basée sur le compte

Relution prend en charge l'inscription utilisateur basée sur le compte pour les Mac qui ne sont pas en mode supervisé → (Supervised Mode).

La connexion s'effectue sur le Mac, dans les Réglages Système, via la connexion à un compte professionnel ou scolaire, c'est-à-dire avec le compte Apple géré. Grâce à la découverte de service, le Mac détermine le serveur MDM compétent et redirige vers la page de connexion de Relution, où la connexion s'effectue avec le compte utilisateur Relution. La connexion avec le compte Apple géré est ensuite confirmée sur le Mac, le profil MDM est installé et le Mac apparaît dans l'inventaire des appareils de l'organisation Relution correspondante.

Prérequis

- macOS 14 ou une version ultérieure.
- Un certificat APNs enregistré dans Relution (Certificats de poussée APNS →).
- Un compte Apple géré et un compte utilisateur Relution pour chaque utilisateur. L'Identifiant Apple géré est enregistré à cet effet dans les détails de l'utilisateur ; sans Identifiant Apple géré, Relution utilise l'Adresse e-mail de l'utilisateur. Cette valeur doit correspondre au compte Apple géré utilisé pour la connexion sur le Mac.
- Soit le paramètre Inscription des utilisateurs Apple en fonction du compte activé dans l'organisation, soit une inscription utilisateur → créée pour l'utilisateur.
- Une découverte de service pour le domaine des comptes Apple gérés, soit automatiquement via Apple School/Business Manager, soit via un fichier well-known.

Pour la version 26.4.0

Activer l'inscription utilisateur Apple basée sur le compte

Le paramètre se trouve sous `Paramètres` → `Gestion des appareils`, dans la section Inscription des utilisateurs Apple en fonction du compte. Il s'applique par organisation ; la section n'est pas affichée dans l'organisation globale.

Lors de la connexion d'un utilisateur, Relution utilise d'abord une inscription utilisateur macOS créée pour cet utilisateur avec le statut Créé et encore valable au moins cinq minutes. S'il n'existe aucune inscription de ce type et que le curseur Inscription des utilisateurs Apple en fonction du compte est activé, Relution crée automatiquement une inscription utilisateur avec la propriété Apportez votre propre appareil (BYOD) et une validité de cinq jours. Le curseur est désactivé par défaut ; sans inscription utilisateur correspondante, l'inscription du Mac échoue alors.

Configurer la découverte de service

Une découverte de service doit être configurée afin qu'Apple puisse orienter les appareils vers le bon serveur MDM. Deux méthodes sont disponibles.

Automatiquement via Apple School/Business Manager

À partir de macOS 15.2, aucun fichier propre n'est nécessaire si Apple School/Business Manager est connecté à Relution pour l'Inscription automatisée des appareils (ADE, DEP dans le portail) via un compte DEP. Relution enregistre automatiquement l'URL de découverte de service dans Apple School/Business Manager lors de chaque synchronisation des appareils ADE. Il faut pour cela que Relution y soit défini comme serveur MDM par défaut pour Mac sous `Preferences` → `Your MDM Servers` → `MDM Server Assignment` → `Default MDM Server Assignment`.

Via un fichier well-known

Pour les Mac équipés d'une version de macOS antérieure à 15.2, ou sans Apple School/Business Manager connecté, un fichier de ressource HTTP `well-known` doit être déposé sur le domaine avec lequel les utilisateurs se connectent. Relution répond déjà lui-même à cette requête pour son propre nom d'hôte ; un fichier propre n'est donc nécessaire que si le domaine des comptes Apple gérés en diffère. Apple doit pouvoir récupérer ce fichier via une requête HTTP GET à l'URL suivante :

Pour la version 26.4.0

```
https://votredomaine.com/.well-known/com.apple.remotemanagement
```

À l'emplacement `votredomaine.com`, indiquer le domaine également utilisé pour les comptes Apple gérés. Le fichier doit être déposé sur un domaine capable de traiter des requêtes HTTP GET.

Le fichier est créé au format JSON avec le type de contenu `application/json`. Pour renseigner les bonnes informations dans le fichier, les informations nécessaires peuvent être copiées directement depuis le portail Relution :

1. Ouvrir `Paramètres` → `Gestion des appareils`.
2. Dans la section Inscription des utilisateurs Apple en fonction du compte, copier l'intégralité du texte JSON affiché sous Réponse, accolades extérieures comprises (bouton Copier dans le presse-papiers), et l'insérer dans le fichier. Le texte JSON est affiché indépendamment du curseur.

Pour que le fichier fonctionne correctement, il ne doit avoir aucune extension de fichier.

Exemple : maxmustermann@musterhausen.de

Dans cet exemple, le domaine serait `musterhausen.de`. C'est à cet endroit que la découverte de service doit être déposée.

Créer une inscription utilisateur dans Relution

Une inscription utilisateur est créée sous `Appareils` → `Inscriptions` via Ajouter. macOS est sélectionné comme Plateforme et le bouton Inscription des utilisateurs comme Type. Le type ne peut être sélectionné qu'avec l'autorisation de lire les utilisateurs.

Une inscription utilisateur est toujours affectée à exactement un utilisateur ; une inscription distincte est créée pour chaque utilisateur. Un Identifiant Apple géré ou une Adresse e-mail doit être enregistré dans les détails de l'utilisateur. Si aucun Identifiant Apple géré n'est enregistré, l'adresse e-mail est utilisée comme compte Apple géré. Les utilisateurs assignés aux appareils ne peuvent plus être modifiés ou supprimés des appareils inscrits via l'inscription des utilisateurs.

Une inscription utilisateur créée de cette manière est utilisée pour l'inscription utilisateur basée sur le compte lorsque l'utilisateur se connecte sur le Mac. Sur les Mac jusqu'à macOS 14, elle peut également servir à l'inscription utilisateur basée sur un profil.

Pour la version 26.4.0

Inscription utilisateur basée sur un profil (jusqu'à macOS 14)

Le lien d'inscription de l'inscription utilisateur créée est envoyé à l'étudiant ou à l'employé concerné. Via ce lien, l'inscription est effectuée sur le Mac en utilisant le compte Apple géré de l'utilisateur, et l'appareil apparaît automatiquement dans l'inventaire des appareils de l'organisation Relution correspondante.

Inscription manuelle

L'inscription s'effectue en téléchargeant et en installant manuellement un profil MDM sur le Mac. Pour ce faire, il faut soit scanner un code QR, soit ouvrir manuellement l'URL correspondante dans le navigateur. Le profil MDM est ensuite installé dans les Réglages Système.

Avantages

- L'inscription peut être effectuée sans avoir à réinitialiser les appareils aux paramètres d'usine.

Inconvénients

- L'inscription peut être supprimée à tout moment dans les paramètres des appareils (profil MDM), sauf si Utiliser le mot de passe de suppression de profil est activé dans l'inscription.
- Ne convient que partiellement aux appareils BYOD, car les administrateurs peuvent voir quelles applications sont installées. L'inscription des utilisateurs → est prévue pour les appareils privés.
- Toutes les actions et configurations de politiques ne sont pas possibles.
- Les appareils ne sont souvent pas supervisés (mode supervisé).

Pour la version 26.4.0

Créer l'inscription dans Relution

Un certificat APNs enregistré dans Relution est nécessaire (Certificats de poussée APNS →). Sans ce certificat, les plateformes Apple ne peuvent pas être sélectionnées lors de la création d'une inscription.

Pour effectuer une inscription manuelle, il faut d'abord la créer dans Relution. Pour ce faire, ouvrir `Appareils` → `Inscriptions` dans le menu, puis cliquer sur Ajouter.

Les inscriptions dépendent du système d'exploitation. Par conséquent, macOS est sélectionné comme Plateforme et l'inscription d'appareil comme Type (bouton macOS, et non Inscription des utilisateurs). La Propriété est choisie en conséquence.

Si un `Utilisateur` doit être associé à l'appareil à inscrire, il est sélectionné sous Utilisateur. En option, un Nom de l'appareil et une Description de l'appareil peuvent être définis pour

l'affichage dans l'inventaire des appareils ; sans nom d'appareil, Relution génère le nom automatiquement.

La section Configuration propose les options suivantes pour macOS :

- Utiliser le mot de passe de suppression de profil : le profil MDM ne peut alors être supprimé du Mac qu'avec un mot de passe généré automatiquement. Le mot de passe peut être consulté dans les détails de l'appareil, dans la section Sécurité, sous Mot de passe pour la suppression du profil (voir aussi Optimisations de sécurité pour les inscriptions →).
- Groupes d'appareils statiques : l'appareil est ajouté directement à ces groupes ; les politiques attribuées à ces groupes sont appliquées après l'inscription.
- Accords : sélection d'accords créés sous `Paramètres` → `Général` → `Accords`. Relution met leurs textes à la disposition de l'appareil pendant l'inscription.

Chaque inscription ne peut être utilisée qu'une seule fois, à moins que le commutateur Inscription à usages multiples ne soit activé. Dans ce cas, de nouveaux appareils peuvent être inscrits via le lien d'inscription jusqu'à ce que la date de validité soit dépassée ou qu'il n'y ait plus de licences d'appareils disponibles dans Relution. La date de validité est définie sous Valable jusqu'au ; par défaut, elle est fixée à sept jours après la création. Inscription à usages multiples ne peut plus être modifié après l'enregistrement.

Si les notifications d'inscription par e-mail ou SMS sont activées dans les paramètres de l'organisation, le lien d'inscription peut être envoyé directement à l'utilisateur affecté dans la section Notification.

Pour la version 26.4.0

Une fois l'inscription enregistrée et créée, l'URL affichée peut être ouverte dans le navigateur du Mac ou le code QR créé peut être scanné. Le profil MDM est téléchargé via le bouton Inscription, puis installé dans les Réglages Système (voir les étapes ci-dessous).

Instructions pas à pas

1. Démarrer l'inscription en appuyant sur le bouton Inscription
2. Appuyer ensuite sur le bouton Autoriser
3. Fermer la fenêtre suivante via Fermer
4. Passer à l'option Réglages Système
5. Là, dans la section Profils
6. Sélectionner le profil MDM chargé
7. Vérifier le profil MDM et appuyer sur Installer, puis confirmer le dialogue à nouveau en appuyant sur Installer
8. Un message de sécurité s'affiche. Appuyer à nouveau sur Installer
9. Faire confiance à l'administration à distance

10. Appuyer sur Terminé pour confirmer que le profil MDM est installé

L’inscription est terminée.
Une nouvelle entrée devrait maintenant apparaître dans l’inventaire des appareils du portail Relution. Si des licences Apps et livres (VPP dans le portail) sont disponibles pour l’agent Relution, celui-ci est ensuite installé automatiquement sur l’appareil.

> L’utilisateur géré ne doit être supprimé que lorsqu’un autre utilisateur (idéalement avec des droits d’administrateur) existe déjà sur l’appareil. Dans le cas contraire, l’accès au Mac peut être perdu et une réinitialisation du Mac peut s’avérer nécessaire.

Pour la version 26.4.0

Actions disponibles

Relution propose une sélection d'actions permettant de contrôler et de diriger directement les Mac. Les actions peuvent être appliquées de manière ciblée à un seul appareil ou, via la sélection multiple dans la liste des appareils, à plusieurs appareils à la fois. Elles peuvent en outre être déclenchées par événement ou de manière planifiée via l'appartenance à des groupes d'appareils : Actions de groupes d'appareils →

La boîte de dialogue des actions s'ouvre sous `Appareils` → `Inventaire` via Appliquer l'action, soit pour les appareils sélectionnés dans la liste, soit dans la vue détaillée d'un appareil. Seules les actions prises en charge par tous les appareils sélectionnés sont proposées.

Actions pour macOS

on 26.4.0

Action	Description
Démarrer la lecture AirPlay	Permet la recopie de l'écran sans fil via AirPlay. Cas d'utilisation : présentations sur un grand écran.
Arrêter la lecture AirPlay	Arrête la transmission AirPlay. Disponible uniquement pour les appareils supervisés. Cas d'utilisation : fin de la recopie de l'écran.
Supprimer l'application	Désinstalle une application de l'appareil. Cas d'utilisation : suppression des applications qui ne sont plus nécessaires.
Déployer une application depuis l'Apple App Store	Installe des applications depuis l'App Store. Cas d'utilisation : distribution d'applications standard.
Activer le bureau à distance	Active le partage d'écran. macOS 10.14.4 ou version ultérieure. Cas d'utilisation : maintenance à distance.
Désactiver le bureau à distance	Désactive le partage d'écran. macOS 10.14.4 ou version ultérieure. Cas d'utilisation : fin de la maintenance à distance.

Action	Description
Activer ou désactiver le Bluetooth	Active ou désactive le Bluetooth sur l'appareil. macOS 10.13.4 ou version ultérieure. Cas d'utilisation : contrôle pour des raisons de sécurité.
Effacer l'appareil	Réinitialise l'appareil aux paramètres d'usine et supprime toutes les données. Un code PIN numérique à 6 chiffres doit être défini lors du déclenchement de l'action. Cas d'utilisation : préparation à la remise de l'appareil.
Arrêter l'appareil	Éteint l'appareil. Disponible uniquement pour les appareils supervisés, macOS 10.13 ou version ultérieure. Cas d'utilisation : extinction centralisée des appareils, par exemple à la fin des cours ou de la journée de travail.
Redémarrer l'appareil	Redémarre l'appareil. macOS 10.13 ou version ultérieure. Avec l'option Notifier à l'utilisateur de redémarrer l'appareil (pas de redémarrage forcé), l'utilisateur est uniquement invité à redémarrer (macOS 11 ou version ultérieure). Cas d'utilisation : résolution de problèmes logiciels.
Verrouiller complètement l'appareil	Redémarre l'appareil et le verrouille complètement pour toute utilisation ou connexion. Le code PIN à 6 chiffres défini lors du déclenchement de l'action est nécessaire pour le déverrouiller. Sur les Mac dotés d'une puce Apple et exécutant une version de macOS antérieure à 11.5, l'action désactive le Mac ; sa réactivation nécessite une connexion réseau et l'authentification d'un administrateur local disposant d'un Secure Token activé. Cas d'utilisation : protection des données sensibles.
Actualiser les informations sur l'appareil	Actualise toutes les informations disponibles sur l'appareil, répertoriées sous Détails. Cas d'utilisation : informations à jour dans Relution.
Continuer dans l'Assistant Configuration de l'appareil	Informe l'appareil que la préconfiguration est terminée et qu'il peut poursuivre dans l'assistant de configuration. Disponible uniquement pour les appareils inscrits via l'Inscription automatisée des appareils (ADE, DEP dans le portail). N'a d'effet que si l'option Attendre la configuration est activée dans le Profil du DEP. Cas d'utilisation : configuration automatisée.

Action	Description
Mot de passe de l’administrateur local	Modifie le mot de passe d’un compte administrateur local. Le compte est sélectionné parmi les utilisateurs locaux signalés par l’appareil ou indiqué par son GUID via la saisie manuelle. Disponible uniquement si un seul appareil est sélectionné. Cas d’utilisation : renforcement de la sécurité.
Mettre à jour le profil MDM	Réinstalle le profil MDM sur l’appareil. Le certificat d’identité est renouvelé et les paramètres actuels, tels que l’épinglage de certificats, sont appliqués. L’URL du serveur MDM reste inchangée ; une URL externe modifiée n’est donc pas transmise à l’appareil. Relution renouvelle automatiquement le profil MDM avant l’expiration du certificat d’identité. L’action manuelle n’est donc nécessaire que dans des cas particuliers.
Envoyer un message	Affiche un message texte sur l’appareil. Cas d’utilisation : information rapide des utilisateurs.
Déployer l’application Relution Store	Installe une application du Relution Store. Les applications de type DMG ne peuvent être installées qu’avec le compagnon macOS activé. Cas d’utilisation : distribution d’applications internes.
Exécuter un script shell	Exécute un script shell géré sur l’appareil. Nécessite que le compagnon macOS soit activé (`Paramètres` → `Applications client Relution`, section Compagnon macOS, option Activer le compagnon macOS). Le compagnon macOS n’est déployé que sur les Mac équipés de macOS 12 ou version ultérieure. Cas d’utilisation : tâches de maintenance automatisées.
Installer la mise à jour	Installe une mise à jour macOS sélectionnée dans la liste des mises à jour disponibles signalées par l’appareil. Le mode d’exécution de la mise à jour est également défini, par exemple téléchargement uniquement, téléchargement avec notification de l’utilisateur ou installation suivie d’un redémarrage forcé. Disponible uniquement pour les appareils supervisés. L’action n’est proposée que si Relution a déterminé une mise à jour disponible pour tous les appareils sélectionnés. Les mises à jour disponibles sont à nouveau déterminées à chaque actualisation des informations de l’appareil, par exemple via Actualiser les informations sur l’appareil.

Action	Description
Définir le verrouillage de récupération →	Définit, modifie ou supprime le mot de passe de verrouillage de récupération. Disponible uniquement pour les appareils supervisés, macOS 11.5 ou version ultérieure. Cas d'utilisation : empêcher le démarrage en mode de récupération ou depuis un support externe sans connaître le mot de passe.
Vérifier le verrouillage de récupération →	Contrôle si un mot de passe connu correspond au verrouillage de récupération défini sur l'appareil. Disponible uniquement pour les appareils supervisés, macOS 11.5 ou version ultérieure. Cas d'utilisation : vérifier que le mot de passe enregistré du verrouillage de récupération est toujours valide.

Si au moins un des appareils sélectionnés n'est pas supervisé, Arrêter la lecture AirPlay, Arrêter l'appareil, Installer la mise à jour ainsi que les deux actions relatives au verrouillage de récupération ne sont pas affichés dans la boîte de dialogue. Il en va de même pour Continuer dans l'Assistant Configuration de l'appareil dès qu'un appareil sélectionné n'a pas été inscrit via l'Inscription automatisée des appareils. Exécuter un script shell n'apparaît que si le compagnon macOS est activé.

Pour les Mac inscrits via l'Inscription des utilisateurs →, seules les actions suivantes sont disponibles : Démarrer la lecture AirPlay, Déployer une application depuis l'Apple App Store, Actualiser les informations sur l'appareil, Mettre à jour le profil MDM, Envoyer un message et Déployer l'application Relution Store.

Pour la version 26.4.0

Verrouillage de récupération

Le verrouillage de récupération (Recovery Lock) empêche le démarrage d'un Mac en mode de récupération ou depuis un support externe sans connaître un mot de passe. Deux actions sont disponibles dans Relution pour gérer ce verrouillage. Toutes deux nécessitent un appareil supervisé sous macOS 11.5 ou version ultérieure et sont proposées dans la boîte de dialogue des actions, soit pour un seul appareil, soit, via la sélection multiple dans la liste des appareils, pour plusieurs appareils à la fois : Actions disponibles →

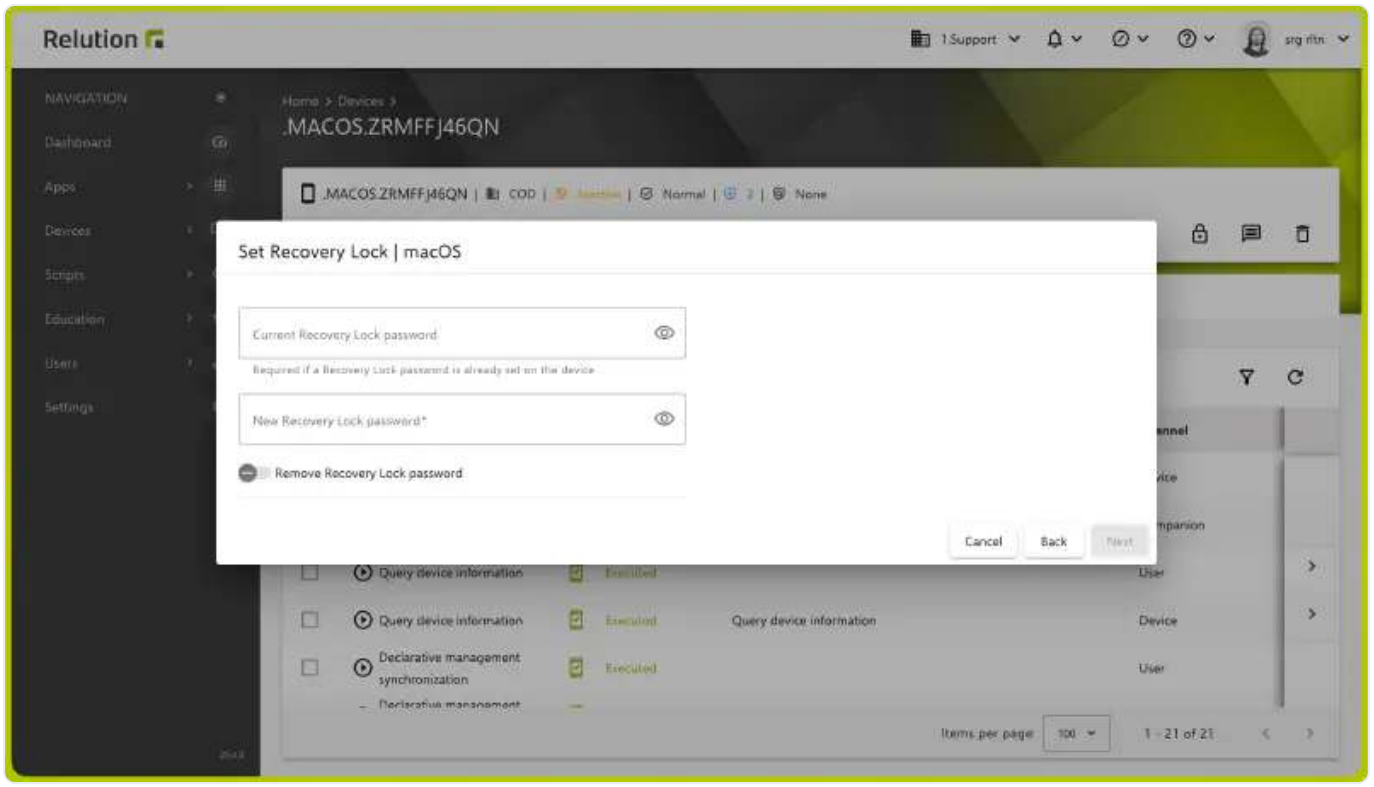
Relution ne restitue pas les mots de passe saisis dans ces actions ; ils ne peuvent plus être consultés ultérieurement dans le portail et doivent donc être conservés séparément.

Définir le verrouillage de récupération

Nouveau dans 26.4

Pour la version 26.4.0

Depuis la version 26.4, le mot de passe du verrouillage de récupération peut être défini, modifié ou supprimé directement depuis Relution via l'action Définir le verrouillage de récupération. Si un mot de passe de verrouillage de récupération est déjà défini sur l'appareil, il doit être saisi dans le champ Mot de passe actuel du verrouillage de récupération. Le nouveau mot de passe est saisi dans le champ obligatoire Nouveau mot de passe du verrouillage de récupération. Si l'interrupteur Supprimer le mot de passe du verrouillage de récupération est activé, le mot de passe existant est supprimé sans en définir un nouveau ; le champ du nouveau mot de passe est alors masqué et le champ Mot de passe actuel du verrouillage de récupération doit être renseigné.



Pour la version 26.4.0

Vérifier le verrouillage de récupération

Nouveau dans 26.5

L'action Vérifier le verrouillage de récupération contrôle si un mot de passe connu correspond au verrouillage de récupération défini sur l'appareil. Le mot de passe à contrôler est saisi dans le champ Mot de passe du verrouillage de récupération ; si aucun mot de passe n'est défini sur l'appareil, le champ reste vide. Si le mot de passe correspond, l'action reçoit le statut Exécuté. S'il ne correspond pas, elle reçoit le statut Erreur avec le message d'erreur `The Recovery Lock password does not match`.

Statut du verrouillage de récupération

La présence d'un verrouillage de récupération actif sur un appareil est consultable dans la carte Sécurité des détails de l'appareil via la valeur Le verrouillage de la récupération est-il activé.

Vue d'ensemble

Relution offre une variété d’options de configuration pour contrôler efficacement les périphériques macOS. Ces configurations peuvent être sélectionnées et personnalisées dans les politiques. Le grand avantage est que les politiques et les configurations incluses peuvent être facilement distribuées à un grand nombre d’appareils.

Configurations Disponibles

Configuration	Description
Active Directory →	Configuration de l’intégration d’Active Directory
Domaines gérés	Définition des domaines de messagerie gérés
AirPlay	Gestion de la diffusion de contenu sans fil vers des récepteurs compatibles AirPlay
AirPrint →	Gestion des paramètres des imprimantes AirPrint
Fenêtre de connexion	Gestion de la fenêtre de connexion sur l’appareil
Conformité App	Gestion des restrictions spécifiques aux applications
Restrictions de l’App Store	Gestion des restrictions de l’App Store
Mappage App vers VPN →	Configuration du VPN utilisé par les différentes applications
Configuration d’Apple Configurator 2 →	Applique aux appareils un profil de configuration (`.mobileconfig`) créé avec Apple Configurator 2
Accessibilité	Configuration des fonctions d’accessibilité de l’appareil
Accès conditionnel →	Exige la configuration de l’accès conditionnel sur l’appareil via le Relution Agent pour utiliser les ressources protégées
Notifications	Configuration des paramètres de notification des applications

Configuration	Description
Économiseur d’écran	Configuration d’un économiseur d’écran protégé par mot de passe
Contrôle parental	Configuration des paramètres du contrôle parental
Bureau →	Configuration des paramètres du bureau
Proxy DNS	Configuration du proxy DNS
Paramètres DNS cryptés	Configuration des paramètres DNS chiffrés (à partir de macOS 11)
Dock	Configuration du Dock
E-Mail	Ajout de configurations e-mail pour plusieurs utilisateurs
Paramètres de gestion des disques	Installation des paramètres de gestion des disques sur l’appareil (à partir de macOS 15, appareils supervisés uniquement)
Signature unique extensible	Configuration d’une extension d’application qui effectue l’authentification unique
Exchange	Configuration des comptes Exchange
Paramètres d’intelligence externe →	Contrôle des intégrations d’IA externes basées sur le cloud via Siri et Apple Intelligence (à partir de macOS 26.4)
FileVault →	Configuration du chiffrement du disque d’un appareil macOS
Filtre de contenu Web →	Autorisation ou blocage d’URL web spécifiques (appareils supervisés uniquement)
Paramètres du Finder	Configuration des paramètres du Finder d’un appareil macOS
Pare-feu	Configuration du pare-feu
Paramètres de l’appareil	Configuration des paramètres généraux de l’appareil (appareils supervisés uniquement)
Nom de l’appareil →	Configuration du nom de l’appareil (appareils supervisés uniquement)
Préférences globales	Configuration des préférences globales

Configuration	Description
Paramètres globaux de l’Ethernet	Gestion des paramètres globaux de connexion Ethernet
Proxy HTTP global	Configuration des paramètres de proxy globaux (appareils supervisés uniquement)
Cache de contenu	Configuration du service de mise en cache de contenu
Paramètres Intelligence →	Contrôle centralisé des fonctionnalités Apple Intelligence telles que Genmoji, Image Playground et les outils d’écriture (à partir de macOS 26.4)
Calendrier →	Gestion des comptes CalDAV
Extensions du noyau →	Gestion des extensions du noyau
Contact	Gestion des comptes CardDAV
Comptes	Configuration des paramètres des comptes
Éléments de connexion	Gestion des éléments lancés automatiquement lors de la connexion
App gérée →	Envoi de configurations aux applications gérées
Paramètres mathématiques →	Configuration centralisée des fonctions et modes de l’app Calculette d’Apple (à partir de macOS 15)
Paramètres de l’Assistant de migration →	Contrôle du comportement de l’Assistant de migration, notamment la migration gérée ainsi que les comptes et chemins exclus (à partir de macOS 26.4, appareils supervisés uniquement)
Code d’accès	Gestion de la stratégie de code d’accès des appareils Apple
Proxies	Configuration des proxies
Relution Decon →	Filtre de contenu basé sur DNS pour les sites web et les applications
Restrictions →	Gestion des restrictions d’appareils
Paramètres de Safari →	Contrôle centralisé du comportement du navigateur Safari, p. ex. historique, navigation privée et page d’accueil (à partir de macOS 26)

Configuration	Description
Extensions Safari	Gestion des paramètres des extensions Safari (à partir de macOS 15, appareils supervisés uniquement)
SCEP	Gestion des paramètres SCEP
Police	Ajout de polices sur l'appareil
Script	Gestion de l'exécution planifiée de scripts via le compagnon macOS (sélectionnable uniquement si le compagnon macOS est activé)
Assistant d'installation →	Masquer les étapes de configuration affichées après la configuration initiale
Préférences de sécurité	Configuration des préférences de sécurité
Paramètres de Siri →	Contrôle centralisé du comportement de Siri, notamment le filtre de grossièretés (à partir de macOS 26.4)
Paramètres de mise à jour du logiciel →	Contrôle du comportement de mise à jour des appareils, p. ex. téléchargement automatique, report et notifications (à partir de macOS 15, appareils supervisés uniquement)
Contrôle de la politique du système	Configuration des paramètres de contrôle de la politique du système
Économiseur d'énergie	Configuration des paramètres de l'économiseur d'énergie
Extensions du système	Gestion des extensions du système
Mises à jour système →	Gestion des mises à jour des appareils macOS (obsolète, remplacée par Mises à jour logicielles gérées)
Préférences système	Configuration des préférences système
Paramètres du clavier →	Contrôle centralisé des fonctions du clavier telles que la dictée et les suggestions mathématiques (à partir de macOS 26.4)
Time Machine	Gestion des paramètres Time Machine sur l'appareil
Mises à jour logicielles gérées →	Application forcée des mises à jour du système en ciblant une version précise avant une échéance (à partir de macOS 14, appareils supervisés uniquement)

Configuration	Description
VPN	Gestion des paramètres VPN
Weblink	Ajout d’un lien web aux appareils
Wi-Fi	Gestion des paramètres Wi-Fi
Certificat	Sélection d’un certificat à installer par défaut sur l’appareil

Les configurations Active Directory, Configuration d’Apple Configurator 2, Paramètres DNS cryptés, E-Mail, Signature unique extensible, Exchange, Filtre de contenu Web, Calendrier, Contact, App gérée, Extensions Safari, SCEP, Police, Script, Contrôle de la politique du système, VPN, Weblink, Wi-Fi et Certificat peuvent être ajoutées plusieurs fois à une politique ; toutes les autres une seule fois. Dès qu’une configuration autorisée une seule fois fait partie de la politique, elle n’est plus proposée dans la boîte de dialogue de sélection. Il en va de même si une Configuration d’Apple Configurator 2 contient déjà un profil de ce type.

Dans la boîte de dialogue de sélection, des badges signalent les prérequis, par exemple une version minimale de macOS, des appareils supervisés (Supervisé) ou la prise en charge de l’Inscription des utilisateurs → (Prend en charge l’inscription des utilisateurs). Sur les Mac inscrits via l’inscription des utilisateurs, seule une partie des configurations est appliquée.

La configuration Script n’apparaît dans la boîte de dialogue de sélection que si l’option Activer le compagnon macOS est activée sous `Paramètres` → `Applications client Relution` (activée par défaut).

Pour la version 26.4.0

Paramètres Intelligence

Avec la configuration Paramètres Intelligence, les fonctions d'Apple Intelligence peuvent être contrôlées de manière centralisée sur les appareils macOS gérés. Cette politique permet d'autoriser ou de bloquer des fonctions individuelles basées sur l'IA telles que le rapport Apple Intelligence, Genmoji, Image Playground et les outils d'écriture, ainsi que des fonctions Intelligence spécifiques aux applications dans Mail, Notes et Safari. Il est également possible d'imposer que la dictée soit traitée exclusivement en local sur l'appareil, sans connexion aux serveurs Apple.

La configuration est disponible pour les appareils macOS à partir de la version 26.4 et ne peut être appliquée que dans le cadre de l'inscription des appareils (Device Enrollment), pas de l'inscription utilisateur (BYOD). Une seule configuration de ce type est possible par politique. Les appareils qui ne prennent pas en charge ces paramètres ne reçoivent pas la configuration.

> Le formulaire est identique pour iOS, macOS et visionOS. Les options Autoriser Image Wand, Autoriser les résultats d'écriture manuscrite personnalisés, Autoriser le résumé Visual Intelligence et Forcer la traduction uniquement sur l'appareil s'affichent également pour macOS, mais ne sont pas prises en charge par macOS. Elles ne sont donc pas décrites ici, voir Paramètres Intelligence pour iOS →.

Pour la version 26.4.0

Genmoji, Image Playground, les outils d'écriture, le rapport Apple Intelligence et la dictée uniquement sur l'appareil peuvent également être contrôlés via la configuration Restrictions →. Les champs correspondants y sont marqués comme Obsolète et sont remplacés par cette configuration. Pour les appareils dont la version est antérieure à macOS 26.4, ils restent le seul moyen de contrôler ces fonctions. Les résumés dans Mail et Safari ainsi que le résumé de transcription dans Notes sont également proposés dans les restrictions. La connexion de services d'IA externes est gérée via la configuration Paramètres d'intelligence externe →.

Paramètres

- Autoriser le rapport Apple Intelligence
  - Si désactivé, le rapport Apple Intelligence est désactivé sur l'appareil. Activé par défaut.
- Autoriser Genmoji
  - Si désactivé, la fonction Genmoji est désactivée. Activé par défaut.
- Autoriser Image Playground
  - Si désactivé, Image Playground est désactivé. Activé par défaut.
- Autoriser les outils d'écriture

    - Si désactivé, les outils d’écriture (Writing Tools) sont désactivés. Activé par défaut.
- Forcer la dictée uniquement sur l’appareil
    - Si activé, la dictée est traitée exclusivement en local sur l’appareil, sans connexion aux serveurs Apple. Désactivé par défaut.

Mail

- Autoriser les réponses intelligentes
    - Si désactivé, les réponses intelligentes (Smart Replies) dans Mail sont désactivées. Activé par défaut.
- Autoriser le résumé
    - Si désactivé, la fonction de résumé dans Mail est désactivée. Activé par défaut.

Notes

- Autoriser la transcription
    - Si désactivé, la transcription dans Notes est désactivée. Activé par défaut.
- Autoriser le résumé de transcription
    - Si désactivé, le résumé des transcriptions dans Notes est désactivé. Activé par défaut.

Pour la version 26.4.0

Safari

- Autoriser le résumé
    - Si désactivé, la fonction de résumé dans Safari est désactivée. Activé par défaut.

Paramètres d'intelligence externe

La configuration Paramètres d’intelligence externe permet de contrôler de manière centralisée si et comment les services d’IA externes basés sur le cloud (par ex. ChatGPT) peuvent être utilisés via Siri et Apple Intelligence sur les appareils macOS. Cette politique est disponible à partir de macOS 26.4 — exclusivement pour les appareils avec inscription complète des appareils, pas en mode inscription utilisateur/BYOD — et est transmise à l’appareil via la gestion déclarative des appareils (DDM). Les appareils qui ne prennent pas en charge ces paramètres ne reçoivent pas la configuration. Une seule configuration de ce type est possible par politique. La même configuration est également disponible sous la même forme pour les appareils iOS et visionOS à partir de leur version respective 26.4.

> Remarque : cette configuration basée sur la DDM remplace les champs relatifs aux intégrations d’intelligence externe de la configuration Restrictions →. Ces champs sont marqués comme Obsolète dans le portail depuis Relution 26.3. Pour les appareils dont la version est antérieure à macOS 26.4, les intégrations d’intelligence externe ne peuvent toujours être contrôlées que via ces champs de restriction.

Pour la version 26.4.0

Intégrations d’intelligence externe

- Autoriser les intégrations d’intelligence externe
  - Si désactivé, les intégrations d’IA externes sont entièrement bloquées. Activé par défaut.
- Autoriser la connexion pour les intégrations d’intelligence externe
  - Si désactivé, la connexion (Sign-In) aux intégrations d’IA externes n’est pas possible. Activé par défaut.
- Identifiant d’espace de travail autorisé
  - Définit l’identifiant de l’espace de travail auquel l’intégration d’IA externe est limitée. Actuellement limité à un seul identifiant d’espace de travail. Les espaces en début et en fin de saisie sont supprimés. Si le champ reste vide, aucun identifiant d’espace de travail n’est imposé.

Paramètres du clavier

À partir de macOS 26.4 et de Relution 26.3, la configuration Paramètres du clavier est disponible ; elle est mise en œuvre via la gestion déclarative des appareils (DDM). Cette politique permet d'activer ou de désactiver de manière centralisée, sous macOS, la recherche de définitions, la dictée ainsi que les suggestions mathématiques du clavier. D'autres options de clavier telles que la correction automatique, le texte prédictif, la vérification orthographique, la saisie par glissement ou le remplacement de texte ne sont disponibles via cette politique que pour les appareils iOS →.

> Remarque : la configuration nécessite macOS 26.4 ou une version ultérieure et n'est disponible que pour les appareils gérés via l'inscription des appareils (Device Enrollment). Tous les paramètres sont activés par défaut ; leur désactivation restreint la fonction de clavier correspondante.

Une politique peut contenir une seule configuration Paramètres du clavier. Relution la transmet uniquement aux appareils qui signalent ce type de configuration ; les appareils équipés de versions plus anciennes de macOS ne la reçoivent pas, sans message d'erreur.

Pour la version 26.4.0

Paramètres pour le clavier

- Autoriser la recherche de définitions
  - Si désactivé, la recherche de définitions de mots (Look Up) n'est plus disponible sur le clavier.
- Autoriser la dictée
  - Si désactivé, la fonction de dictée du clavier ne peut plus être utilisée.
- Autoriser les suggestions mathématiques du clavier
  - Si désactivé, le clavier n'affiche plus de suggestions automatiques de résolution pour les expressions mathématiques.
  - La configuration Paramètres mathématiques → contient également une option pour les suggestions mathématiques du clavier, Activer les suggestions au clavier.

Paramètres de Siri

À partir de macOS 26.4 et de Relution 26.3, la configuration Paramètres de Siri est disponible ; elle est mise en œuvre via la gestion déclarative des appareils (DDM). Cette politique permet de contrôler de manière centralisée la disponibilité générale de Siri ainsi que le filtre de grossièretés. D'autres options de cette configuration — le traitement du contenu généré par l'utilisateur et l'accès à Siri en état verrouillé — ne sont disponibles que sous iOS et ne s'affichent pas dans le formulaire pour macOS. Une seule configuration de ce type est possible par politique.

> Remarque : la configuration nécessite macOS 26.4 ou une version ultérieure et n'est disponible que pour les appareils gérés via l'inscription des appareils (Device Enrollment) ; elle n'est pas disponible pour les appareils avec inscription des utilisateurs (User Enrollment/BYOD).

> Des commutateurs Siri comparables (autorisation de Siri et filtre de grossièretés) existent également dans la configuration Restrictions →. Ils y sont marqués comme Obsolète et sont remplacés par les Paramètres de Siri. Pour les appareils dont la version est antérieure à macOS 26.4, Siri ne peut toujours être contrôlé que via les restrictions.

Pour la version 26.4.0

Paramètres pour Siri

- Activer Siri
  - Active ou désactive Siri sur l'appareil. Activé par défaut.
- Forcer le filtre de grossièretés
  - Impose le filtre de grossièretés de Siri. Désactivé par défaut.

Paramètres de Safari

Avec la configuration Paramètres de Safari, le comportement du navigateur Safari peut être géré de manière centralisée sur les appareils macOS gérés. Cela comprend la suppression de l'historique, la navigation privée, le résumé de contenu ainsi que la page de démarrage affichée à l'ouverture d'un nouvel onglet. Sur les appareils iOS, des options supplémentaires sont disponibles pour les cookies, l'avertissement de fraude, JavaScript et les pop-ups ; celles-ci ne font pas partie de cette configuration sous macOS.

> Remarque : la configuration n'est disponible que pour les appareils disposant d'un profil d'inscription des appareils (pas d'inscription des utilisateurs/BYOD) et nécessite au moins macOS 26. Elle s'applique par compte utilisateur géré connecté, et non à l'ensemble de l'appareil pour tous les comptes locaux.

Une seule configuration de ce type est possible par politique.

Paramètres pour le navigateur Safari

Pour la version 26.4.0

- Permettre l'effacement de l'historique
  - Si désactivé, l'historique de navigation dans Safari ne peut pas être supprimé. Activé par défaut.
- Autoriser la navigation privée
  - Si désactivé, le mode de navigation privée n'est pas disponible dans Safari. Activé par défaut.
- Permettre de résumer le contenu
  - Si désactivé, le résumé automatique de contenu dans Safari est désactivé. Activé par défaut.
- Page de démarrage *(champ obligatoire)*
  - Détermine quelle page est affichée à l'ouverture d'un nouvel onglet dans Safari.
    - Démarrage – Safari utilise sa page de démarrage par défaut ; la page d'accueil est désactivée. *(valeur par défaut)*
    - Extension – Safari utilise comme page de démarrage l'extension Safari référencée par l'identifiant indiqué ; la page d'accueil est désactivée. Nécessite d'indiquer, dans le champ Extension du même nom, un identifiant d'extension au format `Identifiant (IdentifiantEquipe)`, par ex. `com.example.app (ABCD1234)`.

- URL de la page d’accueil – Safari utilise l’URL indiquée à la fois comme page de démarrage pour les nouveaux onglets et comme page d’accueil. Nécessite d’indiquer, dans le champ URL de la page d’accueil du même nom, une URL qui doit commencer par `https://` ou `http://`.

Des espaces réservés pour l’utilisateur et l’appareil peuvent être utilisés dans l’URL de la page d’accueil. Les espaces réservés disponibles sont affichés sous le formulaire et sont remplacés lors du transfert vers l’appareil, voir Espaces réservés avancés →.

Pour la version 26.4.0

Paramètres mathématiques

À partir de la version 26.1.0 de Relution, la configuration Paramètres mathématiques est également disponible pour les appareils macOS à partir de macOS 15+.

Cette politique permet de contrôler de manière centralisée les fonctions et modes de l'application Calculatrice Apple et de les adapter aux exigences pédagogiques ou organisationnelles. Par rapport à iOS, la calculatrice macOS propose en plus un mode Programmeur ainsi que la saisie en notation polonaise inversée (RPN), qui peuvent également être configurés ici.

> Remarque : cette politique n'est disponible que pour les appareils gérés via l'inscription des appareils (Device Enrollment), pas en inscription utilisateur (BYOD).

Configuration

Pour la version 26.4.0

Dans le portail, la configuration est divisée en deux sections, Calculatrice et Comportement du système. Lors de la création, toutes les options sont activées, à l'exception de Ajouter la racine carrée. Une politique peut contenir une seule configuration Paramètres mathématiques. Relution transmet les paramètres via la gestion déclarative des appareils (DDM) et uniquement aux appareils qui prennent en charge ce type de configuration ; les appareils plus anciens ne les reçoivent pas.

Paramètres pour l'application Calculatrice Apple

Mode de base

- Ajouter la racine carrée : ajoute une touche de racine carrée à la calculatrice de base, en remplaçant la touche +/-. Par défaut, la fonction de racine carrée n'est disponible qu'en mode scientifique. Cette option permet d'accéder à la racine carrée même lorsque le mode scientifique est restreint.

Mode notes de mathématiques

- Activé : détermine si le mode notes de mathématiques peut être utilisé dans l'application Calculatrice.

Mode Programmeur

- Activé : détermine si le mode Programmeur peut être utilisé dans l'application Calculatrice. Disponible uniquement pour macOS.

Mode scientifique

- Activé : détermine si le mode scientifique de l'application Calculatrice est disponible.

Options d'entrée globales de la calculatrice

- Activer la notation polonaise inversée (RPN) : détermine si la saisie en notation polonaise inversée peut être utilisée. Disponible uniquement pour macOS.
- Activer la conversion des unités : permet d'utiliser la conversion d'unités intégrée dans l'application.

Comportement système

- Activer les suggestions au clavier : contrôle si des solutions mathématiques sont automatiquement affichées dans les suggestions du clavier. La configuration Paramètres du clavier → contient également une option pour les suggestions mathématiques du clavier, Autoriser les suggestions mathématiques du clavier.
- Activer les notes de mathématiques pour d'autres applications : détermine si la fonction `Math Notes` peut également être utilisée dans d'autres applications (par ex. Notes).

Pour la version 26.4.0

Mises à jour logicielles

Pour les appareils macOS à partir de la version 15 en mode supervisé (Supervised), Relution propose la configuration Apple Paramètres de mise à jour du logiciel. Elle repose sur la gestion déclarative des appareils (Declarative Device Management) d'Apple et remplace les paramètres généraux hérités de la configuration Mises à jour système, qu'Apple considère désormais comme obsolète. L'application forcée des mises à jour est assurée par la configuration Mises à jour logicielles gérées (voir ci-dessous).

Afin de garantir de manière fiable les mises à jour sur l'ensemble du parc d'appareils, les configurations Paramètres de mise à jour du logiciel et Mises à jour système peuvent être configurées en parallèle et déployées sur tous les appareils macOS.

> Remarque : la configuration obsolète Mises à jour système sera abandonnée par Apple à moyen terme.

Pour la version 26.4.0

Général

Autoriser un utilisateur standard à effectuer des mises à jour du système d'exploitation

- Activer / Désactiver (par défaut : activé)

Afficher toutes les notifications de mise à jour du logiciel

- Activer / Désactiver (par défaut : activé)

Si l'option est désactivée, l'appareil n'affiche que les notifications déclenchées une heure avant l'échéance d'application ainsi que la notification du compte à rebours de redémarrage.

Inscription au programme bêta *(à partir de macOS 15.4)*

- Autorisé (par défaut) — l'utilisateur peut s'inscrire aux programmes bêta associés à son compte Apple.
- Toujours désactivé — l'appareil n'est pas autorisé à s'inscrire à un programme bêta et est retiré des programmes bêta auxquels il est déjà inscrit.

Actions de mise à jour automatique des logiciels *(uniquement en mode supervisé)*

Choix de l’utilisateur est présélectionné pour les trois paramètres.

Télécharger automatiquement les mises à jour disponibles du système d’exploitation

- Choix de l’utilisateur
- Toujours désactivé
- Toujours activé

Installer automatiquement les mises à jour disponibles du système d’exploitation

- Choix de l’utilisateur
- Toujours désactivé
- Toujours activé

Installer automatiquement les mises à jour de sécurité disponibles

- Choix de l’utilisateur
- Toujours désactivé
- Toujours activé

Pour la version 26.4.0

Report des mises à jour du système d’exploitation *(uniquement en mode supervisé)*

- Nombre de jours pour différer une mise à jour majeure du logiciel du système d’exploitation sur l’appareil (1–90)
- Nombre de jours pour différer une mise à jour mineure du logiciel du système d’exploitation sur l’appareil (1–90)
- Nombre de jours pour différer les mises à jour du système ou les mises à jour non-OS (1–90)

Rapid Security Response

- Permettre à l’utilisateur de bénéficier d’améliorations de la sécurité en arrière-plan
- Permettre à l’utilisateur de revenir sur l’amélioration de la sécurité en arrière-plan

Les deux commutateurs sont activés par défaut.

Mises à jour logicielles gérées

Nouveau dans 26.4

La configuration Mises à jour logicielles gérées impose les mises à jour du système d'exploitation en ciblant une version précise avant une échéance. Elle succède à la configuration obsolète Mises à jour système et complète la configuration Paramètres de mise à jour du logiciel décrite ci-dessus : celle-ci pilote le *comportement* de mise à jour (téléchargement automatique, report, notifications), tandis que Mises à jour logicielles gérées définit de manière contraignante *quelle* version doit être installée et *pour quand*.

macOS 14 ou une version ultérieure en mode supervisé est requis. La configuration est également disponible pour iOS à partir de 17, tvOS à partir de 18.4 et visionOS à partir de 26.

Version cible

- Version à imposer (par défaut : Dernière version mineure)
  - Dernière version majeure — l'appareil est porté à la version majeure la plus récente disponible.
  - Dernière version mineure — la mise à jour s'effectue au sein de la version majeure installée.
  - Version minimale spécifique — une version concrète est définie comme niveau minimal. Elle est sélectionnée dans le champ obligatoire Version parmi les versions du système d'exploitation publiées par Apple. Une version déjà enregistrée reste sélectionnable même si elle n'est plus proposée dans la liste.

Pour la version 26.4.0

Mise en application

- Calendrier de mise en application (par défaut : Par rapport à la date de sortie)
  - Par rapport à la date de sortie — l'échéance découle des champs Jours après la sortie (obligatoire, 0 ou plus) et Heure de la journée (préréglée sur 00:00). La même règle s'applique alors automatiquement à chaque version future.
  - Date et heure spécifiques — l'Échéance est définie comme un moment fixe.
- Délai de grâce après l'inscription — facultatif. Reporte l'échéance à ce nombre de jours après l'inscription d'un appareil, afin que les appareils récemment inscrits ne soient pas forcés de se mettre à jour immédiatement. Ce réglage s'applique aux deux calendriers et ne fait que prolonger une échéance, jamais la raccourcir. Si le champ reste vide, la fonction est désactivée.

> Si les versions disponibles du système d'exploitation ne peuvent pas être chargées dans le portail, la configuration le signale à l'ouverture. La sélection d'une version minimale spécifique n'est alors pas possible, les deux autres modes restent utilisables.

Une échéance déjà dépassée est tout de même transmise à l’appareil ; la mise à jour est alors imposée au prochain redémarrage. S’il n’existe aucune mise à jour adaptée pour un appareil, par exemple aucune version mineure plus récente, aucune mise en application n’est transmise.

Détails

- URL de la page de détails — lien facultatif que macOS affiche aux utilisateurs dans l’annonce de mise à jour.

Déclencher une mise à jour

Il existe deux façons d’effectuer des mises à jour macOS :

Configuration de la politique La configuration Mises à jour logicielles gérées impose une version cible avant une échéance (voir ci-dessus). La configuration obsolète Mises à jour système définit toujours les jours (Répète sur) et une Heure de début pour les mises à jour planifiées. La mise à jour disponible la plus récente est installée, limitée en option par Version maximale à mettre à jour. Si les deux configurations sont actives sur un appareil, Mises à jour logicielles gérées est prioritaire.

Pour la version 26.4.0

Action sur l’appareil L’action Installer la mise à jour dans l’inventaire des appareils installe une mise à jour choisie parmi celles disponibles pour l’appareil. L’action définit en outre le mode de mise à jour, p. ex. télécharger et installer les mises à jour, télécharger uniquement les mises à jour sans les installer, Télécharger les mises à jour et les installer plus tard (avec Report maximal de l’utilisateur) ou Télécharger, installer et forcer le redémarrage après.

Pour que les appareils macOS puissent effectuer une mise à jour avec succès, les points suivants s’appliquent :

- Les appareils doivent être suffisamment chargés ou branchés sur une source d’alimentation.
- Les appareils doivent être déverrouillés ; sinon, les utilisateurs doivent saisir le mot de passe de leur appareil.
- Les mises à jour peuvent prendre beaucoup de temps, selon l’infrastructure réseau et le nombre d’appareils.
- Les appareils macOS pris en charge vérifient une fois par jour la disponibilité de mises à jour, indépendamment de la configuration Mises à jour système.

- La configuration Mises à jour système remplace les restrictions existantes relatives au report des mises à jour.

Bureau

Avec la configuration Bureau pour les appareils macOS, l'arrière-plan du bureau est défini en indiquant un chemin vers un fichier image. Contrairement à la configuration comparable Fond d'écran → pour les appareils iOS, Android et Windows, aucun fichier image n'est téléchargé vers Relution ni distribué par Relution dans le cadre de cette politique.

> Le chemin indiqué dans le champ « Chemin d'accès à l'image de bureau à utiliser » fait référence à un fichier qui doit déjà exister localement sur l'appareil macOS — et non à une URL. Relution transmet ce chemin directement au profil de configuration natif « Desktop » d'Apple, qui indique uniquement au système d'exploitation où chercher une image d'arrière-plan existante, sans télécharger ni installer le fichier lui-même.

Paramètres

La configuration n'est possible qu'une fois par politique et contient un seul champ dans la section Général :

- Chemin d'accès à l'image de bureau à utiliser : chemin du fichier image sur l'appareil macOS, par ex. `/Library/Desktop Pictures/Entreprise.jpg`. Relution reprend la valeur telle quelle dans le profil de configuration. Les espaces réservés ne sont pas remplacés dans ce champ. Si le champ reste vide, un profil « Desktop » sans image définie est installé.

Mise à disposition du fichier image

Étant donné que le fichier référencé doit déjà être présent sur l'appareil avant l'application de la politique, l'image elle-même doit être distribuée séparément — par exemple via une configuration de script (uniquement pour les appareils avec inscription de l'appareil, pas avec inscription utilisateur), un package d'installation ou un autre mécanisme de distribution de fichiers qui place le fichier au chemin configuré au préalable.

Pour la version 26.4.0

FileVault

Avec la configuration FileVault pour les appareils macOS, le chiffrement intégral du disque est activé de manière centralisée sur les Mac gérés. La configuration n'est possible qu'une fois par politique et n'est disponible que pour les appareils avec inscription de l'appareil, pas pour les appareils avec inscription utilisateur (User Enrollment) →.

> L'installation de la configuration FileVault ne démarre pas immédiatement le chiffrement du disque, car FileVault dérive sa clé de chiffrement du mot de passe de connexion de l'utilisateur. Le moment où l'activation est demandée à l'utilisateur dépend des options de report de l'activation.

Moment de l'activation

Avec les paramètres par défaut :

- Diffère l'activation de FileVault jusqu'à ce que l'utilisateur désigné se déconnecte. est activé.
- Ne pas demander l'activation de FileVault lorsque l'utilisateur se déconnecte est désactivé.
- Nombre maximal de fois où les utilisateurs peuvent contourner l'activation de FileVault vaut `0`.

Pour la version 26.4.0

L'activation est alors demandée à l'utilisateur lors de la prochaine déconnexion. Elle est exigée au plus tard lors de la connexion suivante.

Une valeur supérieure à `0` (au maximum `9999`) autorise le nombre de contournements correspondant. Avec `-1`, l'activation n'est pas imposée à la connexion. Si Ne pas demander l'activation de FileVault lorsque l'utilisateur se déconnecte est activé, la demande lors de la déconnexion est supprimée. Ces deux sous-options ne sont disponibles que tant que le report est activé. Si le report est désactivé, le nom d'utilisateur et le mot de passe d'un utilisateur doivent être indiqués dans le profil.

Paramètres

La section Général propose les paramètres suivants :

- État de FileVault : activé ou désactivé (obligatoire, activé par défaut).

- Type de clé de recouvrement : clé de recouvrement institutionnelle et personnelle, uniquement institutionnelle ou uniquement personnelle. Une clé institutionnelle nécessite un Certificat.
- Chemin de la clé de recouvrement : emplacement de la clé de recouvrement et des informations sur l'ordinateur, par ex. `/Library/Keychains/recovery.plist`.
- Autoriser l'affichage de la clé de récupération personnelle après l'activation de FileVault sur l'appareil : détermine si la clé personnelle est affichée à l'utilisateur après l'activation.
- Utilisateur de FileVault Open Directory et Mot de passe : utilisateur ajouté à FileVault. L'option Activer la demande de nom d'utilisateur ou de mot de passe manquant permet de demander les informations manquantes sur l'appareil.
- Options de report de l'activation (voir ci-dessus).

Dans la section Gestion des clés de recouvrement personnelles, l'option Permettre à Relution d'accéder à la clé de recouvrement personnelle détermine si Relution enregistre la clé de recouvrement personnelle (activée par défaut). La clé peut ensuite être consultée dans les détails de l'appareil, dans la carte Sécurité, sous Clé de récupération personnelle FDE. Cela n'est possible que si l'option était déjà activée avant l'activation de FileVault ; si FileVault est déjà activé sur le Mac, l'option n'a aucun effet.

La section Options supplémentaires propose Interdire la désactivation de FileVault, Interdire l'activation de FileVault et Supprimer la clé FileVault en veille.

Pour la version 26.4.0

Déploiement via l'inscription automatisée des appareils (ADE)

La configuration FileVault peut être déployée via l'inscription automatisée des appareils (ADE, DEP dans le portail) avant ou pendant l'assistant de configuration, de sorte qu'elle est déjà présente au premier démarrage de l'appareil. La dérivation de la clé de chiffrement nécessitant un compte utilisateur et son mot de passe de connexion, le chiffrement effectif ne peut commencer qu'après la création d'un compte utilisateur et sa première connexion.

Pour que Relution enregistre la clé de recouvrement personnelle, la configuration avec l'option Permettre à Relution d'accéder à la clé de recouvrement personnelle activée doit être présente sur l'appareil avant l'activation de FileVault. Dans le profil DEP, l'étape FileVault de l'assistant de configuration peut être ignorée. Relution ne prend pas en charge l'activation forcée de FileVault dans l'assistant de configuration.

Extensions du noyau

Les KEXT (Kernel Extensions) sont des modules qui s'intègrent profondément dans le système d'exploitation macOS afin d'en étendre les fonctionnalités ou de prendre en charge du matériel et des exigences système spécifiques. Ils fonctionnent au niveau du noyau — le « système nerveux » de l'OS — et permettent ainsi d'accéder à des ressources et des fonctions inaccessibles depuis l'espace utilisateur.

Pourquoi a-t-on besoin des KEXT ?

- Prise en charge de matériel non natif, comme des cartes graphiques, cartes réseau ou périphériques de stockage externes spécifiques.
- Implémentation de systèmes de fichiers (par ex. NTFS, FUSE) non disponibles par défaut sous macOS.
- Extension des fonctionnalités réseau, par exemple pour des protocoles VPN ou des interfaces réseau virtuelles.
- Intégration de solutions et de contrôles de sécurité au niveau du noyau.
- Développement de plateformes de virtualisation et de leur interaction avec le noyau.

Avantages des KEXT

Pour la version 26.4.0

- Accès système profond : permettent d'ajouter des fonctions impossibles sans accès direct au noyau.
- Compatibilité matérielle : les périphériques et fonctionnalités non pris en charge nativement par macOS peuvent être pleinement intégrés.
- Extensibilité flexible : les développeurs peuvent créer des solutions personnalisées pour des besoins spécifiques.

Généralités

La configuration Extensions du noyau est ajoutée à une politique macOS sous `Appareils` → `Politiques` via Ajouter. Chaque politique peut contenir une seule configuration de ce type. Elle n'est disponible que pour les appareils inscrits via une inscription de l'appareil, pas pour les inscriptions utilisateur.

Les options de configuration suivantes sont disponibles dans la section Général :

- Autoriser les utilisateurs non administratifs à approuver les extensions du noyau dans les préférences de sécurité et de confidentialité : commutateur, désactivé par défaut. S'il est activé, les utilisateurs sans privilèges administrateur peuvent eux aussi approuver des extensions du noyau supplémentaires. Effectif à partir de macOS 11.
- Permettre à l'utilisateur d'approuver des extensions supplémentaires du noyau : commutateur, désactivé par défaut. S'il est activé, les utilisateurs peuvent approuver des extensions du noyau qui ne sont pas explicitement autorisées par la configuration.
- Autoriser toutes les extensions du noyau signées par ces identifiants d'équipe : champ de liste pour les identifiants d'équipe. Les extensions du noyau valablement signées avec ces identifiants d'équipe peuvent être chargées. Si la liste reste vide, aucun identifiant d'équipe n'est transmis.

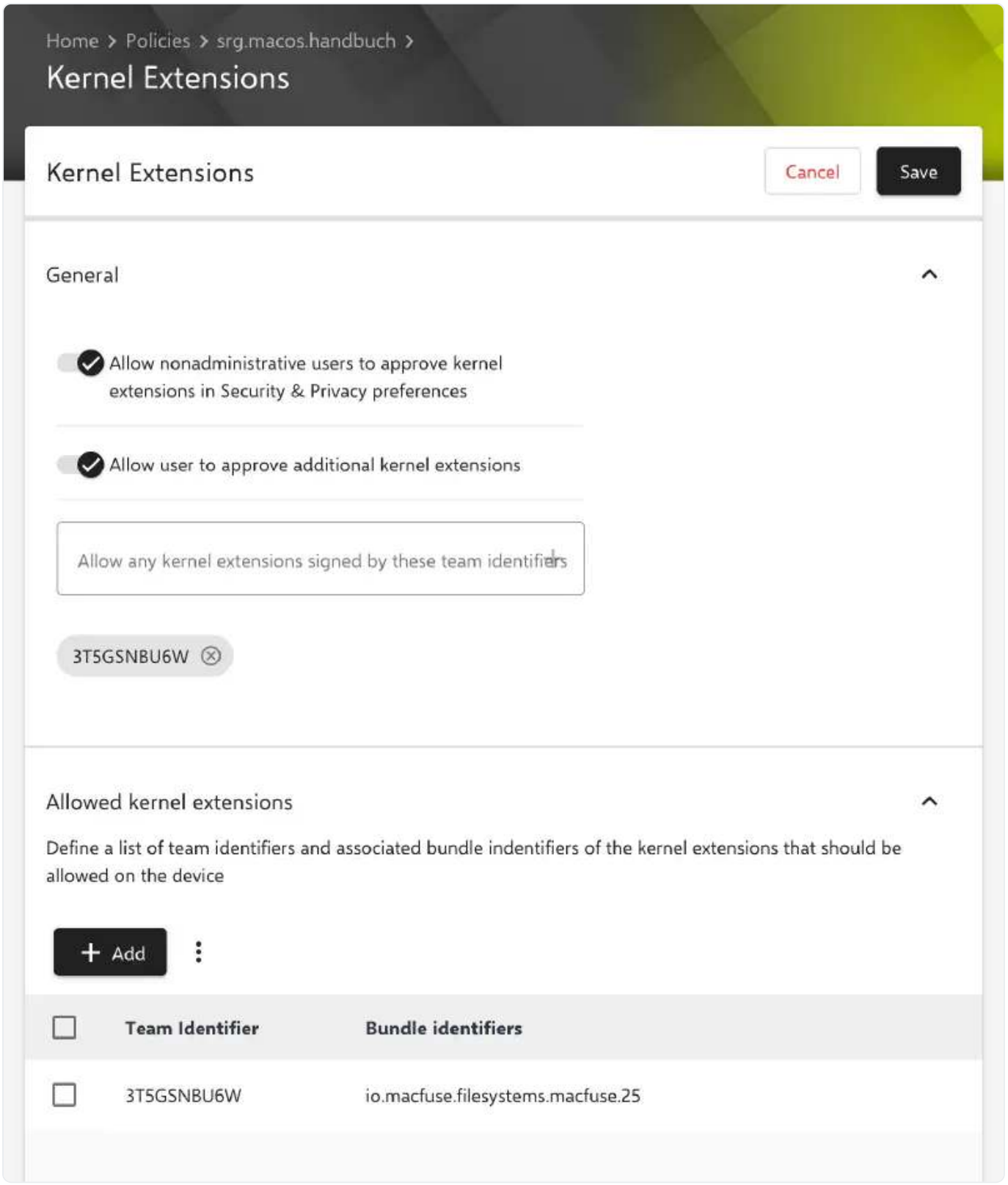
En règle générale, toutes les KEXT portant le même identifiant d'équipe peuvent être autorisées. Alternativement, la section suivante permet de définir explicitement des extensions avec un identifiant d'équipe.

Extensions autorisées du noyau

Ajouter ouvre la boîte de dialogue Ajouter un nouveau mappage de l'identifiant de l'équipe. L'Identifiant de l'équipe (obligatoire) y est saisi, et les ID de bundle associés sont indiqués sous forme de liste dans le champ des ID de bundle.

Pour la version 26.4.0

Identifiant de l'équipe	ID de bundle
3T5GSNBU6W	io.macfuse.filesystems.macfuse.25



Lecture de l’identifiant d’équipe et de l’ID de bundle

L’identifiant d’équipe peut être lu à partir du fichier macfuse-5.1.1.dmg téléchargé avec la commande suivante :

```
codesign -d --verbose=2 macfuse-5.1.1.dmg 2>&1 | grep -i teamidentifier
```

Résultat :

```
TeamIdentifier=3T5GSNBU6W
```

L'ID de bundle peut être obtenu à partir d'une KEXT installée manuellement (exemple : macFUSE) comme suit :

```
kextstat | grep -i fuse
```

Résultat :

ersion 26.4.0

```
Executing: /usr/bin/kmutil showloaded
No variant specified, falling back to release
  265    0 0                 0x1830     0x1830     io.macfuse.filesystems.mac
```

Ainsi, io.macfuse.filesystems.macfuse.25 est l'ID de bundle requis.

Remarque

Dans la section Extensions autorisées du noyau, plusieurs ID de bundle peuvent être associés à un même identifiant d'équipe — soit lors de la création d'une nouvelle entrée via Ajouter, soit lors de la modification d'une entrée existante via le menu à trois points et Éditer.

Chaque identifiant d'équipe ne peut être ajouté qu'une seule fois. Une deuxième entrée avec le même identifiant d'équipe est refusée avec le message L'identifiant de l'équipe existe déjà ; les ID de bundle supplémentaires sont donc ajoutés à l'entrée existante.

Apple KEXT →

Assistant Migration

L'Assistant Migration est un outil intégré à macOS qui facilite la configuration d'un nouveau Mac. Il transfère les données utilisateur, les applications, les paramètres et les fichiers de l'ancien appareil vers le nouveau — sans avoir à tout reconfigurer manuellement.

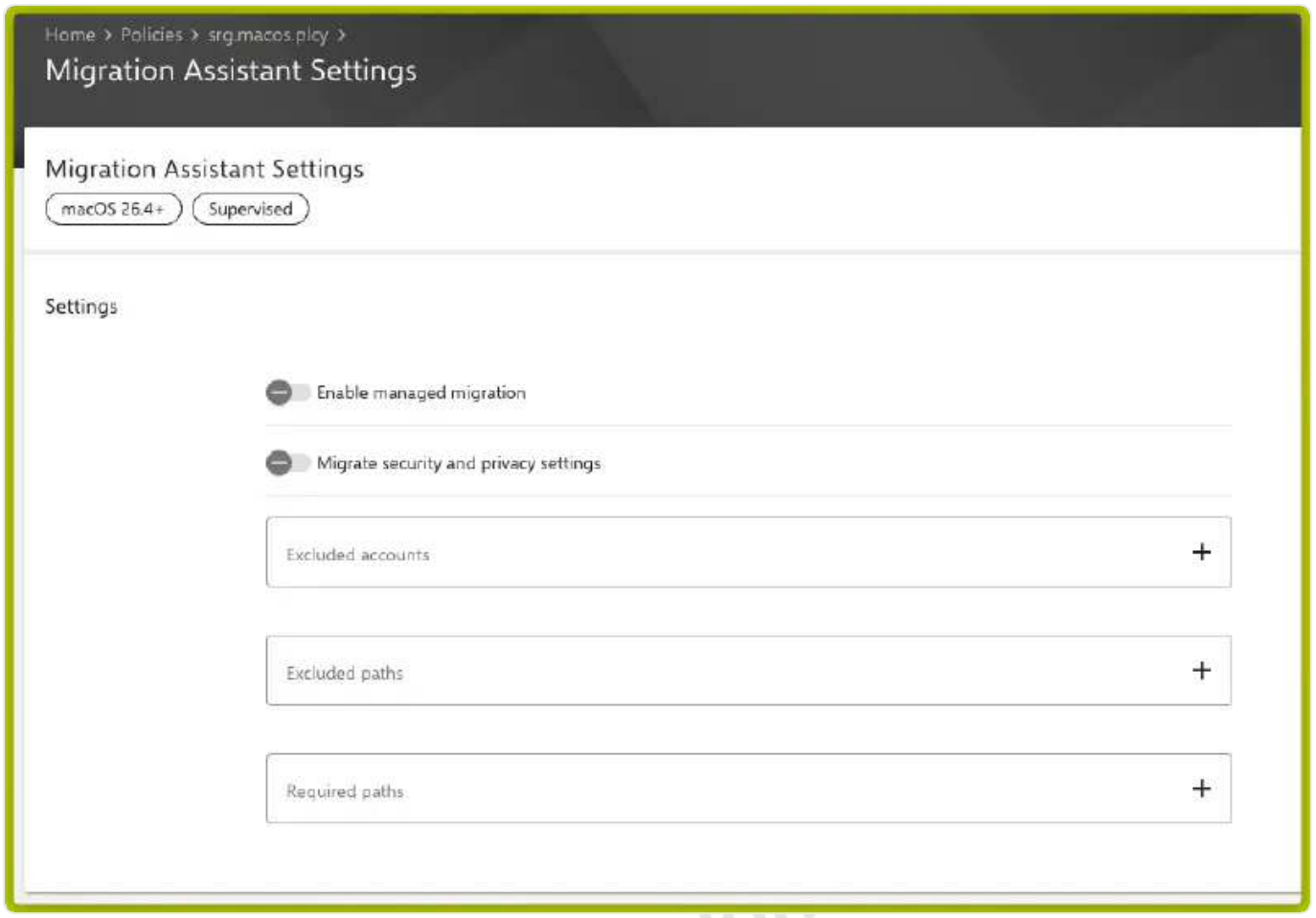
À partir de macOS 26.4, Apple prend en charge la gestion de l'Assistant Migration via la Gestion Déclarative des Appareils (DDM). Relution 26.3 implémente entièrement cette prise en charge : les paramètres peuvent être transmis aux appareils via une politique, et l'état actuel de la migration est renvoyé à Relution sous forme de rapport de statut.

> La configuration nécessite macOS 26.4 ou version ultérieure et un appareil supervisé.

Déclaration de paramètres

Nouveau dans 26.3

Pour la version 26.4.0



Activer la migration gérée

Active la migration gérée sur l'appareil. Tant que ce commutateur est désactivé, aucune restriction supplémentaire ne s'applique. Le commutateur est désactivé par défaut.

Migrer les paramètres de sécurité et de confidentialité

Détermine si les paramètres de sécurité et de confidentialité sont transférés de la source vers le nouvel appareil. Lorsque cette option est désactivée, seules les données utilisateur sont migrées ; les paramètres de sécurité à l'échelle du système conservent leur état par défaut. L'option est désactivée par défaut.

Comptes exclus

Liste des comptes utilisateur à exclure du processus de migration. Chaque entrée correspond au nom abrégé d'un compte utilisateur. Le bouton + permet d'ajouter des noms de compte individuellement.

Exemples :

Nom du compte	Cas d’usage
`administrator`	Le compte administrateur local ne doit pas être transféré
`utilisateurinvite`	Compte invité temporaire à exclure

Chemins exclus

Liste des fichiers et répertoires qui ne seront pas migrés. Le bouton + permet d’ajouter des chemins individuellement.

Les chemins sont relatifs au répertoire personnel de l’utilisateur et ne doivent pas commencer par `/` ou `~` ; les chemins de répertoire se terminent par `/`. Les entrées non valides sont refusées lors de l’ajout. Les chemins système situés en dehors du répertoire personnel ne peuvent pas être indiqués.

Exemples :

Pour la version 26.4.0

Chemin	Cas d’usage
`Library/Caches/`	Les données de cache seront reconstruites sur l’appareil cible
`Downloads/`	Les téléchargements temporaires ne sont pas transférés
`Documents/Excluded/`	Un dossier de documents précis n’est pas transféré

Chemins requis

Liste des fichiers et répertoires qui doivent obligatoirement être migrés. Si un chemin requis est absent de l’appareil source, la migration est interrompue. Le bouton + permet d’ajouter des chemins. Les mêmes règles de format que pour Chemins exclus s’appliquent.

Exemples :

Chemin	Cas d’usage
`Documents/`	Les documents de travail doivent être entièrement transférés
`Library/Keychains/`	Les trousseaux sont nécessaires au fonctionnement

Rapports de statut

Relution lit automatiquement deux rapports de statut depuis l’appareil. Après sélection de l’appareil sous `Appareils` → `Inventaire`, les valeurs apparaissent dans l’onglet Informations, dans la carte Détails de l’appareil. Les entrées ne s’affichent qu’une fois que l’appareil a transmis les valeurs correspondantes.

État de la migration

L’entrée Assistant de migration indique l’état actuel de l’Assistant Migration sur l’appareil :

Pour la version 26.4.0

État	Signification
En attente	L’Assistant Migration n’a pas encore été lancé ou aucune migration n’a eu lieu
En cours de migration	La migration est en cours
Terminé	La migration s’est terminée avec succès
Échec	La migration a échoué
Annulé	L’utilisateur a annulé la migration
Inconnu	L’appareil transmet un état que Relution ne peut pas attribuer

Rapport de migration

Contient des informations détaillées sur la migration effectuée :

- Utilisateur source : compte utilisateur sur le Mac source
- Utilisateur cible : compte utilisateur sur le nouveau Mac
- Heure de début et Heure de fin : début et fin de la migration
- Fichiers transférés : fichiers transférés par rapport au nombre total de fichiers
- Données transférées : volume de données transféré par rapport au volume total
- Erreurs : erreurs signalées pendant la migration

Configuration dans Relution

1. Sous `Appareils` → `Politiques`, créer une politique macOS via Ajouter ou ouvrir une politique macOS existante.
2. Sélectionner la configuration Paramètres de l'Assistant de migration via Ajouter.
3. Activer l'option Activer la migration gérée.
4. Configurer les comptes et chemins souhaités.
5. Enregistrer la configuration, publier la politique et l'affecter aux appareils cibles.

Chaque politique peut contenir une seule configuration Paramètres de l'Assistant de migration. Si un appareil reçoit plusieurs de ces configurations via différentes politiques, une seule d'entre elles est transmise à l'appareil.

Pour la version 26.4.0

Nom de l'appareil

Avec Relution, il est possible de définir le nom de l’appareil pour iOS, iPadOS, tvOS et macOS. Une politique avec la configuration Nom de l’appareil peut être créée et attribuée à des groupes d’appareils. La configuration n’est possible qu’une fois par politique ; le champ Nom de l’appareil est obligatoire et accepte 255 caractères au maximum.

La configuration est prévue pour les appareils supervisés (badge Supervisé) et n’est pas disponible pour les appareils avec inscription utilisateur (User Enrollment) →.

Le nom peut être défini de manière statique, par exemple `Valise iPad`, ce qui signifie que tous les appareils du groupe auront ce même nom.

Pour plusieurs appareils dans un groupe, il peut être plus judicieux d’utiliser des espaces réservés dans la configuration. Le portail affiche les espaces réservés utilisateur et appareil disponibles sous le formulaire, dans la carte Espaces réservés disponibles.

Par exemple : `Valise ${device.model} ${user.name}` Ce qui donnera un nom tel que : `Valise iPad12,1 Max.Mustermann` Cela facilite la gestion et la vue d’ensemble de l’inventaire.

D’autres fonctions telles que les sous-chaînes, les valeurs par défaut pour les champs non définis ou le remplacement des trémas sont décrites dans l’article Espaces réservés avancés →.

Si la configuration est active sur un appareil, Relution reprend dans l’inventaire le nom signalé par l’appareil à chaque interrogation de l’appareil. Sans cette configuration, le nom signalé n’est repris que tant qu’aucun nom n’est encore défini dans l’inventaire.

Pour la version 26.4.0

Active Directory

Avec Relution, il est possible de configurer les appareils macOS de manière à ce que la connexion avec des comptes d'un domaine Windows soit possible. Pour ce faire, le contrôleur de domaine doit être accessible.

Prérequis

Les conditions habituelles pour le contrôleur de domaine s'appliquent. Les instructions suivantes sont basées sur des tests et des expériences avec Windows Server 2019 Standard Edition.

- Contrôleur de domaine
- Autorisations administratives dans le domaine.
- Le périphérique macOS doit être en mesure de résoudre le FQDN du contrôleur de domaine. (L'entrée dans le fichier hosts n'est pas suffisante).
- L'appareil macOS doit pouvoir atteindre le contrôleur de domaine.
- Compte d'ordinateur dans le domaine

Pour la version 26.4.0

Configuration de la politique Active Directory

La configuration présentée ici n'est qu'un exemple et a été testée avec macOS 13 et plus.

1. Ajouter la configuration Active Directory dans une politique pour macOS.
2. Configurer au moins les paramètres suivants :

Option	Valeur
Nom (facultatif)	Nom de la configuration ; à défaut, la valeur de Domaine Active Directory à rejoindre est reprise
Domaine Active Directory à rejoindre	Nom du domaine (par ex. relution.loc)
Nom d'utilisateur du compte pour le domaine	Nom d'utilisateur d'un administrateur de domaine

Option	Valeur
Mot de passe du compte pour le domaine	Mot de passe de l'administrateur du domaine
Créer un compte mobile lors de la connexion	ON
Groupes Active Directory avec accès administrateur (facultatif)	DOMAINE\Nom-du-groupe

Le seul champ obligatoire est Domaine Active Directory à rejoindre ; la valeur doit être un nom d'hôte valide. Le portail n'impose ni le nom d'utilisateur ni le mot de passe, mais ceux-ci sont nécessaires pour rejoindre le domaine.

3. Si la politique a été appliquée avec la configuration sur le Mac, redémarrer celui-ci dans tous les cas pour réduire les problèmes de connexion.

> Lorsque la politique est supprimée du Mac, le compte de l'ordinateur est également supprimé dans AD.

Pour la version 26.4.0

Paramètres facultatifs

Outre les paramètres ci-dessus, la configuration propose d'autres réglages qui ne sont définis qu'en cas de besoin :

- Général : Identifiant du client définit le nom de l'objet ordinateur dans le domaine. Autoriser l'authentification à partir de n'importe quel domaine de l'espace de noms autorise les connexions depuis tous les domaines de la forêt.
- Comptes : Unité d'organisation à laquelle ajouter l'objet informatique de rattachement définit l'unité d'organisation (OU) du compte d'ordinateur. Pour le compte mobile, les options Avertissement avant la création du compte mobile, Forcer un répertoire local, Protocole de réseau domestique (AFP ou SMB), Utiliser le chemin UNC d'Active Directory pour dériver l'emplacement d'origine du réseau, Shell par défaut de l'utilisateur et Convention de dénomination du compte d'utilisateur principal (Domain ou Forest) sont disponibles.
- Options avancées : Serveur de domaine préféré, Interfaces autorisées pour les mises à jour dynamiques du DNS, Politique de signature des paquets, Politique de cryptage des paquets, l'association de l'UID, du GID et du GID de groupe à des attributs AD ainsi que le Nombre de

jours avant d'exiger un changement du mot de passe du compte fiduciaire de l'ordinateur (0 à 3650 ; `0` désactive le changement et correspond à la valeur par défaut).

Configuration supplémentaire

Pour activer la connexion sur un Mac, la configuration Fenêtre de connexion doit également être ajoutée. Les paramètres suivants doivent y être activés :

- Afficher les champs nom et mot de passe au lieu de la liste des utilisateurs
- Afficher les utilisateurs du réseau
- Afficher "Autres…" dans la liste des utilisateurs

La configuration Fenêtre de connexion n'est disponible que pour les appareils avec inscription de l'appareil, pas pour les appareils avec inscription utilisateur (User Enrollment) →.

Erreurs possibles

1. `(1) La charge utile "Directory Binding Account" n'a pas pu être installée. Les tentatives de liaison au serveur 'rltn.mway' ont renvoyé un problème non spécifié. (-319)`
    - Vérifier si un compte d'ordinateur portant le nom du périphérique existe sur le DC.
2. `(1) La charge utile 'Account for mounting in directories' n'a pas pu être installée. Le serveur 'rltn.mway' n'a pas été trouvé ou ne répond pas.`
    - Vérifier si le contrôleur de domaine est accessible depuis le Mac. Le FQDN doit pouvoir être résolu.

Pour la version 26.4.0

Mappage App vers VPN

Lors de la mise en place d'un VPN inter-appareils, toutes les données des appareils sont acheminées via le réseau privé. Il peut arriver qu'une entreprise souhaite configurer un VPN uniquement pour ses applications d'entreprise. Apple permet de configurer des connexions VPN pour les iPhones, les iPads et les Mac, application par application. Dans ce cas, les administrateurs peuvent contrôler exactement les données qui transitent par le VPN. La configuration d'une politique de mappage entre applications et VPN aide les entreprises à séparer le trafic au niveau des applications, ce qui permet de séparer les données personnelles de celles de l'entreprise.

Prérequis

Un mappage entre applications et VPN peut être mis en place directement par Relution. Cela ne fonctionne que pour les applications qui sont installées et gérées par le MDM sur les appareils.

Relution prend en charge les types de connexion suivants pour établir une connexion VPN par application sur les appareils iOS et macOS :

- IPSec
- JuniperSSL
- SonicWALL
- AnyConnect Legacy
- AnyConnect
- IKEv2
- SSL personnalisé

Pour la version 26.4.0

Pour les autres types de VPN, la configuration VPN indique les types pris en charge ; pour le type IKEv2 Always On (IKEv2 toujours activé dans le portail), l'option n'est pas disponible.

Configurer le mappage entre applications et VPN pour les appareils iOS et macOS

1. Un VPN par application nécessite deux configurations dans la même politique :
    - VPN
    - Mappage App vers VPN

2. Dans la configuration du VPN, l'option VPN par application et par compte doit être activée et selon le type de VPN, tous les champs nécessaires doivent être remplis.

3. Dans la configuration Mappage App vers VPN, les applications sont associées à une configuration VPN de la même politique. La configuration n'est possible qu'une fois par politique. Via Ajouter, la configuration VPN (Configuration) est d'abord sélectionnée, puis la source de l'application : Appli Relution App Store, Apple App Store App, Système iOS ou application intégrée, Conformité App ou Ajouter une application manuellement.

4. Une fois l'option VPN par application et par compte activée, la configuration VPN affiche la section VPN par compte. L'option Connectez-vous automatiquement au VPN si une application associée demande une connexion réseau permet d'établir automatiquement la connexion en cas de besoin. Des Domaines associés, Domaines exclus, Domaines Safari et Domaines SMB peuvent également y être définis. Sous Sélectionnez les configurations, des configurations de compte de la même politique peuvent être liées au VPN ; sur macOS, il s'agit des configurations e-mail, CalDAV et CardDAV.

La liste des mappages indique dans les colonnes Activé et VPN par application activé si la configuration VPN associée est active et si l'option VPN par application et par compte y est activée. Le mappage ne prend effet que si les deux conditions sont remplies.

Particularités de macOS

Pour la version 26.4.0

Dans les politiques macOS, chaque application associée dispose en plus des champs obligatoires Identifiant de signature et Exigence désignée. Lors de l'ajout d'une application, Relution renseigne d'abord ces deux champs avec l'identifiant de bundle de l'application ; les valeurs peuvent être modifiées via Éditer. L'identifiant de signature est affiché par `codesign -dv /Applications/Safari.app` à la ligne `Identifier`, l'exigence désignée (Designated Requirement) par `codesign -d --requirements - /Applications/Safari.app`.

Calendrier (CalDAV)

La configuration Calendrier transmet également un compte CalDAV à l'application Calendrier native sur les appareils macOS, via un profil de configuration. Les champs de configuration ainsi que le prérequis côté serveur — la détection automatique selon la RFC 6764 via une redirection sous `/.well-known/caldav` — sont identiques à ceux d'iOS.

Configuration et prérequis côté serveur

La description complète des champs de configuration, de la détection automatique via `/.well-known` ainsi que de la mise en place de la redirection côté serveur, y compris la résolution des problèmes, est documentée dans l'article iOS et s'applique à macOS sans modification :

- Calendrier (CalDAV) pour iOS →

Il convient de noter en particulier que la redirection doit impérativement pointer vers une adresse `https://` sans port interne, et que l'URL principale (Principal URL) — si elle est définie — doit être indiquée sous forme de chemin simple.

Pour la version 26.4.0

Particularités de macOS

Sur macOS, Relution transmet la configuration via le canal utilisateur. Le compte CalDAV est donc installé dans le profil de l'utilisateur connecté et non pour l'ensemble de l'appareil. Si l'appareil ne prend pas en charge de canal utilisateur, la configuration est transmise via le canal de l'appareil.

La configuration est également disponible pour les Mac avec inscription utilisateur (User Enrollment) →.

Configuration d'Apple Configurator 2

Cette configuration de politique permet de transférer des fichiers `.mobileconfig` sur les appareils Apple. Un tel fichier peut par exemple contenir une connexion Wi-Fi accompagnée du certificat d'identité correspondant (PKCS#12, `.p12`).

Configuration

Dans le portail, la configuration s'appelle Configuration d'Apple Configurator 2. Le champ Nom permet d'attribuer un nom à la configuration. Le fichier est importé via le champ de sélection du fichier `.mobileconfig`. Son contenu apparaît ensuite à la place de la sélection de fichier dans le champ Contenu de la charge utile, où il peut être modifié. Le contenu doit être du XML valide. Les profils signés ne sont pas du XML lisible et ne peuvent donc pas être utilisés. Dans Apple Configurator 2, le fichier est par conséquent enregistré sans signature. Si le champ Contenu de la charge utile est vidé, un fichier peut à nouveau être sélectionné.

Des espaces réservés pour l'utilisateur, l'appareil et les certificats peuvent être utilisés dans le champ Contenu de la charge utile. Les espaces réservés disponibles sont affichés sous le formulaire et sont remplacés lors du transfert vers l'appareil, voir Espaces réservés avancés →.

Pour la version 26.4.0

Plusieurs configurations Apple Configurator 2 peuvent être créées par politique. Il est ainsi possible de répartir plusieurs types de configuration sur des configurations distinctes.

> Sous macOS, le portail indique que cette configuration ne doit être utilisée que si le fichier ne contient aucun des types de configuration suivants : CardDAV, CalDAV, LDAP, Exchange, e-mail et Web Clip. Relution propose des configurations distinctes pour ces types.

Exigences relatives au fichier

Le contenu est vérifié lors de l'enregistrement. Le fichier doit remplir les conditions suivantes :

- Le niveau supérieur contient les clés `PayloadType`, `PayloadVersion` (sous forme de nombre), `PayloadIdentifier`, `PayloadUUID` et `PayloadDisplayName`.
- `PayloadContent` contient exactement un type de configuration. Des charges utiles de certificat peuvent s'y ajouter.

Les fichiers illisibles, ceux auxquels il manque l'une de ces clés ou ceux qui ne contiennent aucune charge utile ou plusieurs types de configuration sont refusés lors de l'enregistrement.

> Seuls les certificats au format PKCS#12 (`com.apple.security.pkcs12`) sont transférés avec la configuration. Les certificats PKCS#1 (`com.apple.security.pkcs1`) sont acceptés lors de la vérification, mais ne sont pas transférés vers l'appareil. Les autres certificats, comme les certificats racine (`com.apple.security.root`), comptent comme un type de configuration à part entière. Associés à une autre configuration, ils provoquent une erreur lors de l'enregistrement et sont donc déposés dans une configuration distincte.
>
> La configuration proprement dite doit figurer en première position dans `PayloadContent` . Si le fichier contient plusieurs charges utiles du même type, seule la première est transférée vers l'appareil.

Si le fichier contient un type de configuration que Relution propose également sous forme de configuration propre, autorisée une seule fois par politique, cette configuration ne peut plus être ajoutée à la même politique. À l'inverse, un tel fichier est refusé lors de l'enregistrement si la politique contient déjà la configuration correspondante ou une autre configuration Apple Configurator 2 active avec le même type de charge utile.

> Types de charge utile concernés sous macOS

Pour la version 26.4.0

Exemple

Le fichier suivant transfère une connexion Wi-Fi (`com.apple.wifi.managed`). Le SSID, le mot de passe, les identifiants et les UUID sont des valeurs d'exemple à remplacer par des valeurs réelles. Chaque `PayloadUUID` doit être unique.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/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>mot-de-passe-WiFi</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>WiFi-Entreprise</string>
   </dict>
  </array>
  <key>PayloadDescription</key>
  <string>Configuration Wi-Fi pour les appareils Apple</string>
  <key>PayloadDisplayName</key>
  <string>Wi-Fi</string>
  <key>PayloadIdentifier</key>
  <string>com.example.wifi</string>
  <key>PayloadOrganization</key>
  <string>Exemple SAS</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>
```

Configuration gérée

Il est possible de préconfigurer certaines apps avec la configuration de politique App gérée. Cette configuration n'est disponible que pour les appareils iOS à partir de la version 7 et les appareils macOS à partir de la version 11+.

Configuration

La configuration contient l'ID de bundle de l'application à configurer dans le champ Identifiant du bundle et une charge utile de configuration d'application valide dans le champ Charge utile. L'ID de bundle est repris via une boîte de dialogue de sélection : parmi les applications enregistrées dans Relution, depuis l'App Store d'Apple ou par saisie manuelle. Le champ Charge utile est prérempli avec une structure plist vide. Un XML non valide est signalé comme erreur et la configuration ne peut alors pas être enregistrée. Une politique peut contenir plusieurs configurations App gérée, par exemple pour différentes applications.

Dans la charge utile, les espaces réservés affichés au bas de la page peuvent être utilisés. Par exemple, une application de client de messagerie peut être configurée en utilisant l'espace réservé `${user.email}`. De cette manière, il est possible de rendre la configuration utilisable pour différents utilisateurs. Les espaces réservés sont remplis lorsque la configuration est transmise aux appareils. Les espaces réservés inconnus ou mal orthographiés sont remplacés par une valeur vide, sans message d'erreur.

Pour la version 26.4.0

> L'application à configurer doit être installée sur les appareils pour que la configuration de l'application soit appliquée. Si Relution installe l'application – depuis l'App Store, via Apps et livres (VPP dans le portail) ou en tant qu'application d'entreprise – et qu'une politique avec une configuration App gérée pour le même ID de bundle est déjà appliquée sur l'appareil, Relution transmet la configuration avec la commande d'installation. L'ordre des configurations dans la politique n'a aucune influence sur ce point.

Fondamentalement, le fabricant de chaque application est responsable des options de configuration. Les exemples suivants fonctionnaient avec les applications concernées au moment de la rédaction du présent document. Il n'existe aucune garantie que ce sera toujours le cas.

Microsoft Outlook pour 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/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 pour un serveur Exchange sur site

```
com.microsoft.Office.Outlook
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/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>
```

SecurePIM pour Office365

```
com.virtual-solution.securepim-enterprise
```

```
<?xml version="1.0" ?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://www.apple.com
<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>
```

Configuration incomplète

Lorsqu'une configuration existante est exportée depuis un autre système MDM au format XML puis convertie en fichier `plist`, une valeur marquée comme optionnelle et laissée vide peut devenir une valeur `<string></string>` vide dans le `plist`. La clé `subscriptionWebServiceEndPointURL` est notamment concernée par ce comportement.

Dans ce cas, SecurePIM affiche en permanence le message « Configuration incomplète » au démarrage de l'application, bien que la clé fonctionnait sans valeur dans le système d'origine. Le fait de saisir une valeur non vide dans la clé concernée, ou de supprimer entièrement la clé du `plist`, résout le problème.

Pour la version 26.4.0

FileBrowser for Education

```
com.stratospherix.filebrowsereducation
```

Configuration d'un partage SMB

```
<?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>
```

Pour la version

IBM Verse client

```
com.ibm.lotus.traveler
```

> Afficher l'exemple de configuration complet

Filtre de contenu Web

La configuration Filtre de contenu Web intègre sur les appareils macOS le filtre de contenu d'une app tierce (type de filtre Plugin), par exemple une app de filtrage avec Network Extension. Le filtrage lui-même est assuré par cette app.

> Relution n'a aucun contrôle sur le contenu filtré. Les contenus filtrés sont déterminés par le fournisseur de l'app de filtrage.

Les politiques macOS ne proposent pas de choix Type de filtre : le type de filtre est fixé sur Plugin. Le filtre intégré (Intégré) avec Activer le filtre automatique, URL bloquées, URL autorisées et Signets autorisés n'est disponible que dans les politiques iOS, voir Filtre de contenu sous iOS →. Un filtre web intégré à macOS avec listes de blocage et d'autorisation est proposé par la configuration macOS Contrôle parental, dans la section Filtre de contenu web.

Prérequis

- L'appareil est supervisé (badge Supervisé) et inscrit via une inscription de l'appareil ; la configuration n'est pas disponible pour les inscriptions utilisateur.
- L'app de filtrage du fournisseur est installée sur l'appareil.

Pour la version 26.4.0

Configuration

Sous `Appareils` → `Politiques`, la configuration Filtre de contenu Web est ajoutée à une politique macOS via Ajouter. Une politique peut contenir plusieurs de ces configurations ; elles se distinguent par leur Nom défini par l'utilisateur.

Champ	Description
Nom défini par l'utilisateur	Obligatoire. Nom du filtre
ID du bundle de plugins	Obligatoire. ID de bundle de l'app qui contient le fournisseur de filtre

Champ	Description
Adresse de service	Facultatif. Adresse du service de filtrage, p. ex. nom d’hôte ou URL
Nom utilisateur	Facultatif. Nom d’utilisateur pour la connexion au service de filtrage
Mot de passe	Facultatif. Mot de passe pour la connexion au service de filtrage ; uniquement avec un Nom utilisateur
Certificat de charge utile	Facultatif. Certificat (PKCS#1 ou PKCS#12) issu de la gestion des certificats pour la connexion au service de filtrage
Type de filtre de trafic	Socket (par défaut, libellé « Douille » dans le portail) filtre le trafic réseau au niveau des sockets, WebKit le trafic des navigateurs WebKit ; une seule option est active

Appliquer la conservation de l’historique de Safari

Le commutateur Appliquer la conservation de l’historique de Safari s’applique à partir de macOS 26 et est activé par défaut. S’il est activé, l’historique de Safari ne peut pas être effacé sur l’appareil et la navigation privée est désactivée. S’il est désactivé, l’historique peut toujours être effacé.

Pour la version 26.4.0

Relution Decon (filtre)

À partir de la version 26.5, Relution permet la configuration d'un filtre de contenu basé sur DNS pour les appareils macOS. Cette fonctionnalité assure un accès Internet sécurisé et ciblé en restreignant l'accès à certains sites web et applications. Grâce à la catégorisation des contenus basée sur l'IA, Relution Decon fournit également un contrôle parental complet avec des options avancées de configuration.

Qu'est-ce que Relution Decon ?

Relution Decon est un module complémentaire basé sur l'IA pour macOS qui filtre le contenu en temps réel, créant un environnement numérique sécurisé. Grâce au contrôle de contenu basé sur DNS, Decon bloque les sites web et applications indésirables, permettant aux utilisateurs de travailler et d'apprendre dans un espace protégé et sans distraction.

Relution Decon utilise un proxy DNS pour transmettre toutes les requêtes au serveur Decon. Les sites web sont classés et soit autorisés, soit bloqués selon les règles définies par les politiques. Toutes les communications sont chiffrées SSL, garantissant la sécurité des activités des utilisateurs.

Pour la version 26.4.0

Application Decon

L'application Decon est automatiquement déployée sur les appareils macOS lors de l'installation de la politique. Elle surveille les requêtes DNS de l'appareil et garantit que seuls les contenus autorisés sont accessibles.

Fonctionnalités de l'application :

- Active un proxy DNS global, qui ne peut pas être désactivé par l'utilisateur
- Affiche le statut actuel de Relution Decon
- Fournit des informations sur les sites bloqués et les catégories de filtrage appliquées

> Recommandation : disposer d'un nombre suffisant de licences pour l'app via Apps et livres (VPP dans le portail) avant le déploiement.

Configurer Apps et livres (VPP) dans Relution →
Relution Decon sur l'Apple App Store →

Politique Decon

Dans la politique des appareils, la configuration est ajoutée via `Ajouter` → `Relution Decon`. Cette politique installe automatiquement l'application Decon sur les appareils, où elle agit comme proxy pour toutes les requêtes DNS. Contrairement à iOS, macOS nécessite en plus une Configuration gérée → ainsi que l'autorisation de l'extension système — Relution met en place les deux automatiquement.

La configuration est complétée lors de la publication de la politique.

Sur macOS, Relution Decon n'est disponible que pour les appareils inscrits via l'inscription de l'appareil. Avec l'Inscription des utilisateurs →, la configuration ne peut pas être ajoutée.

Une licence incluant Relution Decon est requise. Sans cette licence, la configuration affiche un avertissement et ne peut pas être enregistrée.

> Si les politiques appliquées à un appareil contiennent déjà une configuration **Proxy DNS**, Relution ne définit pas le proxy DNS pour Decon. L'appareil reçoit alors l'avis de conformité **Impossible de définir le proxy DNS pour Decon car le type de configuration existe déjà**.

Pour la version 26.4.0

Hiérarchie de configuration des politiques (de la plus haute à la plus basse priorité)

1. Apps autorisées
2. Apps bloquées
3. Domaines autorisés
4. Domaines bloqués
5. Catégories bloquées

Decon dans Relution Teacher

Sur les appareils macOS, Decon peut être sélectionné et géré dans les profils de classe à partir de Relution Server 26.5. Prérequis : une politique Decon est assignée aux appareils des élèves. Relution Teacher n'affiche un avertissement concernant une configuration Decon manquante que pour les appareils iOS, pas pour les appareils macOS.

En savoir plus sur Relution Teacher →

Remarque : Si Decon est activé dans le profil de classe, la configuration Decon habituellement valable est entièrement remplacée pendant la durée du cours. Les domaines autorisés ou bloqués via les Demandes de Relution Decon ne s’appliquent pas pendant ce temps.

Filtrage

Dans la section Filtrage de la politique Decon, le champ Type de filtre détermine le mode de filtrage des sites web :

- Arrêt : aucun filtrage par catégories ni par niveau d’âge.
- Catégories (par défaut) : les catégories à bloquer sont sélectionnées individuellement à l’aide de commutateurs. Ces commutateurs ne s’affichent que pour ce type de filtre. Par défaut, Contenu pour adultes, Publicité et Hameçonnage sont bloqués.
- Niveau d’âge : le filtrage s’effectue selon un niveau d’âge (0+, 6+, 12+ ou 16+, par défaut 12+).

Deux autres commutateurs sont disponibles indépendamment du type de filtre :

- Liste BPJM : filtre en plus les contenus classés comme inadmissibles par la BPjM. Les entrées sous Domaines autorisés peuvent néanmoins permettre l’accès à ces contenus.
- Recherche sécurisée : se règle indépendamment des catégories bloquées et du niveau d’âge. Le blocage de la catégorie Contenu pour adultes n’active pas la recherche sécurisée.

Pour la version 26.4.0

Si plusieurs configurations Decon sont utilisées sur un même appareil, le filtrage le plus fort prend automatiquement effet : les filtres basés sur l’âge priment sur les filtres basés sur les catégories. Les configurations sans filtrage sont ignorées.

Classification par catégorie

Relution Decon attribue automatiquement chaque site web à une catégorie. Avec le type de filtre Catégories, les administrateurs peuvent définir quelles catégories doivent être bloquées :

Catégorie	Description	Exemples
Contenu pour adultes	Sites inappropriés pour les jeunes	Pornographie, Violence, Armes, Drogues, Jeux d’argent, Divertissement adulte, Shopping adulte, Rencontres

Catégorie	Description	Exemples
Publicité	Sites publicitaires	Fournisseurs de publicité
Réseaux sociaux	Contenus de réseaux sociaux	Facebook, Instagram, TikTok, etc.
Divertissement	Sites de divertissement comme streaming ou jeux	Films, Jeux, Vidéos
Musique	Services de streaming musical	Spotify, Tidal, etc.
Actualités	Sites d’information et magazines	News, Météo
Achats	Boutiques en ligne (hors contenus adultes)	Amazon, eBay, etc.
Éducation	Sites éducatifs pour l’apprentissage	Wikipedia, Google Scholar
IA générative	Sites liés à l’intelligence artificielle	ChatGPT, Perplexity.ai, etc.
Hameçonnage	Sites potentiellement frauduleux	Escroqueries potentielles, Vol de données
Divers	Tous les autres sites	Restants

Apps et domaines autorisés et bloqués

- Apps autorisées / Apps bloquées (section Apps) : l’accès Internet de certaines applications est autorisé ou bloqué de manière ciblée ; les fonctions de base restent disponibles.
- Domaines autorisés / Domaines bloqués (section Domaines) : permet de spécifier des domaines autorisés ou bloqués indépendamment des catégories. Seul le domaine doit être indiqué, pas le chemin. Les domaines autorisés restent accessibles même si le filtre les juge inappropriés. Le nombre de domaines bloqués devrait être limité à environ 500.

Indépendamment de ces listes, l'URL du serveur Relution, le serveur Decon et les applications Relution (Relution Agent, Teacher, Files, Assets et Decon) sont toujours autorisés. En outre, Relution ajoute à chaque configuration Decon les domaines autorisés et bloqués à l'échelle de l'organisation sous `Paramètres` → `Demandes de Relution Decon`.

Configuration DNS avancée

Serveurs DNS sur l'appareil : Des serveurs DNS alternatifs peuvent être configurés si le DNS Relution Decon n'est pas disponible. Fallback : Cloudflare Families DNS (1.1.1.3).

Serveurs DNS sur le serveur Relution Decon : Un serveur DNS alternatif peut remplacer le DNS standard sur le serveur Decon. Des adresses IP (UDP) ou DNS-over-HTTPS (DoH) comme Zero ou Quad9 sont possibles.

Limitations

- Mise en cache : Les blocages et les modifications de politique peuvent prendre jusqu'à 1 minute pour être appliqués.
- Indépendance du chemin : Le DNS fonctionne au niveau du domaine, les sous-pages ne sont pas différenciées.
- Blocage d'applications : Seul l'accès Internet est bloqué ; les fonctions de base et les contenus mis en cache restent disponibles.

Pour la version 26.4.0

AirPrint

La configuration de politique AirPrint met également à disposition des imprimantes compatibles AirPrint sur les appareils macOS au moyen d’un profil de configuration. Les imprimantes définies sont ensuite disponibles dans la boîte de dialogue d’impression, sans devoir être détectées sur le réseau local via Bonjour — par exemple lorsque le Mac et l’imprimante se trouvent dans des sous-réseaux ou VLAN différents.

Configuration

La configuration est créée sous `Appareils` → `Politiques` dans une politique macOS via Ajouter une configuration → AirPrint. Les champs Nom d’hôte ou adresse IP, Port, Chemin d’accès aux ressources et Utiliser TLS, ainsi que les prérequis et la détermination du chemin d’accès aux ressources, sont identiques à iOS et décrits dans l’article iOS :

- AirPrint pour iOS →

Pour la version 26.4.0

Assistant d'installation

La configuration Assistant d’installation permet de masquer les étapes de configuration que macOS affiche sur un Mac déjà configuré, p. ex. lors de la première connexion d’un autre utilisateur ou après une mise à jour logicielle. Elle n’est pas disponible pour les appareils avec inscription utilisateur (User Enrollment/BYOD).

Différence avec le profil DEP

Les étapes de configuration sélectionnées dans le profil → de l’Inscription automatisée des appareils (ADE, DEP dans le portail) ne s’appliquent qu’à la configuration initiale du Mac. La configuration Assistant d’installation est en revanche installée sur l’appareil inscrit via une politique et agit sur les étapes de configuration que macOS affiche ensuite.

La configuration n’est donc pas une condition préalable à l’inscription. Elle n’est nécessaire que si aucune étape de configuration supplémentaire ne doit être affichée après la configuration initiale.

Pour la version 26.4.0

Paramètres

Dans la section Général, chaque étape de configuration peut être ignorée individuellement :

- Sauter l’accessibilité
- Passer l’apparence
- Skip Cloud Setup (connexion avec le compte Apple)
- Ignorer la configuration du stockage (stockage iCloud)
- Ignorer la configuration (confidentialité)
- Ignorer la configuration Siri
- Sauter la configuration True Tone
- Passer la configuration du temps d’écran
- Ignorer la configuration Touch ID
- Sauter le déverrouillage avec la montre
- Papier peint Skip (fond d’écran)

> Apple a marqué ces paramètres individuels comme obsolètes à partir de macOS 15. Pour les versions plus récentes de macOS, Apple prévoit à la place une liste des étapes de

configuration à ignorer. Relution ne propose actuellement cette liste que dans la configuration iOS.

Apple n’autorise qu’une seule configuration Assistant d’installation par appareil. Il convient donc de ne pas attribuer simultanément à un appareil plusieurs politiques contenant cette configuration.

Pour la version 26.4.0

Restrictions

La configuration de stratégie Restrictions limite ou autorise des fonctions sur les appareils macOS gérés. Elle correspond à la charge utile Apple dédiée aux restrictions ; les réglages effectivement appliqués par un appareil dépendent de la version de macOS et du fait que l'appareil soit géré en mode supervisé.

L'aperçu ci-dessous suit la structure du formulaire dans le portail. De nombreuses restrictions nécessitent une version précise de macOS ; la version minimale est indiquée dans le formulaire à côté de la restriction (par ex. macOS 14+) et figure dans l'aperçu. Les restrictions portant la mention Supervisé ne s'appliquent qu'aux appareils supervisés, celles portant la mention Prend en charge l'inscription des utilisateurs s'appliquent également aux appareils inscrits par inscription des utilisateurs. Les restrictions portant la mention Obsolète ont été déclarées obsolètes par Apple ; celles portant la mention Obsolète sur les appareils non supervisés ne sont obsolètes que sur les appareils non supervisés.

> Relution transmet chaque interrupteur à l'appareil avec sa valeur actuelle. Une fonction désactivée est en règle générale bloquée sur l'appareil ; les options qui imposent un comportement (par ex. « Forcer ⋯ ») ne prennent effet que lorsqu'elles sont activées.

Pour la version 26.4.0

Par défaut, toutes les options sont activées, à l'exception de Forcer la dictée sur l'appareil uniquement, des trois interrupteurs de report forcé de la visibilité des mises à jour, de Activer le filtre de langage grossier de Siri, de Permettre la présentation d'une alerte de capture d'écran et des quatre restrictions Classroom. Les limites d'âge sont réglées sur Tous et la liste des identifiants d'espace de travail autorisés pour l'intégration externe est vide. Sans adaptation, une nouvelle configuration ne restreint donc aucune fonction.

L'icône de téléchargement en haut du formulaire permet d'exporter les valeurs configurées, y compris les modifications non enregistrées, dans un fichier CSV.

Parmi les Restrictions recommandées pour iOS/iPadOS →, seules les remarques concernant l'effacement de tout le contenu et des réglages et le report des mises à jour du système d'exploitation s'appliquent également à macOS.

Appareil

Les restrictions relatives à l'appareil sont réparties en trois sections.

Restrictions relatives à l’appareil

Afficher toutes les restrictions

Restrictions d’authentification

Afficher toutes les restrictions

Restrictions de mise à jour

> Cette section porte dans le portail la mention Obsolète, car Apple a déclaré ces réglages obsolètes. Pour les nouvelles stratégies, la configuration Mises à jour logicielles → est prévue à la place.

Les champs de report en jours ne sont modifiables, et ne sont transmis à l’appareil, que lorsque l’interrupteur de report forcé correspondant est activé. Les valeurs autorisées vont de 1 à 90 jours.

Afficher toutes les restrictions

Pour la version 26.4.0

Apps

Les restrictions suivantes concernent des applications et services spécifiques.

Restrictions des applications

Afficher toutes les restrictions

Relution ne propose pas d’options Safari pour JavaScript, les fenêtres pop-up ou l’avertissement de fraude sous macOS. L’effacement de l’historique, la navigation privée, le résumé de contenus et la page de démarrage des nouveaux onglets peuvent en outre être contrôlés à partir de macOS 26 via la configuration Paramètres Safari →.

Paramètres

Les restrictions suivantes concernent les réglages système de l’appareil et l’application Classroom.

Restrictions des paramètres

Afficher toutes les restrictions

Restrictions Classroom

Afficher toutes les restrictions

Médias

Les restrictions suivantes concernent les contenus multimédias. Toutes les options de cette section nécessitent macOS 15 (macOS 15+).

Pour la version 26.4.0

Restrictions des médias

Afficher toutes les restrictions

Modifications

Ces restrictions déterminent quels réglages peuvent être modifiés sur l’appareil.

Restrictions en matière de modifications

Afficher toutes les restrictions

iCloud

Les restrictions suivantes concernent les services iCloud sur l'appareil.

Restrictions iCloud

> Afficher toutes les restrictions

Restrictions des fonctionnalités de l'IA

Ces restrictions contrôlent les fonctions Apple Intelligence.

> Toutes les restrictions de cette section portent dans le portail la mention Obsolète. Pour les appareils à partir de macOS 26.4, les configurations Paramètres Intelligence → (rapport Apple Intelligence, Genmoji, Image Playground, outils d'écriture) et Paramètres d'intelligence externe → (intégrations d'intelligence externe, connexion, identifiant d'espace de travail) sont disponibles à la place. Pour les appareils équipés de versions antérieures de macOS, les restrictions décrites ici continuent de s'appliquer.

Pour la version 26.4.0

Général

> Afficher toutes les restrictions

Sujets connexes

- Restrictions pour iOS et iPadOS → — Aperçu des réglages pour iOS et iPadOS.
- Mises à jour logicielles → — Successeur des restrictions de mise à jour.
- Paramètres Safari → — Options Safari supplémentaires à partir de macOS 26.
- Paramètres Intelligence → — Successeur des restrictions des fonctionnalités de l'IA à partir de macOS 26.4.
- Paramètres d'intelligence externe → — Services d'intelligence externes à partir de macOS 26.4.

Licence en volume MS Office 2024

Comment licencier Microsoft Office LTSC 2024 sur des appareils macOS à l'aide du VL Serializer dans Relution.

Pour que les applications Microsoft Office puissent être utilisées sur macOS, elles doivent être licenciées avec le paquet `Microsoft_Office_LTSC_2024_VL_Serializer.pkg`.

La difficulté ici est que le PKG modifie son nom de paquet interne pendant l'installation. Comme il ne s'agit pas d'une application classique, la procédure habituelle pour les applications natives dans Relution échoue.

Des étapes supplémentaires sont donc nécessaires pour :

- Équiper correctement les appareils avec le PKG.
- Licencier avec succès les applications Office.
- Maintenir les appareils conformes.

Pour la version 26.4.0

Préparer le VL Serializer

Le PKG requis peut être téléchargé depuis le Microsoft Admin Center →.

Configuration Relution

1. Téléverser le PKG dans l'App Store Relution.
2. Dans la section Règles de détection de l'application, créer via Ajouter une règle de type Nom du paquet (sans règle de détection, l'application ne peut pas être enregistrée) et saisir la valeur suivante dans le champ Nom du paquet, afin que Relution puisse interpréter correctement le statut d'installation :

```
com.microsoft.office.licensingV2.helper
```

Déploiement du PKG

Le PKG doit être transféré sur les appareils. Deux méthodes sont disponibles :

Installation manuelle

Le PKG est copié manuellement sur chaque appareil et exécuté localement. Cette méthode n'est toutefois pas efficace pour des déploiements de grande envergure.

Installation automatisée (recommandée)

- Déploiement via un script Relution créé sous `Scripts` → `Scripts` et exécuté par le compagnon macOS : une seule fois via l'action Exécuter un script shell ou Exécuter sur l'appareil, ou de manière planifiée via la configuration Script d'une politique macOS.
- Téléchargement du fichier vers `/Users/Shared/`.
- Installation silencieuse ultérieure via le Terminal.

Téléchargement et installation

Ce script télécharge le serializer depuis une source externe (par ex. un serveur de fichiers interne) et l'installe directement.

Pour la version 26.4.0

```
#!/bin/bash

# Configuration
URL="https://votre-partage.com/lien/vers/le/fichier"
PKG="/Users/Shared/Microsoft_Office_LTSC_2024_VL_Serializer.pkg"

echo "Le téléchargement démarre..."
if ! curl -fL "$URL" -o "$PKG"; then
    echo "Erreur : le téléchargement a échoué."
    exit 1
fi

echo "Serializer trouvé – l'installation démarre..."
/usr/sbin/installer -pkg "$PKG" -target /

if [ $? -eq 0 ]; then
    echo "Installation terminée avec succès."
```

```
    rm "$PKG" # Optionnel : supprimer l'installateur après succès
    exit 0
else
    echo "Erreur : l'installation a échoué."
    exit 1
fi
```

Installation d’un PKG déjà présent localement

Si le fichier a déjà été déposé dans le dossier partagé, utiliser ce script :

```
#!/bin/bash

PKG="/Users/Shared/Microsoft_Office_LTSC_2024_VL_Serializer.pkg"

if [ -f "$PKG" ]; then
    echo "Serializer trouvé – l'installation démarre..."

    sudo /usr/sbin/installer -pkg "$PKG" -target /

    if [ $? -eq 0 ]; then
        echo "Installation terminée avec succès."
        exit 0
    else
        echo "Erreur : l'installation a échoué."
        exit 1
    fi
else
    echo "Erreur : fichier PKG introuvable sous $PKG."
    exit 1
fi
```

Distribution via la Conformité de l’application

Une fois le PKG téléversé dans Relution et la règle de détection définie, il peut être géré via la configuration Conformité App d’une politique macOS :

1. Dans la configuration, ajouter l'application sous Apps requises et publier la politique. Si l'option Installation automatique est activée pour l'application, Relution installe lui-même le PKG téléversé sur les appareils où l'identifiant est absent ; la règle de détection empêche alors les réinstallations.
2. Relution vérifie, à l'aide de la règle de détection, si l'identifiant `com.microsoft.office.licensingV2.helper` figure dans la liste des applications installées sur l'appareil (et, si la vérification de la version est activée, sa version). Relution ne vérifie pas si Office est effectivement sous licence.
3. Les appareils sans cet identifiant sont marqués comme Non conforme, à condition que l'option Ajouter une violation de conformité lorsque des applications requises sont manquantes soit activée sous `Paramètres` → `Gestion des appareils` → `Gestion des appareils` (par défaut). Le script peut alors être à nouveau exécuté sur ces appareils.

Pour la version 26.4.0

Applications Adobe Creative Cloud

Comment déployer les applications Adobe (Creative Cloud, Acrobat) sur des appareils macOS via Relution et les maintenir à jour avec le Remote Update Manager.

Les applications Adobe ne peuvent pas être installées via Relution comme une application native classique. La raison : les paquets Adobe ne sont pas de simples installateurs silencieux — ils démarrent pendant l'installation leurs propres processus en arrière-plan (Creative Cloud Desktop / HyperDrive). Ceux-ci ne s'exécutent pas de manière fiable dans le contexte restreint de la commande MDM native — le téléversement du PKG réussit, mais l'installation se bloque ou échoue.

L'installation s'effectue donc via un script (macOS Companion). Les mises à jour sont gérées de manière centralisée via le Remote Update Manager.

Pourquoi un script est nécessaire

- Installation : `installer -pkg … -target /` s'exécute avec les pleins droits root, comme documenté par Adobe. L'utilisateur connecté n'a pas besoin de droits administrateur.
- Pas de transfert de fichier : le macOS Companion ne livre aucun fichier. Le PKG doit donc être récupéré (téléchargé) via le réseau.
- Mises à jour : dans le paquet géré, la mise à jour automatique pour les utilisateurs finaux est désactivée. Les mises à jour s'effectuent via un script de mise à jour exécuté de manière récurrente qui appelle le Remote Update Manager (RUM) — voir Mises à jour continues.

Pour la version 26.4.0

Créer le paquet dans l'Admin Console

1. Se connecter à l'Adobe Admin Console → et accéder à Packages.
2. Créer un Managed Package. Sélectionner toutes les applications à installer sur les appareils — plusieurs applications (par ex. Photoshop, Illustrator, Acrobat) sont regroupées dans un seul PKG.
3. Dans les options de gestion, activer Remote Update Manager (RUM). Le binaire RUM est ainsi livré avec le PKG sur les appareils et sera disponible pour les mises à jour ultérieures.
4. Télécharger le paquet une fois terminé. L'installateur se trouve dans le dossier du paquet sous `Build/<NomDuPaquet>_Install.pkg`.

Remarque sur la répartition : si tous les utilisateurs reçoivent le même ensemble d'applications, un paquet combiné suffit. Si différents groupes doivent recevoir des applications différentes, créer un paquet distinct par application ou par ensemble et l'attribuer au groupe d'appareils correspondant. Le script de mise à jour (voir ci-dessous) reste le même dans les deux cas.

Déployer le PKG

Comme le Companion ne livre aucun fichier, le PKG doit être hébergé à un emplacement accessible par le réseau, à partir duquel le script le télécharge — par ex. un serveur web interne ou un stockage cloud.

Important : utiliser un emplacement de stockage permanent. Le lien de téléchargement de l'Adobe Admin Console est temporaire et lié à la session ; il ne convient pas comme source fixe. Télécharger le paquet une seule fois et l'héberger soi-même. Veiller également à ce que le nom de fichier ne contienne aucun espace.

Scripts d'automatisation

Pour la version 26.4.0

Prérequis : le compagnon macOS est activé sous `Paramètres` → `Applications client Relution` via Activer le compagnon macOS. Le compagnon n'est pas déployé sur les appareils dont la version de macOS est inférieure à 12 ni sur les appareils inscrits par l'utilisateur ; cette procédure n'y est donc pas applicable.

Le déploiement se compose d'une installation initiale unique et d'une mise à jour récurrente. Les deux scripts sont créés sous `Scripts` → `Scripts` via Ajouter un script en tant que scripts shell pour macOS, puis exécutés sur l'appareil par le compagnon macOS :

- Installation initiale : le script est lancé une seule fois via l'action Exécuter un script shell sur l'appareil ou le groupe d'appareils, ou bien via Exécuter sur l'appareil dans la liste des scripts (voir Vue d'ensemble des actions →).
- Mise à jour : dans une politique macOS, la configuration Script est ajoutée et le script de mise à jour est sélectionné. Dans la section Exécution en fonction du temps, les jours de la semaine (Se répète sur) et l'Heure de début sont définis (voir Vue d'ensemble des configurations →).

En plus du fichier journal sur l'appareil, l'état d'exécution ainsi que la sortie de résultat et d'erreur de chaque exécution peuvent être consultés dans l'historique du script concerné sous `Scripts` → `Scripts`.

Installation initiale (recommandée)

Les paquets Adobe pèsent souvent plusieurs gigaoctets. Un téléchargement direct dans un script Relution peut dépasser le délai d'expiration du script et être alors interrompu. Ce délai est défini sur le script dans le champ Délai d'attente (en minutes) (5 minutes par défaut, 30 minutes au maximum). Le script suivant contourne ce problème : il installe un LaunchDaemon qui exécute le téléchargement, l'installation et la première mise à jour de manière découplée en arrière-plan. Le script Relution lui-même se termine en quelques secondes.

Pour chaque paquet, définir simplement `PKG_URL` et `APP_LABEL`.

> Afficher l'exemple de configuration complet

Le résultat est journalisé dans `/var/log/relution_adobe_deploy.log`.

Mises à jour continues

Ce script est attribué en tant que configuration Script dans une politique macOS et ainsi exécuté de manière récurrente (par ex. une fois par semaine). Il ne nécessite aucun téléchargement — le Remote Update Manager récupère les mises à jour directement auprès d'Adobe. Sans indication de produits, toutes les applications Adobe installées sont mises à jour ensemble ; un script distinct par application n'est pas nécessaire.

Pour la version 26.4.0

```
#!/bin/bash
RUM_BIN="/usr/local/bin/RemoteUpdateManager"
RUM_PRODUCTS=""   # vide = toutes les applications ; sinon codes SAP, par ex.
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 "ERREUR : RUM introuvable – une application Adobe est-elle installée ?
    exit 2
fi

log "=== Mise à jour RUM démarrée ==="
if [ -n "$RUM_PRODUCTS" ]; then
    "$RUM_BIN" --action=install --productVersions="$RUM_PRODUCTS" >>"$LOG" 2>&
else
    "$RUM_BIN" --action=install >>"$LOG" 2>&1
```

```
fi
log "RUM terminé (RC $?)."
```

Codes SAP pour la mise à jour ciblée d'applications individuelles : `APRO` (Acrobat), `PHSP` (Photoshop), `ILST` (Illustrator), `IDSN` (InDesign), `PPRO` (Premiere Pro), `AEFT` (After Effects).

Alternative : libre-service

Si les utilisateurs doivent installer leurs applications Adobe eux-mêmes, plutôt que via un déploiement centralisé, créer à la place un paquet Self-Service dans l'Admin Console (ou activer dans le paquet les options Enable self-service install et Allow non-admins to update and install apps). Le script installe alors uniquement l'application Creative Cloud Desktop ; les utilisateurs choisissent et installent ensuite eux-mêmes les applications proprement dites. Cela nécessite une licence Named User avec des profils de produits adaptés. Un script de mise à jour centralisé n'est pas nécessaire, les mises à jour passant par l'application Desktop.

> Afficher l'exemple de configuration complet

Remarque : si le paquet est très volumineux et que le téléchargement direct dépasse le délai d'expiration du script, utiliser la variante LaunchDaemon découplée de l'installation initiale — définir simplement `PKG_URL` sur le paquet de l'application Creative Cloud Desktop et omettre l'étape RUM.

Pour la version 26.4.0

Surveillance du statut via la Conformité de l'application

Dans cette configuration, l'installation s'effectue via le script — aucun PKG n'est téléversé dans Relution. La Conformité de l'application (configuration Conformité App d'une politique macOS dans le portail) ne sert donc pas à la distribution, mais à la surveillance du statut : l'application est créée via Ajouter une application manuellement, et l'identifiant de bundle est saisi dans le champ Nom interne.

1. Dans la configuration Conformité App, sélectionner la source Ajouter une application manuellement sous Apps requises via Ajouter (sans téléversement de PKG).
2. Attribuer un Nom et saisir l'identifiant de bundle dans le champ Nom interne, par ex. `com.adobe.acc.AdobeCreativeCloud`.
3. Relution vérifie régulièrement si cet identifiant de bundle figure dans la liste des applications installées sur l'appareil.
4. Les appareils sans l'application sont marqués comme Non conforme, à condition que l'option Ajouter une violation de conformité lorsque des applications requises sont

manquantes soit activée sous `Paramètres` → `Gestion des appareils` → `Gestion des appareils` (par défaut). Le script d'installation peut ensuite y être (ré)exécuté.

Détection spécifique à une application (par ex. seulement Photoshop) : Relution vérifie chaque identifiant de bundle enregistré par rapport à la liste des applications installées sur l'appareil. Pour une vérification spécifique à une application, c'est donc l'identifiant de bundle de l'application individuelle qui est enregistré à la place de `com.adobe.acc.AdobeCreativeCloud` (via Ajouter une application manuellement). L'identifiant de bundle peut être consulté dans la liste des applications installées d'un appareil sur lequel l'application est déjà installée. Cela suppose que macOS signale l'application dans cette liste.

Remarques

- Licence (Named User Licensing) : après l'installation, l'utilisateur se connecte avec son identifiant Adobe au premier lancement. Chaque application nécessite un profil de produit correspondant dans l'Admin Console — sans droit d'accès, l'application est installée mais inutilisable.
- Montées de version majeures : le Remote Update Manager ne met à jour qu'au sein de la version majeure installée (mises à jour de base et de sécurité). Le passage à une nouvelle génération annuelle nécessite un nouveau paquet.
- Environnements éducatifs : pour les clients Adobe Éducation, la mise à jour automatique pour les utilisateurs finaux n'est pas disponible ; la gestion via le Remote Update Manager est ici la voie prévue.
- Spotlight : le script d'installation initiale indexe les applications installées via `mdimport`, afin qu'elles soient immédiatement trouvables via la recherche Spotlight — et pas seulement dans le Finder.

Pour la version 26.4.0

Platform SSO (PSSO)

Relution permet de configurer les appareils macOS de manière à ce que les utilisateurs puissent se connecter directement à la fenêtre de connexion avec leur compte Microsoft Entra ID (Platform Single Sign-On). Lors de la première connexion, un compte utilisateur local est créé et associé à l'identité Entra ID.

Prérequis

- macOS 13 (Ventura) ou une version ultérieure pour Extensible SSO, macOS 15 (Sequoia) ou une version ultérieure pour les politiques de connexion, de déverrouillage et FileVault, les délais de grâce et les comptes SSO hors plate-forme, macOS 26 (Tahoe) pour l'enregistrement via l'assistant de configuration et le mode invité authentifié. Microsoft recommande au moins macOS 14 (Sonoma).
- Mac avec Apple Silicon, si la méthode recommandée *clé Secure Enclave* est utilisée (voir Choisir la méthode d'authentification →). Sur les Mac Intel, seule la méthode *Mot de passe* est possible.
- Locataire (tenant) Microsoft Entra ID
- Autorisation d'enregistrement des appareils dans Microsoft Entra ID pour les utilisateurs
- Microsoft Company Portal pour Mac doit être disponible en tant qu'application et installé *avant* que les utilisateurs ne soient adressés pour PSSO. Pour l'enregistrement pendant l'assistant de configuration (macOS 26+), la version 5.2604.0 (avril 2026) est requise. La version actuelle est toujours recommandée – elle satisfait aux deux exigences.
- Accès réseau aux URLs de connexion Microsoft/Apple (voir Section Général →). Ces URLs doivent être accessibles et exclues de toute inspection TLS, sinon l'enregistrement échoue.

Pour la version 26.4.0

Platform SSO en soi ne nécessite pas que Relution soit connecté à Microsoft Entra ID ; la configuration fonctionne sans cette connexion. Celle-ci n'est requise que si des utilisateurs doivent en plus être synchronisés depuis Entra ID ou si Conditional Access → est utilisé : Connecter Relution à Entra ID →. Conditional Access requiert en outre OIDC →.

Préparation dans Microsoft Entra ID

Avant de déployer la configuration dans Relution, les points suivants doivent être vérifiés dans le Centre d'administration Microsoft Entra :

- Paramètres des appareils : sous `Identité` → `Appareils` → `Paramètres des appareils`, Les utilisateurs peuvent joindre des appareils à Microsoft Entra ID doit être défini sur Tous (ou sur le groupe cible concerné).
- Authentification multifacteur : si la MFA classique par utilisateur est activée sur le compte, l'enregistrement PSSO peut échouer. Conditional Access est alors utilisé pour l'exigence MFA.
- Complexité du mot de passe : avec la méthode *Mot de passe*, les exigences de complexité du compte local et d'Entra ID doivent correspondre pour que la synchronisation fonctionne.

Téléverser l'application Company Portal

1. La version actuelle de Microsoft Company Portal pour Mac (.pkg) est téléchargée depuis Microsoft →, puis téléversée dans Relution en tant qu'application native : dans le menu `Apps` → `App Store`, Ajouter permet de sélectionner Appli native (voir Applications macOS natives →).
2. L'application doit être publiée pour le groupe cible ou l'organisation.

L'application Company Portal contient l'extension SSO `com.microsoft.CompanyPortalMac.ssoextension`, nécessaire pour Platform SSO. Elle doit être en version 5.2404.0 minimum (pour l'enregistrement via l'assistant de configuration sous macOS 26+ : 5.2604.0).

Pour la version 26.4.0

Remarque sur les numéros de version : Company Portal affiche deux numéros de version. La version indiquée dans À propos de cette application suit le schéma `5.AAMM.x` (par ex. `5.2604.0` = avril 2026), tandis que le numéro de build visible dans le paquet ou via `pkgutil` se présente différemment – par ex. `4.83.26040910`, où `260409` correspond à la date de build (2026-04-09). Les deux désignent la même version ; un build de 2026 satisfait sans problème à l'exigence PSSO.

Attribuer le groupe d'appareils et les politiques

1. Un groupe d'appareils est créé pour les Mac sur lesquels PSSO doit être déployé.
2. Dans la section Politiques du groupe d'appareils, une politique macOS contenant les deux configurations suivantes est attribuée via Ajouter (une politique commune ou deux politiques distinctes) :
   - Authentification unique extensible (voir Configuration de la politique Authentification unique extensible →)

- Conformité App : sous Apps requises, l’application Company Portal téléversée est ajoutée via Ajouter. Si la case de la colonne Installation automatique est cochée (par défaut lors de l’ajout), Relution installe l’application automatiquement. Sans installation automatique, l’appareil est seulement signalé comme non conforme si l’application manque.

3. Les configurations ne parviennent aux appareils qu’une fois la politique publiée.

> Sans l'application Company Portal installée, l'extension SSO ne peut pas s'enregistrer. Relution distribue le profil SSO indépendamment de l'installation de l'application ; aucun ordre entre les deux n'est imposé.

Choisir la méthode d’authentification

La méthode d’authentification détermine comment les utilisateurs se connectent à l’appareil et aux applications. C’est la décision la plus importante lors de la configuration ; elle se définit dans la Section Plate-forme SSO → de la configuration.

ersion 26.4.0

Méthode	Sans mot de passe	Mot de passe local	macOS min.	Adapté pour
Clé Secure Enclave *(recommandée)*	Oui, résistante au hameçonnage	reste inchangé	13 / 14	Appareils personnalisés, Apple Silicon uniquement
Mot de passe	Non	synchronisé avec Entra ID	13 / 14	Mac Intel, appareils partagés/labo
Carte à puce	Oui (via CBA)	reste inchangé	14+	Organisations disposant de cartes à puce physiques

Recommandation : pour les Mac professionnels personnalisés (Apple Silicon), la méthode clé Secure Enclave est recommandée – elle est sans mot de passe, liée au matériel et satisfait à la MFA résistante au hameçonnage. Pour les appareils Intel ou partagés, *Mot de passe* est à privilégier.

Important : *Carte à puce* n'est pas prise en charge pendant l'assistant de configuration.

Enregistrement dans l'assistant de configuration (macOS 26+) : si PSSO est déjà enregistré pendant l'assistant de configuration (Activer l'inscription pendant l'Assistant de configuration sur ACTIVÉ), l'option Activer la création du premier utilisateur pendant l'Assistant de configuration doit également être ACTIVÉE – quelle que soit la méthode choisie. Sinon, aucun compte local n'est créé lors de la configuration et l'enregistrement échoue (confirmé en pratique) :

- Méthode *clé Secure Enclave* : la connexion se retrouve dans une boucle de connexion.
- Méthode *Mot de passe* : le message Connexion impossible – l'enregistrement a échoué s'affiche.

Si le commutateur est activé, le premier compte local est créé via PSSO et la connexion s'effectue correctement dans les deux cas.

Configuration de la politique Authentification unique extensible

Pour la version 26.4.0

La configuration Authentification unique extensible (libellé du portail : Signature unique extensible) est ajoutée dans une politique pour macOS.

Section Général

Paramètre	Valeur
Identificateur d'extension	`com.microsoft.CompanyPortalMac.ssoextension`
Identifiants de bundle refusés	laisser vide (par défaut)
Données d'extension → `AppPrefixAllowList`	`com.microsoft.,com.apple.`
Données d'extension → `browser_sso_interaction_enabled`	`1`

Paramètre	Valeur
Données d’extension → `disable_explicit_app_prompt`	`1`
Realm	laisser vide
Jeton d’enregistrement	laisser vide (non requis pour Entra ID – voir remarque)
Comportement de l’écran verrouillé	Ne pas traiter (par défaut : Annuler)
Identifiant de l’équipe	`UBF8T346G9` (identifiant d’équipe Microsoft)
Type	Redirection (par défaut : Informations d’identification)

URL	`https://login.microsoftonline.com`
	`https://login.microsoft.com`
	`https://sts.windows.net`

Pour la version 26.4.0

Les champs obligatoires sont Identificateur d’extension, Identifiant de l’équipe et, pour le type Redirection, URL. Avec le type Informations d’identification, le champ Hôtes apparaît à la place de URL.

> Jeton d’enregistrement : pour Microsoft Entra ID, aucun jeton d’enregistrement n’est requis dans la charge utile Extensible SSO ; le champ reste vide. (Ce champ est prévu pour d’autres scénarios IdP/Kerberos.)

> URLs / TLS : les trois URLs de connexion doivent être accessibles sur le réseau et exclues de toute inspection TLS.

Section Plate-forme SSO

Paramètre	Valeur	Remarque
Nom d’affichage du compte	laisser vide	optionnel

Paramètre	Valeur	Remarque
Méthode d’authentification	Clé Secure Enclave (dans le portail : Clé d’enclave sécurisée de l’utilisateur)	Recommandée ; pour les appareils Intel/partagés : *Mot de passe* (par défaut pour les nouvelles configurations)
├── Politique de connexion	– (sans objet)	visible uniquement avec la méthode *Mot de passe* ; macOS 15+
├── Politique de déverrouillage	– (sans objet)	visible uniquement avec la méthode *Mot de passe* ; macOS 15+
├── Politique de FileVault	– (sans objet)	visible uniquement avec la méthode *Mot de passe* ; macOS 15+
├── Délai de grâce hors ligne	– (sans objet)	visible uniquement avec la méthode *Mot de passe* ; macOS 15+
└── Délai de grâce de l’authentification	– (sans objet)	visible uniquement avec la méthode *Mot de passe* ; macOS 15+
Comptes SSO hors plate-forme	non défini	macOS 15+
Fréquence de connexion	`64800` (secondes, soit 18 h)	Intervalle de ré-authentification ; par défaut `64800`, minimum `3600`
Utiliser des clés d’appareil partagées	ACTIVÉ	Requis pour la création de compte JIT, voir Clés d’appareil partagées et création de compte → ; par défaut : DÉSACTIVÉ

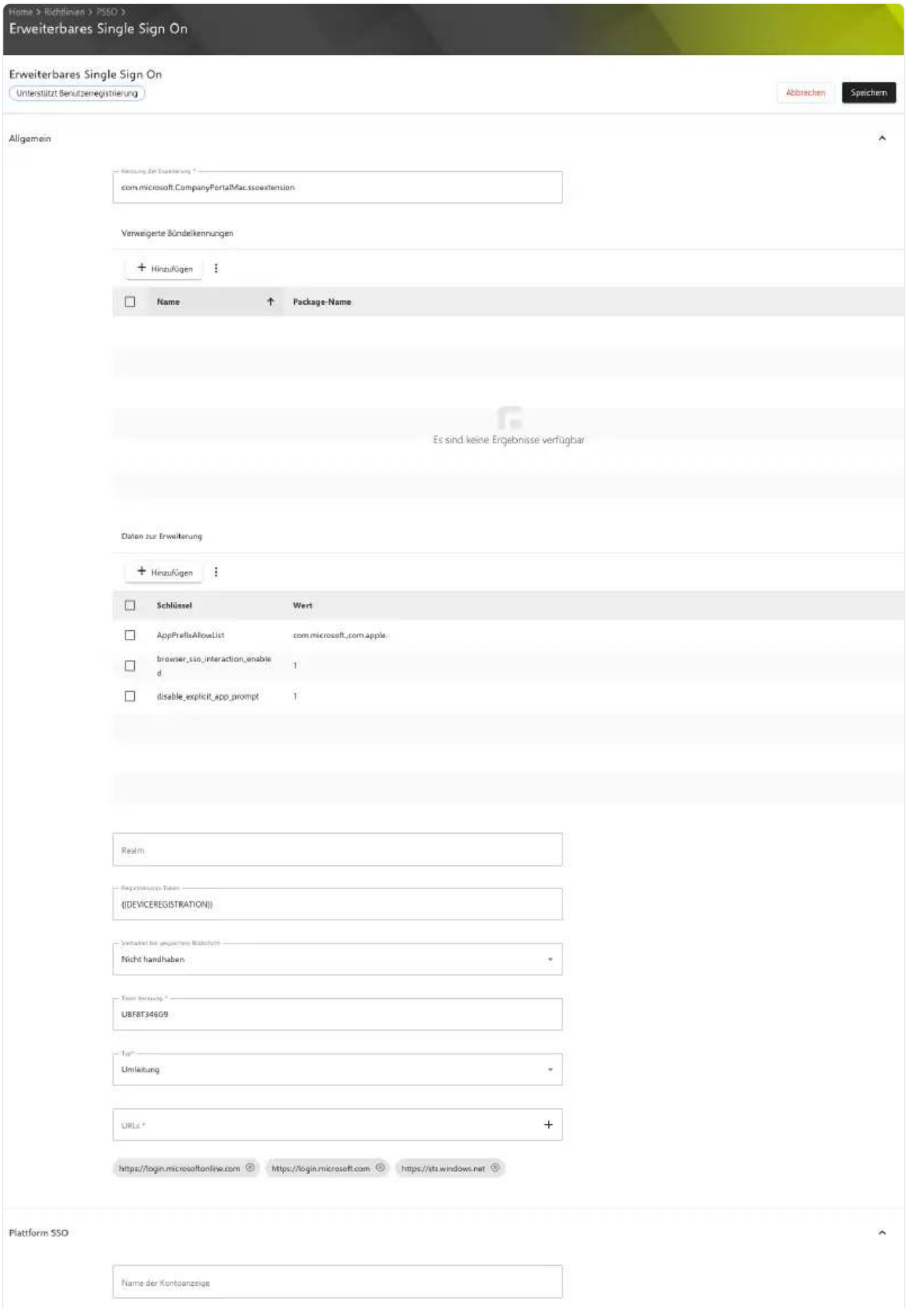
Paramètre	Valeur	Remarque
├── Activer l’autorisation	ACTIVÉ	
└── Activer la création d’un utilisateur lors de la connexion	ACTIVÉ	Provisionnement juste-à-temps (JIT) du compte local
Groupes supplémentaires	non défini	optionnel
Groupes d’administrateurs	non défini	optionnel
Groupes d’autorisation	non défini	optionnel
Mode d’autorisation pour nouvel utilisateur	Standard	
Mode d’autorisation de l’utilisateur	Standard	
Autoriser les identifiants d’appareils dans l’attestation	DÉSACTIVÉ	macOS 15.4+
Activer la création du premier utilisateur pendant l’Assistant de configuration	ACTIVÉ (par défaut)	macOS 26+ — requis en cas d’enregistrement pendant l’assistant de configuration (sinon l’enregistrement échoue)
Méthodes d’authentification	non défini	macOS 26+ ; choix parmi Mot de passe, Carte à puce et Access

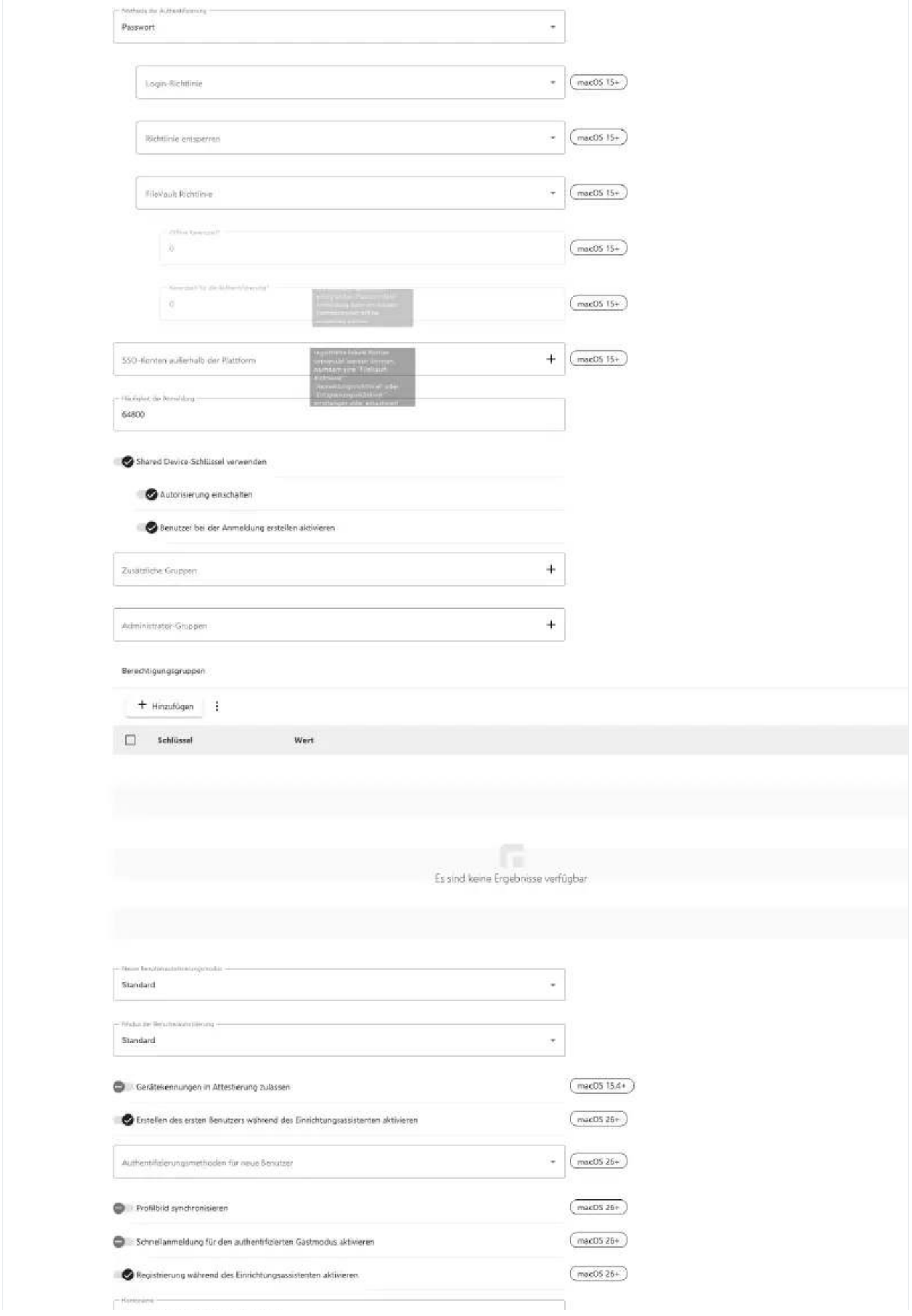
Paramètre	Valeur	Remarque
des nouveaux utilisateurs		Key. Avec Access Key, des champs supplémentaires apparaissent pour l’identifiant de groupe du lecteur, l’identité du terminal, le certificat de l’émetteur et le mode express
Synchroniser la photo de profil	DÉSACTIVÉ	macOS 26+
Activer la connexion rapide pour le mode invité authentifié	DÉSACTIVÉ	macOS 26+
Activer l’inscription pendant l’Assistant de configuration	ACTIVÉ	macOS 26+
Nom du compte	`com.apple.PlatformSSO.AccountShortName`	Espace réservé pour le nom court local
Nom complet	`name`	Espace réservé pour le nom complet

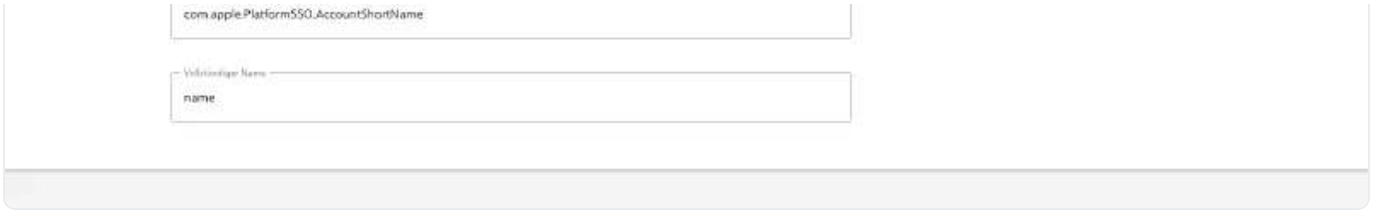
Avec la méthode Mot de passe, le portail affiche en plus Politique de connexion, Politique de déverrouillage et Politique de FileVault. Chacune de ces politiques propose les options Tentative d’authentification, Exiger l’authentification, Autoriser un délai de grâce hors ligne et Autoriser un délai de grâce pour l’authentification ; Politique de déverrouillage propose en outre Autoriser le déverrouillage par Touch ID ou par la montre. Les champs Délai de grâce hors ligne et Délai de grâce de l’authentification (prérenseignés avec `0`) ne sont modifiables que si l’option correspondante Autoriser un délai de grâce hors ligne ou Autoriser un délai de grâce pour l’authentification est sélectionnée dans au moins une des trois politiques. Avec les méthodes Carte à puce et Clé d’enclave sécurisée de l’utilisateur, ces champs ne sont ni affichés ni transmis.

Les champs marqués macOS 26+ n’ont d’effet que sur les appareils sous macOS Tahoe 26 ou une version ultérieure, et supposent que l’enregistrement s’effectue déjà pendant l’assistant de configuration (Setup Assistant).

Pour la version 26.4.0


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+



La capture d'écran montre à titre d'exemple la méthode *Mot de passe*. Avec *clé Secure Enclave* (recommandée, voir tableau), le portail masque Politique de connexion, Politique de déverrouillage, Politique de FileVault ainsi que les deux délais de grâce ; le reste de la configuration est identique.

Configuration complémentaire

- Une politique attribuée au groupe d'appareils doit également contenir la configuration Conformité App pour Company Portal, afin que l'extension soit déjà disponible au moment de l'enregistrement.
- Pour l'Inscription automatisée des appareils (ADE, DEP dans le portail), il est recommandé d'attribuer le groupe d'appareils contenant les configurations PSSO dès l'inscription automatique (`Appareils` → `Inscriptions automatiques`, dans l'entrée de l'appareil, section Groupes d'appareils → Groupes d'appareils statiques), afin que l'enregistrement puisse s'effectuer pendant l'assistant de configuration (macOS 26+).

Pour la version 26.4.0

Clés d'appareil partagées et création de compte

Utiliser des clés d'appareil partagées doit être ACTIVÉ, car dans ce flux les comptes locaux sont créés par provisionnement juste-à-temps (commutateurs Activer l'autorisation et Activer la création d'un utilisateur lors de la connexion). Sans clés d'appareil partagées, des clés liées à l'utilisateur seraient nécessaires – mais celles-ci ne peuvent pas être générées tant que le compte utilisateur n'existe pas encore (problème de l'œuf et de la poule).

> Activer l'autorisation et Activer la création d'un utilisateur lors de la connexion ne sont modifiables que si Utiliser des clés d'appareil partagées est activé. Si ce commutateur est désactivé, les deux options sont grisées et ne sont pas appliquées, même si elles apparaissent encore comme activées. Aucun compte n'est alors créé lors de la connexion.

Choix de la méthode selon le type d'appareil :

- Appareil personnalisé (recommandé) : méthode *clé Secure Enclave* – sans mot de passe, liée au matériel, Touch ID.

- Appareil partagé / multi-utilisateur (par ex. salle de classe, travail en équipes) : méthode *Mot de passe*, car les utilisateurs changeants n'ont pas d'identifiants sans mot de passe préconfigurés. Ces appareils sont enregistrés sans affinité utilisateur ; Conditional Access n'est pas pris en charge sur les Mac partagés.

Autoriser les éléments en arrière-plan pour Microsoft AutoUpdate

À partir de macOS Ventura, les processus en arrière-plan comme Microsoft AutoUpdate (MAU) sont bloqués par défaut, ou les utilisateurs reçoivent une notification Élément en arrière-plan ajouté qu'ils doivent confirmer manuellement. Sans cette autorisation, MAU ne peut pas se mettre à jour automatiquement en arrière-plan – cela concerne également Company Portal, dont les mises à jour passent par MAU.

Les éléments en arrière-plan peuvent être autorisés à l'avance au moyen d'un profil contenant la charge utile `com.apple.servicemanagement` (éléments de connexion gérés), par exemple avec une règle pour l'identifiant d'équipe de Microsoft (`UBF8T346G9`). Relution ne propose pas de configuration dédiée à cette charge utile ; un tel profil peut toutefois être distribué sous forme de fichier `.mobileconfig` via la Configuration d'Apple Configurator 2 (voir Configuration d'Apple Configurator 2 →).

La configuration Relution Eléments de connexion ne convient pas à cet usage : elle définit les applications lancées automatiquement à l'ouverture de session, mais n'autorise pas les éléments en arrière-plan.

Pour la version 26.4.0

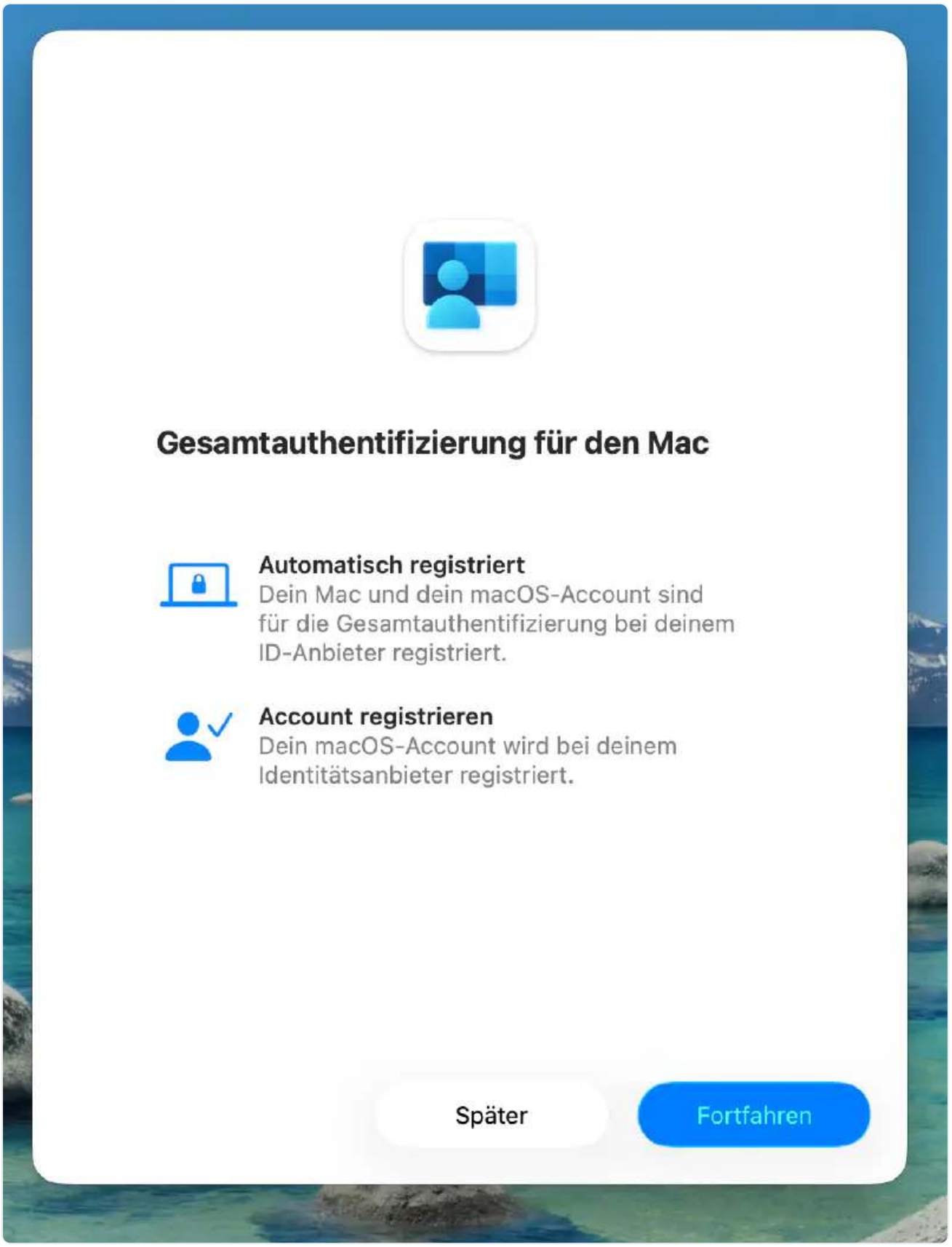
> Sans cette autorisation, les utilisateurs reçoivent à répétition des notifications système concernant de nouveaux éléments en arrière-plan, et MAU risque de ne pas mettre à jour automatiquement et de manière fiable les composants liés au SSO.

Enregistrement par les utilisateurs finaux

Une fois la configuration parvenue à l'appareil et l'application Company Portal installée, le premier enregistrement se déroule ainsi :

1. La notification Enregistrement requis (*Registration Required*) apparaît sur l'appareil. Elle peut également être déclenchée via les Réglages Système.

2. Immédiatement après la première connexion, la boîte de dialogue Authentification globale pour le Mac s'ouvre avec l'option Enregistrer le compte. L'enregistrement se poursuit via Continuer (il apparaît de la même manière pour les méthodes *Mot de passe* et *clé Secure Enclave*).



3. Les utilisateurs se connectent avec leur compte Microsoft Entra ID et confirment la MFA si nécessaire (par ex. via Microsoft Authenticator).

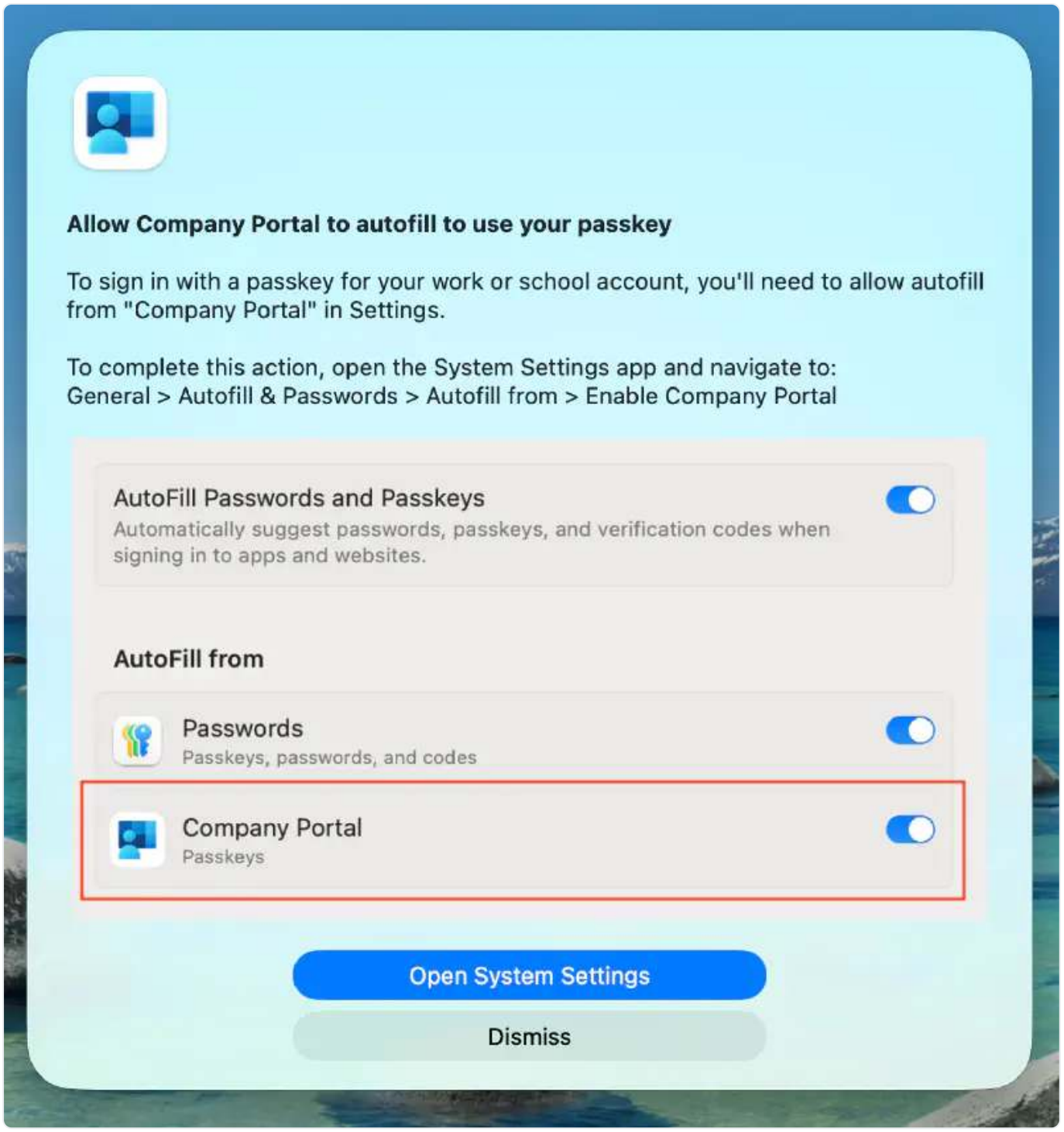
4. Le compte utilisateur local est associé à l’identité Entra ID. À partir de ce moment, l’authentification unique s’applique aux applications et navigateurs utilisant Entra ID.

Autoriser le remplissage automatique par clé d’accès pour Company Portal

Après la première connexion, un message Allow Company Portal to autofill to use your passkey apparaît. Pour que la connexion par clé d’accès (Platform Credential, en particulier avec la méthode *clé Secure Enclave*) fonctionne, les utilisateurs doivent activer une seule fois le remplissage automatique pour Company Portal :

1. Les Réglages Système s’ouvrent via Open System Settings (ou manuellement).
2. `Général` → `Remplissage automatique et mots de passe` y est ensuite ouvert.
3. Sous Remplissage automatique depuis, le commutateur pour Company Portal est activé.

Pour la version 26.4.0



Sans cette autorisation, Company Portal ne peut pas proposer la clé d'accès pour la connexion ; la connexion sans mot de passe échoue alors, ou le message apparaît à répétition.

Avec la méthode *clé Secure Enclave*, le mot de passe local reste inchangé ; après un redémarrage, le mot de passe local est d'abord nécessaire pour le déverrouillage FileVault, après quoi Touch ID peut être utilisé.

Vérification

Voici comment vérifier si l'enregistrement a réussi :

- Sur l'appareil (Terminal) : `app-sso platform -s` affiche le statut d'enregistrement de l'extension Platform SSO.
- Dans Microsoft Entra : sous *Appareils*, l'appareil apparaît comme enregistré/associé.
- Company Portal : le statut de l'appareil est affiché comme conforme/enregistré.

Erreurs possibles

- L'invite d'enregistrement n'apparaît pas → il convient de vérifier que Company Portal (version 5.2404.0+) est installé et que la conformité App a déjà été évaluée.
- La connexion échoue → l'identifiant de l'équipe, l'identificateur d'extension et les URLs sont à vérifier (fautes de frappe) ; les URLs doivent être exclues de l'inspection TLS.
- L'enregistrement échoue lors de la MFA → la MFA par utilisateur est désactivée sur le compte et Conditional Access est utilisé à la place.
- Secure Enclave non disponible → concerne les Mac Intel ; la méthode *Mot de passe* y est utilisée.
- Boucle de connexion ou Connexion impossible – l'enregistrement a échoué → en cas d'enregistrement dans l'assistant de configuration (macOS 26+), Activer la création du premier utilisateur pendant l'Assistant de configuration doit être ACTIVÉ – quelle que soit la méthode. Si le commutateur est désactivé, aucun compte local n'est créé : avec Secure Enclave, une boucle de connexion se produit ; avec Mot de passe, le message L'enregistrement a échoué apparaît.

Pour d'autres problèmes connus et conseils de diagnostic, voir : documentation Microsoft →

Pour la version 26.4.0

SFTP Upload (téléchargement SFTP)

Relution peut être utilisé pour créer des comptes Apple gérés (Identifiant Apple géré dans le portail) en grand nombre. Cela est possible via le portail Relution dans les paramètres et facilite la configuration automatique de ces comptes par les écoles et les autorités scolaires afin qu'ils puissent être mis à la disposition des étudiants et des enseignants.
Ce processus permet également de migrer automatiquement les classes créées dans Relution vers des classes dans Apple School Manager.

Exigences

- Autoriser le port 22 en sortie vers les serveurs Apple, en particulier pour l'URL : `upload.appleschoolcontent.com`.
- Un Apple School Manager
- Une licence Education ou Free dans Relution
- Droits de lecture et de modification pour Téléchargement SFTP d'Apple School Manager dans le rôle de l'administrateur (sans droit de modification, l'assistant de configuration ne peut pas être terminé)
- Au moins un domaine vérifié dans Apple School Manager (les adresses de réserve d'Apple ne sont pas possibles)
- Une classe dans Relution avec au moins un enseignant et un étudiant utilisateur
- Les enseignants doivent faire partie du groupe système `Teacher` et les étudiants doivent faire partie du groupe système `Student`.

Pour la version 26.4.0

Configuration

- Ouvrir le portail Relution et Apple School Manager.
- Naviguer jusqu'au point suivant dans Relution : `Paramètres` → `Éducation` → `Téléchargement SFTP d'Apple School Manager`
- Continuer dans l'assistant de configuration jusqu'à la saisie de l'URL du serveur, de l'utilisateur et du mot de passe.
- Dans School Manager, naviguer jusqu'au point suivant : dans le coin inférieur gauche, cliquer sur `Utilisateur` → `Paramètres` → `Comptes Apple gérés` → `Démarrer les premières étapes de la synchronisation des répertoires de liaison`.
- Cliquer sur Créer de nouveaux comptes
- Cliquer sur Utiliser un fichier CSV au format Apple

- A l'étape 1, Set up SFTP
- Copier les valeurs, les saisir dans les champs de Relution, puis cliquer sur Suivant.
- Saisir le domaine vérifié dans Apple School Manager dans le champ Identifiant Apple (domaine géré).
- Cliquer sur Save Settings : les paramètres sont enregistrés et un premier téléchargement SFTP démarre automatiquement.
- Cliquer sur Suivant dans Apple School Manager et attendre l'importation.

Les comptes sont maintenant affichés et peuvent être vérifiés pour des erreurs ici.

Dans Apple School Manager, sous Créer des comptes et des cours, le même domaine vérifié et le format de nom d'utilisateur `Prénom.Nom` sont configurés pour les enseignants et pour les étudiants (par ex. `Jean.Dupont@ecole.fr`). Pour les utilisateurs qui n'ont pas encore de compte Apple géré, Relution enregistre l'adresse exactement dans ce format (`Prénom.Nom@<domaine>`) sur l'utilisateur. Si un autre format est configuré dans Apple School Manager, les comptes qui y sont créés ne correspondent pas aux adresses enregistrées dans Relution.

Téléchargement et périmètre

Pour la version 26.4.0

Après la configuration, Relution télécharge par défaut les données automatiquement une fois par jour vers Apple School Manager. En outre, un téléchargement peut être déclenché manuellement sous `Paramètres` → `Éducation` → `Téléchargement SFTP d'Apple School Manager` via Commencer le téléchargement. Apple School Manager envoie un e-mail une fois l'importation terminée.

Sont transférés :

- tous les membres du groupe système `Teacher` en tant qu'enseignants et tous les membres du groupe système `Student` en tant qu'étudiants, même s'ils n'appartiennent au groupe que via un sous-groupe ; un utilisateur présent dans les deux groupes est transféré uniquement en tant qu'enseignant
- les classes de l'organisation avec les enseignants et les étudiants qui leur sont attribués directement ou via des groupes

Sur la même page, Politique relative aux mots de passe pour les étudiants définit la politique de mot de passe appliquée aux comptes Apple gérés des étudiants :

- Utiliser la localisation par défaut : les nouveaux comptes utilisent la politique de mot de passe par défaut de l'établissement dans Apple School Manager ; les comptes existants conservent leur politique actuelle.

- Définir une politique à 8 chiffres (standard), Définissez une politique à 6 chiffres ou Définissez une politique à 4 chiffres : les comptes nouveaux et existants passent à la politique correspondante.

Emplacement

Le téléchargement SFTP crée un nouvel emplacement dans Apple School Manager pour chaque organisation Relution qui utilise le téléchargement SFTP. Le nom de cet emplacement est le même que le nom unique de l'organisation Relution concernée.

Par exemple :

- Nom de l'organisation: `Utilisateur-Import-Test`
- Nom unique de l'organisation: `UIT`
- Nouvel emplacement dans ASM: `UIT`

Si l'emplacement dans Apple School Manager utilisé pour l'achat d'applications et qui existe déjà porte le même nom, cela peut causer des problèmes. Il est recommandé d'en discuter au préalable avec l'opérateur de serveur ou le partenaire concerné.

Pour la version 26.4.0

Déconnexion

Ne jamais déconnecter la connexion de téléchargement SFTP si les comptes sont encore activement utilisés et si d'autres comptes doivent être créés à l'avenir. En cas de déconnexion, tous les comptes créés via le téléchargement SFTP seront remplacés par la source Manuellement à partir de SFTP. Une reconnexion ultérieure risque de créer des comptes Apple gérés en double. Étant donné que la version 5.26 de Relution a également introduit l'importation d'utilisateurs, cela peut créer un cercle vicieux.

Dans Relution, les paramètres sont réinitialisés via Effacer les paramètres du serveur SFTP → Supprimer. Seuls les paramètres dans Relution sont alors supprimés : les informations d'identification SFTP restent valides jusqu'à ce que la synchronisation des annuaires soit déconnectée dans les préférences d'Apple School Manager.

Installer des applications macOS natives

Relution permet de téléverser des applications macOS natives de manière centralisée dans l'App Store et de les distribuer sur les Mac gérés. Les formats de fichier pris en charge sont `.pkg` (paquet d'installation) et `.dmg` (image disque). Pour une distribution fiable et sans surveillance, la combinaison d'un format de paquet adapté, d'une règle de détection correcte et d'une signature valide est déterminante. Les sections suivantes décrivent ces éléments en détail.

> Les applications macOS natives sont installées via l'App Store Relution ou une action de distribution. Un Mac géré (inscrit) dans Relution est requis.

Comparaison entre PKG et DMG

Le choix du format de paquet détermine la manière dont une application est installée et si le processus peut être automatisé.

version 26.4.0

Caractéristique	**`.pkg`** (paquet d'installation)	**`.dmg`** (image disque)
Structure	Programme d'installation avec scripts optionnels (`preinstall` / `postinstall`)	Conteneur/archive, contient généralement une `.app`
Emplacement d'installation	souple, possible à plusieurs emplacements cibles	en règle générale une copie vers `/Applications`
Logique d'installation	routine d'installation propre au paquet	copie de l'`.app` contenue
Installation automatisée	possible en arrière-plan sans interaction	exploitable uniquement si le paquet contient exactement une `.app`
Recommandation	à privilégier pour la distribution MDM	adapté si aucun PKG n'est proposé

Un `.pkg` est le format le plus robuste pour la distribution automatisée, car la routine d'installation est contenue dans le paquet lui-même et peut s'exécuter silencieusement en arrière-plan. Les scripts intégrés au paquet peuvent prendre en charge des étapes supplémentaires, par exemple la création de fichiers de configuration. Lors du téléversement, Relution lit le fichier Distribution du paquet et en reprend l'identifiant de produit et la version. Les paquets sans fichier Distribution (simples paquets de composants) sont refusés comme fichier non pris en charge.

Un `.dmg` est une image de support de données. Il ne convient à la distribution que s'il contient un seul fichier programme (`.app`) qui est copié vers `/Applications`. Les images comportant un assistant d'installation interactif ou plusieurs éléments ne peuvent pas être installées sans surveillance.

Une différence essentielle concerne le canal de distribution : les applications `.pkg` sont installées directement via le protocole MDM, tandis que les applications `.dmg` sont déployées via le Compagnon macOS. Le Compagnon macOS doit pour cela être activé sous `Paramètres` → `Applications client Relution` via Activer le compagnon macOS. Il n'est pas disponible sur les Mac dotés d'une version de macOS antérieure à 12 ni sur les Mac inscrits par inscription utilisateur ; les applications DMG ne peuvent pas y être distribuées.

Remarque : si une application est proposée à la fois en `.pkg` et en `.dmg`, le `.pkg` est à privilégier pour la distribution centralisée.

Pour la version 26.4.0

Créer une application native dans Relution

Les applications macOS natives sont créées dans le menu sous `Apps` → `App Store`. Le bouton Ajouter ouvre la boîte de dialogue Ajouter une nouvelle application. Sous Source, l'option Appli native est sélectionnée.

Après un clic sur Suivant, le fichier `.pkg` ou `.dmg` est téléversé via Choisissez un fichier. Ajouter des détails ouvre ensuite le formulaire Ajouter une application.

> Pour les paquets volumineux, la taille du fichier peut être limitée par la base de données ou le reverse proxy. Dans ce cas, la configuration côté serveur doit être adaptée en conséquence.

Les indications suivantes sont obligatoires dans le formulaire :

- Nom interne : pour les fichiers `.pkg`, l'identifiant de produit est repris du fichier Distribution. Pour les fichiers `.dmg`, le nom du fichier est prérempli comme espace réservé et remplacé par un nom unique. Si une application portant le même nom interne existe déjà, l'enregistrement crée une nouvelle version de cette application.

- Nom de la version : pour les fichiers `.pkg`, la version est reprise du fichier Distribution ; pour les fichiers `.dmg`, elle est saisie manuellement.
- Règles de détection : au moins une règle de détection est saisie dans la section du même nom – sans règle de détection, l'application ne peut pas être enregistrée (voir la section sur la règle de détection ci-dessous).

Après indication de l'État de la version souhaité, l'application est créée via Enregistrer.

Gestion des versions et statut de publication

Les applications macOS natives permettent en outre une gestion des versions : différentes versions d'une application peuvent être mises à disposition en parallèle pour différents groupes de personnes. Une version peut ainsi être en usage productif pendant qu'une nouvelle version est testée par un groupe restreint, sans que les autres utilisateurs en soient affectés.

Chaque version passe par l'un des statuts suivants :

- Statut de production (Version dans le portail) : version distribuée et installée normalement via le Relution Agent.
- Développement ou statut de vérification (Critique dans le portail) : statuts des versions testées avant leur mise en production.
- Archive : statut d'une version antérieure remplacée par une version plus récente au statut Version.

Pour la version 26.4.0

À l'exception du statut Archive, chaque statut ne peut contenir qu'une seule version de l'application.

Tester une nouvelle version en parallèle

Pour tester une nouvelle version en parallèle de la version en production, celle-ci est téléversée via le bouton Ajouter une nouvelle version puis placée dans le statut Développement ou Critique. Pour les fichiers `.pkg`, le nom interne de la nouvelle version doit correspondre à celui de l'application existante. Pour les fichiers `.dmg`, un écart peut être autorisé via Ignorer la non-concordance des noms d'applications internes.

Une date peut être indiquée pour la nouvelle version dans le champ Date de mise en ligne. La version ne passe automatiquement au statut Version à cette date que si un processus de validation des applications → est actif et que la version au statut Critique a franchi toutes les étapes de validation. Sans processus de validation actif, la date ne sert que de date souhaitée, et la version est placée manuellement au statut Version (voir ci-dessous).

Les deux versions restent consultables dans les propriétés de l'application ; les utilisateurs disposant des droits correspondants peuvent déjà voir, installer et tester la nouvelle version sur les appareils.

Mise en production manuelle

Si la nouvelle version se trouve au statut Critique, elle est placée au statut Version sur la page de détail de l'application via le bouton Version. Si elle se trouve encore au statut Développement, le changement s'effectue via `Déplacer vers` → `Version`. Une version se trouvant déjà au statut Version est alors automatiquement déplacée vers l'Archive. Les versions publiées des applications globales ne peuvent pas être déplacées vers un autre statut.

> L'application n'est pas mise à jour automatiquement sur les appareils. La mise à jour est déclenchée par les utilisateurs dans le Relution Agent ou par les administrateurs via l'action Déployer l'application Relution Store ou, dans la vue de l'application sous Appareils équipés de cette application, via le bouton de mise à jour de l'application.

Règle de détection via l'identifiant de bundle

Pour la version 26.4.0

La règle de détection indique à Relution à quoi reconnaître l'état installé d'une application. Pour les applications macOS natives, le type de règle Nom du paquet est disponible à cet effet. Il contient l'identifiant de bundle de l'application installée (par exemple `com.fabricant.nomapplication`) ; seuls les lettres, chiffres, points et traits d'union sont autorisés. Cette valeur permet de vérifier dans la liste des applications installées de l'appareil si l'application est déjà présente et si une installation est considérée comme réussie.

Les règles de détection sont créées dans la section Règles de détection via Ajouter une nouvelle règle de détection – lors du téléversement dans le formulaire Ajouter une application, et pour les applications existantes sur la page de détail de l'application dans l'onglet Paramètres. En option, une vérification de la version compare en outre la version installée : sous Opérateur, La version est égale à (=) ou La version n'est pas égale à (≠) est sélectionné, et la version est saisie sous Valeur. Une application peut avoir plusieurs règles de détection, par exemple lorsqu'un paquet installe plusieurs applications. L'application n'est considérée comme installée que si toutes les règles sont remplies.

La méthode la plus fiable pour déterminer l'identifiant de bundle correct passe par un Mac déjà géré :

1. L'application est installée une fois manuellement sur un Mac géré dans Relution.

2. Dans le portail Relution, l'appareil est ouvert sous `Appareils` → `Inventaire`.
3. L'application est recherchée dans l'onglet Apps installées. L'identifiant de bundle figure dans la colonne Nom interne.
4. Cette valeur est saisie dans le champ Nom du paquet de la règle de détection.

> Après une installation manuelle, un certain délai peut s'écouler avant que la prochaine synchronisation d'inventaire n'affiche l'application dans le portail. L'action Actualiser les informations sur l'appareil accélère l'affichage.

L'identifiant de bundle peut également être lu directement sur le Mac via le Terminal :

```
osascript -e 'id of app "Nom-de-l-application"'
```

Si le chemin du fichier programme est connu, la valeur peut aussi être lue dans les métadonnées du paquet :

```
mdls -name kMDItemCFBundleIdentifier -raw /Applications/Nom-de-l-application.a
```

Si la règle de détection doit être déterminée avant une installation, le contenu d'un `.pkg` peut être inspecté avec un outil tiers tel que Suspicious Package. Un tel outil affiche, outre les chemins d'installation et les scripts contenus, l'identifiant de bundle, sans que le paquet doive être exécuté.

Remarque : les outils tiers servent exclusivement à l'analyse. L'identifiant de bundle déterminant reste la valeur indiquée dans l'inventaire Relution après une installation.

Alternatives en l'absence de détection fonctionnelle

Pour certaines applications natives, Relution ne peut pas vérifier de manière fiable l'état installé — par exemple parce qu'aucun identifiant de bundle unique n'existe ou parce que le paquet place l'application à un emplacement inhabituel. Une installation automatique via la Conformité App ne convient pas dans ces cas : Relution ne reconnaît une application PKG ou DMG comme installée que si toutes les règles de détection sont remplies. Dans le cas contraire, l'installation est replanifiée à chaque vérification de conformité.

Deux approches se passent d’une règle de détection fiable :

- Mise à disposition via l’App Store Relution : l’application est mise à disposition des utilisateurs dans le Relution Agent et y est installée manuellement. L’installation étant déclenchée activement, aucune vérification automatique de l’état n’est nécessaire.
- Distribution par action : l’action Déployer l’application Relution Store sur des appareils ou des groupes sélectionnés déclenche l’installation de manière ciblée. La commande d’installation est transmise à l’appareil et y est exécutée, indépendamment d’une règle de détection.

> Sans règle de détection pertinente, Relution ne peut évaluer que de manière limitée le succès de l'installation. L'état d'installation réel doit alors être vérifié sur l'appareil.

Signature et notarisation

macOS vérifie via Gatekeeper si un logiciel provient d’une source fiable. Les paquets qui ne sont ni signés ni notarisés par Apple peuvent être bloqués ou exiger une interaction de l’utilisateur, ce qui empêche une distribution sans surveillance.

Pour la version 26.4.0

- Signature : le paquet est signé avec un Developer ID valide. L’origine est ainsi traçable et toute manipulation exclue.
- Notarisation : le paquet a en outre été vérifié par Apple (notarisé). Ce n’est qu’alors qu’il est accepté sans avertissement sur les versions récentes de macOS.

La signature et la notarisation d’un paquet peuvent être vérifiées sur le Mac dans le Terminal :

```
spctl --assess --type install -vv /chemin/vers/App.pkg
pkgutil --check-signature /chemin/vers/App.pkg
```

Remarque : si une installation échoue silencieusement pour certains paquets seulement, l’absence de signature ou de notarisation en est l’une des causes les plus fréquentes.

Analyse des erreurs via les journaux et la journalisation des appareils

Si une installation reste sans succès, les causes peuvent être circonscrites à l'aide de la journalisation.

Journalisation des appareils dans Relution

La journalisation des appareils est activée pour un appareil individuel dans l'organisation globale : l'appareil est sélectionné dans l'inventaire des appareils, puis Activer la journalisation basée sur l'appareil est réglé via Modifier la journalisation des appareils pour la durée indiquée sous Durée (en minutes). Pendant cette période, les commandes telles que l'installation d'application sont journalisées avec la réponse de l'appareil. Les Journaux des appareils collectés sont téléchargés sous forme de fichier dans la même boîte de dialogue. Il devient ainsi visible si une commande d'installation a atteint l'appareil et avec quel statut elle a été acquittée.

> La journalisation s'arrête automatiquement après la durée définie. Le fichier journal est supprimé un jour après la fin de la journalisation et ne survit pas à un redémarrage du serveur Relution.

Pour la version 26.4.0

Journaux d'installation sur le Mac

En complément, les journaux système du Mac renseignent sur le déroulement de l'installation. Le déroulement d'une installation PKG est journalisé localement et peut être analysé dans le Terminal :

```
tail -n 100 /var/log/install.log
```

Pour une observation en continu pendant une installation, le flux en direct du journal système est adapté :

```
log stream --predicate 'process == "installer"' --info
```

Ces sorties permettent de déterminer si le paquet a été décompressé, si un script a été exécuté ou si le processus a été interrompu par Gatekeeper.

Désinstallation

Les applications macOS natives installées via Relution peuvent également être désinstallées via Relution — aussi bien les applications `.pkg` que `.dmg`. Un identifiant de bundle (règle de détection) est requis pour adresser l'application de manière univoque sur l'appareil. Sans identifiant de bundle valide, aucune désinstallation n'est déclenchée. Comme pour l'installation, la suppression passe par des canaux différents selon le format — `.pkg` via MDM, `.dmg` via le Compagnon macOS — mais la procédure dans le portail est identique.

Deux voies existent pour la désinstallation :

- De manière ciblée via une action : l'action Supprimer l'application sur des appareils ou des groupes sélectionnés désinstalle l'application. Dans l'historique des commandes de l'appareil, l'opération apparaît sous la forme `Supprimez <identifiant-de-bundle>`.
- Automatiquement lors de la suppression de l'attribution : si une application installée automatiquement via la Conformité App (case cochée dans la colonne Installation automatique) n'est plus requise après une modification ou une suppression de la politique, Relution la désinstalle automatiquement. Contrairement à iOS, la configuration macOS Conformité App ne propose aucune option pour désactiver cette désinstallation.

Pour la version 26.4.0

> C'est l'identifiant de bundle qui est déterminant pour la désinstallation, et non le format de paquet. Sans règle de détection valide, Relution ne peut pas résoudre l'application sur l'appareil et ne peut donc pas la supprimer de manière ciblée.

Ne peuvent pas être supprimées via Relution : les applications sans identifiant de bundle ainsi que les applications installées manuellement, en dehors de Relution. Pour les applications `.dmg`, le Compagnon macOS est en outre nécessaire ; s'il est désactivé ou inutilisable sur l'appareil (macOS antérieur à la version 12, inscription utilisateur), aucune désinstallation via Relution n'est possible. Dans ces cas, la suppression est mise en œuvre par un script qui ferme l'application et supprime les répertoires associés, script distribué de manière ciblée via une action.

Gérer les apps de l'App Store

Avec Relution, il est possible de distribuer des applications de l’App Store d’Apple à des appareils. Pour ce faire, une licence d’application doit toujours être achetée, que l’application soit payante ou non. Une licence d’application peut être achetée via Apps et livres (VPP dans le portail) ou obtenue via un identifiant Apple connecté sur l’appareil. Selon le cas d’utilisation, l’un ou l’autre scénario est plus judicieux. Pour travailler sur des appareils sans identifiant Apple, il n’y a pas d’autre solution qu’une licence Apps et livres. La configuration d’Apps et livres est décrite dans le chapitre correspondant →.

Les applications achetées dans Apple School / Business Manager sont automatiquement synchronisées avec Relution (à partir de la version 5.10). Les applications sont publiées dans Relution au statut de production (Version dans le portail) et peuvent être distribuées aux appareils par la suite. Les applications qui ne doivent pas être mises à la disposition de tous les utilisateurs peuvent également être manuellement assignées à un statut de publication différent. Une application peut également être ajoutée manuellement à l’App Store de Relution à tout moment. Cependant, les licences Apps et livres ne sont pas automatiquement disponibles pour ces applications et l’installation n’est possible que si des utilisateurs disposant d’un identifiant Apple sont connectés sur les appareils correspondants. Il est possible d’obtenir ultérieurement des licences Apps et livres pour ces applications.

Pour la version 26.4.0

Si des licences Apps et livres sont disponibles pour une application, Relution attribue automatiquement une licence lors de l’installation – y compris pour les applications ajoutées manuellement, dès que les licences ont été synchronisées. Sur les Mac inscrits par inscription utilisateur, une licence basée sur l’utilisateur est utilisée à cet effet.

Distribuer les applications

Les applications de l’App Store sont normalement distribuées aux Mac en tant qu’applications requises via la configuration de politique Conformité App.

Deux actions sont disponibles pour des appareils individuels :

- Déployer l’application Relution Store : propose les applications de l’App Store de Relution, c’est-à-dire, outre les applications natives, les applications de l’App Store qui y ont été créées.
- Déployer une application depuis l’Apple App Store : l’application est recherchée directement dans l’Apple App Store et installée, sans devoir être créée au préalable dans l’App Store de Relution.

Gérer les applications

Les applications de l'App Store sont mises à jour automatiquement par le système d'exploitation. Dans de rares cas, cependant, cela ne fonctionne pas. Il existe alors deux moyens de déclencher une mise à jour :

- Dans la vue détaillée de l'application, les appareils concernés sont sélectionnés dans l'onglet Appareils équipés de cette application, puis mis à jour via le bouton de mise à jour (Mise à jour de dans le portail). Le bouton est désactivé dès que l'un des appareils sélectionnés dispose déjà de la version au statut Version.
- Sinon, l'action Déployer l'application Relution Store (ou Déployer une application depuis l'Apple App Store) est exécutée à nouveau avec l'application concernée sur les appareils concernés.

Dans les deux cas, une réinstallation est déclenchée et les appareils valident la version de l'application avec l'App Store d'Apple. Si la version disponible est plus récente que la version installée, l'application existante est mise à jour.

Pour la version 26.4.0

Configuration d'application gérée pour les applications natives

Les applications macOS natives — c'est-à-dire les applications téléversées soi-même sous forme de `.pkg` ou de `.dmg` — peuvent être préconfigurées dans Relution. La méthode prévue à cet effet diffère toutefois de celle des applications issues de l'App Store. C'est la source de l'application qui est déterminante, car elle définit la méthode disponible.

La source de l'application détermine la méthode de configuration

La configuration de politique App gérée → suppose que l'application a été installée via un canal géré par Apple. macOS ne l'applique qu'aux applications installées depuis l'App Store ou via Apps et livres (VPP dans le portail). Pour ces applications, le système d'exploitation se charge d'associer la configuration à l'application à l'aide de l'identifiant de bundle.

Pour les applications natives, ce mécanisme ne s'applique pas, celles-ci n'ayant pas été installées via le canal géré de l'App Store. Elles peuvent certes être sélectionnées dans la configuration App gérée du portail, mais la configuration n'a aucun effet sur elles. La configuration d'une application native doit donc être transmise sous forme de charge utile via la configuration de politique Configuration d'Apple Configurator 2 →.

Pour la version 26.4.0

Source de l'application	Méthode de configuration
App Store / Apps et livres	App gérée
Application native (`.pkg` / `.dmg`)	Charge utile via Configuration d'Apple Configurator 2

Configuration des applications natives via Apple Configurator 2

Les clés et valeurs prises en charge dans la charge utile (property list) sont définies par l'éditeur de l'application concernée. La mise en place s'effectue en quelques étapes :

1. L'application native est d'abord mise à disposition comme à l'accoutumée, de sorte qu'elle soit installée sur les appareils cibles (voir Installer des applications macOS natives →).
2. La configuration d'application souhaitée est assemblée sous forme de fichier `.mobileconfig` (voir la recommandation ci-dessous).
3. Une Configuration d'Apple Configurator 2 est ajoutée à la politique, un Nom est saisi et le fichier `.mobileconfig` est importé dans son intégralité via Sélectionnez le fichier .mobileconfig. Son contenu s'affiche ensuite dans le champ Contenu de la charge utile et peut y être adapté si nécessaire.
4. La politique est publiée puis attribuée aux groupes d'appareils concernés.

> L'application doit déjà être installée sur l'appareil avant que la configuration ne prenne effet. L'ordre des configurations au sein d'une politique ne peut pas être défini. Si l'application est installée via la même politique, la Configuration d'Apple Configurator 2 peut donc arriver sur l'appareil avant l'application.

Un fichier `.mobileconfig` ne peut contenir qu'un seul type de configuration (type de charge utile) dans `PayloadContent` ; des charges utiles de certificat supplémentaires sont autorisées. Si le fichier contient plusieurs types, par exemple des paramètres pour plusieurs applications, la configuration ne peut pas être enregistrée. Une Configuration d'Apple Configurator 2 distincte est donc créée pour chaque application. Si le fichier contient plusieurs charges utiles du même type, seule la première est transmise. Les autres exigences relatives au fichier sont décrites dans l'article Configuration d'Apple Configurator 2 →.

Recommandation : créer la charge utile avec l'iMazing Profile Editor

La rédaction manuelle d'une charge utile est source d'erreurs. Pour une création confortable, l'outil tiers iMazing Profile Editor est recommandé. Il permet d'assembler la configuration via une interface graphique, sans rédiger à la main la property list sous-jacente.

Le déroulement est le suivant :

Pour la version 26.4.0

1. Dans l'iMazing Profile Editor, les paramètres souhaités pour l'application sont définis via l'interface.
2. Le résultat est exporté sans signature sous forme de fichier `.mobileconfig`. Relution lit le fichier en tant que XML ; les profils signés ne peuvent pas être enregistrés.
3. Le fichier `.mobileconfig` complet est importé dans la Configuration d'Apple Configurator 2 de Relution.

> L'iMazing Profile Editor est un outil tiers et ne fait pas partie de Relution. Il sert exclusivement à créer la charge utile.

Dans la charge utile, les espaces réservés fournis par Relution peuvent également être utilisés (par exemple `${user.email}`) afin de remplir la configuration en fonction de l'utilisateur. Les espaces réservés disponibles sont affichés sous le formulaire de configuration et remplacés lors de la transmission de la configuration aux appareils, voir Espaces réservés avancés →.

Pour la version 26.4.0

Vue d'ensemble des inscriptions

Le Vision Pro devient un élément central des organisations modernes et ouvre des possibilités entièrement nouvelles. Grâce à différentes méthodes d'inscription, Relution garantit que le Vision Pro peut être intégré de manière fluide et utilisé de façon optimale. Outre l'Inscription automatisée des appareils (ADE, DEP dans le portail), l'option d'inscription utilisateur Apple (User Enrollment) est également disponible.

Inscription automatisée des appareils (ADE) via un profil DEP

Apple School ou Business Manager a été introduit par Apple pour aider les organisations et les établissements d'enseignement à déployer des appareils Apple à distance. Grâce à ASM/ABM, des appareils Apple flambant neufs peuvent être enregistrés dans Relution sans qu'un technicien n'ait jamais besoin de les manipuler.

Profil pour l'ADE →
Configurer DEP →

Pour la version 26.4.0

Prérequis

- visionOS 1.1 ou une version ultérieure.
- L'organisation doit être inscrite auprès d'Apple School / Apple Business Manager.
- Si les appareils ont été achetés directement auprès d'Apple, le numéro client Apple attribué à l'organisation est nécessaire pour relier les commandes et appareils éligibles à Apple School / Business Manager.
- Si les appareils ont été achetés directement auprès d'un revendeur ou d'un opérateur agréé, ils doivent être liés à l'ID revendeur (Reseller ID) de ce revendeur. La date réelle d'éligibilité est déterminée par l'historique des ventes du revendeur ou de l'opérateur agréé.
- Un certificat APNs enregistré dans Relution (Certificats de poussée APNS →).
- Un compte DEP connecté à Relution et un profil DEP attribué aux appareils. Le champ Version minimale de visionOS du profil DEP permet en outre de définir une version minimale de visionOS pour l'inscription.

Inscription utilisateur basée sur le compte

Il s'agit de la méthode d'inscription typique pour les appareils personnels (BYOD, Bring Your Own Device). Les utilisateurs peuvent effectuer eux-mêmes l'inscription et les appareils n'ont pas besoin d'être réinitialisés aux paramètres d'usine.

Relution prend en charge l'inscription utilisateur basée sur le compte pour les appareils visionOS qui ne sont pas en `mode supervisé` (Supervised Mode).

La connexion s'effectue sur le Vision Pro, dans les réglages de l'appareil, avec un compte Apple géré (Identifiant Apple géré dans le portail). Grâce à la découverte de service, l'appareil détermine le serveur MDM compétent et redirige vers la page de connexion de Relution, où la connexion s'effectue avec le compte utilisateur Relution. Relution crée alors automatiquement une inscription utilisateur avec la propriété BYOD (appareil personnel). Pour visionOS, il n'est pas possible de créer manuellement une inscription utilisateur dans le portail.

Prérequis

- Un certificat APNs enregistré dans Relution (Certificats de poussée APNS →).
- Un compte Apple géré et un compte utilisateur Relution pour chaque utilisateur.
- Le paramètre Inscription des utilisateurs Apple en fonction du compte activé dans l'organisation.
- Une découverte de service pour le domaine des comptes Apple gérés, soit automatiquement via Apple School/Business Manager, soit via un fichier well-known.

Pour la version 26.4.0

Activer l'inscription utilisateur Apple basée sur le compte

Le paramètre se trouve sous `Paramètres` → `Gestion des appareils`, dans la section Inscription des utilisateurs Apple en fonction du compte. Il s'applique par organisation ; la section n'est pas affichée dans l'organisation globale.

Lorsque le curseur Inscription des utilisateurs Apple en fonction du compte est activé, Relution crée automatiquement une inscription utilisateur lors de la connexion d'un utilisateur. Le curseur est désactivé par défaut ; dans ce cas, l'inscription des appareils visionOS échoue.

Configurer la découverte de service

Une découverte de service doit être configurée afin qu'Apple puisse orienter les appareils vers le bon serveur MDM. Deux méthodes sont disponibles.

Automatiquement via Apple School/Business Manager

À partir de visionOS 2.2, aucun fichier propre n'est nécessaire si Apple School/Business Manager est connecté à Relution via un compte DEP. Relution enregistre automatiquement l'URL de découverte de service dans Apple School/Business Manager lors de chaque synchronisation des appareils ADE. Il faut pour cela que Relution y soit défini comme serveur MDM par défaut pour Apple Vision Pro sous `Preferences` → `Your MDM Servers` → `MDM Server Assignment` → `Default MDM Server Assignment`.

Via un fichier well-known

Pour les appareils équipés d'une version de visionOS antérieure à 2.2, ou sans Apple School/Business Manager connecté, un fichier de ressource HTTP `well-known` doit être déposé sur le domaine avec lequel les utilisateurs se connecteront. Relution répond déjà lui-même à cette requête pour son propre nom d'hôte ; un fichier propre n'est donc nécessaire que si le domaine des comptes Apple gérés en diffère. Apple doit pouvoir récupérer ce fichier via une requête HTTP GET à l'URL suivante :

```
https://votredomaine.com/.well-known/com.apple.remotemanagement
```

À l'emplacement `votredomaine.com`, indiquer le domaine également utilisé pour les comptes Apple gérés. Le fichier doit être déposé sur un domaine capable de traiter des requêtes HTTP GET.

Créer le fichier au format JSON avec le type de contenu `application/json`. Pour renseigner les bonnes informations dans le fichier, les informations nécessaires peuvent être copiées directement depuis le portail Relution :

1. Ouvrir `Paramètres` → `Gestion des appareils`.
2. Dans la section Inscription des utilisateurs Apple en fonction du compte, copier l'intégralité du texte JSON affiché sous Réponse, accolades extérieures comprises (bouton Copier dans le presse-papiers), et l'insérer dans le fichier. Le texte JSON est affiché indépendamment du curseur.

> Important : pour que le fichier fonctionne correctement, il ne doit avoir aucune extension de fichier.

Exemple : maxmustermann@musterhausen.de

Dans cet exemple, le domaine serait `musterhausen.de`. C'est à cet endroit que la découverte de service doit être déposée.

Inscription ultérieure via Apple Configurator 2

Apple Configurator 2 est une application gratuite disponible sur le Mac App Store. Elle permet de configurer manuellement, via USB, des appareils Apple connectés à un appareil macOS avant leur remise aux utilisateurs. Pour cela, des profils peuvent être créés et appliqués aux appareils. Apple Configurator 2 permet également d'ajouter ultérieurement à l'ADE des appareils Apple qui n'y ont pas encore été enregistrés par un revendeur agréé. De manière générale, il est recommandé d'acquérir directement des appareils compatibles ADE, car un ajout ultérieur implique un travail manuel.

Prérequis

- visionOS 1.1 ou une version ultérieure.
- Appareil macOS avec Apple Configurator 2.5 ou une version ultérieure.
- L'appareil macOS et le Vision Pro doivent être connectés au même réseau Wi-Fi ou Ethernet.

Pour la version 26.4.0

Pour les appareils visionOS, le chemin suivant doit être indiqué comme URL du serveur MDM si les appareils doivent être gérés sur le système de production Relution. Pour une instance Relution personnelle, remplacer `live.relution.io` par le nom d'hôte du serveur utilisé.

```
https://live.relution.io/api/enrollment/v1/appleMdm/depenroll
```

Les appareils Apple enregistrés ultérieurement dans Apple School/Business Manager via Apple Configurator 2 ne se comportent pas, durant les 30 premiers jours suivant le déploiement, comme des appareils enregistrés directement via l'ADE lors de l'achat auprès d'un revendeur agréé. Même si la suppression manuelle de la gestion MDM sur les appareils a été bloquée via le profil DEP associé dans le système MDM, les utilisateurs peuvent supprimer la gestion MDM sous `Réglages` → `Général` → `Profils`.

> Une fois le délai de 30 jours à compter de l'enregistrement écoulé, les utilisateurs ne peuvent plus supprimer la gestion MDM sur les appareils.

Ajout ultérieur d'appareils Apple à l'ADE →

Actions disponibles

Relution propose une sélection d’actions permettant de contrôler directement le Vision Pro. Les actions peuvent être appliquées de manière ciblée à des appareils individuels, à plusieurs appareils à la fois par sélection multiple dans la liste des appareils, ou automatiquement via les Actions de groupes d’appareils →.

Aperçu des actions

Action	Description
Actualiser les informations sur l’appareil	Actualise toutes les informations disponibles sur l’appareil, répertoriées sous Détails.
Déployer l’application Relution Store	Installe une application du Relution Store sur les appareils. Outre les applications visionOS, les applications iOS sont également proposées.
Mettre à jour le profil MDM	Réinstalle le profil MDM sur l’appareil. Le certificat d’identité est renouvelé et les paramètres actuels, tels que l’épinglage de certificats, sont appliqués. L’URL du serveur MDM reste inchangée ; une URL externe modifiée n’est donc pas transmise à l’appareil. Relution renouvelle automatiquement le profil MDM avant l’expiration du certificat d’identité. L’action manuelle n’est donc nécessaire que dans des cas particuliers.
Continuer dans l’Assistant Configuration de l’appareil	Informe l’appareil que la préconfiguration est terminée et qu’il peut poursuivre dans l’assistant de configuration. N’a d’effet que sur les appareils inscrits via l’Inscription automatisée des appareils (ADE, DEP dans le portail) dont le Profil du DEP a l’option Attendre la configuration activée. L’action n’est pas disponible pour les appareils inscrits via l’inscription utilisateur.

Les actions Redémarrer l’appareil, Verrouiller l’appareil, Arrêter l’appareil et Effacer l’appareil ne sont pas proposées pour les appareils visionOS.

Configurations disponibles

Une politique est un ensemble d'une ou plusieurs configurations. Chaque politique peut être appliquée à un ou plusieurs appareils simultanément. De plus, une ou plusieurs politiques peuvent être associées à chaque appareil.

Configurations disponibles

Configuration	Description
Conformité de l'application →	Gestion des restrictions spécifiques aux applications
Configuration Apple Configurator 2 →	Applique aux appareils un profil de configuration (`.mobileconfig`) créé avec Apple Configurator 2
Paramètres d'intelligence externe →	Contrôle des intégrations d'IA externes basées sur le cloud via Siri et Apple Intelligence (à partir de visionOS 26.4)
Paramètres Intelligence →	Contrôle centralisé des fonctionnalités d'Apple Intelligence telles que Genmoji, Image Playground et les outils d'écriture (à partir de visionOS 26.4)
Code d'accès →	Politique de mot de passe pour les appareils Apple
Restrictions →	Gestion des restrictions d'appareils
Paramètres de Siri →	Contrôle centralisé du comportement de Siri, notamment le filtre de langage grossier et l'accès en mode verrouillé
Paramètres de mise à jour du logiciel →	Contrôle du comportement de mise à jour des appareils, p. ex. téléchargement automatique, report et notifications (à partir de visionOS 26)
Mises à jour logicielles gérées →	Imposer les mises à jour du système en ciblant une version précise avant une échéance (à partir de visionOS 26, appareils supervisés uniquement)

Configuration	Description
Wi-Fi	Gestion des paramètres Wi-Fi
Certificat	Sélection d’un certificat à installer par défaut sur l’appareil

Pour la version 26.4.0

Code d'accès

La politique de mot de passe Apple définit les exigences de sécurité pour les codes des appareils visionOS. Sous visionOS, cette configuration est prévue pour l'inscription des appareils.

La politique offre de nombreuses options permettant d'adapter davantage les exigences de sécurité du mot de passe. Cela inclut notamment des exigences relatives à la complexité, à la longueur, à la durée de validité et au nombre de tentatives échouées autorisées.

Dès que la politique est appliquée à un appareil, un code d'accès y est toujours exigé. Les champs laissés vides ne sont pas transmis à l'appareil ; la politique n'impose alors aucune exigence pour ces réglages.

> Un minimum de visionOS 2.x est requis.

Options de configuration

Pour la version 26.4.0

- Autoriser un code d'accès simple (activé par défaut) : autorise les codes contenant des caractères répétés ou des suites croissantes/décroissantes telles que `aaa`, `abc` ou `123`.
- Demander des valeurs alphanumériques (désactivé par défaut) : détermine si le code doit contenir des lettres ou si des chiffres suffisent.
- Longueur minimale du code d'accès : valeurs de 0 à 25 caractères.
- Nombre de caractères spéciaux requis (1-4) : valeurs de 0 à 4.
- Âge maximum du code d'accès (en jours) : nombre de jours au terme desquels un nouveau code doit être défini ; valeurs de 0 à 730.
- Temps d'inactivité (en minutes) : délai maximal de verrouillage automatique après inactivité que l'utilisateur peut sélectionner sur l'appareil.
- Historique du code d'accès : nombre de codes déjà utilisés qui ne peuvent pas être redéfinis ; valeurs de 1 à 50.
- Délai de grâce pour le verrouillage de l'appareil (en minutes) : période après le verrouillage pendant laquelle l'appareil peut encore être déverrouillé sans saisir le code. Avec

Immédiatement, le code est demandé à chaque déverrouillage. Ce réglage ne détermine pas quand l'appareil se verrouille – c'est le rôle de Temps d'inactivité (en minutes).

  - Immédiatement
  - 1 minute
  - 5 minutes
  - 15 minutes
  - 60 minutes
  - 4 heures
- Nombre maximum de tentatives infructueuses : valeurs de 2 à 11.

> Si ce nombre est dépassé, une action d'effacement est déclenchée.

Pour la version 26.4.0

Configuration d'Apple Configurator 2

Cette configuration de politique permet de transférer des fichiers `.mobileconfig` sur les appareils Apple. Un tel fichier peut par exemple contenir une connexion Wi-Fi accompagnée du certificat d'identité correspondant (PKCS#12, `.p12`).

Configuration

Le champ Nom permet d'attribuer un nom à la configuration. Le fichier est importé via le champ de sélection du fichier `.mobileconfig`. Son contenu apparaît ensuite à la place de la sélection de fichier dans le champ Contenu de la charge utile, où il peut être modifié. Le contenu doit être du XML valide. Les profils signés ne sont pas du XML lisible et ne peuvent donc pas être utilisés. Dans Apple Configurator 2, le fichier est par conséquent enregistré sans signature. Si le champ Contenu de la charge utile est vidé, un fichier peut à nouveau être sélectionné.

Des espaces réservés pour l'utilisateur, l'appareil et les certificats peuvent être utilisés dans le champ Contenu de la charge utile. Les espaces réservés disponibles sont affichés sous le formulaire et sont remplacés lors du transfert vers l'appareil, voir Espaces réservés avancés →.

Plusieurs configurations Apple Configurator 2 peuvent être créées par politique. Il est ainsi possible de répartir plusieurs types de configuration sur des configurations distinctes.

Pour la version 26.4.0

Exigences relatives au fichier

Le contenu est vérifié lors de l'enregistrement. Le fichier doit remplir les conditions suivantes :

- Le niveau supérieur contient les clés `PayloadType`, `PayloadVersion` (sous forme de nombre), `PayloadIdentifier`, `PayloadUUID` et `PayloadDisplayName`.
- `PayloadContent` contient exactement un type de configuration. Des charges utiles de certificat peuvent s'y ajouter.

Les fichiers illisibles, ceux auxquels il manque l'une de ces clés ou ceux qui ne contiennent aucune charge utile ou plusieurs types de configuration sont refusés lors de l'enregistrement.

> Seuls les certificats au format PKCS#12 (`com.apple.security.pkcs12`) sont transférés avec la configuration. Les certificats PKCS#1 (`com.apple.security.pkcs1`) sont acceptés lors de la vérification, mais ne sont pas transférés vers l'appareil. Les autres certificats, comme les certificats racine (`com.apple.security.root`), comptent comme

un type de configuration à part entière. Associés à une autre configuration, ils provoquent une erreur lors de l'enregistrement et sont donc déposés dans une configuration distincte.

La configuration proprement dite doit figurer en première position dans `PayloadContent`. Si le fichier contient plusieurs charges utiles du même type, seule la première est transférée vers l'appareil.

Si le fichier contient un type de configuration que Relution propose également sous forme de configuration propre, autorisée une seule fois par politique, cette configuration ne peut plus être ajoutée à la même politique. Sous visionOS, cela concerne Mot de passe → (`com.apple.mobiledevice.passwordpolicy`) et Restrictions → (`com.apple.applicationaccess`).

À l'inverse, un tel fichier est refusé lors de l'enregistrement si la politique contient déjà la configuration correspondante ou une autre configuration Apple Configurator 2 active avec le même type de charge utile.

Exemple

Le fichier suivant transfère une connexion Wi-Fi (`com.apple.wifi.managed`). Le SSID, le mot de passe, les identifiants et les UUID sont des valeurs d'exemple à remplacer par des valeurs réelles. Chaque `PayloadUUID` doit être unique.

Pour la version 26.4.0

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/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>mot-de-passe-WiFi</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>WiFi-Entreprise</string>
   </dict>
  </array>
  <key>PayloadDescription</key>
  <string>Configuration Wi-Fi pour les appareils Apple</string>
  <key>PayloadDisplayName</key>
  <string>Wi-Fi</string>
  <key>PayloadIdentifier</key>
  <string>com.example.wifi</string>
  <key>PayloadOrganization</key>
  <string>Exemple SAS</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>
```

Paramètres Intelligence

Avec Relution, la configuration Paramètres Intelligence peut être gérée de manière centralisée afin de contrôler les fonctions d'Apple Intelligence sur les appareils visionOS gérés. Cette politique permet d'autoriser ou de bloquer des fonctions individuelles pilotées par l'IA, telles que le rapport Apple Intelligence, Genmoji, Image Playground, Image Wand et les outils d'écriture. Elle permet en outre de contrôler les fonctions Intelligence dans Mail et Safari, ainsi que d'imposer un traitement de la dictée exclusivement local sur l'appareil, sans connexion aux serveurs d'Apple.

La configuration est disponible pour les appareils visionOS à partir de la version 26.4.

> Le formulaire est identique pour iOS, macOS et visionOS. Les options Autoriser les résultats d'écriture manuscrite personnalisée, Autoriser le résumé Visual Intelligence, Forcer la traduction uniquement sur l'appareil ainsi que Autoriser la transcription et Autoriser le résumé de transcription dans la section Notes s'affichent également pour visionOS, mais ne sont pas prises en charge par visionOS. Elles ne sont donc pas décrites ici, voir Paramètres Intelligence pour iOS →.

Pour la version 26.4.0

Paramètres

- Autoriser le rapport Apple Intelligence
  - Si désactivé, le rapport Apple Intelligence est désactivé sur l'appareil. Activé par défaut.
- Autoriser Genmoji
  - Si désactivé, la fonction Genmoji est désactivée. Activé par défaut.
- Autoriser Image Playground
  - Si désactivé, Image Playground est désactivé. Activé par défaut.
- Autoriser Image Wand
  - Si désactivé, Image Wand est désactivé. Activé par défaut.
- Autoriser les outils d'écriture
  - Si désactivé, les outils d'écriture (Writing Tools) sont désactivés. Activé par défaut.
- Forcer la dictée uniquement sur l'appareil
  - Si activé, la dictée est traitée exclusivement en local sur l'appareil, sans connexion aux serveurs d'Apple. Désactivé par défaut.

Mail

- Autoriser les réponses intelligentes
  - Si désactivé, les réponses intelligentes (Smart Replies) dans Mail sont désactivées. Activé par défaut.
- Autoriser le résumé
  - Si désactivé, la fonction de résumé dans Mail est désactivée. Activé par défaut.

Safari

- Autoriser le résumé
  - Si désactivé, la fonction de résumé dans Safari est désactivée. Activé par défaut.

Pour la version 26.4.0

Restrictions

Voici une vue d'ensemble des restrictions visionOS disponibles.

La plupart des restrictions nécessitent visionOS 2 (indication visionOS 2+ dans le formulaire) ; les versions minimales différentes, comme visionOS 1.1+, visionOS 2.4+ ou visionOS 26+, sont indiquées dans la vue d'ensemble ci-dessous. Les restrictions portant la mention Supervisé ne s'appliquent qu'aux appareils supervisés, celles portant la mention Prend en charge l'inscription des utilisateurs s'appliquent également aux appareils inscrits par inscription des utilisateurs ; les deux sont signalées en conséquence dans la vue d'ensemble. Les restrictions des fonctionnalités de l'IA portent dans le portail la mention Obsolète.

Par défaut, toutes les options sont activées, à l'exception de la dictée uniquement sur l'appareil, des deux options relatives aux contacts sous Applications et documents gérés, de l'application des paramètres Autoriser l'ouverture… au copier-coller, de l'option considérant toujours les destinations AirDrop comme non gérées, ainsi que du réglage automatique forcé de la date et de l'heure et de la liste blanche Wi-Fi forcée. La liste des identifiants d'espace de travail autorisés pour l'intégration externe est vide. Avec les valeurs par défaut, toutes les fonctions sont donc autorisées ; seule l'option Forcer l'authentification avant le remplissage automatique est activée par défaut, si bien qu'une authentification est requise avant le remplissage automatique.

Pour la version 26.4.0

L'icône de téléchargement en haut du formulaire permet d'exporter les valeurs configurées, y compris les modifications non enregistrées, dans un fichier CSV.

Parmi les Restrictions recommandées pour iOS/iPadOS →, seules les remarques concernant l'effacement de tout le contenu et des réglages, le réglage automatique forcé de la date et de l'heure et la liste blanche Wi-Fi forcée s'appliquent également à visionOS.

Appareil

› Afficher toutes les restrictions

Apps

Les restrictions relatives aux applications sont regroupées par domaine d'utilisation.

Général

Afficher toutes les restrictions

Safari

Afficher toutes les restrictions

Siri

Afficher toutes les restrictions

Autres applications

Afficher toutes les restrictions

Applications et documents gérés

Ces réglages contrôlent les échanges de données entre applications gérées et non gérées.

Restrictions sur les applications et documents gérés

Afficher toutes les restrictions

Réglages

Les restrictions suivantes concernent les réglages système de l’appareil.

Restrictions des paramètres

Afficher toutes les restrictions

Pour la version 26.4.0

Médias

Les restrictions suivantes concernent les contenus multimédias et leur lecture.

Restrictions des médias

Afficher toutes les restrictions

Modifications

Ces restrictions définissent quels réglages peuvent être modifiés sur l'appareil.

Restrictions relatives aux modifications

Afficher toutes les restrictions

Pour la version 26.4.0

iCloud

Les restrictions suivantes concernent les services iCloud sur l'appareil.

Restrictions iCloud

Afficher toutes les restrictions

Restrictions des fonctionnalités de l'IA

Ces restrictions contrôlent les fonctions Apple Intelligence.

> Toutes les restrictions de cette section portent dans le portail la mention Obsolète. Pour les appareils à partir de visionOS 26.4, les configurations Paramètres Intelligence → (Genmoji, Image Playground, outils d'écriture, Image Wand) et Paramètres d'intelligence externe → (intégrations d'intelligence externe, connexion, identifiant d'espace de travail) sont disponibles à la place ; l'article sur les paramètres d'intelligence externe décrit cette configuration à

l’exemple d’iOS. Pour les appareils équipés de versions antérieures de visionOS, les restrictions décrites ici continuent de s’appliquer.

Général

Afficher toutes les restrictions

Pour la version 26.4.0

Conformité de l'application

L’installation d’applications issues d’Apps et livres (VPP dans le portail) sur les appareils Apple Vision est particulièrement simple grâce à la politique de conformité des applications (Conformité App) de Relution. Cette configuration permet une distribution simple et centralisée des applications sur un grand nombre d’appareils.

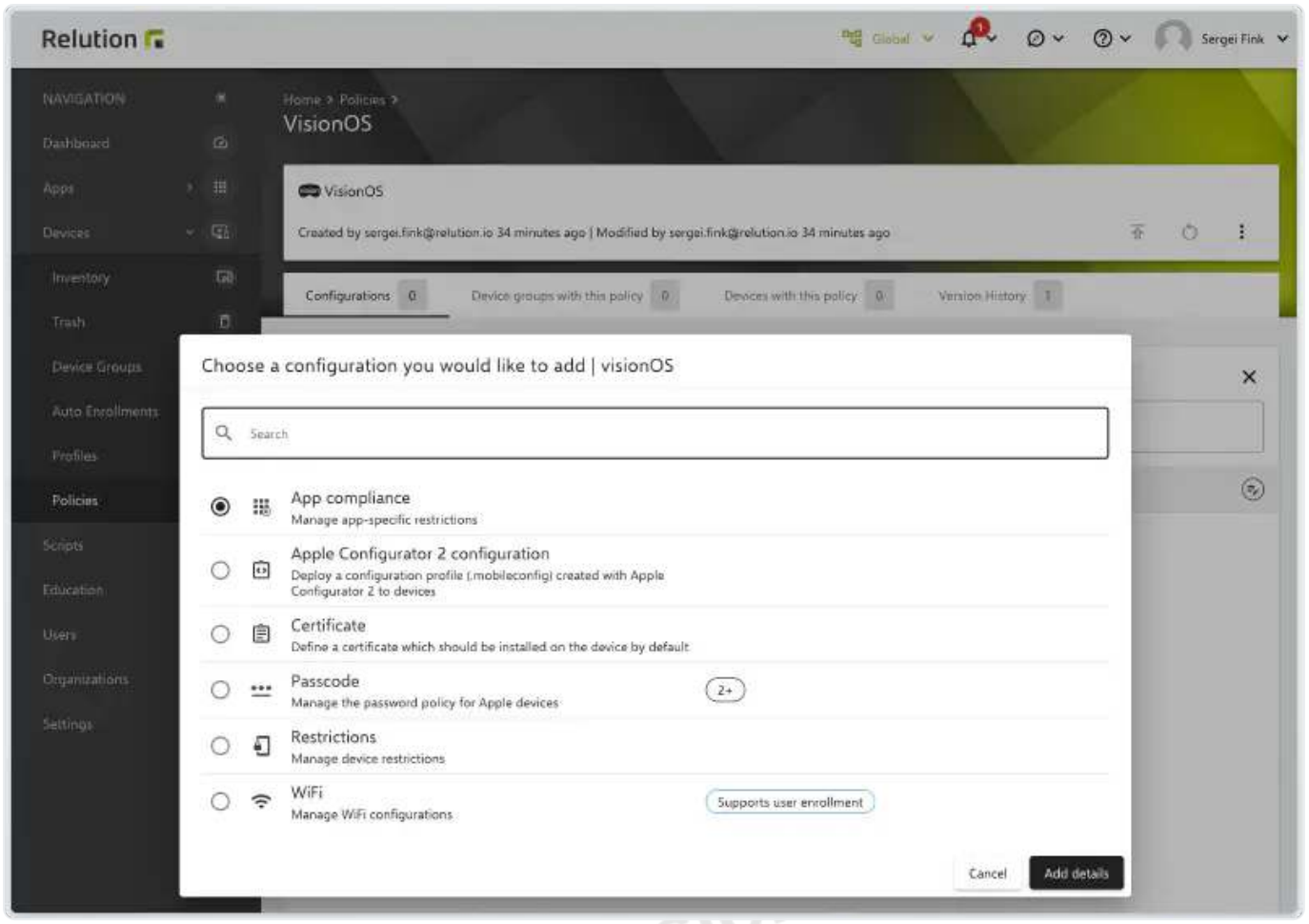
Pour commencer la distribution, seuls les éléments suivants sont nécessaires :

- Un compte Apple School ou Apple Business.
- L’intégration du jeton Apps et livres → de l’organisation dans Relution.
- Des licences acquises pour les applications souhaitées depuis Apple School Manager (ASM) ou Apple Business Manager (ABM).

Configuration de la conformité de l’application

La distribution d’applications sur les appareils Apple Vision (de manière analogue aux appareils iOS) s’effectue via la configuration de politique Conformité App. Elle est sélectionnée sous `Appareils` → `Politiques` dans une politique visionOS via Ajouter une configuration, puis créée via Ajouter des détails.

Pour la version 26.4.0



Comme pour les appareils iOS, la disponibilité des applications est contrôlée dans la section Général sous Type de liste : soit sous forme de liste de blocage (Liste de blocage — Les applications ci-dessous ne sont pas autorisées, valeur par défaut des nouvelles configurations), soit sous forme de liste d'autorisation (Liste d'autorisation : les applications ci-dessous sont autorisées). Les applications sont saisies via Ajouter dans la section Apps bloquées ou Apps autorisées située en dessous.

La liste d'autorisation et la liste de blocage ne sont appliquées que sur les appareils supervisés.

Liste d'autorisation (applications autorisées)

La liste d'autorisation permet de définir explicitement les applications autorisées à être disponibles sur les appareils. Deux options supplémentaires sont disponibles :

- Mettre toutes les applications déployées automatiquement sur la liste verte : les applications distribuées aux utilisateurs des appareils via des déploiements automatiques sont automatiquement ajoutées à la liste d'autorisation.
- Autorisation des invites de sécurité locales, par exemple pour la connexion iCloud (dans le portail : Autoriser les invites secrètes locales (par exemple, iCloud, Google login)) : la boîte

de dialogue système des invites de sécurité locales est ajoutée à la liste d'autorisation afin que ces invites ne soient pas bloquées.

Liste de blocage (applications bloquées)

La liste de blocage permet de masquer ou de bloquer certaines applications sur les appareils visionOS.

Applications requises

La section Apps requises permet de définir les applications à installer obligatoirement sur les appareils. Ajouter propose les sources suivantes (identiques pour la liste d'autorisation et la liste de blocage) :

- Appli Relution App Store : sélection d'applications dans le Relution App Store. Sont proposées les applications des plateformes visionOS et iOS, c'est-à-dire les applications publiques (p. ex. avec licences Apps et livres) et les applications natives téléversées. Les applications iOS ne sont utilisables sur les appareils Apple Vision que si elles sont compatibles avec visionOS.
- Apple App Store App : recherche d'une application dans l'App Store public d'Apple.
- Ajouter une application manuellement : saisie d'une application avec son Nom et son Nom interne (identifiant de bundle).

Pour la version 26.4.0

Si une application requise n'est pas installée sur l'appareil, celui-ci est considéré comme non conforme. L'application n'est installée activement que si la case de la colonne Installation automatique est cochée ; elle est cochée par défaut lors de l'ajout d'une application. Peuvent être installées automatiquement les applications natives du Relution App Store ainsi que les applications de l'App Store dont les licences Apps et livres sont attribuées aux appareils. Les colonnes Licences VPP et Licences VPP disponibles indiquent, pour chaque application, les licences existantes et celles encore libres.

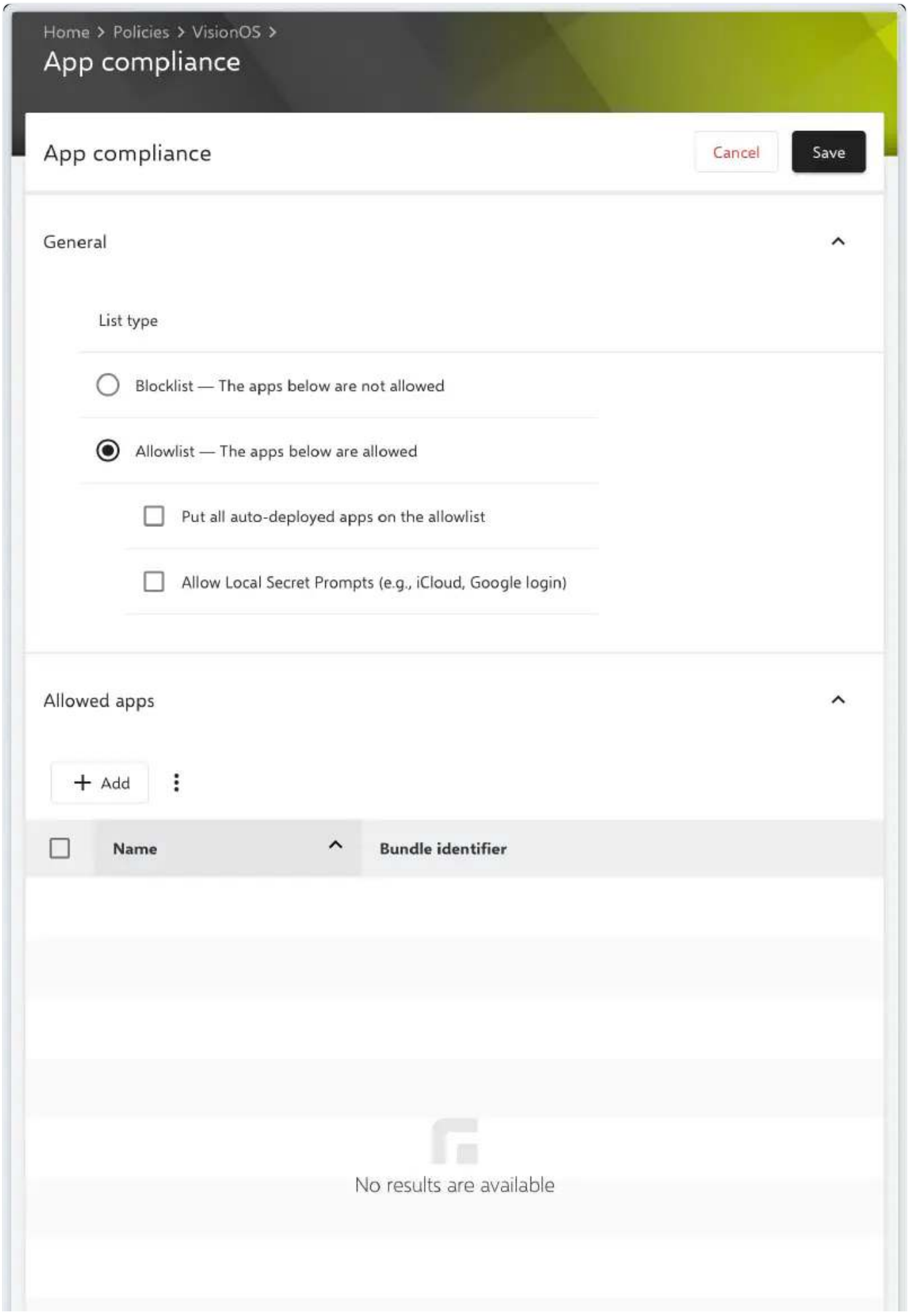
Deux commutateurs sont disponibles au-dessus de la liste :

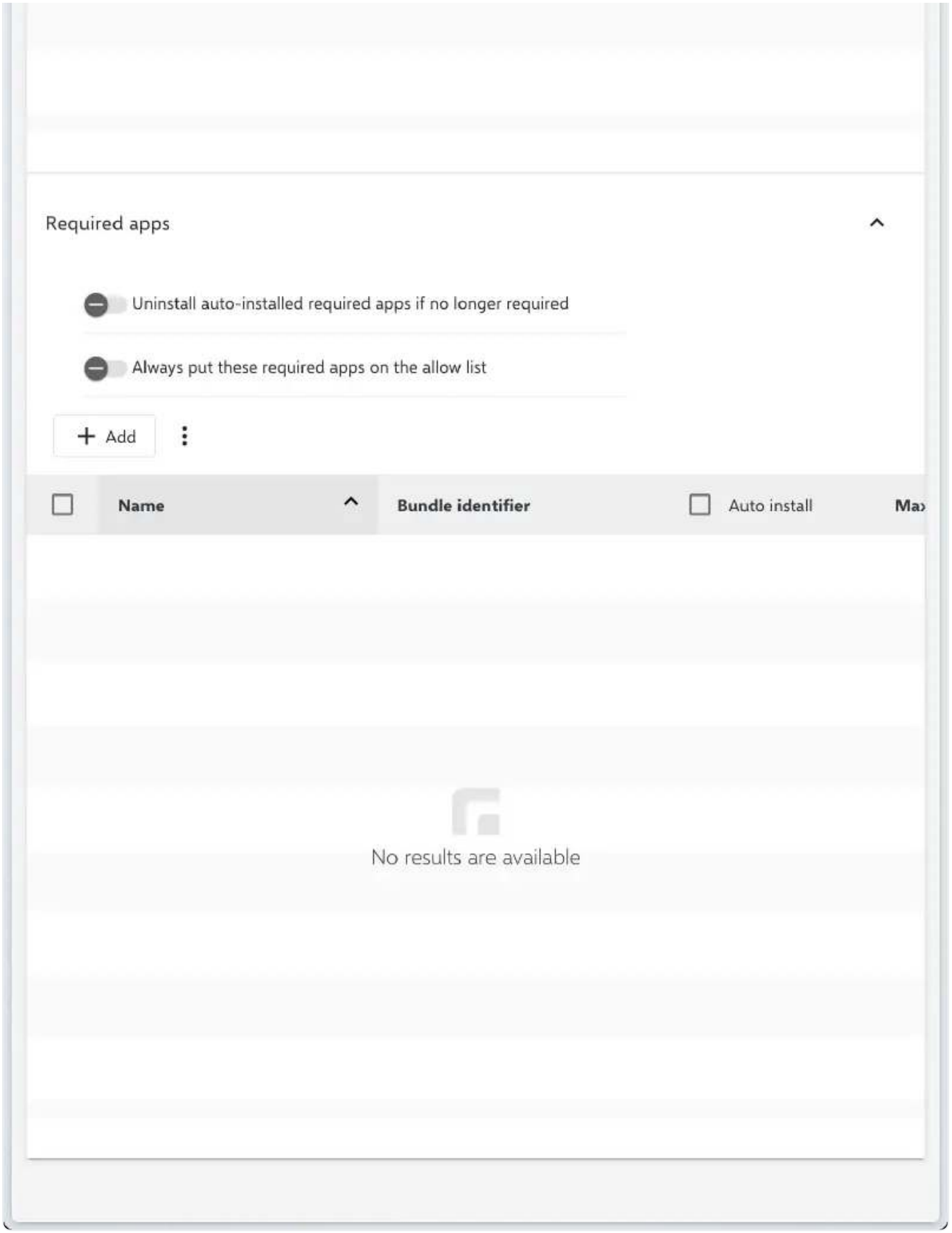
- Désinstallation automatique des applications requises qui ne sont plus nécessaires : si une application requise installée automatiquement est retirée de la configuration, ou si la configuration est retirée de l'appareil, l'application est désinstallée. Le commutateur est désactivé pour les nouvelles configurations.
- Ajout systématique des applications requises à la liste des applications autorisées : si cette politique ou une autre configure une liste d'autorisation pour l'appareil, les applications requises y sont ajoutées.

Lors de l’enregistrement, les listes sont vérifiées afin de détecter les contradictions : une application requise ne doit pas figurer sur la liste de blocage. Si le second commutateur est désactivé pour une liste d’autorisation, toutes les applications requises doivent également figurer sur la liste d’autorisation.

Une fois la configuration terminée, elle peut être enregistrée, publiée et attribuée aux appareils correspondants.

Pour la version 26.4.0


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

Inscription sous watchOS

La configuration iOS Inscription à l'Apple Watch permet d'inscrire et de gérer des appareils Apple Watch (watchOS) dans Relution via un iPhone géré. L'Apple Watch elle-même ne peut pas être ajoutée directement à Relution ; elle est enregistrée via un iPhone couplé et géré dans Relution.

Prérequis

- Un iPhone sous iOS 17 ou version ultérieure, déjà inscrit et géré dans Relution. La configuration est distribuée via la gestion déclarative des appareils d'Apple (Declarative Device Management) et n'atteint que les appareils qui la prennent en charge. Les iPhone plus anciens ne la reçoivent pas, sans qu'aucun avertissement ne s'affiche.
- Une Apple Watch pouvant être couplée à cet iPhone.
- Une connexion Internet active sur l'iPhone.
- Le couplage avec une Apple Watch est autorisé sur l'iPhone. Si l'option Autoriser la montre jumelée est désactivée dans les Restrictions →, aucun couplage n'est possible ; toute Apple Watch déjà couplée est immédiatement découplée et effacée.

Pour la version 26.4.0

Procédure

1. Créer la configuration
    - Sous `Appareils` → `Politiques`, la configuration Inscription à l'Apple Watch est créée dans une politique iOS via Ajouter une configuration.
2. Appliquer la configuration
    - La politique est attribuée à l'iPhone géré.
    - Le couplage ne devrait commencer qu'une fois que l'iPhone a reçu la configuration.
    - La configuration est transmise via la gestion déclarative des appareils. Dans l'onglet Actions de l'iPhone, l'action Synchronisation déclarative de la gestion indique si l'iPhone a accepté la synchronisation. Relution n'indique pas séparément si la configuration elle-même a été appliquée.
3. Coupler l'Apple Watch
    - L'Apple Watch est approchée de l'iPhone configuré.
    - Le processus de couplage est démarré sur l'iPhone.
    - Pendant le couplage, une invitation à accepter l'inscription dans Relution apparaît.

Une fois cette invitation confirmée, l'Apple Watch est enregistrée dans Relution. Une fois le couplage réussi, l'Apple Watch apparaît comme un appareil autonome (watchOS) dans l'inventaire des appareils. Elle reprend l'organisation et l'utilisateur de l'iPhone et est enregistrée comme Appareil appartenant à l'entreprise (COD). Dans les détails de l'iPhone, elle figure également dans l'onglet Dispositifs appariés. Des restrictions ou profils spécifiques pris en charge par watchOS peuvent ensuite être appliqués via les politiques.

Remarques

- Si l'Apple Watch est découplée d'un iPhone, elle perd automatiquement son association MDM.
- Si l'iPhone est supprimé ou retiré dans Relution, l'Apple Watch couplée est également retirée de la gestion.
- Seules les versions watchOS compatibles peuvent être inscrites via cette méthode.

Pour la version 26.4.0

Actions disponibles

Relution propose une sélection d'actions permettant de contrôler et de diriger directement l'Apple Watch. Les actions peuvent être appliquées de manière ciblée à un seul appareil ou, via la sélection multiple dans la liste des appareils, à plusieurs appareils à la fois. Elles peuvent en outre être déclenchées par événement ou de manière planifiée via l'appartenance à des groupes d'appareils : Actions de groupes d'appareils →

Aperçu des actions

Action	Description
Actualiser les informations sur l'appareil	Actualise toutes les informations disponibles sur l'appareil, répertoriées sous Détails.
Déployer l'application Relution Store	Rechercher une application dans le Relution Store et l'installer sur les appareils.
Mettre à jour le profil MDM	Renouvelle les données d'enregistrement MDM sur l'appareil afin de garantir la cohérence avec les paramètres actuels du serveur et du profil.

Configurations disponibles

Une politique est un ensemble d’une ou plusieurs configurations. Chaque politique peut être appliquée à un ou plusieurs appareils simultanément. De plus, une ou plusieurs politiques peuvent être associées à chaque appareil.

Configurations disponibles

Configuration	Description
Conformité de l’application →	Gestion des restrictions spécifiques aux applications
Configuration Apple Configurator 2 →	Applique aux appareils un profil de configuration (`.mobileconfig`) créé avec Apple Configurator 2
Code d’accès →	Politique de code d’accès pour les appareils Apple
Restrictions →	Gestion des restrictions d’appareils
Paramètres de Siri	Gestion des paramètres de Siri
Wi-Fi	Gestion des paramètres Wi-Fi
Certificat	Choisir un certificat qui doit être installé par défaut sur l’appareil

Les configurations Wi-Fi, Certificat et Configuration d’Apple Configurator 2 peuvent être ajoutées plusieurs fois à une politique ; toutes les autres une seule fois.

Code d'accès

La politique de mot de passe Apple définit les exigences de sécurité pour les codes des appareils watchOS.

La politique offre de nombreuses options permettant d'adapter davantage les exigences de sécurité du mot de passe. Cela inclut notamment des exigences relatives à la complexité, à la longueur, à la durée de validité et au nombre de tentatives échouées autorisées.

Dès que la politique est appliquée à un appareil, un code d'accès y est toujours exigé. Les champs laissés vides ne sont pas transmis à l'appareil ; la politique n'impose alors aucune exigence pour ces réglages.

> Un minimum de watchOS 10.x est requis.

Options de configuration

Pour la version 26.4.0

- Autoriser un code d'accès simple (activé par défaut) : autorise les codes contenant des caractères répétés ou des suites croissantes/décroissantes telles que `aaa`, `abc` ou `123`.
- Demander des valeurs alphanumériques (désactivé par défaut) : détermine si le code doit contenir des lettres ou si des chiffres suffisent.
- Longueur minimale du code d'accès : valeurs de 0 à 25 caractères.
- Nombre de caractères spéciaux requis (1-4) : valeurs de 0 à 4.
- Âge maximum du code d'accès (en jours) : nombre de jours au terme desquels un nouveau code doit être défini ; valeurs de 0 à 730.
- Temps d'inactivité (en minutes) : délai maximal de verrouillage automatique après inactivité que l'utilisateur peut sélectionner sur l'appareil.
- Historique du code d'accès : nombre de codes déjà utilisés qui ne peuvent pas être redéfinis ; valeurs de 1 à 50.
- Délai de grâce pour le verrouillage de l'appareil (en minutes) : période après le verrouillage pendant laquelle l'appareil peut encore être déverrouillé sans saisir le code. Avec

Immédiatement, le code est demandé à chaque déverrouillage. Ce réglage ne détermine pas quand l'appareil se verrouille – c'est le rôle de Temps d'inactivité (en minutes).

  - Immédiatement
  - 1 minute
  - 5 minutes
  - 15 minutes
  - 60 minutes
  - 4 heures
- Nombre maximum de tentatives infructueuses : valeurs de 2 à 11.

> Si ce nombre est dépassé, une action d'effacement est déclenchée.

Pour la version 26.4.0

Configuration d'Apple Configurator 2

Cette configuration de politique permet de transférer des fichiers `.mobileconfig` sur les appareils Apple. Un tel fichier peut par exemple contenir une connexion Wi-Fi accompagnée du certificat d'identité correspondant (PKCS#12, `.p12`).

Configuration

Le champ Nom permet d'attribuer un nom à la configuration. Le fichier est importé via le champ de sélection du fichier `.mobileconfig`. Son contenu apparaît ensuite à la place de la sélection de fichier dans le champ Contenu de la charge utile, où il peut être modifié. Le contenu doit être du XML valide. Les profils signés ne sont pas du XML lisible et ne peuvent donc pas être utilisés. Dans Apple Configurator 2, le fichier est par conséquent enregistré sans signature. Si le champ Contenu de la charge utile est vidé, un fichier peut à nouveau être sélectionné.

Des espaces réservés pour l'utilisateur, l'appareil et les certificats peuvent être utilisés dans le champ Contenu de la charge utile. Les espaces réservés disponibles sont affichés sous le formulaire et sont remplacés lors du transfert vers l'appareil, voir Espaces réservés avancés →.

Plusieurs configurations Apple Configurator 2 peuvent être créées par politique. Il est ainsi possible de répartir plusieurs types de configuration sur des configurations distinctes.

Pour la version 26.4.0

Exigences relatives au fichier

Le contenu est vérifié lors de l'enregistrement. Le fichier doit remplir les conditions suivantes :

- Le niveau supérieur contient les clés `PayloadType`, `PayloadVersion` (sous forme de nombre), `PayloadIdentifier`, `PayloadUUID` et `PayloadDisplayName`.
- `PayloadContent` contient exactement un type de configuration. Des charges utiles de certificat peuvent s'y ajouter.

Les fichiers illisibles, ceux auxquels il manque l'une de ces clés ou ceux qui ne contiennent aucune charge utile ou plusieurs types de configuration sont refusés lors de l'enregistrement.

> Seuls les certificats au format PKCS#12 (`com.apple.security.pkcs12`) sont transférés avec la configuration. Les certificats PKCS#1 (`com.apple.security.pkcs1`) sont acceptés lors de la vérification, mais ne sont pas transférés vers l'appareil. Les autres certificats, comme les certificats racine (`com.apple.security.root`), comptent comme

un type de configuration à part entière. Associés à une autre configuration, ils provoquent une erreur lors de l'enregistrement et sont donc déposés dans une configuration distincte.

La configuration proprement dite doit figurer en première position dans `PayloadContent`. Si le fichier contient plusieurs charges utiles du même type, seule la première est transférée vers l'appareil.

Si le fichier contient un type de configuration que Relution propose également sous forme de configuration propre, autorisée une seule fois par politique, cette configuration ne peut plus être ajoutée à la même politique. Sous watchOS, cela concerne Mot de passe → (`com.apple.mobiledevice.passwordpolicy`) et Restrictions → (`com.apple.applicationaccess`).

À l'inverse, un tel fichier est refusé lors de l'enregistrement si la politique contient déjà la configuration correspondante ou une autre configuration Apple Configurator 2 active avec le même type de charge utile.

Exemple

Le fichier suivant transfère une connexion Wi-Fi (`com.apple.wifi.managed`). Le SSID, le mot de passe, les identifiants et les UUID sont des valeurs d'exemple à remplacer par des valeurs réelles. Chaque `PayloadUUID` doit être unique.

Pour la version 26.4.0

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/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>mot-de-passe-WiFi</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>WiFi-Entreprise</string>
   </dict>
  </array>
  <key>PayloadDescription</key>
  <string>Configuration Wi-Fi pour les appareils Apple</string>
  <key>PayloadDisplayName</key>
  <string>Wi-Fi</string>
  <key>PayloadIdentifier</key>
  <string>com.example.wifi</string>
  <key>PayloadOrganization</key>
  <string>Exemple SAS</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

Voici une vue d'ensemble des restrictions watchOS disponibles.

La configuration Les restrictions est disponible pour les appareils watchOS à partir de watchOS 10 (indication watchOS 10+ dans le formulaire). Certaines restrictions portent dans le portail la mention Supervisé et ne s'appliquent qu'aux appareils supervisés ; elles sont signalées en conséquence dans la vue d'ensemble ci-dessous.

Dans le portail, les restrictions sont réparties dans les zones Appareil, Apps (avec les sections Général et Siri), Paramètres, Modifications et Écran de verrouillage. Par défaut, tous les interrupteurs sont activés, à l'exception de Détection forcée du poignet de l'Apple Watch et des deux options permettant d'effectuer la dictée et la traduction uniquement sur l'appareil. Avec les valeurs par défaut, l'appareil n'est donc pas restreint.

L'icône de téléchargement en haut du formulaire permet d'exporter les valeurs configurées, y compris les modifications non enregistrées, dans un fichier CSV.

Pour la version 26.4.0

Appareil

Afficher toutes les restrictions

Apps

La zone Apps est divisée en deux sections : Général et Siri.

Général

Afficher toutes les restrictions

Siri

Afficher toutes les restrictions

Restrictions des paramètres

Afficher toutes les restrictions

Restrictions en matière de modifications

Afficher toutes les restrictions

Restrictions de l’écran de verrouillage

Afficher toutes les restrictions

Pour la version 26.4.0

Conformité de l'application

L’installation d’applications issues d’Apps et livres (VPP dans le portail) sur les appareils Apple Watch est particulièrement simple grâce à la politique de conformité des applications (Conformité App) de Relution. Cette configuration permet une distribution simple et centralisée des applications sur un grand nombre d’appareils.

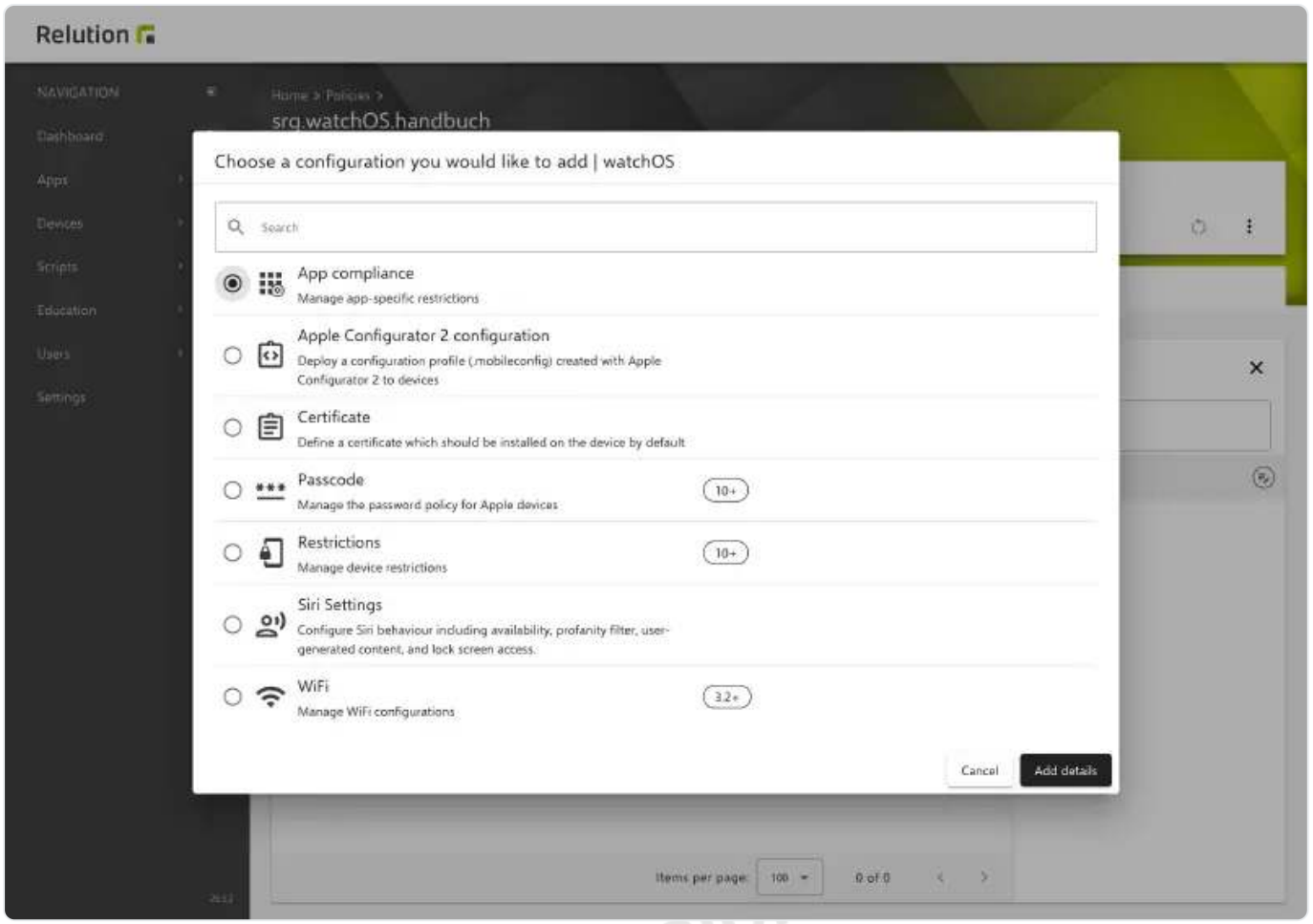
Pour commencer la distribution, seuls les éléments suivants sont nécessaires :

- Un compte Apple School ou Apple Business.
- L’intégration du jeton Apps et livres → de l’organisation dans Relution.
- Des licences acquises pour les applications souhaitées depuis Apple School Manager (ASM) ou Apple Business Manager (ABM).

Configuration de la conformité de l’application

La distribution d’applications sur les appareils Apple Watch (de manière analogue aux appareils iOS) s’effectue via la configuration de politique Conformité App. Elle est sélectionnée sous `Appareils` → `Politiques` dans une politique watchOS via Ajouter une configuration, puis créée via Ajouter des détails.

Pour la version 26.4.0



Comme pour les appareils iOS, la disponibilité des applications est contrôlée dans la section Général sous Type de liste : soit sous forme de liste de blocage (Liste de blocage — Les applications ci-dessous ne sont pas autorisées, valeur par défaut des nouvelles configurations), soit sous forme de liste d'autorisation (Liste d'autorisation : les applications ci-dessous sont autorisées). Les applications sont saisies via Ajouter dans la section Apps bloquées ou Apps autorisées située en dessous.

La liste d'autorisation et la liste de blocage ne sont appliquées que sur les appareils supervisés.

Liste d'autorisation (applications autorisées)

La liste d'autorisation permet de définir explicitement les applications autorisées à être disponibles sur les appareils. Deux options supplémentaires sont disponibles :

- Mettre toutes les applications déployées automatiquement sur la liste verte : les applications distribuées aux utilisateurs des appareils via des déploiements automatiques sont automatiquement ajoutées à la liste d'autorisation.
- Autorisation des invites de sécurité locales, par exemple pour la connexion iCloud (dans le portail : Autoriser les invites secrètes locales (par exemple, iCloud, Google login)) : la boîte

de dialogue système des invites de sécurité locales est ajoutée à la liste d'autorisation afin que ces invites ne soient pas bloquées.

Liste de blocage (applications bloquées)

La liste de blocage permet de masquer ou de bloquer certaines applications sur les appareils watchOS.

Applications requises

La section Apps requises permet de définir les applications à installer obligatoirement sur les appareils. Ajouter propose les sources suivantes (identiques pour la liste d'autorisation et la liste de blocage) :

- Appli Relution App Store : sélection d'applications publiques compatibles watchOS dans le Relution App Store, p. ex. applications avec licences Apps et livres. Il n'existe pas de recherche directe dans l'App Store public d'Apple pour watchOS ; les applications doivent avoir été ajoutées au préalable au Relution App Store.
- Ajouter une application manuellement : saisie d'une application avec son Nom et son Nom interne (identifiant de bundle).

Pour la version 26.4.0

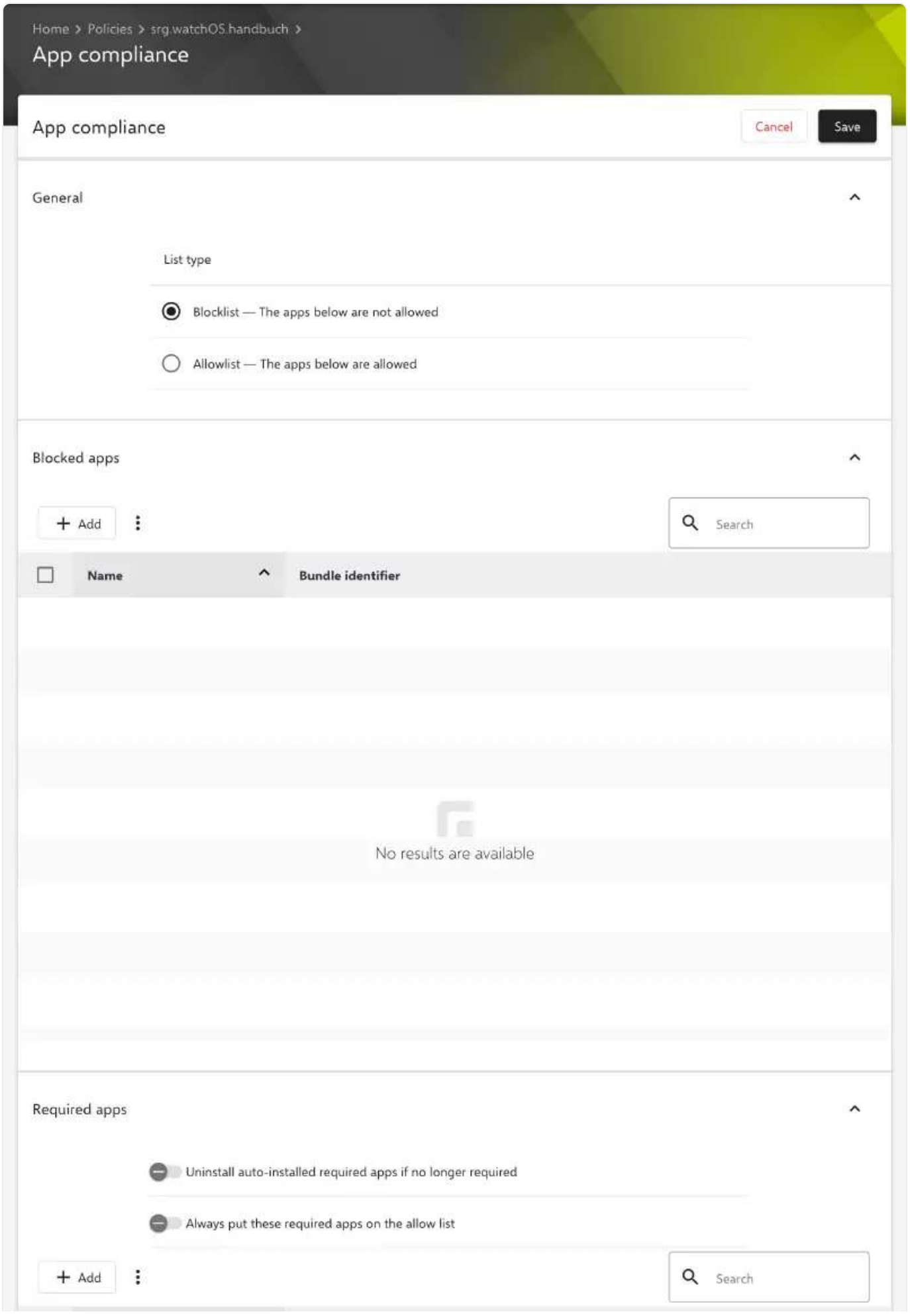
Les applications natives (téléversées) ne sont pas disponibles dans les politiques watchOS, car Relution leur attribue la plateforme iOS.

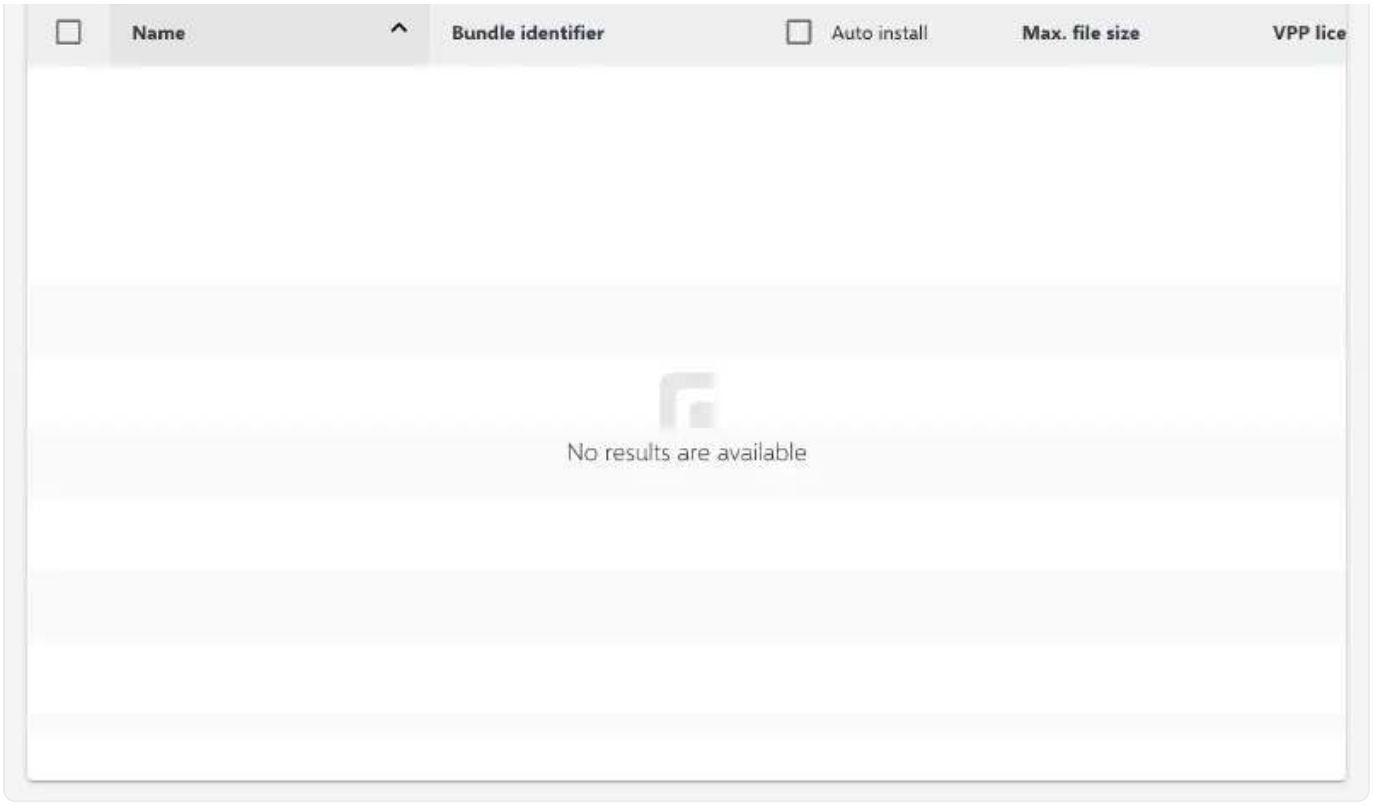
Si une application requise n'est pas installée sur l'appareil, celui-ci est considéré comme non conforme. L'application n'est installée activement que si la case de la colonne Installation automatique est cochée ; elle est cochée par défaut lors de l'ajout d'une application. Les colonnes Licences VPP et Licences VPP disponibles indiquent, pour chaque application, les licences existantes et celles encore libres.

Deux commutateurs sont disponibles au-dessus de la liste :

- Désinstallation automatique des applications requises qui ne sont plus nécessaires : si une application requise installée automatiquement est retirée de la configuration, ou si la configuration est retirée de l'appareil, l'application est désinstallée. Le commutateur est désactivé pour les nouvelles configurations.
- Ajout systématique des applications requises à la liste des applications autorisées : si cette politique ou une autre configure une liste d'autorisation pour l'appareil, les applications requises y sont ajoutées.

Une fois la configuration terminée, elle peut être enregistrée, publiée et attribuée aux appareils correspondants.


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



Pour la version 26.4.0

Groupes Éducation

Les groupes Éducation sont des groupes d'appareils de type Éducation. Ils regroupent des stratégies qui sont automatiquement appliquées aux appareils des élèves participants pendant la durée d'un cours. Le groupe et ses stratégies sont préparés dans le portail ; dans Relution Teacher, ils sont sélectionnés en tant que Configurations dans le modèle de cours. Il est ainsi possible de déployer des paramètres MDM même étendus uniquement pendant le cours.

Fonctionnement

Pour un groupe Éducation, seules les stratégies sont configurées. Relution gère automatiquement les appareils membres via les cours : les appareils des élèves participants sont ajoutés au démarrage d'un cours qui utilise ce groupe comme configuration, puis retirés à la fin du cours. Les appareils ne peuvent pas être affectés manuellement à ce type de groupe, et aucun filtre n'est évalué. Les appareils de l'enseignant ne deviennent pas membres du groupe.

- Au démarrage du cours, les appareils des élèves sont ajoutés au groupe et reçoivent les stratégies liées.
- Pendant le cours, l'affectation est mise à jour dès que des élèves sont ajoutés ou retirés. Si les configurations du cours en cours sont modifiées, les appareils des élèves sont ajoutés aux groupes Éducation nouvellement sélectionnés et retirés de ceux désélectionnés.
- À la fin du cours, les appareils sont de nouveau retirés du groupe et les stratégies ne s'appliquent plus.

> Les stratégies d'infrastructure comme le Wi-Fi ne devraient pas être distribuées via un groupe Éducation : elles seraient retirées des appareils à la fin du cours.

Créer un groupe Éducation

Les groupes Éducation sont créés comme les autres groupes d'appareils sous `Appareils` → `Groupes d'appareils` via Ajouter. Éducation est sélectionné comme Type de groupe. Les stratégies souhaitées sont ensuite attribuées au groupe. Le type Éducation n'est disponible qu'avec une licence Education ou Free.

> Si un groupe d'appareils statique ou dynamique existant est ultérieurement converti en type Éducation, Relution retire tous les appareils existants du groupe lors de l'enregistrement. Les

Pour la version 26.4.0

stratégies liées ne s’appliquent donc plus à ces appareils.

Le nom, la description et les stratégies liées sont affichés dans Relution Teacher. Des noms et descriptions explicites facilitent donc la sélection pendant le cours.

Informations générales sur les groupes d’appareils : Groupes d’appareils →.

Autorisation pour les enseignants

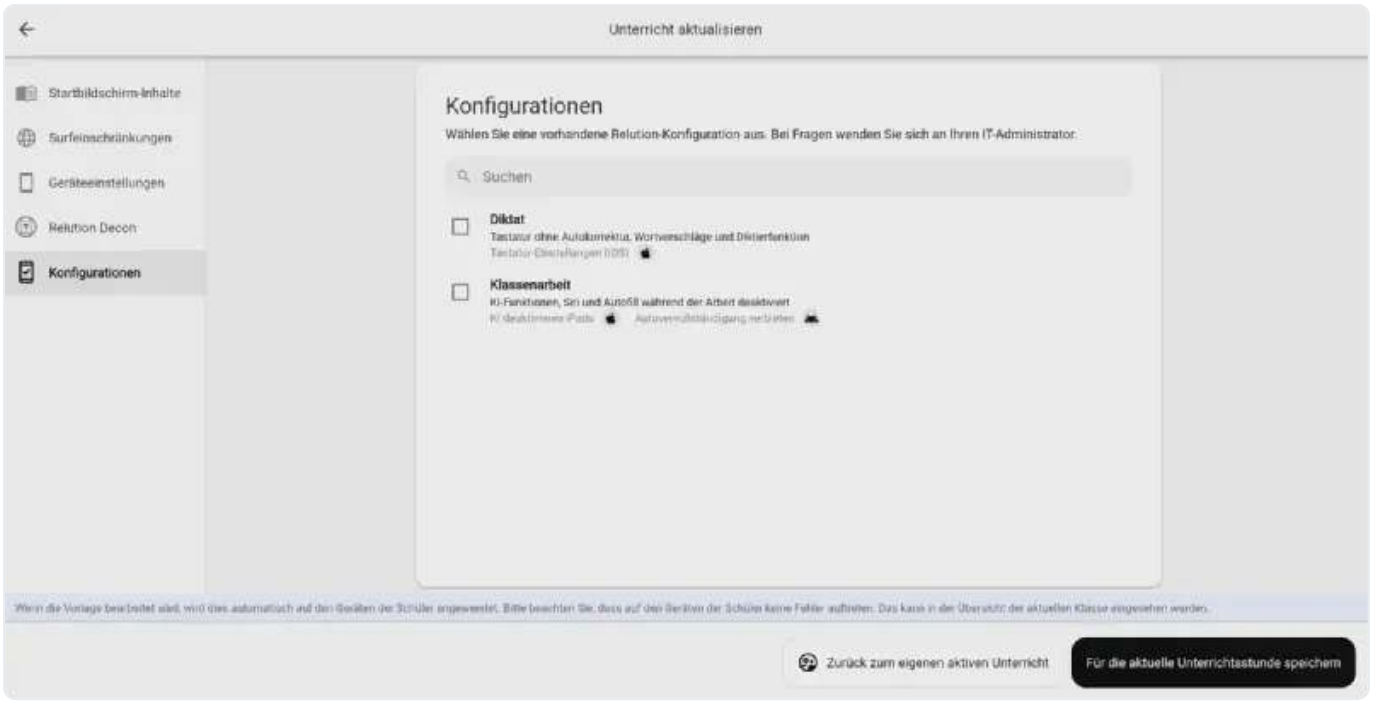
Les enseignants autorisés à voir et à sélectionner des configurations sont déterminés par l’autorisation de lecture `Éducation` → `Groupes d’appareils de cours` dans l’éditeur de rôles. Elle complète l’autorisation `Éducation` → `Utiliser l’application pour enseignants` ; les deux sont nécessaires pour sélectionner des configurations. Sans cette autorisation, aucune configuration n’est affichée dans Relution Teacher. Elle est déjà incluse dans les rôles prédéfinis qui autorisent l’utilisation de l’application pour enseignants. Les rôles personnalisés ne la reçoivent pas automatiquement ; l’autorisation `Éducation` → `Groupes d’appareils de cours` y est ajoutée manuellement si nécessaire.

En savoir plus sur les rôles et les droits : Autorisations →.

Utilisation dans Relution Teacher

Dans le modèle de cours, la zone Configurations liste les groupes Éducation de l’organisation avec leur nom, leur description et les stratégies liées. Une ou plusieurs configurations peuvent être sélectionnées. S’il n’existe aucun groupe Éducation, la mention Aucune configuration disponible s’affiche ; le modèle peut tout de même être utilisé normalement.

Pour la version 26.4.0



Détails sur le modèle de cours : Relution Teacher →.

Pour la version 26.4.0

Apple Classroom

Relution permet de distribuer la configuration nécessaire pour utiliser l'application Classroom sur les appareils Apple gérés par Relution (iPadOS / macOS). Apple Classroom est une application utilisée dans le secteur éducatif pour permettre aux enseignants de contrôler et de surveiller les appareils des élèves pendant les cours.

Prérequis

1. Deux appareils enregistrés dans Relution (en mode Supervision).
2. Au moins deux utilisateurs.
3. L'application Apple Classroom doit être installée sur un appareil (enseignant).
4. Une licence Education ou Free valide pour Relution.

Préparation du réseau

1. Les appareils doivent être connectés au même réseau pour utiliser Classroom.
2. La communication entre les clients doit être possible dans le réseau Wi-Fi.
3. Port 3284: Pour le partage de documents via Classroom.
4. Port 3285: Pour la communication avec l'application Classroom.

Pour la version 26.4.0

Préparation des utilisateurs

1. Au moins deux utilisateurs sont nécessaires (un enseignant et un élève).
2. Les classes doivent être créées sous `Éducation` → `Classes`. Cette étape peut être automatisée par une importation via une interface (par exemple LDAP ou Apple School Manager) ; les utilisateurs et les classes peuvent aussi être importés via un fichier CSV. Articles du manuel pertinents :
   - Importation CSV : Importer des utilisateurs via CSV →
   - Intégration LDAP : Configuration LDAP →
   - Importation ASM : Importation Apple School Manager →
   - Import SchulConnex : Import SchulConnex →
   - OneRoster : Interface OneRoster →
3. Les enseignants et les élèves sont inscrits dans la classe soit individuellement, soit via des groupes d'utilisateurs, par exemple via les groupes `UIT - Teacher` / `UIT - Student`. Aucune appartenance à un groupe particulier n'est requise pour Apple Classroom ; seule

compte l'inscription en tant qu'enseignant ou élève dans une classe. Pour les groupes par défaut `Teacher` / `Student` et leurs droits dans Relution, voir Fonction d'éducation →.

Configuration

Relution distribue des `configurations éducatives` aux appareils. Ces configurations contiennent des informations sur les classes et les élèves qui peuvent être contrôlés par les enseignants. Les classes qui ne comptent pas au moins un enseignant et un élève ne sont pas reprises dans la configuration éducative et n'apparaissent donc pas dans Apple Classroom. En plus des classes, un cours ad hoc en cours dans Relution Teacher est repris dans la configuration éducative sous forme de groupe distinct, voir Relution Teacher →.

Pour que la distribution de la configuration éducative réussisse, les utilisateurs doivent être assignés aux appareils. L'assignation peut être effectuée manuellement ou via un fichier CSV. Alternativement, l'assignation a lieu lors de l'inscription automatisée des appareils (ADE, DEP dans le portail) : dans le profil DEP sous `Appareils` → `Profils`, l'option Nom d'utilisateur + Mot de passe est choisie pour Authentification utilisateur. L'appareil est alors assigné à l'utilisateur qui se connecte lors de l'inscription. Détails : Profil pour l'ADE →. Il convient de noter que les appareils déjà inscrits doivent être réinitialisés (`supprimés`) puis réinscrits si les utilisateurs sont assignés de cette manière.

Les iPad partagés sans utilisateur assigné reçoivent la configuration éducative via les classes enregistrées dans la configuration Réglages iPad partagés d'une stratégie, voir Listes de classes (iPad partagé) →.

Pour la version 26.4.0

Dépannage

Parfois, un ou plusieurs utilisateurs peuvent apparaître comme `hors ligne` pour l'enseignant. Causes possibles et solutions :

1. Configuration éducative invalide ou expirée:
   - Si la configuration est invalide, elle doit être réinstallée. Pour ce faire, l'utilisateur doit être retiré de la classe et réassigné.
   - Si les classes ont été créées automatiquement via LDAP, l'utilisateur doit être supprimé de l'appareil et réassigné. Remarque : Des problèmes peuvent survenir lors de l'utilisation de groupes d'appareils dynamiques basés sur les utilisateurs.
2. Configuration réseau incorrecte (ports ou réseaux Wi-Fi):
   - Si les ports requis sont fermés ou si les appareils se trouvent dans des réseaux WLAN différents, des problèmes de connexion peuvent se produire.

- Pour vérifier cela, un point d’accès mobile peut être utilisé pour connecter les appareils entre eux. Si les appareils apparaissent comme `en ligne` dans cet environnement, la configuration réseau doit être ajustée en conséquence.

Pour la version 26.4.0

Importation Apple School Manager

La configuration d'importation ASM permet à Relution de créer de nouveaux utilisateurs à partir des données d'Apple School Manager (ASM) ou de synchroniser des utilisateurs existants avec les comptes Apple gérés (Identifiant Apple géré dans le portail) issus d'ASM. Les classes d'ASM peuvent en outre être importées.

Le sens inverse, c'est-à-dire la création de comptes Apple gérés dans ASM à partir des données de Relution, est décrit sous SFTP Upload →.

Prérequis

- Un jeton ADE valide (inscription automatisée des appareils, jeton DEP dans le portail) dans l'organisation dans laquelle la configuration doit être créée.
- Des comptes Apple gérés regroupés dans ASM dans au moins une classe (au minimum un élève et un enseignant).

Pour la version 26.4.0

Configuration

1. Accéder aux paramètres : `Paramètres` → `Éducation` → `Configuration de l'importation d'Apple School Manager`
2. Ajouter une nouvelle configuration : Une nouvelle configuration est créée via Ajouter.
3. Saisir le nom du prestataire : Un nom unique est saisi sous Nom du prestataire. Ce nom ne peut plus être modifié après l'enregistrement, car Relution l'utilise pour retrouver les objets déjà synchronisés.
4. Sélectionner le compte DEP : Sous Compte DEP, le bouton Sélectionnez permet de choisir le compte DEP utilisé pour accéder à Apple School Manager. Sans compte DEP, Vérifier la connexion, Localisation des sites et Prévisualisation ne sont pas disponibles, et la configuration ne peut pas être enregistrée.
5. Vérifier la connexion : Vérifier la connexion permet de contrôler si une connexion à Apple School Manager est possible avec le compte DEP.
6. Sélectionner les sites : Sous Localisation des sites, un ou plusieurs sites ASM sont choisis pour l'importation via Sélectionnez. Seules les classes de ces sites sont importées, ainsi

que les enseignants et les élèves membres de l'une de ces classes.

7. Aperçu des classes : Sous Prévisualisation, le bouton Afficher présente les classes qui seront finalement importées.

Dans l'organisation globale et dans les méta-organisations, l'option Localisation des sites n'existe pas. La configuration y est d'abord enregistrée avec le compte DEP. Ensuite, la zone Associer des objets à des organisations permet de définir quels sites ASM sont importés dans quelle organisation. Sans site associé, aucune synchronisation n'a lieu.

Paramètres de synchronisation

La zone Paramètres de synchronisation définit les objets que Relution crée à partir d'ASM et ce qu'il advient des objets qui ne sont plus fournis par ASM.

Créer de nouveaux utilisateurs Relution

- Activé par défaut.
- Relution crée un nouvel utilisateur pour chaque utilisateur ASM pour lequel aucun utilisateur Relution correspondant n'est trouvé. La recherche s'appuie sur l'association issue des synchronisations précédentes, le compte Apple géré et les règles de correspondance activées sous Avancé.
- Les utilisateurs trouvés sans système source (par exemple créés manuellement) ou issus de la même configuration ASM sont associés et repris à la place. Ils reçoivent la configuration ASM comme système source.
- Les utilisateurs d'autres systèmes sources (par exemple LDAP) ne sont pas associés. S'ils ont la même adresse e-mail ou le même nom d'utilisateur que l'utilisateur à créer, la création échoue (erreur de synchronisation Duplicata de courrier électronique ou Nom d'utilisateur en double).
- Si l'option est désactivée, seuls les utilisateurs existants sont associés. Les utilisateurs ASM sans utilisateur Relution correspondant ne sont pas importés.

Pour la version 26.4.0

Mise à jour de l'Identifiant Apple géré pour l'utilisateur Relution correspondant de n'importe quel système source

- Désactivé par défaut.
- Écrase le champ Identifiant Apple géré d'un utilisateur issu d'un autre système source (par exemple LDAP) si l'utilisateur ASM peut être associé à cet utilisateur au moyen de l'une des règles de correspondance activées sous Avancé. Les autres données de l'utilisateur et son système source restent inchangés.

- L’option ne s’applique qu’aux utilisateurs ASM qui n’ont été ni associés ni créés, en pratique uniquement lorsque Créer de nouveaux utilisateurs Relution est désactivé.

Synchroniser les classes

- Activé par défaut.
- Importe depuis ASM les classes des sites sélectionnés et les crée ou les met à jour dans Relution.
- Les classes pour lesquelles aucun enseignant synchronisé ou aucun élève synchronisé n’existe dans Relution sont ignorées (erreur de synchronisation Des membres de la classe manquent à l’appel).
- Recommandé uniquement si :
  - aucune donnée (classe) n’est encore présente dans Relution ;
  - les classes ne sont pas créées manuellement dans Relution ;
  - aucun système LDAP n’est utilisé.
- Important : si les classes sont déjà synchronisées via LDAP, ce point est déconseillé.

Action lorsqu’un utilisateur est supprimé dans ASM

- Définit ce qu’il advient des utilisateurs de cette configuration qui ne sont plus fournis lors d’une synchronisation :
  - Aucun (par défaut) : les utilisateurs restent inchangés ;
  - Désactiver : les utilisateurs sont désactivés dans Relution ;
  - Supprimer : les utilisateurs sont supprimés dans Relution.
- Sont concernés tous les utilisateurs dont le système source est la configuration ASM, c’est-à-dire les utilisateurs nouvellement créés comme les utilisateurs associés qui n’avaient auparavant aucun système source (par exemple créés manuellement).
- Les utilisateurs d’autres systèmes sources (par exemple LDAP) dont seul le compte Apple géré a été mis à jour restent inchangés. Leur compte Apple géré n’est pas supprimé.
- Si une synchronisation ne fournit aucun utilisateur, par exemple en raison d’un problème de connexion ou d’une erreur de configuration, aucun utilisateur n’est désactivé ni supprimé.

Action lorsqu’une classe est supprimée dans ASM

- Définit si les classes sont supprimées dans Relution lorsqu’elles sont supprimées dans ASM : Aucun (par défaut) ou Supprimer.
- Si aucune classe n’a été synchronisée, cette option est sans effet.

Pour la version 26.4.0

Synchronisation automatique via une expression cron

- Définit la fréquence à laquelle Relution importe automatiquement les informations depuis ASM.
- Par défaut, la synchronisation a lieu tous les jours à 6 h et à 21 h (`0 0 6,21 * * ?`).

Avancé

La zone Avancé définit comment les utilisateurs ASM sont associés aux utilisateurs Relution existants et quelle valeur d'ASM sert de nom d'utilisateur.

Correspondance entre l'utilisateur ASM et l'utilisateur Relution

- Définit les règles selon lesquelles un utilisateur ASM est associé à un utilisateur Relution existant. Plusieurs règles peuvent être actives simultanément.
- Avant ces règles, la synchronisation recherche toujours d'abord un utilisateur Relution déjà associé à l'utilisateur ASM ou possédant le même compte Apple géré.
- Les règles activées sont ensuite vérifiées dans cet ordre. La première règle applicable est retenue :
  1. Faire correspondre l'Identifiant Apple géré de l'utilisateur ASM à l'adresse électronique de l'utilisateur Relution (par défaut : activé)
  2. Faire correspondre l'adresse électronique de l'utilisateur ASM à celle de l'utilisateur Relution (par défaut : désactivé)
  3. Faire correspondre le nom de l'utilisateur ASM au nom d'utilisateur de l'utilisateur Relution (par défaut : désactivé)
  4. Faire correspondre le nom et le prénom de l'utilisateur ASM au nom et au prénom de l'utilisateur Relution (par défaut : désactivé)
- Seuls les utilisateurs Relution de la même organisation sans système source ou issus de cette configuration ASM sont pris en compte. Les utilisateurs d'autres systèmes sources (par exemple LDAP) ne sont pas repris. Si Mise à jour de l'Identifiant Apple géré pour l'utilisateur Relution correspondant de n'importe quel système source est activé, les mêmes règles (sans la vérification préalable) déterminent pour quel utilisateur d'un autre système source seul le compte Apple géré est mis à jour.
- Remarque : si Créer de nouveaux utilisateurs Relution n'a pas été sélectionné et qu'aucune des règles ne permet une correspondance, aucune association n'est établie entre les deux systèmes.

Pour la version 26.4.0

Affectation de l’utilisateur ASM à l’utilisateur Relution

- Le champ Champ de l’utilisateur ASM à utiliser comme nom d’utilisateur Relution définit quelle valeur issue d’ASM est utilisée comme nom d’utilisateur dans Relution. Les choix possibles sont Nom (par défaut), Identifiant Apple géré et E-Mail.
- Remarque : à chaque synchronisation, le nom d’utilisateur ainsi que le prénom et le nom des utilisateurs associés sont repris d’ASM. L’adresse e-mail dans Relution est remplacée par le compte Apple géré, et l’utilisateur est activé.

Synchronisation

La synchronisation s’exécute automatiquement selon la planification définie. Elle est lancée manuellement dans la liste des configurations via Synchronisation dans le menu contextuel, ou dans la vue détaillée d’une configuration via l’icône Synchronisation.

Les enseignants et les élèves synchronisés sont ajoutés au groupe par défaut `Teacher` ou `Student` de leur organisation. Pour en savoir plus sur ces groupes : Fonction d’éducation →.

La vue détaillée affiche les résultats des synchronisations séparément pour Utilisateurs et Cours, notamment avec Prochaine synchronisation prévue, Dernière réalisation et Succès. La colonne Erreurs de synchronisation permet d’afficher le détail des erreurs, par exemple Duplicata de courrier électronique, Nom d’utilisateur en double, Des membres de la classe manquent à l’appel ou Échec de la synchronisation des objets du fichier.

Pour la version 26.4.0

Lier l'organisation

Avant de pouvoir enrôler des appareils Android via Android Enterprise, l'organisation Relution doit d'abord être liée à une organisation Google. Ce lien permet aux organisations d'avoir un contrôle total sur leurs appareils Android et de les gérer efficacement, notamment en ce qui concerne la configuration, la gestion des applications et les règles de sécurité.

Enregistrement de l'organisation Relution pour Android Enterprise

Pour ce faire, créer un compte Google approprié dans le portail Relution sous `Paramètres` → `Spécifique à la plate-forme de l'appareil` → `Android pour les entreprises` :

- Cliquer sur S'inscrire maintenant et sélectionner un compte Google existant ou en créer un nouveau.
- Lors de la création d'un nouveau compte Google, choisir entre Pour moi ou Pour mon entreprise et lire l'accord lié à Google Managed Play Store.
- Après avoir accepté le contrat, confirmer le champ J'ai lu et j'accepte le contrat Google Play et cliquer sur Confirmer.
- En cliquant sur Terminer l'enregistrement, le retour au portail de Relution s'effectue automatiquement.

Pour la version 26.4.0

Au retour, le lien est enregistré automatiquement ; aucune étape d'enregistrement supplémentaire n'est nécessaire. L'onglet Général affiche ensuite l'ID de l'organisation et le Type d'entreprise. Le nom d'affichage, la couleur primaire et le logo peuvent, si besoin, être adaptés dans l'onglet Informations sur le compte, voir Informations sur le compte →.

> Seuls les comptes Google non gérés peuvent être utilisés pour établir un lien vers le Google Managed Play Store. Les comptes gérés par des organisations pour les employés ne sont pas possibles.

> La nouvelle fonctionnalité Multi EMM est maintenant disponible. Elle permet à un administrateur informatique de lier plusieurs EMM à son compte de domaine Google géré. Google Multiple EMM Provides →

Pour supprimer un lien existant, y compris les conséquences, voir Supprimer l'organisation →.

ID d’Organisation (Organization ID)

Dans Relution, chaque client / organisation doit être lié à son propre compte Google. Cela garantit que chaque client reçoit un ID d’Organisation unique de Google et peut être géré de manière autonome.

Pour les organisations Relution liées à Google Enterprise il y a plusieurs années, le type d’entreprise affiche souvent encore Compte GooglePlay Enterprise. Pour les organisations nouvellement liées, Google crée désormais automatiquement un domaine Google géré avec son propre ID d’Organisation unique. Pour les organisations plus anciennes, Google propose une mise à niveau du Compte GooglePlay Enterprise vers un domaine Google géré. Relution affiche à cet effet, sous `Paramètres` → `Spécifique à la plate-forme de l'appareil` → `Android pour les entreprises`, dans l’onglet Général, un avis et le bouton Mise à niveau (droit de modification des paramètres Android Enterprise requis). Le bouton ouvre dans un nouvel onglet l’assistant de mise à niveau fourni par Google ; une fois celui-ci terminé, Relution met automatiquement à jour le type d’entreprise (voir aussi la section Mettre à niveau l’entreprise →).

Mise à niveau du compte GooglePlay Enterprise vers un domaine Google géré

Pour la version 26.4.0

> Testé et confirmé par Google (état 08/2026) : la mise à niveau peut être effectuée sans risque, même lorsque plusieurs organisations Relution sont liées au même compte Google Play Enterprise et au même ID d’Organisation.

- Risque lors de la mise à niveau : aucun risque n’est connu. Le processus a été testé avec succès et se déroule sans erreur.
- Effet sur les appareils Android déjà inscrits : ils ne sont ni réinitialisés ni modifiés d’une autre manière par la mise à niveau.
- Compte Google Play Enterprise lié plusieurs fois : même si un compte Google Play Enterprise est lié à plusieurs organisations Relution qui partagent le même ID d’Organisation, la mise à niveau est possible sans problème. Il n’existe pas de mise à niveau séparée pour des organisations Relution individuelles ; la mise à niveau s’applique automatiquement à toutes les organisations Relution liées (voir Portée de la mise à niveau).
- Recommandation : la mise à niveau vers un domaine Google géré devrait être effectuée.
- Portée de la mise à niveau : la mise à niveau s’applique à l’ensemble de l’ID d’Organisation Google et donc à toutes les organisations Relution qui y sont liées. Il suffit donc de la lancer une seule fois via l’une des organisations Relution liées.

Ne pas scinder un ID d’Organisation Google en déconnectant des organisations Relution individuelles

> Si plusieurs organisations Relution sont liées au même ID d’Organisation Google, aucune de ces connexions ne doit être supprimée dans l’onglet Paramètres du compte via Supprimer Android Enterprise afin de scinder ultérieurement l’ID d’Organisation. Comme décrit dans l’article Supprimer l’organisation →, l’organisation Relution concernée perd le contrôle de ses appareils Android Enterprise, quelle que soit l’option choisie. Avec les options Supprimer l’Enterprise et les appareils connus de Relution et Supprimer l’Enterprise et les appareils, toutes les inscriptions existantes de l’organisation Relution concernée sont en outre irrémédiablement perdues et les appareils sont réinitialisés. L’option Supprimer l’Enterprise et les appareils supprime en plus les appareils que Relution ne connaît pas dans cette organisation, c’est-à-dire également les appareils des autres organisations Relution ayant le même ID d’Organisation. Il n’est pas possible de rétablir ultérieurement la connexion pour reprendre le contrôle des appareils.

Pour une attribution durablement univoque entre organisation Relution et ID d’Organisation Google, seules de nouvelles organisations Relution devraient être liées, chacune avec son propre nouveau compte Google.

Pour la version 26.4.0

Paramètres de l’organisation liée

Après la liaison, la page `Paramètres` → `Spécifique à la plate-forme de l'appareil` → `Android pour les entreprises` se divise en onglets Général, Google Play géré, Informations sur le compte, Inscriptions et Paramètres du compte. Les modifications nécessitent le droit de modifier les paramètres Android Enterprise.

Informations sur le compte

L’onglet Informations sur le compte comprend deux zones :

- Apparence : Nom d’affichage de l’entreprise et Couleur primaire (code couleur hexadécimal, par ex. `#ffffff`) sont des champs obligatoires et sont appliqués avec Enregistrer. Un Logo de l’organisation au format JPEG ou PNG est appliqué directement après le téléversement. Relution transmet ces informations à l’Android Enterprise chez Google.
- Informations sur les contacts : affiche en lecture seule les informations enregistrées chez Google, réparties entre Contact de notification (e-mail), Délégué à la protection des données et Représentant de l’UE (chacun avec nom, e-mail et numéro de téléphone). Selon l’avis

affiché dans le portail, elles se modifient sur play.google.com/work/adminsettings →. La zone n'apparaît que si Google fournit des informations de contact.

Conditions d'utilisation

Dans l'onglet Inscriptions, la zone Conditions d'utilisation permet de gérer des textes que Relution transmet à l'Android Enterprise chez Google. Chaque entrée se compose d'un En-tête et d'un Contenu. Lors de l'ajout ou de la modification, un onglet distinct est disponible pour chaque langue, dans lequel les deux champs sont obligatoires ; le texte de la langue par défaut sert de texte par défaut. L'ordre des entrées peut être modifié par glisser-déposer. Les modifications sont appliquées avec Enregistrer.

Zero-Touch

Également dans l'onglet Inscriptions, Relution intègre la vue Zero-Touch de Google dans la zone Android Enterprise Zero Touch, voir Zero Touch Enrollment →.

Réparer l'inscription

Nouveau dans 26.5

Pour la version 26.4.0

Dans l'onglet Paramètres du compte, la zone Réparer l'inscription est disponible au-dessus de Supprimer Android Enterprise. Selon l'avis affiché dans le portail, elle permet de reprendre le contrôle des appareils si Google a supprimé la liaison avec l'Android Enterprise. L'inscription auprès de Google est alors effectuée à nouveau, sans supprimer au préalable la liaison existante.

Avant de démarrer, il convient de vérifier si l'ID de l'organisation affiché correspond à celui enregistré chez Google :

- Compte GooglePlay Enterprise : sur play.google.com/work →
- Domaine Google géré : sur admin.google.com → sous `Appareils` → `Mobiles et points de terminaison` → `Paramètres` → `Intégrations tierces`

Démarrer redirige vers l'inscription auprès de Google. Pour un domaine Google géré, la connexion est limitée à ce domaine. À la fin, Relution vérifie si l'Enterprise connecté correspond à celui lié jusqu'à présent ; si l'ID de l'organisation diffère, la réparation est interrompue avec un message d'erreur.

Types d'inscription

Il existe trois types d’inscription différents pour Android Enterprise. Chacun d’entre eux possède des fonctionnalités spéciales adaptées à des cas d’utilisation spécifiques.

Type d’inscription	Réinitialisation d’usine pour la mise en service	Utilisation privée	Accès des administrateurs
Appareil géré →	requise	non possible	Accès complet à l’ensemble de l’appareil
Profil personnel (COPE) →	requise	possible dans le profil privé	Accès complet à l’appareil, aucun aperçu du profil privé
Profil de travail / BYOD →	non requise	possible sur le reste de l’appareil	aucun accès aux zones privées de l’appareil

Pour la ve

Appareil géré (Managed Device)

Le type d’inscription Appareil géré convient par exemple aux organisations ou aux écoles qui souhaitent remettre des appareils à des utilisateurs n’exerçant que des activités officielles ou scolaires.

- Accès des administrateurs : accès complet à l’appareil, notamment consultation de la liste des applications installées et réinitialisation aux paramètres d’usine.
- Condition préalable : réinitialisation de l’appareil aux paramètres d’usine avant la mise en service.
- Restriction : pas de profil privé, l’appareil est destiné exclusivement à un usage professionnel. Relution n’empêche pas automatiquement l’ajout d’autres comptes, par exemple une GoogleID privée. Pour cela, la configuration Restrictions → propose une option qui interdit l’ajout et la suppression de comptes.

Détails de la mise en place : Appareil géré →

Appareil géré avec profil personnel (Company Owned, Personally Enabled, COPE)

Ce type d'inscription est l'opposé du profil de travail et permet d'attribuer des appareils d'une organisation à des utilisateurs qui peuvent également les utiliser à des fins privées.

- Profil privé : les utilisateurs y enregistrent leur GoogleID privé et installent leurs propres applications ; les données privées et celles liées à l'organisation sont strictement séparées.
- Accès des administrateurs : accès complet à l'appareil, mais aucun aperçu du profil privé (par ex. aucune visibilité sur les applications installées ou les paramètres activés).
- Réinitialisation aux paramètres d'usine : requise avant la mise en service ; une réinitialisation ultérieure effectuée par les administrateurs supprime intégralement les données privées et professionnelles.

Détails de la mise en place : Profil personnel →

Profil de travail / BYOD

Le type d'inscription Profil de travail est le bon choix pour l'approche Apporter son propre appareil (BYOD) : les utilisateurs mettent à disposition leur appareil personnel, sur lequel l'organisation installe un profil de travail.

Pour la version 26.4.0

- Condition préalable : aucune réinitialisation de l'appareil n'est nécessaire.
- Utilisation : l'application de messagerie ou d'autres applications de l'organisation sont par exemple mises à disposition dans le cadre du profil de travail ; les données privées et celles liées à l'organisation sont strictement séparées.
- Accès des administrateurs : aucun aperçu des applications privées installées, aucun droit d'accès aux fonctions ou aux paramètres de l'appareil privé.
- Suppression : lorsque le profil de travail est supprimé, seules les données liées à l'organisation sont effacées des appareils ; les données privées sont conservées.

Détails de la mise en place : Profil de travail / BYOD →

Options d'inscription

Lors de la création d'une inscription sous `Appareils` → `Inscriptions`, le formulaire affiche pour la plateforme Android Enterprise d'autres options en plus du Type et de la Propriété. Elles sont disponibles pour les trois types d'inscription ; les restrictions sont indiquées le cas échéant.

> Relution intègre Langue, Permettre l'inscription cellulaire, Maintenir les applications système activées et les paramètres de la zone Wi-Fi exclusivement dans le code QR affiché pour Appareil géré et Profil personnel sous `Informations sur l'inscription` → `Utilisation du code QR`. L'identifiant DPC, le JSON personnalisé KME et le JSON personnalisé Android Enterprise Zero-Touch ne les contiennent pas. Pour le Profil de travail, le code QR contient uniquement le lien vers l'inscription.

Authentification, Inscription à usages multiples et Permettre l'inscription cellulaire ne peuvent plus être modifiées après l'enregistrement. Selon un avis affiché dans le formulaire, toute modification d'une inscription Android Enterprise existante recrée celle-ci sur les serveurs de Google ; le code QR et l'identifiant DPC précédents deviennent alors invalides.

Authentification

Le champ de sélection Authentification de la section Affectation détermine si un utilisateur doit se connecter pendant l'inscription :

- Non requis (par défaut) : l'inscription s'effectue sans connexion.
- Avec l'app Relution Companion (prend en charge l'usage unique & l'expiration) : l'application Relution Companion exige la connexion de l'utilisateur pendant l'inscription. Inscription à usages multiples et Valable jusqu'au restent disponibles.
- Avec l'app intégrée d'Android (impose l'usage multiple) : la connexion s'effectue sans l'application Companion, pendant la configuration de l'appareil, via la page de connexion de Relution. Si exactement un utilisateur Relution possède l'adresse e-mail du compte connecté à Google, celui-ci est connecté automatiquement ; sinon, la page de connexion s'affiche. Si un utilisateur disposant d'une adresse e-mail est affecté à l'inscription, elle est préremplie avec l'adresse e-mail de celui-ci, sinon avec celle du compte Google. L'inscription est attribuée à l'utilisateur connecté, Relution créant pour chaque appareil une copie distincte de l'inscription, utilisable une seule fois. Le formulaire masque Inscription à usages multiples et Valable jusqu'au.

Le processus de connexion via l'application intégrée d'Android n'est utilisé que si l'option Afficher la connexion au compte Google professionnel est également activée. Cette option n'est proposée que pour le type Appareil géré et nécessite un domaine Google géré, voir Google Work-Account-Setup →. Les inscriptions avec cette option sont toujours utilisables pour plusieurs appareils et n'expirent pas.

Expiration

Dans la section Expiration, Inscription à usages multiples détermine si l'inscription peut être utilisée pour plusieurs appareils. Après la date indiquée sous Valable jusqu'au, l'inscription ne

Pour la version 26.4.0

peut plus être utilisée ; la valeur par défaut est une date située sept jours après la création. Avec l'authentification Avec l'app intégrée d'Android (impose l'usage multiple), la section n'est pas affichée.

Conformité

La section Conformité contient les options suivantes :

- Exiger toujours un mot de passe pour l'appareil (activée par défaut) : un mot de passe de l'appareil est requis même en l'absence d'une politique de mot de passe explicite. Relution ajoute à cet effet dans la politique par défaut de l'inscription une exigence de mot de passe pour l'appareil ainsi qu'une règle de conformité qui désactive les applications tant qu'aucun mot de passe n'est défini.
- Permettre l'inscription cellulaire : la configuration peut s'effectuer via les données mobiles. Relution ajoute une indication correspondante dans le code QR.
- Langue : la langue sélectionnée est intégrée au code QR comme langue de configuration de l'appareil. Sans sélection, l'indication est omise.
- Maintenir les applications système activées : les applications système non essentielles restent activées après l'inscription, voir Appareil géré →.

Pour la version 26.4.0

Wi-Fi

La zone Wi-Fi permet d'enregistrer un réseau pour la configuration de l'appareil :

- Section Connexion : Le SSID du réseau, Ce réseau est masqué, Type de cryptage (Aucun/Ouvert, WEP ou WPA/WPA2 PSK) ainsi que, pour WEP et WPA, le Mot de passe.
- Section Type de proxy : Aucun, Manuelle avec Hôte, Port et Contourner le proxy pour (liste d'adresses qui ne doivent pas être routées via le proxy) ou Configuration automatique avec URL du PAC (adresse du fichier PAC).

Relution n'intègre le Wi-Fi et le proxy au code QR que si Le SSID du réseau est renseigné. Une restriction s'applique à l'inscription via NFC, voir Inscrire des appareils via NFC →.

Accords

Dans la section Configuration, il est possible de sélectionner sous Accords des accords créés sous `Paramètres` → `Général` → `Accords`. Relution met leurs textes à la disposition de l'appareil pendant l'inscription. La sélection n'est affichée qu'aux utilisateurs disposant d'un droit de lecture sur les accords.

Appareil géré

Le type d'enrôlement Appareil géré (Managed Device) convient, par exemple, aux organisations ou aux écoles pour distribuer des appareils aux utilisateurs. Les administrateurs ont un accès complet aux appareils et peuvent, par exemple, consulter la liste des applications installées et réinitialiser les appareils aux paramètres d'usine. Une réinitialisation d'usine est nécessaire pour la mise en service. Relution n'empêche pas automatiquement l'ajout d'autres comptes, par exemple un identifiant Google privé. Pour cela, la configuration Restrictions → propose une option qui interdit l'ajout et la suppression de comptes. En règle générale, ce type d'enrôlement est utilisé pour les appareils appartenant à l'organisation, fournis aux employés ou aux étudiants pour être utilisés exclusivement à des fins professionnelles ou scolaires (pas d'utilisation privée).

> L'organisation Relution doit être liée à une organisation Google pour pouvoir enrôler des appareils Android via Android Enterprise.

Pour la version 26.4.0

Créer un enrôlement dans Relution

- Aller dans `Appareils` → `Inscriptions` puis cliquer sur Ajouter.
- Sélectionner Android Enterprise comme plateforme et, sous Type, l'icône Appareil géré (le nom s'affiche en info-bulle ; présélectionnée par défaut).
- La propriété serait dans ce cas COD (Company Owned Device).
- Attribuer un nom à l'appareil et enregistrer l'enrôlement.

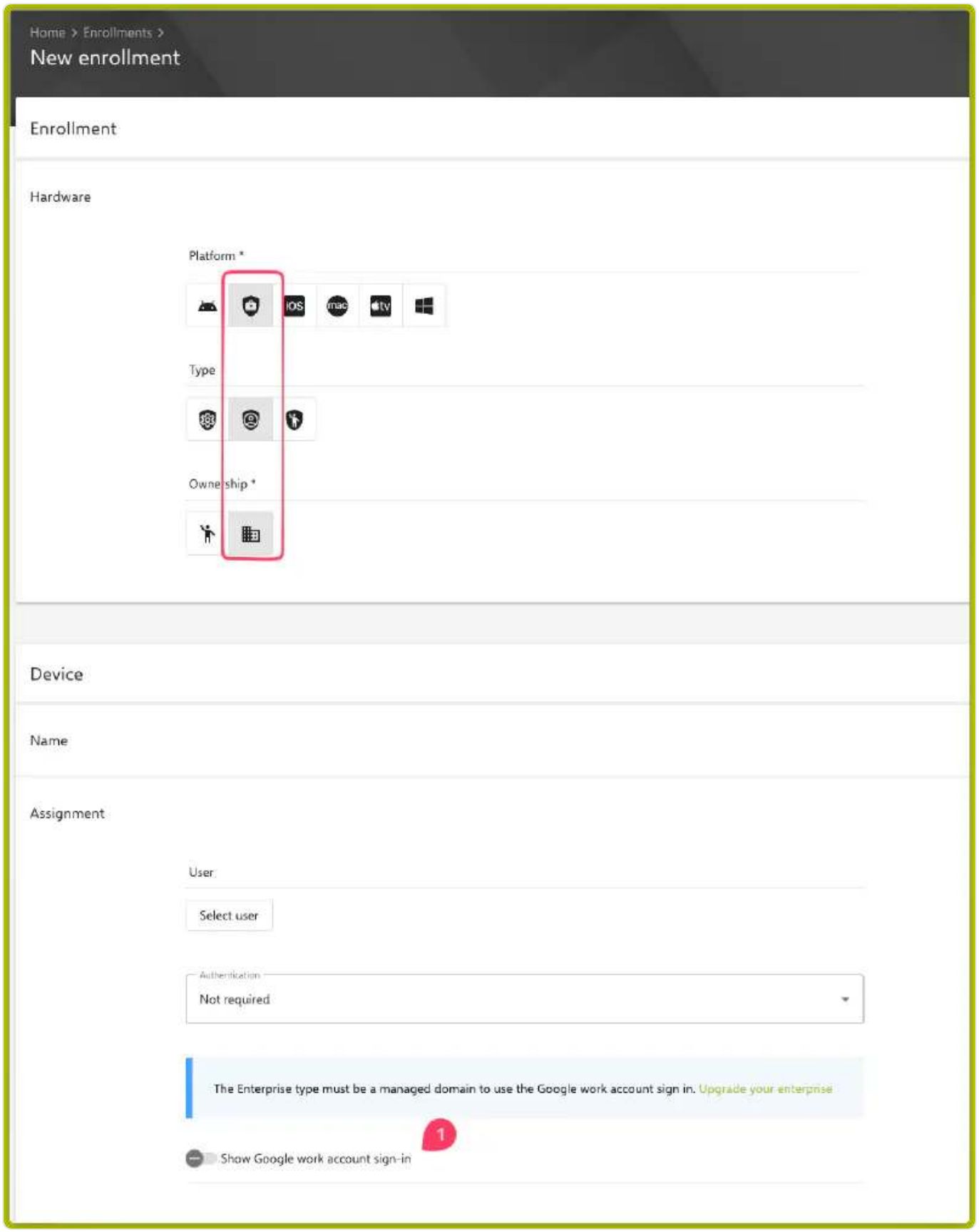
> À partir de Relution 5.33, il est possible de conserver les applications système préinstallées comme Samsung Internet ou d'autres applications tierces. Pour cela, il y a l'interrupteur Maintenir les applications système activées lors de l'enrôlement. À l'inverse, les applications indésirables doivent être bloquées dans la configuration Gérer les applications.

La propriété est un champ obligatoire et est reprise sur l'appareil lors de l'inscription. Avec les paramètres sous `Paramètres` → `Gestion des appareils` → `Inscription`, elle détermine quelles actions sur l'appareil sont autorisées (Effacer l'appareil, Dispositif de verrouillage, Localiser l'appareil, Réinitialiser le code de verrouillage) et si la propriété peut encore être modifiée après l'inscription. Avec COD, toutes ces actions sont autorisées par défaut, et la propriété peut être modifiée par la suite.

Google Work-Account-Setup

Lors de l’enrôlement, l’option Afficher la connexion au compte Google professionnel est disponible. Lorsqu’elle est activée, l’appareil est toujours configuré à l’aide du code QR de l’enrôlement. Après le scan, la connexion s’effectue avec le compte Google professionnel (Google Workspace). Si l’option Avec l’app intégrée d’Android (impose l’usage multiple) est en outre sélectionnée sous Authentification, Relution connecte automatiquement l’utilisateur à l’aide de l’adresse e-mail du compte Google ; en cas d’échec, la page de connexion de Relution s’affiche. L’appareil est ainsi attribué à un utilisateur Relution nommé, voir Options d’inscription →. Les enrôlements avec cette option sont toujours utilisables pour plusieurs appareils et n’expirent pas.

Pour la version 26.4.0



Pour plus de détails sur la configuration de politique du compte professionnel, consulter Configuration du compte professionnel →.

Prérequis : domaine géré

Android Enterprise distingue deux types d’entreprise :

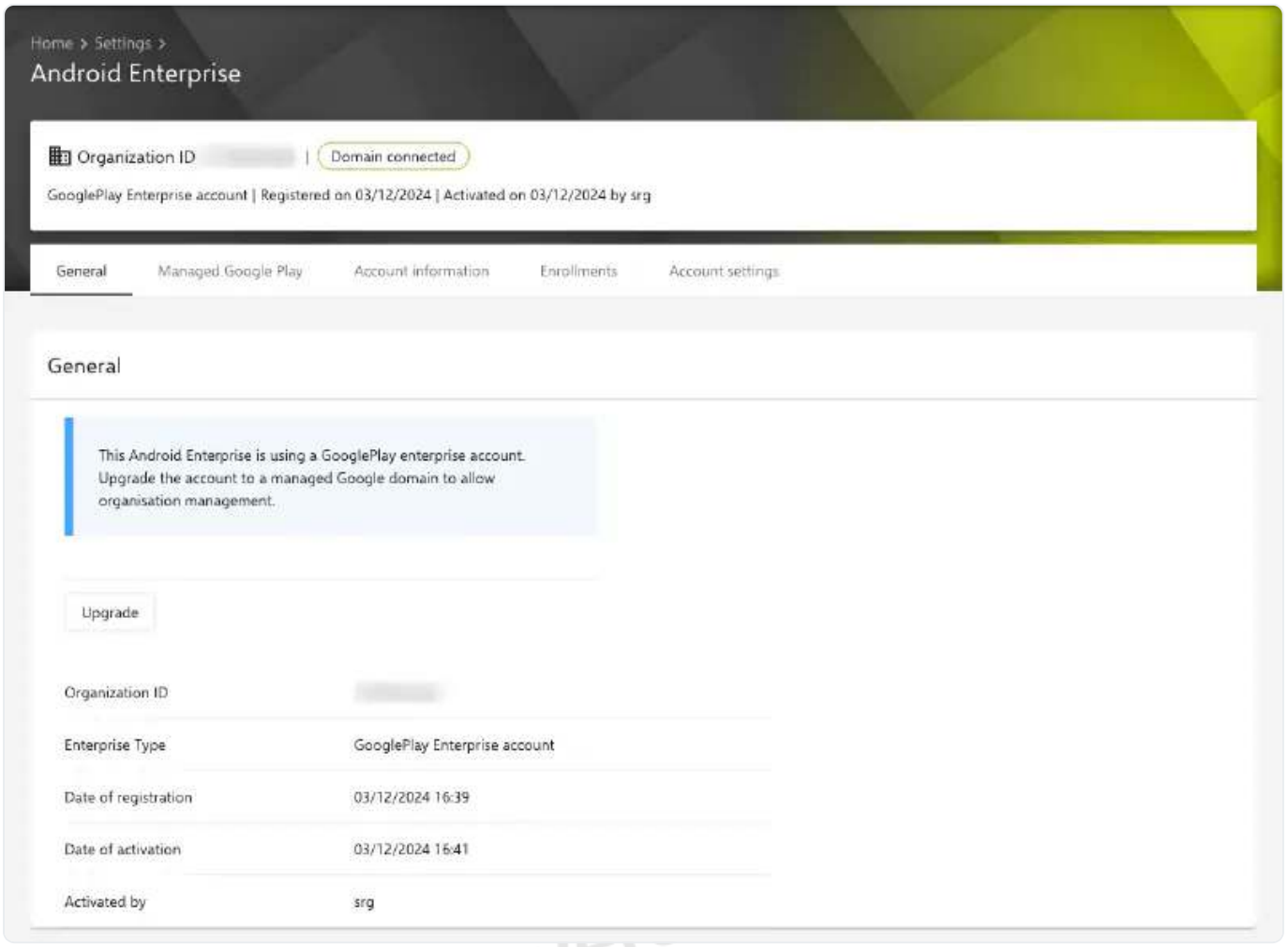
Type d’entreprise	Configuration	Google Work-Account-Setup
Managed Google Play Accounts	Par défaut – enregistré avec n’importe quel compte Google. Les utilisateurs reçoivent automatiquement un compte Google géré lors de l’enrôlement.	Non disponible
Domaine géré	Nécessite une licence Google Workspace active avec un domaine d’entreprise vérifié. Les utilisateurs se connectent avec leur compte `@entreprise.fr` existant.	Disponible

Si l’organisation Relution a été initialement liée avec un compte Google personnel (Managed Google Play Accounts), le formulaire affiche, pour le type Appareil géré, la notice suivante au-dessus de l’interrupteur Afficher la connexion au compte Google professionnel :

« Le type d’entreprise doit être un domaine géré pour utiliser la connexion au compte Google professionnel. »

Pour la version 26.4.0

Mettre à niveau l’entreprise



Le lien Mettre à niveau votre entreprise ouvre la page `Paramètres` → `Android Enterprise`. Dans l'onglet Général, le bouton Mise à niveau y lance, dans un nouvel onglet du navigateur, un assistant fourni par Google qui lie l'Android Enterprise existant à l'organisation Google Workspace. Le lien n'est affiché qu'aux utilisateurs disposant d'un droit de lecture sur les paramètres Android Enterprise ; les autres voient à la place une notice les invitant à contacter un administrateur pour la mise à niveau. Les prérequis suivants doivent être remplis :

- Une licence Google Workspace active (Business, Enterprise, Education, etc.)
- Accès administrateur à la Console d'administration Google Workspace
- Un domaine d'entreprise vérifié dans Google Workspace

Après une mise à niveau réussie, l'option Afficher la connexion au compte Google professionnel devient disponible dans l'enrôlement. En outre, l'authentification des utilisateurs doit être activée pour l'entreprise connectée dans le tableau de bord d'administration Google (admin.google.com). Si elle n'est pas activée, le formulaire d'enrôlement affiche la notice suivante :

« Le compte Enterprise connecté doit activer l'authentification des utilisateurs. Cela ne peut être fait que dans le tableau de bord d'administration à l'adresse admin.google.com. »

Une fois ces deux prérequis remplis, les utilisateurs peuvent s'enrôler avec leurs comptes `@entreprise.fr` existants.

Informations nécessaires pour effectuer l'enrôlement

Dans l'enrôlement créé, un code QR est affiché sous Informations sur l'inscription, qui peut être utilisé pour enrôler des appareils Android. Il est également accessible via la colonne Code QR dans l'aperçu Inscriptions. L'enrôlement est également possible via l'onglet Utilisation de l'identifiant DPC, voir Enrôler des appareils sans caméra →.

Réinitialiser les appareils Android

Pour démarrer l'enrôlement pour Appareil géré, les appareils Android doivent d'abord être réinitialisés aux paramètres d'usine.

Pour la version 26.4.0

Écran de bienvenue sur les appareils

Appuyer 6 fois rapidement sur un endroit de l'écran de bienvenue.

Scanner le code QR de Relution

Les appareils invitent ensuite à scanner le code QR de l'enrôlement créé.

Terminer l'enrôlement

Suivre les instructions supplémentaires pour configurer les appareils. Après un enrôlement réussi, les administrateurs ont un accès complet aux appareils gérés.

Actions

- Installer une application depuis le Google Play Store
- Supprimer une application

- Installer l’application depuis le Relution Store
- Effacer les données de l’application (à partir d’Android 9)
- Envoyer un fichier à l’appareil
- Supprimer l’eSIM
- Ajouter une eSIM
- Réinitialiser l’appareil aux paramètres d’usine
- Éteindre l’appareil
- Redémarrer l’appareil
- Localiser l’appareil →
- Verrouiller complètement l’appareil
- Mettre à jour les informations de l’appareil
- Activer le mode perdu (à partir d’Android 11)
- Désactiver le mode perdu
- Envoyer un message
- Réinitialiser le mot de passe

Configuration des politiques

Pour la version 26.4.0

Les configurations disponibles comprennent notamment :

- Configuration du compte professionnel →
- Gérer les applications →
- Gestion avancée des fonctionnalités du keyguard →
- Remplacements de sécurité avancés →
- Mot de passe de l’appareil →
- Proxy mondial →
- Mode kiosque →
- Gestion des autorisations d’exécution →
- Gestion du Play Store →
- Restrictions →
- Samsung Classroom Management →
- Mode de localisation →
- Mises à jour système →
- Wi-Fi →

Toutes les configurations sont décrites dans l’article Vue d’ensemble →.

Profil personnel

Le type d'inscription Company Owned, Personally Enabled (COPE) permet d'attribuer des appareils d'une organisation à des utilisateurs qui sont autorisés à les utiliser également à des fins privées. Les utilisateurs ont la possibilité d'enregistrer leur GoogleID privé dans un profil privé et d'installer leurs propres applications. Les données privées et celles liées à l'organisation sont strictement séparées sur les appareils. Les administrateurs n'ont pas accès au profil privé et ne peuvent pas, par exemple, voir quelles applications sont installées dans le profil privé et quels paramètres sont activés. En revanche, les administrateurs ont un accès total aux appareils et peuvent, par exemple, effectuer une réinitialisation d'usine, qui supprime toutes les données, qu'elles soient privées ou professionnelles. Une réinitialisation d'usine est nécessaire pour mettre en œuvre le mode d'exploitation.

> L'organisation Relution doit être associée à une organisation Google pour inscrire des appareils Android via Android Enterprise.

Pour la version 26.4.0

Créer une inscription dans Relution

- Aller dans `Appareils` → `Inscriptions` et cliquer sur Ajouter.
- Sélectionner Android Enterprise comme plateforme et, sous Type, l'icône Profil personnel (le nom s'affiche en info-bulle ; Appareil géré est présélectionné par défaut).
- Dans ce cas, le propriétaire sera COD (Company Owned Device).
- Attribuer un nom à l'appareil et enregistrer l'inscription.

La propriété est un champ obligatoire et est reprise sur l'appareil lors de l'inscription. Avec les paramètres sous `Paramètres` → `Gestion des appareils` → `Inscription`, elle détermine quelles actions sur l'appareil sont autorisées et si la propriété peut encore être modifiée après l'inscription. Avec BYOD, Effacer l'appareil, Localiser l'appareil et Réinitialiser le code de verrouillage sont désactivés par défaut, et la propriété ne peut plus être modifiée par la suite. COD est donc le choix approprié pour les appareils avec profil personnel.

Informations nécessaires pour effectuer l'inscription

Dans l'inscription créée, un code QR est affiché sous Informations sur l'inscription qui peut être utilisé pour inscrire des appareils Android. Il est également possible d'y accéder via la colonne

Code QR dans la vue d'ensemble Inscriptions. L'enrôlement est également possible via l'onglet Utilisation de l'identifiant DPC, voir Enrôler des appareils sans caméra →.

Réinitialiser les appareils Android

Pour commencer l'inscription à un appareil géré avec un profil personnel, les appareils Android doivent d'abord être réinitialisés aux valeurs d'usine.

Écran de bienvenue sur les appareils

Sur l'écran de bienvenue, taper 6 fois rapidement.

Scanner le code QR de Relution

Les appareils demandent alors de scanner le code QR de l'inscription créée. Suivre les instructions suivantes pour configurer les appareils gérés.

Pour la version 26.4.0

Container le profil personnel sur les appareils COD

Une fois l'inscription réussie, deux zones distinctes, personnel et travail, sont disponibles sur l'interface utilisateur des appareils Android, entre lesquelles il est possible de basculer à tout moment.

Actions

Les actions disponibles comprennent notamment :

- Nettoyage d'entreprise (à partir d'Android 8) : supprime le profil professionnel et toutes les politiques ; les applications et données du profil personnel sont conservées
- Effacer l'appareil
- Actualiser les informations sur l'appareil

Toutes les actions sont décrites dans l'article Vue d'ensemble →.

Configuration de la politique

Les configurations disponibles comprennent notamment :

- Gérer les applications →
- Code secret du profil professionnel →
- Messages des utilisateurs →
- Affichage →
- Gestion avancée des fonctionnalités du keyguard →
- Remplacements de sécurité avancés →
- Mot de passe de l'appareil →
- Proxy mondial →
- Fond d'écran →
- Mode kiosque →
- Gestion des autorisations d'exécution →
- Usage personnel → : paramètres du profil personnel
- Gestion du Play Store →
- Restrictions →
- Samsung Classroom Management →
- Mode de localisation →
- Mises à jour système →
- Wi-Fi →

Pour la version 26.4.0

Toutes les configurations sont décrites dans l'article Vue d'ensemble →.

> L'option Activer la protection contre la réinitialisation d'usine (FRP) de la configuration Restrictions permet de bloquer la réinitialisation aux valeurs d'usine via les paramètres de l'appareil Android. La réinitialisation via le menu de récupération reste possible. Si l'appareil n'a pas de connexion réseau, Relution ne peut pas lui envoyer d'action de réinitialisation. Plus de détails dans l'article Restrictions →.

Profil de travail / BYOD

Le type d'inscription Profil de travail est le bon choix pour l'approche Bring Your Own Device (BYOD). Les utilisateurs peuvent fournir leurs appareils privés pour qu'un profil de travail y soit installé par l'organisation. Aucune réinitialisation des appareils n'est nécessaire pour la mise en service d'un profil de travail. L'application de messagerie ou d'autres applications de l'organisation peuvent alors être mises à disposition dans le cadre d'un profil de travail. Les données privées et celles liées à l'organisation sont strictement séparées sur les appareils. En outre, les administrateurs n'ont aucun aperçu des applications installées et aucun droit d'accès aux fonctions ou aux paramètres des appareils privés. Lorsqu'un profil de travail est supprimé, toutes les données liées à l'organisation sont supprimées des appareils, tandis que toutes les données privées sont conservées.

> L'organisation Relution doit être associée à une organisation Google pour inscrire des appareils Android via Android Enterprise

Créer une inscription dans Relution

- Aller dans `Appareils` → `Inscriptions` et cliquer sur Ajouter.
- Sélectionner Android Enterprise comme plateforme et, sous Type, l'icône Profil de travail (le nom s'affiche en info-bulle ; Appareil géré est présélectionné par défaut).
- La propriété dans ce cas serait BYOD (Bring Your Own Device)
- Attribuer un nom d'appareil et sauvegarder l'inscription.

La propriété est un champ obligatoire et est reprise sur l'appareil lors de l'inscription. Elle n'a aucune influence sur la configuration du profil de travail. Avec les paramètres sous `Paramètres` → `Gestion des appareils` → `Inscription`, elle détermine toutefois quelles actions sur l'appareil sont autorisées (Effacer l'appareil, Dispositif de verrouillage, Localiser l'appareil, Réinitialiser le code de verrouillage) et si la propriété peut encore être modifiée après l'inscription. Avec BYOD, l'effacement, la localisation et la réinitialisation du code sont désactivés par défaut, et la propriété ne peut plus être modifiée par la suite. Le verrouillage complet est autorisé par défaut.

Pour la version 26.4.0

Informations nécessaires pour effectuer l’inscription.

Dans l’inscription créée, un code QR est affiché sous Informations sur l’inscription pour inscrire les appareils Android. Ce code peut également être consulté dans la colonne Code QR de la vue d’ensemble Inscriptions.

> Le lien doit être ouvert avec Google Chrome, les autres navigateurs tels que Samsung Browser n'affichent qu'une page blanche

Terminer l’inscription

Utiliser l’application appareil photo de l’appareil pour scanner le code QR nouvellement créé, puis suivre les étapes indiquées pour terminer le processus d’inscription.

Container le profil de travail sur les appareils privés

Une fois l’inscription réussie, deux zones distinctes, personnel et travail, sont disponibles sur l’interface utilisateur des appareils Android, entre lesquelles il est possible de basculer à tout moment.

Pour la version 26.4.0

> Veiller à ne pas effectuer d'autres tâches sur l'appareil pendant la création du profil de travail.

Actions

- Installer des applications à partir du Google Play Store
- Supprimer des applications
- Effacer les données de l’application (à partir d’Android 9)
- Envoyer un fichier à l’appareil
- Supprimer l’eSIM
- Ajouter une eSIM
- Éteindre l’appareil
- Localiser l’appareil (désactivé par défaut pour la propriété BYOD)
- Verrouiller complètement l’appareil
- Mettre à jour les informations de l’appareil

- Demander des informations sur l'appareil (à partir d'Android 13)
- Envoyer un message
- Réinitialiser le code de verrouillage (désactivé par défaut pour la propriété BYOD)
- Sélectionner une application Play Store dans l'App Store de Relution

---

Configuration de la politique

Les configurations disponibles comprennent notamment :

- VPN permanent →
- Gérer les applications →
- Code secret du profil professionnel →
- Contrôle de la conformité →
- Remplacements de sécurité avancés →
- Mot de passe de l'appareil →
- Gestion des autorisations d'exécution →
- Gestion du Play Store →
- Restrictions →
- Samsung Classroom Management →
- Applications par défaut → (à partir d'Android 16)
- Restrictions de StrongSwan →
- Profil VPN StrongSwan →
- Configuration du compte de travail →
- Certificat →

Pour la version 26.4.0

Toutes les configurations sont décrites dans l'article Vue d'ensemble →.

Configurations non disponibles

- Messages des utilisateurs →
- Affichage →
- Gestion avancée des fonctionnalités du keyguard →
- Proxy mondial →
- Fond d'écran →
- Mode kiosque →
- Usage personnel →
- Mode de localisation →
- Mises à jour système →
- Wi-Fi →

Knox Mobile Enrollment

Knox est une plateforme de sécurité pour les appareils Samsung permettant une gestion centralisée et sécurisée des terminaux mobiles en entreprise. La plateforme prend en charge le déploiement, la configuration et la protection efficaces des appareils.

Samsung Knox Mobile Enrollment (KME)

Samsung Knox Mobile Enrollment (KME) permet la préparation automatisée des appareils Samsung pour leur gestion dans un système de Mobile Device Management (MDM) tel que Relution.

Lors du premier démarrage d'un appareil et en présence d'une connexion Internet, le processus de configuration démarre automatiquement. Même après une réinitialisation aux paramètres d'usine, l'appareil se réenrôle automatiquement dans le système MDM configuré.

Le programme KME offre des fonctionnalités comparables au Device Enrollment Program (DEP) d'Apple.

Pour la version 26.4.0

Prérequis

1. L'appareil Samsung doit être compatible Knox. La liste des appareils pris en charge est disponible sur la page d'assistance Samsung Knox →.
2. Les appareils Samsung peuvent être enregistrés directement dans le programme KME par des revendeurs agréés à l'aide du numéro de série.
3. Les appareils non achetés auprès de revendeurs agréés peuvent être ajoutés manuellement :
    - en scannant un code QR spécifique lors de la configuration de l'appareil
    - ou en utilisant l'application Knox Mobile Deployment sur un autre appareil Samsung

Le programme KME est fourni gratuitement après inscription sur le Samsung Knox Portal.
Samsung Knox Portal →

> La configuration Knox Mobile Enrollment proposée dans les paramètres de Relution ne doit pas être utilisée. Cette configuration est obsolète, destinée exclusivement à Android Legacy et prise en charge uniquement jusqu'à Android version 10 inclus.

À la place, utiliser le guide suivant : Lier l'organisation →

Combinaison de KME avec Android Enterprise

Samsung Knox Mobile Enrollment peut être combiné avec les types d'enrôlement Android Enterprise suivants :

- Appareil géré (Managed Device)
- Appareil géré avec profil personnel (COPE – Company Owned, Personally Enabled)

Préparation de l'enrôlement dans Relution

1. Accéder à `Appareils` → `Inscriptions`.
2. Sélectionner Ajouter.
3. Configurer :
   - Plateforme : Android pour les entreprises
   - Type : Appareil géré ou Profil personnel (boutons à icône ; le libellé s'affiche en info-bulle)
   - Propriété : COD (appareil appartenant à l'entreprise) ; sans sélection, l'inscription ne peut pas être enregistrée
4. Activer l'option Inscription à usages multiples dans la section Expiration.
5. Définir une date à long terme sous Valable jusqu'au (par exemple 100 ans).
6. Enregistrer l'enrôlement.

Pour la version 26.4.0

Ces étapes nécessitant Inscription à usages multiples et Valable jusqu'au, l'Authentification reste réglée sur Non requis ou Avec l'app Relution Companion (prend en charge l'usage unique & l'expiration). Avec Avec l'app intégrée d'Android (impose l'usage multiple), le formulaire masque ces deux champs. Les paramètres Wi-Fi, Langue et Permettre l'inscription cellulaire ne sont pas contenus dans le JSON personnalisé KME. Si l'inscription est modifiée ultérieurement, Relution recrée l'inscription sur les serveurs de Google ; le JSON enregistré dans le Knox Portal doit alors être remplacé. Détails : Options d'inscription →

Après l'enregistrement :

- Ouvrir l'enrôlement créé.
- Accéder à `Informations sur l'inscription` → `Utilisation de l'identifiant DPC`.
- Copier le JSON personnalisé KME fourni pour une utilisation ultérieure dans le Knox Portal.

Création d’un profil KME dans le Samsung Knox Portal

1. Se connecter au Samsung Knox Portal →
2. Accéder à Profiles.
3. Sélectionner CREATE PROFILE.

Paramètres du profil

- Définir un nom et une description du profil.
- Activer EMM.
- Désactiver Knox Service Plugin.
- Continuer avec Next.
- Compléter les informations de contact.

Informations EMM

- Dans Select your EMM (required) sélectionner : Other
- Dans Link to agent APK (required) saisir :

version 26.4.0

```
https://play.google.com/managed/downloadManagingApp?identifier=setup
```

- Continuer avec Next.
- Insérer dans DPC Extras l’Identifiant DPC affiché dans Relution sous `Informations sur l'inscription` → `Utilisation de l'identifiant DPC`. Le JSON personnalisé KME contient déjà l’identifiant DPC.
- Coller le JSON copié précédemment dans Custom JSON Data.
- Finaliser avec Create.

Optionnel : Création d’un code QR

Un code QR peut être créé pour l’enrôlement des appareils ou pour l’ajout de nouveaux appareils à KME.

Procédure :

1. Sélectionner ADD A QR CODE.
2. Activer Also allow QR Code enrollment for devices not uploaded by a reseller si les appareils n’ont pas été préenregistrés par un revendeur.
3. Configurer éventuellement un réseau Wi-Fi afin de simplifier le déploiement en masse.
4. Confirmer avec ADD.

Pour utiliser le code QR, dessiner un signe plus (+) sur l’écran d’accueil Samsung. Le scanner de code QR s’ouvre automatiquement.

Association des appareils au profil

Si aucun code QR n’est utilisé :

1. Accéder à Devices dans le Knox Portal.
2. Sélectionner les appareils concernés.
3. Choisir `Actions` → `Configure Devices`.
4. Mettre les appareils sous tension.

Pour la version 26.4.0

Zero Touch Enrollment

Android Zero-Touch Enrollment est un service qui permet aux entreprises de déployer automatiquement un grand nombre d'appareils Android, sans configuration manuelle supplémentaire par les administrateurs ou les utilisateurs finaux.

Une fois qu'un appareil est déballé, allumé et connecté à Internet, il est automatiquement configuré avec les politiques, applications et paramètres définis par l'entreprise. Cela permet un déploiement rapide, standardisé et sécurisé des appareils Android dans les environnements professionnels.

Android Zero-Touch Enrollment

Le fonctionnement de Android Zero-Touch Enrollment est comparable à Knox Mobile Enrollment (KME) →.

Dans le portail Zero-Touch, une configuration est d'abord créée, puis assignée aux appareils souhaités depuis la liste des appareils.

> Les appareils destinés à Android Zero-Touch Enrollment (ZTE) ne peuvent pas être ajoutés manuellement par les clients finaux. L'ajout d'appareils dans le portail Zero-Touch doit toujours être réalisé par un revendeur ou OEM autorisé.

Pour la version 26.4.0

Préparation de l'enrôlement dans Relution

1. Accéder à `Appareils` → `Inscriptions`.
2. Sélectionner Ajouter.
3. Configurer :
   - Plateforme : Android pour les entreprises
   - Type : Appareil géré ou Profil personnel (boutons à icône ; le libellé s'affiche en info-bulle)
   - Propriété : COD (appareil appartenant à l'entreprise) ; sans sélection, l'inscription ne peut pas être enregistrée
4. Activer l'option Inscription à usages multiples dans la section Expiration.
5. Définir une date suffisamment lointaine sous Valable jusqu'au.
6. Enregistrer l'enrôlement.

Ces étapes nécessitant Inscription à usages multiples et Valable jusqu'au, l'Authentification reste réglée sur Non requis ou Avec l'app Relution Companion (prend en charge l'usage unique & l'expiration). Avec Avec l'app intégrée d'Android (impose l'usage multiple), le formulaire masque ces deux champs. Les paramètres Wi-Fi, Langue et Permettre l'inscription cellulaire ne sont pas contenus dans le JSON Zero-Touch. Si l'inscription est modifiée ultérieurement, Relution recrée l'inscription sur les serveurs de Google ; le JSON enregistré dans la configuration Zero-Touch doit alors être remplacé. Détails : Options d'inscription →

Après l'enregistrement :

- Ouvrir l'enrôlement créé.
- Accéder à `Informations sur l'inscription` → `Utilisation de l'identifiant DPC`.
- Copier le JSON personnalisé Android Enterprise Zero-Touch fourni dans le presse-papiers.

Zero-Touch dans Relution

En plus du portail Zero-Touch →, Relution intègre la vue Zero-Touch de Google sous `Paramètres` → `Spécifique à la plate-forme de l'appareil` → `Android pour les entreprises`, dans l'onglet Inscriptions, zone Android Enterprise Zero Touch. La vue est chargée dans la langue du portail et préconfigurée avec Android Device Policy comme DPC. Les fonctions proposées sont définies par Google.

Pour la version 26.4.0

Création d'un profil Zero-Touch

1. Se connecter au portail Zero-Touch →.
2. Accéder à Configurations.
3. Cliquer sur le symbole + en haut de la page.
4. Donner un nom à la configuration.
5. Sous EMM DPC, sélectionner Android Device Policy. (Si plusieurs entrées sont disponibles, n'importe laquelle peut être utilisée.)
6. Coller le JSON précédemment copié dans le champ DPC extras.
7. Remplir les autres champs selon les besoins.
8. Cliquer sur ADD pour finaliser.

Liaison des appareils et de la configuration

1. Accéder à Devices dans le portail Zero-Touch.
2. Assigner la configuration souhaitée aux appareils correspondants.
3. Mettre les appareils sous tension.

Le scan d’un code QR n’est pas nécessaire. Lors du premier démarrage, les appareils Android contactent automatiquement le service Zero-Touch, qui transmet la demande d’enrôlement à Android Enterprise puis à Relution.

Pour la version 26.4.0

Inscrire des appareils via NFC

Avec l'application Relution Agent, il est possible d'ajouter facilement des appareils Android Enterprise au MDM via NFC (Near Field Communication). Les deux appareils doivent être compatibles NFC et un appareil support doit déjà être enregistré dans Relution. L'appareil cible ne peut être inscrit qu'en tant que Fully Managed ou avec un Profil personnel. L'Android Work Profile ou une inscription Legacy ne sont pas possibles.

Configuration

1. Dans Relution, sous `Appareils` → `Inscriptions`, créer une inscription pour la plateforme Android pour les entreprises avec le type Appareil géré ou Profil personnel (pas Profil de travail).

   Astuce : si plusieurs appareils doivent être inscrits successivement, activer l'option Inscription à usages multiples dans la section Expiration et choisir une date lointaine sous Valable jusqu'au. La section Expiration n'est pas affichée si Avec l'app intégrée d'Android (impose l'usage multiple) a été sélectionné sous Authentification, voir Options d'inscription →.

   > Actuellement, aucun profil Wi-Fi ne doit être inclus lors de l'inscription NFC.

2. Ouvrir l'application Relution Agent sur l'appareil support.
3. Aller dans `Menu hamburger` → `Informations sur l'appareil` → `Partager l'inscription NFC`
4. Appuyer sur Scanner l'inscription.
5. Scanner le code QR de l'inscription créée.

   Après le scan, l'appareil support peut être utilisé pour inscrire de nouveaux appareils. Il est aussi possible d'écrire sur une étiquette NFC.

6. L'appareil cible doit être réinitialisé et sur l'écran de première configuration.
7. Approcher l'appareil support ou l'étiquette NFC de l'appareil cible et suivre les instructions affichées.

Pour la version 26.4.0

Enrôler des appareils sans caméra

Certains appareils ne sont pas équipés d'une caméra ou d'un scanner de codes QR. Ces appareils peuvent également être enregistrés en tant qu'appareil géré.

Enrôler des appareils sans appareil photo/code QR

Dans un enrôlement créé, l'Identifiant DPC est affiché sous Informations sur l'inscription dans l'onglet Utilisation de l'identifiant DPC (le code mis en évidence au-dessus de Processus d'inscription). Il ne doit pas être confondu avec le champ Code d'inscription sous Détails. Le même onglet est également disponible dans la boîte de dialogue du code QR de l'enrôlement. L'identifiant DPC s'utilise comme suit :

- Réinitialiser les appareils aux paramètres d'usine
- Suivre les instructions pour configurer les appareils
- Si les appareils demandent d'entrer les informations d'identification du compte Google, entrer le code `afw#setup` comme nom d'utilisateur.
- Si les appareils demandent d'entrer l'identifiant DPC, entrer le code correspondant.
- Suivre les instructions pour configurer les appareils gérés Les appareils sont maintenant enrôlés de manière identique dans le processus alternatif QR code.

Pour la version 26.4.0

Désinscrire des appareils

La désinscription met fin à la gestion d'un appareil par Relution. La désinscription s'effectue en supprimant l'appareil : l'action Supprimer est disponible dans l'inventaire des appareils ainsi que dans les détails de l'appareil. Après confirmation de la suppression, les données de l'organisation sont retirées de l'appareil et l'appareil est supprimé de l'inventaire. La désinscription est consignée dans le journal d'audit ; une nouvelle inscription de l'appareil est possible à tout moment.

Si la sélection contient un appareil géré, la boîte de dialogue de suppression propose en outre, sous Appareil géré, les options Gardez la protection contre la réinitialisation d'usine (FRP) activée et Effacez également le stockage externe de l'appareil (comme les cartes SD) ; les deux sont désactivées par défaut (voir Protection réinitialisation →). Le champ Votre message, également affiché, n'a aucun effet sur les appareils appartenant à l'entreprise.

> Pour les appareils inscrits via Samsung Knox Mobile Enrollment (KME), l'attribution de profil de l'appareil doit être supprimée dans le portail Samsung Knox avant la suppression. Sinon, l'appareil est automatiquement réinscrit.

Pour la version 26.4.0

Effet selon le type d'inscription

Ce qui se produit sur l'appareil dépend du type d'inscription :

Type d'inscription	Effet de la suppression
Appareil géré →	L'appareil est effacé et réinitialisé aux paramètres d'usine.
Profil de travail / BYOD →	Seul le profil de travail est supprimé, y compris toutes les applications et données professionnelles. Les données personnelles restent sur l'appareil.
Profil personnel →	Seul le profil de travail est supprimé, y compris toutes les applications et données professionnelles. Les données personnelles restent sur l'appareil.

Corbeille

Les appareils supprimés sont d’abord déplacés dans la corbeille (`Appareils` → `Poubelle`). Ce n’est qu’en supprimant à nouveau un appareil depuis la corbeille qu’il est définitivement retiré de Relution.

Seuls les appareils à l’état Supprimé sont définitivement retirés. Un appareil à l’état Suppression en attente… n’a pas encore confirmé la suppression, par exemple parce qu’il est hors ligne. S’il est supprimé depuis la corbeille, il passe d’abord uniquement à l’état Supprimé et reste dans la corbeille ; seule une nouvelle suppression le retire définitivement.

Pour la version 26.4.0

Supprimer l'organisation

Il est possible de supprimer une connexion existante entre Relution et Android Enterprise.

Avis

Pour les inscriptions à Android Enterprise, les appareils Android communiquent directement avec Android Enterprise via l'API Android Enterprise et non via Relution comme pour les inscriptions à Android Classic/Legacy. Si la connexion à Android Enterprise est annulée en supprimant le compte Google associé, toutes les inscriptions existantes seront perdues et les appareils existants ne pourront plus être gérés dans Relution et aucun nouvel appareil ne pourra être inscrit via Android Enterprise. Les configurations de politique qui se trouvent sur les appareils inscrits à ce moment-là ne peuvent plus être retirées ou supprimées. Il n'est pas possible de se reconnecter ultérieurement pour reprendre le contrôle des appareils. En revanche, les conséquences d'une déconnexion dans Relution dépendent de l'option qui y est choisie (voir la section suivante).

Pour la version 26.4.0

Déconnexion d'une connexion existante côté Relution

La connexion est supprimée sous `Paramètres` → `Spécifique à la plate-forme de l'appareil` → `Android pour les entreprises`, dans l'onglet Paramètres du compte :

- Dans la carte Supprimer Android Enterprise, sélectionner l'option souhaitée sous Options de suppression de l'Enterprise. L'option Supprimer l'Enterprise et les appareils connus de Relution est présélectionnée.
- Cliquer sur Démarrer.
- Confirmer la boîte de dialogue Organisations dissociées avec Supprimer.

Le bouton Démarrer n'est visible qu'avec l'autorisation de modifier les paramètres Android Enterprise.

Les options ont des effets différents sur les appareils :

- Supprimer l'Enterprise et les appareils connus de Relution : les appareils gérés par Relution sont réinitialisés aux paramètres d'usine ou leur profil professionnel est supprimé, et ils sont supprimés dans Relution. Les appareils inconnus de Relution restent dans l'Android Enterprise.

- Supprimer l'Enterprise et les appareils : en plus des appareils gérés par Relution, tous les autres appareils de l'Android Enterprise sont supprimés, y compris ceux inconnus de Relution.

> Dès l'option présélectionnée, tous les appareils gérés par Relution sont réinitialisés ou leurs profils professionnels sont supprimés. Les appareils précédemment inscrits ne sont pas restaurés lors du rétablissement de la connexion.

Déconnexion d'une connexion existante côté Google

La déconnexion dans Relution ne supprime pas l'organisation Google. Après la déconnexion, Relution affiche les étapes nécessaires à la suppression sous `Paramètres` → `Spécifique à la plate-forme de l'appareil` → `Android pour les entreprises`. Ces étapes dépendent du type d'entreprise de l'organisation.

Domaine Google géré

- Aller sur admin.google.com → et se connecter avec le compte utilisé pour créer ou mettre à niveau l'organisation.
- Naviguer vers `Appareils` → `Mobile et terminaux` → `Paramètres` → `Intégrations tierces`.
- Sélectionner l'intégration tierce et cliquer sur Gérer les fournisseurs EMM.
- Dans la liste des fournisseurs, supprimer l'organisation dont l'ID correspond à l'ID de l'organisation affiché dans Relution.

Selon la remarque affichée dans Relution, l'entreprise peut être réactivée dans les 30 jours en se connectant avec le compte utilisé pour établir la connexion.

Compte GooglePlay Enterprise

- Aller sur play.google.com/work → et se connecter avec le compte utilisé pour créer l'organisation.
- Dans le menu de gauche, cliquer sur Paramètres d'administration.
- Comparer l'identifiant, qui apparaît en haut de la page, avec celui du portail Relution.
- Cliquer sur les trois points à droite de la tuile, puis sur Supprimer l'organisation.

Un compte Gmail ne peut être associé qu'à une seule organisation Google et ne peut être utilisé pour une nouvelle organisation qu'après la suppression de celle-ci. Tant que l'organisation

Pour la version 26.4.0

Google n’a pas été supprimée, la connexion dans Relution peut être rétablie avec le même compte Gmail ; les appareils précédemment inscrits ne sont alors pas restaurés.

Pour la version 26.4.0

Vue d'ensemble

Relution propose une sélection d’actions permettant de contrôler et de diriger directement les appareils Android Enterprise. L’avantage principal est que ces actions peuvent être appliquées spécifiquement à des appareils individuels.

Actions disponibles

Toutes les actions ne sont pas disponibles pour tous les types d’inscription. Les restrictions et versions minimales sont indiquées dans la description ; les actions sans mention sont disponibles pour les appareils gérés, les profils professionnels et les appareils avec profil personnel.

Action	Description
Installer l’application depuis Google Play Store	Installe une application sélectionnée depuis le Google Play Store sur l’appareil. Disponible uniquement pour les appareils inscrits en tant qu’appareil géré ou profil professionnel.
Installer l’application depuis le Relution Store	Installe sur l’appareil une application enregistrée dans le Relution Store : applications Play Store ainsi qu’applications natives (APK), à condition que Relution ait déterminé leurs certificats de signature. Les applications natives ne peuvent être sélectionnées que si seuls des appareils entièrement gérés sont sélectionnés. Disponible uniquement pour les appareils entièrement gérés, y compris avec profil personnel. Détails : Gérer les apps APK →
Supprimer l’application	Désinstalle une application sélectionnée de l’appareil. Disponible uniquement pour les appareils inscrits en tant qu’appareil géré ou profil professionnel.
Effacer les données de l’application	Supprime toutes les données associées à une application de l’appareil. Disponible à partir d’Android 9.

Action	Description
Envoyer un fichier à l’appareil	Transfère un fichier (par ex. PDF, document, image) en toute sécurité vers l’appareil.
Nettoyage d’entreprise	Supprime le profil professionnel et toutes les stratégies associées ; les applications et données du profil personnel sont conservées. Disponible uniquement pour les appareils avec un profil personnel activé, à partir d’Android 8.
Supprimer l’eSIM	Supprime un profil eSIM de l’appareil à l’aide de l’ICCID.
Ajouter une eSIM	Ajoute un profil eSIM à l’appareil à l’aide du code d’activation fourni.
Effacer l’appareil	Réinitialise l’appareil aux paramètres d’usine et supprime toutes les données. Disponible uniquement pour les appareils inscrits en tant qu’appareil géré ou avec profil personnel. Remarque : Depuis Relution 5.34.0, il est également possible de supprimer uniquement le profil de gestion sur les appareils avec un profil professionnel ou personnel (via l’icône corbeille dans les détails de l’appareil, ou Supprimer dans l’inventaire des appareils).
Éteindre l’appareil	Éteint complètement l’appareil.
Redémarrer l’appareil	Redémarre l’appareil. Disponible uniquement pour les appareils inscrits en tant qu’appareil géré.
Localiser l’appareil	Détermine l’emplacement actuel de l’appareil.
Verrouiller l’appareil	Disponible uniquement pour les appareils inscrits en tant qu’appareil géré ou profil professionnel. Verrouille l’appareil avec le mot de passe actuel. Si aucun mot de passe n’est défini, l’appareil peut être déverrouillé sans mot de passe. Il n’existe pas d’action de déverrouillage ; si le mot de passe est inconnu, un nouveau mot de passe peut être défini via Réinitialiser le code de verrouillage (sur les appareils inscrits en tant que profil professionnel, cela ne concerne que le mot de passe du profil professionnel).
Actualiser les informations sur l’appareil	Actualise les informations de l’appareil dans la console Relution.

Action	Description
Demander des informations sur l’appareil	Demande l’identifiant eSIM (EID) de l’appareil. L’utilisateur doit approuver la divulgation sur l’appareil. Disponible uniquement pour les appareils inscrits en tant que profil professionnel, à partir d’Android 13.
Activer le mode perdu	Active le mode perdu en cas de perte ou de vol de l’appareil : écran de verrouillage, suivi de la localisation et message sur l’écran de verrouillage. Disponible uniquement pour les appareils inscrits en tant qu’appareil géré (à partir d’Android 11) ou avec profil personnel (à partir d’Android 13).
Désactiver le mode perdu	Déverrouille l’appareil et désactive à nouveau le mode perdu. Même disponibilité que Activer le mode perdu.
Envoyer un message	Affiche un message texte sur l’appareil.
Réinitialiser le code de verrouillage	Réinitialise le mot de passe de l’appareil sur les appareils gérés. Sur les appareils avec profil professionnel ou profil personnel, seul le mot de passe du profil professionnel est réinitialisé ; les appareils avec profil personnel ne peuvent pas être déverrouillés avec le nouveau mot de passe.
Sélectionner l’application Play Store dans le Relution Store	Installe sur l’appareil une application Play Store préalablement approuvée dans le Relution Store. Disponible uniquement pour les appareils inscrits en tant que profil professionnel.

Localiser un appareil Android

Avec Relution, il est possible de localiser les appareils Android Enterprise. L'action peut être déclenchée dans l'Inventaire sur l'appareil à localiser dans l'onglet `Emplacement` → `Localiser l'appareil`. Si une position est déjà disponible, le bouton s'intitule Demander la position actuelle. Après une demande, le bouton est désactivé jusqu'à ce que la localisation ainsi demandée soit terminée, pendant 20 secondes environ au maximum. Si le Relution Companion ne dispose pas des autorisations nécessaires, il est également désactivé ; en mode perdu actif, il n'est pas affiché. Alternativement, dans l'onglet `Actions` → `Appliquer l'action` → `Localiser l'appareil`.

Chaque fois qu'un appareil est localisé, une notification est envoyée au menu de notification de l'appareil. En outre, le processus est affiché dans le compagnon de Relution.

L'appareil localisé avec succès est affiché sur une carte dans l'onglet Emplacement sous `Appareils` → `Inventaire` → `l'appareil concerné` → `Emplacement`.

Exigence

L'appareil doit être équipé d'un module GPS et d'une connexion Internet, il doit être allumé et fondamentalement localisable.

Dans Relution, la localisation doit être activée sous `Paramètres` → `Gestion des appareils` → `Inscription` à la ligne Localiser l'appareil pour le type de propriété de l'appareil (COD ou BYOD). Par défaut, elle est activée pour COD et désactivée pour BYOD. Les appareils dont la propriété est inconnue sont localisables par défaut ; ce réglage ne peut pas être modifié dans le portail. Si la localisation est désactivée, Relution ne propose pas l'action Localiser l'appareil et masque l'onglet Emplacement. Pour les appareils Android Enterprise en mode perdu, l'onglet Emplacement reste visible et actualise la position environ toutes les minutes ; l'action Localiser l'appareil n'est pas disponible non plus dans ce cas.

Les services de localisation doivent également être activés sur l'appareil dans les paramètres ou dans les paramètres rapides. Relution attribue l'autorisation de localisation du Companion via la politique : si Localiser l'appareil est activé pour COD, l'autorisation est accordée automatiquement, sinon elle est refusée. Cela s'applique quel que soit le type de propriété de l'appareil. Ce réglage par défaut peut être remplacé via la configuration Gérer les applications.
Autres paramètres →

Pour la version 26.4.0

Si ces paramètres sont désactivés, Relution affiche le message suivant (en anglais) dans les actions :

```
Unable to determine location; No location available; GPS is disabled; Network
```

Si les services sont activés, un message de réussite (en anglais) ressemble à ceci :

```
Determined current location, using fused provider, accuracy 13,37 meter, age <
```

Afficher la position dans le portail libre-service

Nouveau dans 26.4

Les utilisateurs autorisés peuvent également afficher directement sur une carte, dans le portail libre-service, la dernière position connue de leur propre appareil, sans avoir besoin d'un accès administrateur : Afficher la position sur une carte →

Pour la version 26.4.0

Notes

- Actions en cours
  Des problèmes de positionnement peuvent survenir si des actions sont encore en cours dans Relution. Celles-ci doivent être annulées et l'action doit être soumise à nouveau.
- Précision de localisation
  L'option Précision de localisation dans les paramètres de l'appareil a une influence significative sur la précision de la localisation. Si ce paramètre est désactivé, la précision de la localisation peut être de plusieurs centaines de mètres. Pour les appareils Samsung équipés d'Android 13, le réglage se trouve sous `Réglages` → `Localisation` → `Services de localisation` → `Précision de la localisation`.
- Autorisation de localisation
  Afin de limiter les abus potentiels, Relution à partir de la version 5.31.0 offre la possibilité d'ajuster une autorisation de localisation. Détails : Services de localisation →

Vue d'ensemble

Une politique est un ensemble d’une ou plusieurs configurations. Chaque politique peut être appliquée à un ou plusieurs appareils en même temps. En outre, une ou plusieurs politiques peuvent être associées à chaque appareil.

Configurations Disponibles

Configuration	Description
VPN permanent →	Gérer les paramètres du VPN toujours actif
Gérer les applications →	Installer, mettre à jour et désinstaller des applications sur les appareils gérés
Code secret du profil professionnel →	Gestion de la politique de mot de passe pour le profil professionnel
Accès Conditionnel →	Requiert la configuration de l’accès conditionnel sur l’appareil via l’agent Relution afin d’utiliser les ressources protégées
Messages des utilisateurs →	Définir des messages personnalisés
Activités préférées →	Gère quelle application est utilisée par défaut pour une action donnée
Affichage →	Gérer les paramètres d’affichage de l’appareil
CVTE OEMConfig →	Configurer l’application CVTE OEMConfig
Contrôle de la conformité →	Définir des actions de verrouillage et d’effacement lorsqu’un appareil n’est pas conforme
Gestion avancée des fonctionnalités du keyguard →	Les administrateurs informatiques peuvent contrôler les fonctions avancées du Keyguard (écran de verrouillage) de l’appareil

Configuration	Description
Remplacements de sécurité avancés →	Politiques de sécurité définies par défaut sur des valeurs sécurisées
État radio de l'appareil →	Gérer l'état des paramètres radio de l'appareil
Mot de passe de l'appareil →	Gestion de la politique de mot de passe pour l'appareil
Connectivité des appareils →	Gérer les paramètres de connectivité de l'appareil
Proxy mondial →	Configure un proxy HTTP global indépendant du réseau
Fond d'écran →	Gérer le fond d'écran
Mode kiosque →	Paramètres du mode kiosque
Knox →	Configurer le Knox Service Plugin (KSP) de Samsung
Gestion des autorisations d'exécution →	Définir les réponses par défaut aux demandes de permission des applications gérées
Newline OEMConfig →	Configurer l'application Newline OEMConfig
Usage personnel →	Configurer l'usage personnel pour un appareil entièrement géré
Gestion du Play Store →	Configuration des fonctionnalités de Google Play Store
Partages de Fichiers Relution →	Configuration de partage pour l'application Relution Files
Relution Decon →	Configuration pour l'application Relution Decon
Disposition de l'écran d'accueil de Relution →	Configurer l'application de disposition de l'écran d'accueil Relution
Restrictions →	Gestion des restrictions
Samsung Classroom Management →	Préconfigurer l'application de gestion de classe Samsung
Applications par défaut →	Définir quelles applications sont utilisées par défaut sur l'appareil

Configuration	Description
Mode de localisation →	Configurer les options de la détection de localisation disponible
Restrictions de StrongSwan →	Configurer l'application StrongSwan et définir un profil par défaut
Profil VPN StrongSwan →	Configurer un profil VPN pour l'application StrongSwan
Mises à jour système →	Gérer les mises à jour système
Wi-Fi →	Gestion des paramètres Wi-Fi
Configuration du compte de travail →	Configurer la mise à niveau d'un compte utilisateur vers un domaine Google géré
Certificat →	Définir un certificat d'autorité de certification (CA) ou un certificat et une clé privée à installer

Pour la version 26.4.0

Code secret du profil professionnel

Cette configuration permet de définir les exigences de mot de passe pour le profil professionnel des appareils Android Enterprise. Les exigences relatives au verrouillage de l'appareil sont définies via la configuration Mot de passe de l'appareil →.

Types d'inscription pris en charge

Les badges Profil de travail et Profil personnel du formulaire indiquent les types d'inscription pour lesquels la configuration est prise en charge :

- Appareils avec profil de travail →
- Appareils gérés avec profil personnel →

Il n'existe pas de sélection de profil. Dans les deux cas, les exigences de mot de passe s'appliquent au profil professionnel.

Pour la version 26.4.0

Qualité du code d'accès

Définit la qualité minimale ou le type de verrouillage d'écran ou de mot de passe requis. Le niveau sélectionné est une exigence minimale, les mots de passe d'un niveau de qualité supérieur sont également acceptés.

Les options suivantes sont disponibles :

- Complexe (fort)
  Le mot de passe doit contenir au moins une lettre, un chiffre et un caractère spécial. Lorsque cette option est sélectionnée, les champs obligatoires suivants s'affichent en plus (valeur minimale autorisée entre parenthèses) :
  - Nombre minimum de lettres (1)
  - Nombre minimum de lettres minuscules (0)
  - Nombre minimum de lettres majuscules (0)
  - Nombre minimum de caractères autres que des lettres (0)
  - Nombre minimum de caractères numériques (1)
  - Nombre minimum de symboles (1)

  Ces champs ne sont pas préremplis dans une nouvelle configuration. La configuration ne peut être enregistrée qu'une fois tous les champs renseignés.

- Alphanumérique
  Le mot de passe doit contenir des lettres et des chiffres.
- Alphabétique
  Le mot de passe doit contenir au moins des lettres (ou des symboles).
- Complexe numérique
  Nécessite un mot de passe numérique avec des exigences renforcées, par exemple sans suites de chiffres simples ou faciles à deviner.
- Numérique
  Le mot de passe doit contenir au moins des chiffres (par ex. un code PIN).
- Motif
  Malgré son libellé, cette option n'impose pas de schéma de déverrouillage. Un verrouillage quelconque suffit (par ex. schéma, code PIN ou mot de passe), sans exigence quant à son contenu.
- Biométrique (faible)
  Une méthode de déverrouillage biométrique plus faible peut être utilisée, si elle est prise en charge par l'appareil. Avec cette sélection, les champs Longueur minimale du code d'accès, Âge maximum du code d'accès (en jours), Historique du code d'accès et Nombre de tentatives de code secret ayant échoué avant que toutes les données ne soient effacées sont masqués et ne peuvent pas être configurés.

Pour la version 26.4.0

> Les options réellement disponibles et applicables dépendent de l'appareil, de la version d'Android et des personnalisations du fabricant.

Longueur minimale du code d'accès

Définit le nombre minimum de caractères requis pour le mot de passe. Le champ est obligatoire. La valeur par défaut et la plus petite valeur autorisée est `4`.

Exemple :

- `4` → Le mot de passe doit comporter au moins 4 caractères.

Âge maximum du code d’accès (en jours)

Détermine après combien de jours le mot de passe doit être modifié.

Nombre de jours avant qu’un nouveau mot de passe doive être défini. Si la valeur est définie sur `0`, le mot de passe n’expire jamais.

Exemple :

- `0` → Pas d’expiration du mot de passe.

Historique du code d’accès

Définit combien d’anciens mots de passe ne peuvent pas être réutilisés.

Nombre de mots de passe enregistrés et déjà utilisés qui ne peuvent plus être réutilisés.

Exemple :

- `0` → Il n’y a aucune restriction sur la réutilisation des mots de passe.

Pour la version 26.4.0

Nombre de tentatives échouées avant l’effacement des données

Définit après combien de saisies incorrectes une réinitialisation ou un effacement est déclenché.

Si aucune valeur n’est définie, aucun effacement automatique n’est généralement effectué.

Désactiver les applications de profil professionnel jusqu’à ce que l’utilisateur respecte les exigences

Si cette option est activée, les applications du profil professionnel restent désactivées jusqu’à ce que le mot de passe configuré réponde aux exigences définies. L’option est activée par défaut.

Le délai au terme duquel le blocage puis l’effacement interviennent lorsque les exigences de mot de passe ne sont pas respectées est défini dans la configuration Contrôle de la conformité →. Par défaut, seules les applications du profil de travail sont bloquées. Lors de l’effacement, seul

le profil de travail est supprimé sur les appareils avec profil de travail (BYOD) ; les appareils avec profil personnel (COPE) sont réinitialisés aux paramètres d'usine.

Exiger un code d'accès distinct pour le profil professionnel

Si cette option est activée, un code d'accès distinct doit être défini pour le profil professionnel.

Si cette option est désactivée, le même code de verrouillage de l'appareil peut être utilisé dans certains cas.

> Si cette option n'est pas activée, un délai d'expiration système de 60 secondes est automatiquement appliqué.

Remarques

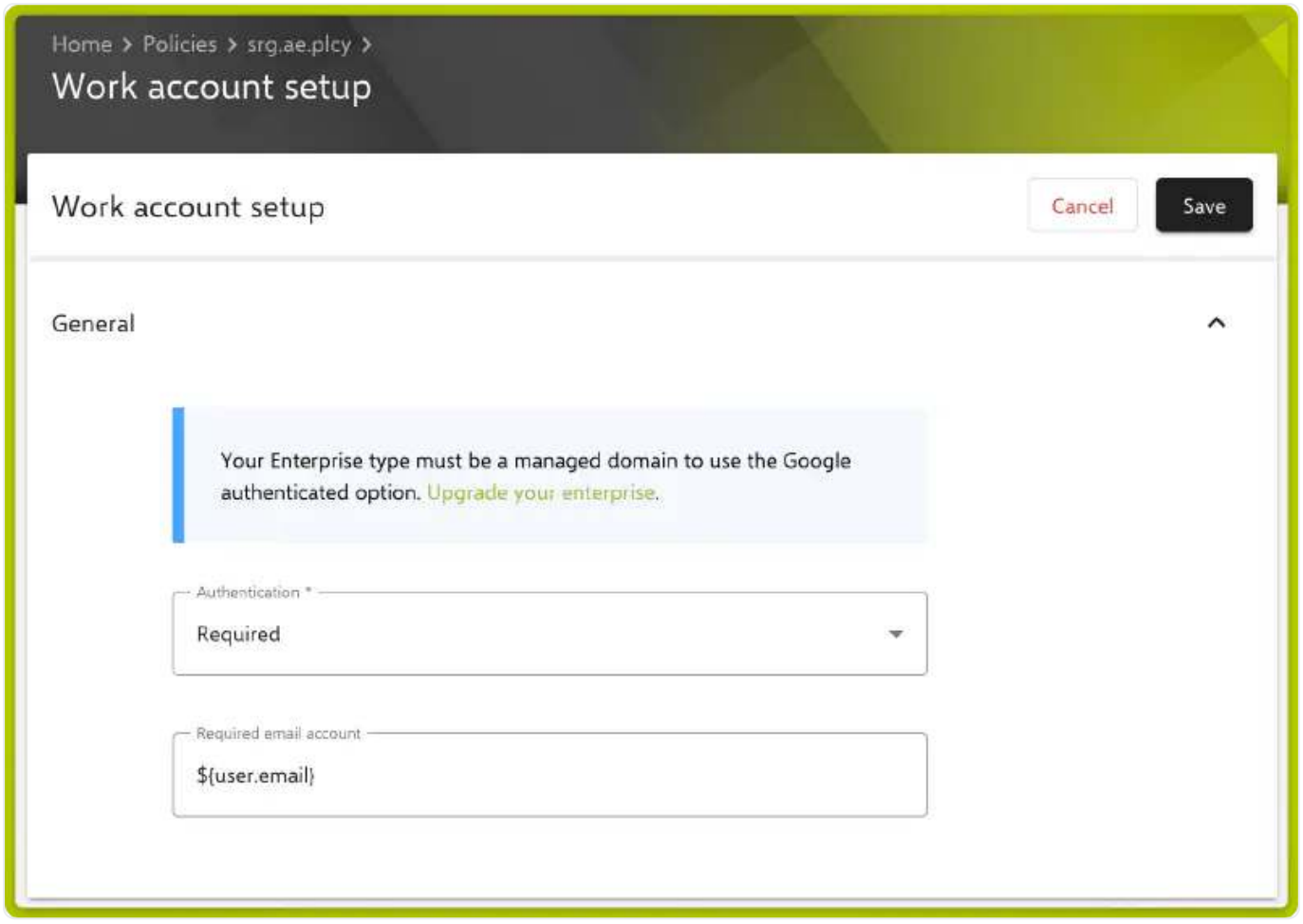
- Ces paramètres s'appliquent exclusivement au profil professionnel, y compris sur les appareils gérés avec profil personnel (COPE).
- Toutes les options ne sont pas disponibles dans la même mesure sur tous les appareils ou toutes les versions d'Android.
- L'application effective dépend du fabricant, de la version d'Android et du mode de l'appareil.

Pour la version 26.4.0

Configuration du compte de travail

La configuration de politique Configuration du compte professionnel permet aux administrateurs de configurer de manière centralisée les paramètres du compte Google professionnel sur les appareils entièrement gérés (Fully Managed Device).

L'option Requis nécessite que l'organisation Relution soit liée à une entreprise de type domaine Google géré. De plus, l'authentification des utilisateurs doit être activée pour le domaine Google géré dans la console d'administration Google (`admin.google.com`), faute de quoi la configuration ne prend pas effet. Si l'organisation est encore liée à un compte Google Play Enterprise, le formulaire affiche une indication concernant la mise à niveau de l'entreprise (voir Mise à niveau du compte GooglePlay Enterprise vers un domaine Google géré →). L'article Appareil géré → contient de plus amples informations sur la configuration.



Authentification

Définit si les utilisateurs doivent s’authentifier avec un compte Google professionnel lors de la configuration de l’appareil.

Option	Description
Non spécifié (par défaut)	Aucune exigence n’est définie. Le comportement correspond à Non requis.
Non requis	Aucune authentification par compte Google professionnel n’est requise.
Requis	Les utilisateurs doivent s’authentifier avec un compte Google professionnel.

Pour la version 26.4.0

Compte de messagerie requis

Lorsque Requis est sélectionné, le champ Compte de messagerie requis apparaît. Le compte e-mail du domaine géré avec lequel l’utilisateur doit se connecter y est saisi. Des espaces réservés peuvent être utilisés pour les créer dynamiquement.

Remplacements de sécurité avancés

Pour les appareils inscrits dans Android Enterprise, la configuration Débrayages de sécurité avancés offre des possibilités de contrôle approfondies. Les administrateurs peuvent y définir si l'installation de fichiers APK provenant de sources tierces est autorisée, si la vérification Google Play Protect est imposée et si le mode développeur est disponible à des fins de test. Des paramètres relatifs à l'extension de marquage mémoire, à la protection du contenu et aux notifications du profil professionnel sont également disponibles.

Autoriser depuis des sources inconnues

Ce paramètre contrôle si les applications peuvent être installées en dehors du Google Play Store (side-loading). Les options suivantes sont disponibles :

- Non spécifié (par défaut pour les nouvelles configurations) : Relution ne définit aucune valeur, le comportement par défaut d'Android Enterprise s'applique.
- Interdire les installations d'applications non fiables sur l'ensemble de l'appareil : Le side-loading est interdit sur tout l'appareil.
- Autoriser les installations d'applications non fiables uniquement dans le profil personnel de l'appareil : Le side-loading est exclusivement autorisé dans l'espace privé de l'utilisateur.
- Autoriser les installations d'applications non fiables sur l'ensemble de l'appareil : Le side-loading est permis sur tout l'appareil.

Pour la version 26.4.0

Forcer la vérification Google Play

Détermine si l'analyse de sécurité par Google Play Protect est obligatoire pour identifier les logiciels malveillants.

- Non spécifié (par défaut pour les nouvelles configurations) : Relution ne définit aucune valeur, le comportement par défaut d'Android Enterprise s'applique.
- Oui : La vérification est imposée au niveau du système et ne peut pas être désactivée par l'utilisateur.
- Choix de l'utilisateur : L'utilisateur final décide lui-même si la vérification doit être active.

Politique de chiffrement de l’appareil

Définit le niveau de sécurité du chiffrement des données sur le stockage physique.

Option	Description
Aucun chiffrement n’est nécessaire (par défaut)	Aucun chiffrement des données utilisateur n’est imposé.
Chiffrement requis, aucun mot de passe n’est nécessaire pour démarrer	Les données sont chiffrées, mais aucun mot de passe n’est requis lors du processus de démarrage.
Chiffrement requis, mot de passe requis pour démarrer	Le chiffrement est actif et nécessite la saisie d’un mot de passe dès le démarrage du système.

Le traitement des appareils qui ne respectent pas le chiffrement requis est défini dans la ligne Débrayages de sécurité avancés de la configuration Contrôle de la conformité →.

Pour la version 26.4.0

Autoriser les paramètres développeur

Ce paramètre définit si le mode développeur peut être déverrouillé sur l’appareil. Cela est principalement utile pour le débogage ou les tests d’applications. En utilisation standard de production, cette option devrait rester désactivée pour des raisons de sécurité.

Mode Critères Communs (Common Criteria)

Le mode Critères Communs est utilisé pour se conformer aux normes de sécurité internationales en matière de technologies de l’information.

Ce paramètre n’est appliqué qu’aux appareils entièrement gérés et aux appareils gérés avec profil personnel (COPE). Relution ne le transmet pas aux appareils avec profil de travail (BYOD).

Fonctionnement : L'activation renforce certains composants de sécurité spécifiques. Cela concerne notamment le chiffrement AES-GCM des clés Bluetooth à long terme (Long Term Keys) ainsi que le stockage sécurisé des configurations Wi-Fi.

Le mode Critères Communs impose un modèle de sécurité extrêmement strict. Celui-ci n'est généralement requis que pour les infrastructures informatiques des systèmes de sécurité nationale ou des organisations hautement sensibles. L'utilisation d'applications standards ou de fonctions quotidiennes de l'appareil peut en être affectée. Ce mode ne devrait être activé que si cela est explicitement requis.

Extension de marquage mémoire

Définit la politique relative à l'extension de marquage mémoire (Memory Tagging Extension, MTE). Le paramètre est signalé par les badges Android 14+, Profil de travail du COPE et Appareil géré.

Les options Non spécifié (par défaut pour les nouvelles configurations), Choix de l'utilisateur, Activé et Désactivé sont disponibles.

Pour la version 26.4.0

Protection du contenu

La protection du contenu analyse les applications trompeuses. Le paramètre est signalé par le badge Android 15+.

Les options Non spécifié (par défaut pour les nouvelles configurations), Choix de l'utilisateur, Activé et Désactivé sont disponibles.

Applications personnelles pouvant lire les notifications du profil professionnel

Définit quelles applications du profil personnel peuvent lire les notifications du profil professionnel. Le paramètre est signalé par le badge Profil de travail du COPE.

Un clic sur Ajouter ouvre une sélection d'applications dans laquelle une ou plusieurs applications sont choisies. Leurs noms de package sont repris ; chaque entrée peut être supprimée individuellement. Si la liste reste vide, Relution ne transmet aucun paramètre à Google.

Relution Files Android

Pour Android, Relution offre la possibilité d'intégrer des partages de fichiers locaux, également appelés lecteurs réseau, via SMB et WebDAV. Grâce à la connexion à des solutions serveur scolaires ou d'entreprise, il est ainsi possible d'accéder aux documents et contenus pertinents, ainsi que d'enregistrer données et résultats de travail en toute sécurité sur un serveur central.

Avantages de Relution Files

Les données ne devraient pas être stockées dans un cloud non sécurisé avec des serveurs situés hors de l'UE lorsqu'une conformité au RGPD est requise. Il est également recommandé de ne pas stocker les données directement sur les appareils lorsque ceux-ci sont utilisés par plusieurs personnes. En enregistrant et en déposant les documents sur des serveurs locaux propres via `Relution Files`, la sécurité et la souveraineté des données sont garanties pour tous les utilisateurs.

Pour la version 26.4.0

Configurer les lecteurs réseau locaux pour Relution Files

Les partages de fichiers locaux peuvent être configurés dans Relution de deux façons :

Pour la configuration manuelle, consulter la documentation de l'application elle-même -> Relution Files →

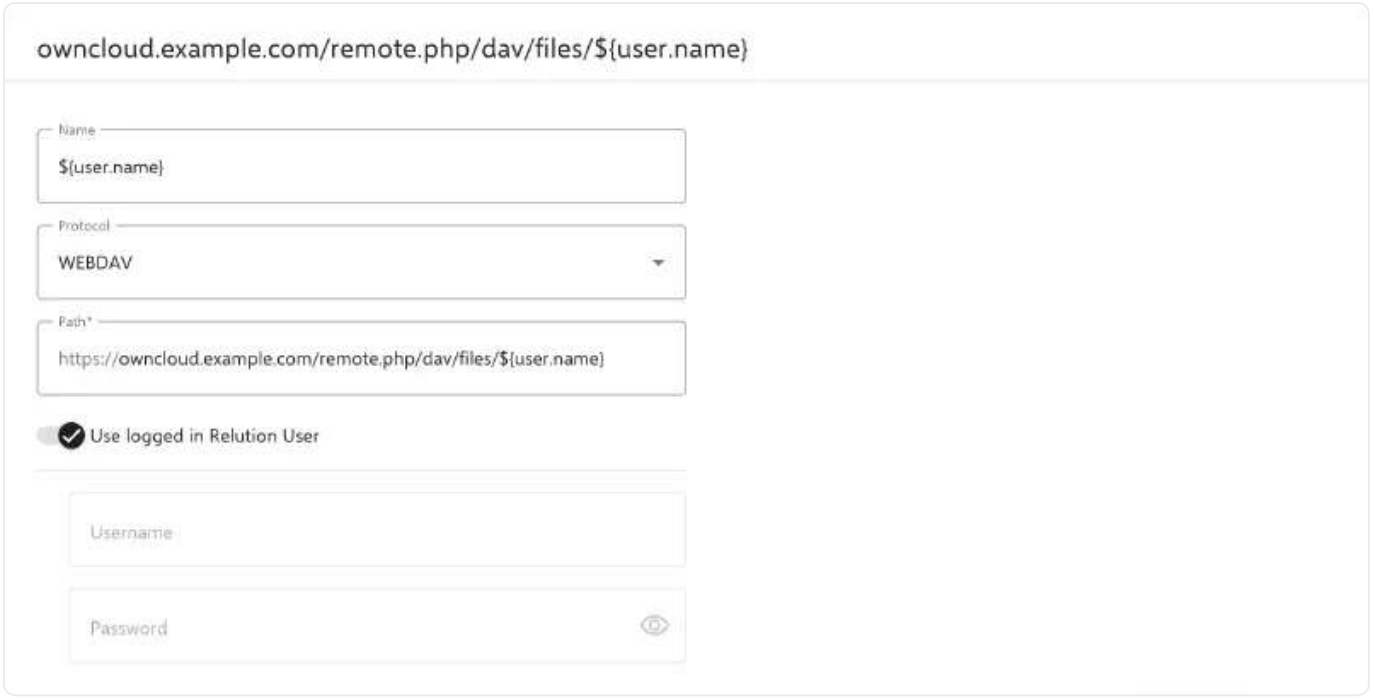
Configuration automatique de Relution Files via des politiques

Grâce à une configuration gérée que l'administrateur effectue via le portail Relution, presque tous les obstacles à la configuration de l'appareil sont supprimés pour l'utilisateur final. De cette façon, le partage de fichiers peut être utilisé de manière transparente.

Avec la configuration `Partages de fichiers Relution` dans une politique, une connexion WebDAV ou SMB peut être préparée pour l'utilisation. Sous Android, la configuration n'est disponible que dans les politiques Android Enterprise et ne peut être ajoutée qu'une fois par politique. Si une politique contient la configuration, Relution installe automatiquement l'application Relution Files en tant qu'application obligatoire et lui transmet la configuration gérée nécessaire. Une distribution séparée de l'application n'est pas nécessaire. Si Relution Files figure également dans Gérer les applications →, les paramètres qui y sont définis s'appliquent (par ex. le type d'installation).

Ajouter ouvre la boîte de dialogue Nouveau partage. Une configuration peut contenir plusieurs partages ; au moins un est nécessaire pour l'enregistrement. Pour chaque partage, un Nom facultatif, le Protocole (SMB ou WEBDAV) et le Chemin (obligatoire) sont indiqués. Sans nom, le dernier segment du chemin est utilisé. Pour SMB, le chemin doit contenir le partage réel (par ex. `server/share` ; le préfixe `smb://` est prédéfini). Les connexions WebDAV passent toujours par HTTPS (le préfixe `https://` est prédéfini). Des variables telles que `${user.name}` peuvent être utilisées dans le nom, le chemin, le nom d'utilisateur et le mot de passe et simplifient le processus de connexion.

De plus, l'option Utiliser l'utilisateur Relution connecté peut être activée pour le partage. Les identifiants de l'utilisateur Relution connecté sur l'appareil sont alors utilisés. Si l'option est désactivée, un Nom d'utilisateur et un Mot de passe fixes peuvent être enregistrés.



Fond d'écran

À partir de Relution 5.33, la configuration Papier peint est disponible pour Android Enterprise et Android Classic/Legacy. Sous Android Enterprise, elle porte le badge Appareil géré et s’applique aux appareils entièrement gérés ainsi qu’aux appareils gérés avec profil personnel (COPE), mais pas aux appareils avec profil de travail (BYOD). Cela permet de définir une image pour l’écran d’accueil qui apparaît sur les appareils après l’application de la politique. La politique permet également d’ajouter du texte (y compris des espaces réservés) pour afficher du texte dynamique sur le fond d’écran.

> Android Enterprise nécessite Relution Companion version 1.18
>
> Android Classic nécessite Relution Companion version 5.37

La configuration Papier peint définit l’image, mais n’empêche pas les utilisateurs de la modifier sur l’appareil.

Pour la version 26.4.0

Relution Decon (filtre)

À partir de la version 26.3, Relution permet la configuration d'un filtre de contenu basé sur DNS pour les appareils Android Enterprise. Cette fonctionnalité assure un accès Internet sécurisé et ciblé en restreignant l'accès à certains sites web. Grâce à la catégorisation des contenus basée sur l'IA, Relution Decon fournit également un contrôle parental complet avec des options avancées de configuration.

Qu'est-ce que Relution Decon ?

Relution Decon est un module complémentaire basé sur l'IA pour Android Enterprise qui filtre le contenu en temps réel, créant un environnement numérique sécurisé. Grâce au contrôle de contenu basé sur DNS, Decon bloque les sites web indésirables, permettant aux utilisateurs de travailler et d'apprendre dans un espace protégé et sans distraction.

Relution Decon utilise un proxy DNS pour transmettre toutes les requêtes au serveur Decon. Les sites web sont classés et soit autorisés, soit bloqués selon les règles définies par les politiques. Toutes les communications sont chiffrées SSL, garantissant la sécurité des activités des utilisateurs.

Pour la version 26.4.0

Application Decon

L'application Decon (`io.relution.decon`) est installée automatiquement par Relution sur les appareils dès qu'une politique contenant une configuration Decon est publiée. Une distribution préalable via Gérer les applications → n'est pas nécessaire. Une entrée à cet endroit ne reprend que des options complémentaires telles que le comportement de mise à jour, la version minimale ou les autorisations, mais pas le type d'installation. Une fois installée, elle agit comme le VPN permanent (Always-On) de l'appareil et surveille les requêtes DNS afin de garantir que seuls les contenus autorisés sont accessibles.

Fonctionnalités de l'application :

- Active un proxy DNS global, qui ne peut pas être désactivé par l'utilisateur
- Affiche le statut actuel de Relution Decon
- Fournit des informations sur les sites bloqués et les catégories de filtrage appliquées

Empêcher les modifications manuelles du VPN

Comme Relution Decon fonctionne comme un VPN permanent (Always-On), les utilisateurs pourraient sinon le désactiver ou le remplacer en modifiant les paramètres VPN de l'appareil. Pour l'empêcher, combiner les deux configurations suivantes :

- Restrictions → : activer l'option Désactiver la configuration VPN
- VPN permanent → : sélectionner `io.relution.decon` comme application VPN permanente

---

Politique Decon

Dans la politique des appareils, cliquer sur `Ajouter` → `Relution Decon`. Cette politique configure automatiquement l'application Decon sur les appareils associés et pris en charge, et agit comme proxy pour toutes les requêtes DNS.

La configuration est complétée lors de la publication de la politique.

Pour la version 26.4.0

Hiérarchie de configuration des politiques (de la plus haute à la plus basse priorité)

1. Domaines autorisés
2. Domaines bloqués
3. Catégories bloquées

Decon dans Relution Teacher

Sur les appareils Android Enterprise, Decon peut être sélectionné et géré dans les profils de classe à partir de Relution Server 26.3. Prérequis : l'application Decon est installée sur les appareils des élèves et une politique Decon leur est assignée. Relution Teacher n'affiche un avertissement concernant une configuration Decon manquante que pour les appareils iOS.

En savoir plus sur Relution Teacher →

Filtrage

Dans la section Filtrage de la politique Decon, le champ Type de filtre détermine le mode de filtrage des sites web :

- Arrêt : aucun filtrage par catégories ni par niveau d'âge.
- Catégories (par défaut) : les catégories à bloquer sont sélectionnées individuellement à l'aide de commutateurs. Ces commutateurs ne s'affichent que pour ce type de filtre. Par défaut, Contenu pour adultes, Publicité et Hameçonnage sont bloqués.
- Niveau d'âge : le filtrage s'effectue selon un niveau d'âge (0+, 6+, 12+ ou 16+, par défaut 12+).

Deux autres commutateurs sont disponibles indépendamment du type de filtre :

- Liste BPJM : filtre en plus les contenus classés comme inadmissibles par la BPjM. Les entrées sous Domaines autorisés peuvent néanmoins permettre l'accès à ces contenus.
- Recherche sécurisée : se règle indépendamment des catégories bloquées et du niveau d'âge. Le blocage de la catégorie Contenu pour adultes n'active pas la recherche sécurisée.

Si plusieurs configurations Decon sont utilisées sur un même appareil, le filtrage le plus fort prend automatiquement effet : les filtres basés sur l'âge priment sur les filtres basés sur les catégories. Les configurations sans filtrage sont ignorées.

Pour la version 26.4.0

Classification par catégorie

Relution Decon attribue automatiquement chaque site web à une catégorie. Avec le type de filtre Catégories, les administrateurs peuvent définir quelles catégories doivent être bloquées :

Catégorie	Description	Exemples
Contenu pour adultes	Sites inappropriés pour les jeunes	Pornographie, Violence, Armes, Drogues, Jeux d'argent, Divertissement adulte, Shopping adulte, Rencontres
Publicité	Sites publicitaires	Fournisseurs de publicité
Réseaux sociaux	Contenus de réseaux sociaux	Facebook, Instagram, TikTok, etc.

Catégorie	Description	Exemples
Divertissement	Sites de divertissement comme streaming ou jeux	Films, Jeux, Vidéos
Musique	Services de streaming musical	Spotify, Tidal, etc.
Actualités	Sites d’information et magazines	News, Météo
Achats	Boutiques en ligne (hors contenus adultes)	Amazon, eBay, etc.
Éducation	Sites éducatifs pour l’apprentissage	Wikipedia, Google Scholar
IA générative	Sites liés à l’intelligence artificielle	ChatGPT, Perplexity.ai, etc.
Hameçonnage	Sites potentiellement frauduleux	Escroqueries potentielles, Vol de données
Divers	Tous les autres sites	Restants

Pour

Domaines autorisés et bloqués

- Domaines autorisés / Domaines bloqués (section Domaines) : Permet de spécifier des domaines autorisés ou bloqués indépendamment des catégories. Seul le domaine doit être indiqué, pas le chemin. Les domaines autorisés restent accessibles même si le filtre les juge inappropriés. Le nombre de domaines bloqués devrait être limité à environ 500.

Confidentialité

Pour Android Enterprise, la section Confidentialité propose l’option Acceptation automatique de la divulgation des données (désactivée par défaut). Lorsqu’elle est activée, la divulgation des données est acceptée automatiquement au nom de l’utilisateur.

Gérer les applications

Avec Relution, les appareils Android Enterprise peuvent être équipés d'applications configurées. Une configuration Gérer les applications peut être utilisée pour distribuer les applications souhaitées aux appareils.
Plusieurs sources sont disponibles pour la sélection des applications :

- Applications du Relution App Store
- Applications du Managed Google Play Store
- Applications ajoutées manuellement.

Applications du Relution App Store

Le Relution App Store fournit toutes les applications ajoutées à partir du Managed Google Play Store.
L'avantage est le nombre réduit d'applications affichées, car l'intégralité du Managed Google Play Store n'est pas présentée.

> De plus, à partir de Relution Server 26.2 et des Relution Client Apps version 26.x, les APKs du Relution App Store peuvent être distribuées. Cela peut se faire via la liste Gérer les applications (type d'installation Sur mesure) ou les utilisateurs peuvent télécharger les APKs directement via l'agent Relution. L'action Installer l'application depuis le Relution Store est également disponible. Cela ne fonctionne que sur les appareils entièrement gérés, y compris avec profil personnel. Sur les appareils inscrits en tant que profil professionnel, les applications APK ne sont pas installées.

Pour la version 26.4.0

Plus de détails : Gérer les apps APK →

Applications du Managed Google Play Store

Toutes les applications du Managed Google Play Store sont disponibles. Ce magasin est similaire au Play Store utilisé dans les environnements personnels.

Applications privées du Managed Google Play Store

Le Managed Google Play Store permet également de télécharger des applications privées. Les applications privées sont également appelées applications payantes, car Google ne propose pas

d’option de paiement dans l’environnement entreprise.
Il existe trois options pour ce cas d’utilisation :

Installation via le Play Store privé

Les développeurs créent des applications avec un Unique Package Name.
Ces applications sont téléchargées dans le magasin privé de Google à l’aide d’un compte Google appartenant à l’entreprise et peuvent ensuite être sélectionnées dans Relution sous Managed Google Play Store.

Installation via le Play Store public

Les développeurs rendent les applications disponibles dans la section publique du Managed Google Play Store pour tout le monde.
Ces applications peuvent être ajoutées au Relution App Store comme décrit ci-dessus ou sélectionnées directement dans le Managed Google Play Store.

Installation manuelle via le mode développeur avec distribution manuelle (application non signée)

Pour cela, les options développeur doivent être activées et l’installation à partir de sources inconnues doit être autorisée sur tous les appareils recevant ces applications.
Les fichiers `.apk` sont ensuite installés manuellement sur les appareils. Dans ce cas, les applications ne sont pas gérées, ne peuvent pas être gérées via Relution et ne reçoivent pas de mises à jour.

Pour la version 26.4.0

Ajouter des applications manuellement

Les applications déjà préinstallées sur un appareil peuvent être gérées via cette méthode.
Le Package Name de l’application est requis pour identifier de manière unique les applications sur les appareils.

Noms des packages d’applications pour les appareils Samsung

- `com.samsung.android.dialer` | Application Téléphone
- `com.samsung.android.messaging` | Application Messages
- `com.sec.android.widgetapp.samsungapps` | Widget Homescreen
- `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` | Enregistreur vocal

- `com.samsung.android.oneconnect` | Smart Things
- `com.samsung.android.voc` | Samsung Members
- `com.sec.android.app.popupcalculator` | Calculatrice Samsung
- `com.mobeam.barcodeService` | Scanner de codes-barres
- `com.samsung.android.app.dressroom` | Fonds d'écran Samsung
- `com.samsung.android.scloud` | Samsung Cloud
- `com.samsung.android.widgetapp.yahooedge.finance` | Widget Finance
- `com.samsung.android.widgetapp.yahooedge.sport` | Widget Sports
- `com.samsung.app.highlightplayer` | Éditeur vidéo Samsung Story
- `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` | Calendrier Samsung
- `com.sec.android.gallery3d` | Galerie Samsung
- `com.sec.android.app.camera` | Appareil photo Samsung

Types d'installation

Pour la version 26.4.0

- Disponible – Les applications sont disponibles pour les utilisateurs via le Play Store pour téléchargement et installation.
- Préinstallé – Les applications sont préinstallées sur les appareils. Cependant, les utilisateurs peuvent supprimer les applications.
- Installé de force – Les applications sont toujours automatiquement téléchargées et installées sur les appareils.
- Bloqué – Les installations des applications sont explicitement bloquées.
- Sur mesure – défini automatiquement pour les applications APK du Relution App Store ; ce type ne peut être ni sélectionné ni modifié.

Configuration

Certains développeurs d'applications proposent une Configuration gérée. Relution l'affiche si elle est disponible.
Pour les applications APK du Relution Store, des configurations peuvent être fournies au format JSON.

Autorisations

Les autorisations des applications du Google Play Store peuvent être définies ici, par exemple :

- Réponse par défaut aux demandes d’autorisation
- Accès à la position approximative
- Accès à la position précise
- Connexion via Bluetooth

Avancé

Configurations avancées pour les applications du Play Store, par exemple :

- Partager des informations entre les profils
- Mode de mise à jour automatique
- Installer des certificats
- Gérer les configurations
- Empêcher la désinstallation
- VPN toujours sur l’exemption de verrouillage – définit si l’application peut communiquer sans connexion VPN lorsque le mode verrouillage est activé (voir VPN permanent →)

Ces options sont également disponibles pour les applications ajoutées manuellement. Pour les applications APK du Relution App Store, Avancé contient uniquement l’option Mode de désinstallation d’application par l’utilisateur avec les valeurs Non spécifié, Autoriser et Ne pas autoriser. Avec Autoriser, l’utilisateur peut désinstaller l’application ; une application supprimée de cette manière n’est pas réinstallée par Relution. Non spécifié équivaut à Ne pas autoriser.

Pour la version 26.4.0

Restrictions

Pour les appareils Android avec l'inscription Android Enterprise, une variété de restrictions est disponible dans Relution. En principe, il est conseillé de savoir précisément quelles restrictions sont combinées entre elles. Cela permet d'éviter que des appareils soient configurés de telle manière qu'ils ne soient plus utilisables.

Dans le portail, la configuration est divisée en plusieurs sections. L'aperçu suivant suit cette structure. Si une option ne s'applique qu'à certains types d'inscription ou à certaines versions d'Android, cela est indiqué pour l'option concernée.

Restrictions relatives aux comptes

- Désactiver l'ajout de nouveaux utilisateurs et profils
- Désactiver la suppression d'autres utilisateurs
- Désactiver l'ajout et la suppression de comptes
- Désactiver la configuration des informations d'identification
- Activer la sélection d'une clé privée si aucune règle de correspondance n'est définie : L'utilisateur peut choisir une clé privée si aucune règle n'est définie pour sélectionner automatiquement une clé privée et un certificat permettant d'authentifier l'appareil auprès d'un serveur. Pour les appareils dotés d'une version d'Android antérieure à Android 9, ce paramètre peut compromettre les clés d'entreprise.

Pour la version 26.4.0

Restrictions par défaut

Cette section n'est affichée que si l'ancien paramètre Applications provenant de sources inconnues est défini, dans une configuration existante, sur une valeur autre que Interdire les installations d'applications non fiables sur l'ensemble de l'appareil.

> Le paramètre Applications provenant de sources inconnues est obsolète. La configuration Débrayages de sécurité avancés est utilisée à la place. Si celle-ci est configurée, le paramètre obsolète est ignoré.

Pour plus d'informations : Remplacements de sécurité avancés →

Restrictions relatives aux applications

- Désactiver l'installation des applications
- Désactiver la désinstallation des applications
- Désactiver l'œuf de Pâques dans les paramètres

Restrictions relatives à la personnalisation

- Désactiver la personnalisation des icônes utilisateur
- Désactiver la personnalisation du fond d'écran
- Activer la date et le fuseau horaire automatiques (uniquement Appareil géré) : Détermine si la date, l'heure et le fuseau horaire automatiques sont activés sur un appareil appartenant à l'entreprise. Les options disponibles sont Par défaut, Choix de l'utilisateur et Appliqué.

Restrictions relatives à l'appareil

Cette section contient les restrictions générales de l'appareil ainsi que les paramètres inter-profils pour les appareils dotés d'un profil de travail.

Pour la version 26.4.0

Général

- Désactiver le keyguard (uniquement Appareil géré) : Concerne le keyguard dans son ensemble. Les fonctions individuelles de l'écran de verrouillage sont désactivées via Gestion avancée des fonctionnalités du keyguard →.
- Activer la protection contre la réinitialisation d'usine (FRP) (uniquement Appareil géré et Profil personnel) et Courriel du compte Google pour le FRP : voir Protection contre la réinitialisation d'usine →.
- Types de comptes pour lesquels la gestion est désactivée : Types de comptes que l'utilisateur ne peut pas gérer.
- Méthodes d'entrée autorisées et Services d'accessibilité autorisés : Les options disponibles sont Tous autorisés, Applications système uniquement et Système et applications supplémentaires spécifiées. Avec cette dernière option, les applications autorisées en plus sont enregistrées dans une liste.
- Visibilité du nom d'affichage de l'entreprise : Détermine si le nom d'affichage de l'entreprise est affiché sur l'appareil (Non spécifié, Visible sur l'appareil, Caché sur l'appareil). Le nom d'affichage lui-même est défini dans le champ Nom d'affichage de l'entreprise sous

`Paramètres` → `Spécifique à la plate-forme de l'appareil` → `Android pour les entreprises`.

- Politique de contenu d'assistance (à partir d'Android 15) : Contrôle si des contenus d'assistance tels que des captures d'écran et des informations sur les applications peuvent être envoyés à une application privilégiée comme une application d'assistance (Non spécifié, Autorisé, Non autorisé).
- Politique de remplissage automatique : Contrôle le service de remplissage automatique du système (à partir d'Android 8) avec les options Non spécifié, Choix de l'utilisateur et Désactivé. Pour restreindre complètement la gestion des identifiants, la Politique du fournisseur d'identifiants par défaut est également configurée.
- Politique du fournisseur d'identifiants par défaut (à partir d'Android 14) : Non spécifié, Non autorisé ou Non autorisé sauf pour le système.
- Impression : Non spécifié, Autorisé ou Non autorisé.

Paramètres du profil transversal

Ces paramètres s'appliquent uniquement aux types d'inscription Profil de travail et Profil personnel. Ils ne sont pas appliqués sur les appareils gérés sans profil de travail.

Pour la version 26.4.0

- Valeur par défaut des widgets du profil de travail : Détermine si les applications du profil de travail peuvent par défaut ajouter des widgets à l'écran d'accueil lorsque rien d'autre n'est défini pour l'application (Non spécifié, Autorisé, Non autorisé). Non spécifié correspond à Non autorisé.
- Copier-coller : Non spécifié, Autorisé ou Interdiction de passer du profil professionnel au profil personnel.
- Partage des données : Non spécifié, Autorisé, Interdiction de passer du profil professionnel au profil personnel ou Refusé.
- Afficher les contacts professionnels dans le profil personnel (section Contacts) : Non spécifié, Refusé, Autorisé ou Autoriser uniquement les applications système à accéder aux contacts professionnels dans le profil personnel. Une liste d'applications peut également être gérée : avec Non spécifié et Autorisé, elle contient les applications qui ne sont pas autorisées à y accéder ; avec les autres options, les applications qui sont autorisées à y accéder.

Restrictions multimédias

- Désactiver la capture d'écran
- Désactiver le réglage du volume principal
- Désactiver le partage de la position
- Désactiver le partage de contacts via Bluetooth

- Accès à la caméra : Par défaut, Choix de l'utilisateur, Caméra désactivée ou Accès aux caméras imposé. Contrôle l'utilisation de la caméra et détermine si l'utilisateur peut utiliser le bouton d'accès à la caméra (à partir d'Android 12). La désactivation de la caméra s'applique à l'ensemble de l'appareil sur les appareils entièrement gérés, et uniquement au sein du profil de travail sur les appareils dotés d'un profil de travail.
- Accès au microphone : Par défaut, Choix de l'utilisateur, Microphone désactivé ou Accès au microphone imposé. Contrôle l'utilisation du microphone et détermine si l'utilisateur peut utiliser le bouton d'accès au microphone (à partir d'Android 12). Ce paramètre n'a d'effet que sur les appareils entièrement gérés.

Restrictions réseau

- Désactiver la configuration Bluetooth
- Désactiver la configuration des réseaux mobiles
- Désactiver la réinitialisation des paramètres réseau
- Désactiver la configuration VPN
- Désactiver la modification des réseaux Wi-Fi (obsolète, voir la remarque ci-dessous) : voir Interdire la configuration du Wi-Fi →.
- Désactiver Android Beam (NFC) pour partager des données entre les applications
- Désactiver le Bluetooth
- Activer la trappe d'échappement réseau : Si aucune connexion réseau ne peut être établie au démarrage, la trappe d'échappement invite l'utilisateur à se connecter temporairement à un réseau afin d'actualiser la politique de l'appareil. Après l'application de la politique, le réseau temporaire est supprimé.
- Service de réseau préférentiel (uniquement Profil de travail) : Contrôle si le service de réseau préférentiel est activé dans le profil de travail (Non spécifié, Désactivé, Activé). Sur les appareils entièrement gérés, ce paramètre n'a aucun effet.

Pour la version 26.4.0

Restrictions relatives au stockage

- Désactiver le montage de supports externes physiques
- Désactiver le transfert de fichiers USB (obsolète, voir la remarque ci-dessous)

Restrictions de téléphonie

- Désactiver l'envoi et la réception de messages SMS
- Désactiver les appels sortants

- Désactiver les services de données itinérants
- Désactiver la configuration du partage de connexion et des points d'accès mobiles (obsolète, voir la remarque ci-dessous)
- Désactiver la configuration de diffusion cellulaire

> Les options Désactiver la modification des réseaux Wi-Fi, Désactiver le transfert de fichiers USB et Désactiver la configuration du partage de connexion et des points d'accès mobiles sont obsolètes. La configuration Connectivité des appareils → est utilisée à la place. Si les deux configurations sont présentes, ces trois options sont ignorées.

Pièges potentiels

Les options suivantes peuvent faire en sorte que les appareils ne soient plus utilisables ou joignables comme prévu.

Protection contre la réinitialisation d'usine

Avec l'option Activer la protection contre la réinitialisation d'usine (FRP), la réinitialisation aux paramètres d'usine via les paramètres de l'appareil Android peut être bloquée sur les appareils gérés. La réinitialisation via le menu de récupération n'est pas concernée.

Pour la version 26.4.0

Dans le champ Courriel du compte Google pour le FRP, les adresses e-mail des administrateurs de l'appareil sont enregistrées. Ces adresses doivent être des comptes Google. Si l'appareil a été réinitialisé aux paramètres d'usine, l'un de ces administrateurs doit se connecter avec son compte Google (e-mail et mot de passe) pour déverrouiller l'appareil. Si aucune adresse n'est indiquée, l'appareil n'offre aucune protection lors de la réinitialisation aux paramètres d'usine. Ce paramètre doit donc être utilisé avec prudence.

Interdire la configuration du Wi-Fi

Si Désactiver la modification des réseaux Wi-Fi est actif et qu'aucun réseau Wi-Fi n'est prédéfini, le Wi-Fi est désactivé sur l'appareil. Si les appareils ne peuvent pas établir de connexion Wi-Fi parce que les réseaux configurés sont inaccessibles ou défectueux, il n'est pas possible d'intervenir manuellement. Le paramètre ne peut alors plus être annulé non plus, car les appareils sont hors ligne.

Cette option ne doit être utilisée qu'en combinaison avec Activer la trappe d'échappement réseau. Si aucune connexion réseau ne peut être établie au démarrage, celle-ci permet de configurer temporairement un réseau Wi-Fi afin d'actualiser la politique de l'appareil.

Mises à jour système

Les mises à jour système sont un élément clé de la gestion des appareils dans Android Enterprise. Elles permettent de configurer les politiques de mise à jour pour les appareils gérés afin de garantir leur sécurité et leur stabilité.

Type de mise à jour système

Dans la section Gérer les mises à jour système, il est possible de définir le Type de mise à jour système pour les appareils gérés. Les options disponibles sont :

- Non spécifié (Unspecified) : Suit le comportement par défaut de l'appareil pour les mises à jour système. Cela nécessite généralement une acceptation manuelle des mises à jour.
- Automatique (Automatic) : Installe automatiquement les mises à jour système dès qu'elles sont disponibles.
- Fenêtre de maintenance (Maintenance Window) : Installe automatiquement les mises à jour système dans une fenêtre de maintenance quotidienne définie. Cela garantit également que les applications Play sont mises à jour pendant cette période. Cette option est recommandée pour les appareils kiosques afin de maintenir les applications épinglées au premier plan à jour.
- Ajourner (Postpone) : Retarde l'installation automatique des mises à jour système jusqu'à 30 jours maximum.

Pour la version 26.4.0

Lorsque Fenêtre de maintenance est sélectionné, les champs obligatoires Heure de début et Heure de fin apparaissent (préréglés sur 00:00 et 00:30). Les heures se rapportent à l'heure locale de l'appareil. Si l'heure de fin est antérieure à l'heure de début, la fenêtre de maintenance s'étend au-delà de minuit. L'heure de début et l'heure de fin doivent être espacées d'au moins 30 minutes, sinon la configuration ne peut pas être enregistrée.

Période annuelle de gel des mises à jour système

La Période annuelle de gel des mises à jour système définit des périodes pendant lesquelles aucune mise à jour système n'est installée. La date de début et la date de fin se composent uniquement d'un mois et d'un jour ; la période se répète chaque année.

Caractéristiques de la période de gel

- Pendant la période de gel, toutes les mises à jour système entrantes (y compris les correctifs de sécurité) sont bloquées.
- En dehors de la période de gel, le comportement normal des mises à jour s’applique.
- Les périodes de gel sont créées via Ajouter. Plusieurs périodes peuvent être définies et supprimées individuellement.
- Une période peut couvrir au maximum 90 jours. Au moins 60 jours doivent séparer deux périodes.
- Si la date de fin est antérieure à la date de début, la période inclut le changement d’année.

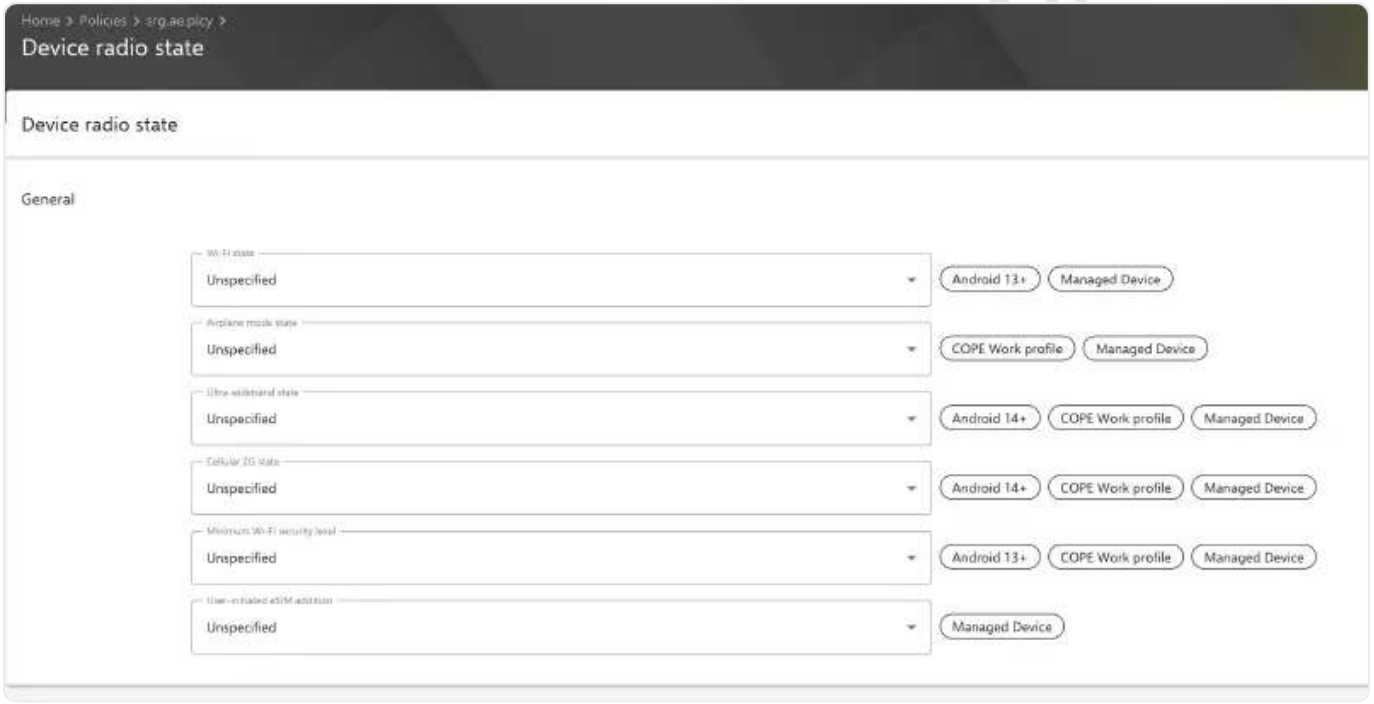
Pour la version 26.4.0

État radio de l'appareil

Cette politique gère de manière centralisée le statut et l'utilisation des technologies sans fil sur les appareils Android gérés.

La politique État radio de l’appareil permet une gestion centralisée des différentes technologies sans fil sur les appareils Android Enterprise. Les administrateurs peuvent définir si les utilisateurs sont autorisés à contrôler certaines fonctionnalités eux-mêmes ou si celles-ci doivent être activées ou désactivées de manière forcée.

Chaque paramètre propose en outre l’option Non spécifié, présélectionnée dans une nouvelle configuration. Dans ce cas, le comportement par défaut d’Android Enterprise défini par Google s’applique : Choix de l’utilisateur pour le Wi-Fi, le mode avion, l’Ultra Large Bande et le réseau cellulaire 2G, Sécurité réseau ouverte pour le niveau de sécurité Wi-Fi minimal et Autorisé pour l’ajout d’eSIM.



État du Wi-Fi

Définit l’état de la fonction Wi-Fi.

Options :

- Choix de l’utilisateur – Les utilisateurs peuvent activer ou désactiver le Wi-Fi eux-mêmes.

- Activé – Le Wi-Fi est toujours activé.
- Désactivé – Le Wi-Fi est toujours désactivé.

Support :

- Android 13+
- Appareils gérés

État du mode avion

Contrôle si le mode avion peut être activé.

Options :

- Choix de l'utilisateur – Les utilisateurs peuvent activer ou désactiver le mode avion eux-mêmes.
- Désactivé – Le mode avion est toujours désactivé.

Support :

- Profil de travail COPE
- Appareils gérés

Pour la version 26.4.0

État de l'ultra large bande (UWB)

Régule l'utilisation de l'Ultra Large Bande (par exemple, pour une localisation précise).

Options :

- Choix de l'utilisateur – Les utilisateurs peuvent activer ou désactiver l'UWB eux-mêmes.
- Désactivé – L'UWB est toujours désactivé.

Support :

- Android 14+
- Profil de travail COPE
- Appareils gérés

État de la connexion cellulaire 2G

Permet de restreindre l'utilisation des réseaux 2G (pertinent pour des raisons de sécurité).

Options :

- Choix de l'utilisateur – Les utilisateurs peuvent contrôler l'utilisation des réseaux 2G eux-mêmes.
- Désactivé – Les réseaux 2G sont toujours désactivés.

Support :

- Android 14+
- Profil de travail COPE
- Appareils gérés

Niveau de sécurité Wi-Fi minimal

Pour la version 26.4.0

Définit les normes de sécurité minimales que les connexions Wi-Fi doivent respecter.

Options :

- Sécurité réseau ouverte – Aucune restriction.
- Sécurité réseau personnelle – Exige au minimum WPA/WPA2.
- Sécurité réseau entreprise – Exige WPA2-Enterprise.
- Sécurité réseau entreprise 192 bits – Exigence de sécurité maximale.

Remarque : Les réseaux non sécurisés peuvent être bloqués si des politiques plus strictes sont définies.

Support :

- Android 13+
- Profil de travail COPE
- Appareils gérés

Ajout d'eSIM initié par l'utilisateur

Détermine si les utilisateurs sont autorisés à ajouter des profils eSIM de manière indépendante.

Options :

- Autorisé – Les utilisateurs peuvent ajouter des profils eSIM.
- Refusé – Les utilisateurs ne peuvent pas ajouter de profils eSIM.

Support :

- Appareils gérés

Pour la version 26.4.0

Mode kiosque

Avec la configuration de politique Mode kiosque Relution offre la possibilité de restreindre fortement le fonctionnement des appareils Android avec l'inscription Android Enterprise et de protéger les appareils contre une mauvaise utilisation.

Disposition de l'écran d'accueil de Relution

Sur les appareils entièrement gérés (Device Owner), la configuration Disposition de l'écran d'accueil de Relution active automatiquement le Mode kiosque en arrière-plan et définit l'application Relution Homescreen Layout App comme lanceur. Pour les autres inscriptions Android Enterprise (appareil géré avec profil personnel et profil de travail), l'application reçoit certes la disposition configurée, mais n'est pas définie comme lanceur kiosque. La configuration Disposition de l'écran d'accueil de Relution offre la possibilité de glisser-déposer la disposition de l'application sur les appareils via le Relution Portal. En outre, il est possible de définir une image de fond et d'y placer des textes statiques ou dynamiques personnalisés.

Dans cette configuration, le Relution Homescreen supprime les notifications sur l'écran de verrouillage.

Pour la version 26.4.0

> Les configurations Disposition de l'écran d'accueil de Relution et Mode kiosque s'excluent mutuellement. Si la politique contient déjà l'une des deux (même désactivée), l'autre ne peut pas être ajoutée.

Utiliser le lanceur par défaut

La configuration Mode kiosque remplace l'écran d'accueil de l'appareil par le lanceur par défaut d'Android Enterprise. Celui-ci affiche uniquement les applications gérées qui ont été installées via la configuration Gérer les applications (par exemple avec le type d'installation Installé de force ou Pré-installé), sur une seule page par ordre alphabétique. Toutes les autres applications sur les appareils sont masquées pour l'utilisateur et ne peuvent pas être utilisées.

L'utilisation du mode kiosque nécessite un appareil entièrement géré ou un appareil géré avec profil personnel (COPE) ; elle n'est pas disponible sur les appareils avec profil de travail (BYOD). L'activation du mode kiosque par défaut empêche l'utilisation de la fonction téléphone, ce qui supprime également la possibilité de passer des appels d'urgence.

Paramètres

Outre la section Personnaliser l'application Kiosk Launcher (voir ci-dessous), la configuration Mode kiosque comprend les sections Général et Personnalisation du kiosque.

Général

- Reste allumé lorsque la batterie est branchée – sélection multiple des modes de charge `AC`, `USB` et `WIRELESS` dans lesquels l'appareil reste allumé.
- Délai maximum de verrouillage du dispositif – sélection entre 15 secondes et 20 minutes. Sans sélection, le réglage par défaut de l'appareil s'applique. Un délai d'expiration fixe de l'écran défini dans la configuration Affichage → n'est transmis que s'il est inférieur à cette valeur.
- Désactiver les toasts et les superpositions – empêche l'affichage de toasts et de superpositions sur l'appareil.

Pour la version 26.4.0

Personnalisation du kiosque

Les valeurs suivantes sont présélectionnées dans une nouvelle configuration :

Champ	Présélection	Autres options
Actions du bouton d'alimentation	Disponible	Indisponible, Disponible - (par défaut)
Avertissements d'erreur système	Muet	Activé, Muted - (Par défaut)
Navigation dans le système	Désactivé	Activé, Bouton Home uniquement, Désactivé - (Par défaut)

Champ	Présélection	Autres options
Barre d’état	Désactivé	Activé, Informations système uniquement, Désactivé - (Par défaut)
Paramètres de l’appareil	Autorisé	Bloqué, Autorisé - (par défaut)

Les options portant la mention (par défaut) appliquent le comportement par défaut d’Android Enterprise. La section Personnalisation du kiosque n’est disponible que dans la configuration Mode kiosque, et non dans Disposition de l’écran d’accueil de Relution.

Utiliser un lanceur alternatif

Si des fonctionnalités et des applications supplémentaires autres que les applications ajoutées dans la configuration de la politique Gérer les applications doivent être disponibles sur les appareils Android, par exemple les applications système, il est nécessaire d’utiliser un lanceur alternatif. Pour ce faire, le commutateur Utilisez une application de lancement de kiosque personnalisée au lieu du lanceur par défaut est activé dans la section Personnaliser l’application Kiosk Launcher. Le bouton Sélectionnez du champ Sélectionnez une application de lancement personnalisée ouvre ensuite la boîte de dialogue Sélectionnez une application. La source Application Google Play Store gérée (Android Enterprise) y est choisie, puis l’application de lancement est ajoutée. Les sources Appli Relution App Store et Ajouter une application manuellement sont également disponibles. Ensuite, il est possible de configurer le lanceur. Utiliser la fonction Configurer l’application de lancement personnalisée pour le configurer manuellement.

Pour la version 26.4.0

Gestion du Play Store

Avec la configuration de politique Gestion du Play Store, Relution offre la possibilité de contrôler le fonctionnement des appareils Android avec l'inscription Android Enterprise en réduisant le contenu disponible dans le Google Play Store au contenu de la configuration Gérer les applications. Il est également possible de configurer les mises à jour des applications.

Google Play Store restreint

Activer le Play Store restreint - Désactivé

- Lorsque l'utilisateur ouvre le Google Play Store sur l'appareil, il peut voir et installer toutes les applications publiques.

Activer le Play Store restreint - Activé

- Lorsque l'utilisateur ouvre le Google Play Store sur l'appareil, aucune application ou seulement les applications de la configuration Gérer les applications sont visibles. En fonction du type d'installation spécifié dans la liste Gérer les applications, l'utilisateur peut installer les applications publiées.

Pour la version 26.4.0

> Si le Google Play Store restreint est activé, les applications qui ne figurent pas dans la configuration Gérer les applications sont automatiquement désinstallées de l'appareil. Les applications système et les applications que Relution ajoute elle-même à la politique (par ex. Relution Agent et Companion) sont exclues. Cela s'applique également si le Google Play Store restreint est activé via une leçon.

Mises à jour des applications

Le champ Mise à jour automatique de l'application de la configuration Gestion du Play Store propose 4 options :

- Choix de l'utilisateur
- Jamais
- Wi-Fi uniquement
- Toujours

Le mode kiosque peut empêcher les mises à jour automatiques.

Les options Désactiver l’installation des applications et Désactiver la désinstallation des applications (configuration Restrictions, section Restrictions relatives aux applications) empêchent toute installation ou désinstallation, y compris celles déclenchées par MDM.

Pour la version 26.4.0

Messages des utilisateurs

Sur les appareils Android Enterprise gérés, il est possible d'afficher un message sur l'écran de verrouillage. Cela facilite l'identification de l'appareil ou peut être utilisé pour indiquer un moyen de contact en cas de perte. De plus, un message de support court et un message de support long peuvent être configurés ; ceux-ci s'affichent sous forme de pop-up dans les paramètres système, par exemple lors de l'accès à un paramètre verrouillé.

Message	Emplacement d'affichage	Déclencheur
Message de l'écran de verrouillage	Écran de verrouillage de l'appareil	affiché en permanence
Message de support court	Pop-up dans les paramètres système	accès à un paramètre verrouillé
Message de support long	Pop-up dans les paramètres système	accès au paramètre d'administrateur de l'appareil

Pour la

> Tous les messages peuvent en outre être adaptés selon le pays : si un appareil est par exemple configuré en anglais, le message correspondant à la langue du système sera affiché. Chaque message se compose d'un Message par défaut et, en option, de messages localisés, créés dans le tableau situé en dessous avec la Langue correspondante. Si la langue du système de l'appareil ne correspond à aucun message localisé, le message par défaut s'affiche. Dès qu'un message localisé a été créé, le message par défaut devient un champ obligatoire.

Les trois messages prennent en charge des espaces réservés que Relution remplace individuellement pour chaque appareil, par exemple `${device.name}`, `${device.serialnumber}`, `${device.uuid}` ou des espaces réservés liés à l'utilisateur. Les espaces réservés disponibles sont affichés dans la zone Espaces réservés disponibles sous le formulaire.

Message de l’écran de verrouillage

Ce message s’affiche sur l’écran de verrouillage de l’appareil. Les contenus suivants sont recommandés :

- Nom de l’entreprise / de l’organisation
- Nom, numéro de série ou identifiant de l’appareil (via un espace réservé)
- E-mail de contact ou numéro de téléphone

Message de support court

Ce message s’affiche sous forme de pop-up dans les paramètres de l’appareil dès qu’un accès à un paramètre verrouillé est tenté.

Message de support long

Ce message s’affiche sous forme de pop-up dans les paramètres de l’appareil dès qu’un accès au paramètre d’administrateur de l’appareil est tenté.

Pour la version 26.4.0

Gestion des autorisations d'exécution

Via la configuration de politique Gestion des autorisations d’exécution, les Réponses par défaut aux demandes d’autorisation des applications gérées peuvent être définies globalement.

Dans la section Réponse par défaut pour les demandes d’autorisation, le champ Si une application demande une autorisation : propose les options Demander à l’utilisateur (par défaut), Accorder l’autorisation ou Refuser l’autorisation. La valeur prédéfinie est Demander à l’utilisateur (par défaut).

> La prudence est de mise avec les interdictions générales. Si l'approche est trop restrictive, certaines applications risquent de ne plus fonctionner comme souhaité.

De plus, en plus du comportement par défaut défini, il existe des exceptions pour des autorisations spécifiques.

Permissions Android par défaut

Les demandes d’autorisation présentes dans le système d’exploitation Android peuvent être configurées dans la configuration Gestion des autorisations d’exécution, ainsi que le comportement souhaité. Lors de l’ajout d’une autorisation, l’une des trois options est sélectionnée dans le champ Comportement (valeur par défaut : Demander à l’utilisateur (par défaut)).

> Les autorisations définies ici remplacent le paramètre défini plus haut dans la section Réponse par défaut pour les demandes d’autorisation. Cela vaut également pour les autorisations personnalisées.

Autorisations Personnalisées

Des demandes d’autorisation spécifiques à l’application peuvent être configurées si cela est requis par une application. Les noms de ces autorisations se trouvent généralement dans la documentation du fabricant d’applications respectif. Ici aussi, l’une des trois options est sélectionnée dans le champ Comportement lors de l’ajout d’une autorisation (valeur par défaut : Demander à l’utilisateur (par défaut)).

Pour la version 26.4.0

Wi-Fi

Cette politique distribue de manière centralisée des définitions de réseaux Wi-Fi aux appareils Android Enterprise.

La politique Wi-Fi permet de configurer de manière centralisée des réseaux Wi-Fi sur les appareils Android Enterprise, sans que les utilisateurs aient à saisir eux-mêmes les identifiants. Plusieurs configurations Wi-Fi peuvent être ajoutées simultanément à une même politique.

Le partage de connexion n'est pas contrôlé par cette politique, mais par l'option Paramètres de connexion de la configuration Connectivité des appareils →.

Définition du réseau

- Nom de la configuration Wi-Fi – nom interne pour l'identification dans Relution.
- Le SSID du réseau – nom du réseau en texte clair. Alternativement Représentation hexadécimale du SSID du réseau, nécessaire pour les SSID qui ne peuvent pas être encodés en UTF-8. Au moins l'un des deux champs est obligatoire. Si les deux sont renseignés, ils doivent correspondre.
- Ce réseau est masqué – à activer si le réseau ne diffuse pas son SSID.
- Rejoindre le réseau automatiquement – connecte l'appareil automatiquement dès que le réseau est à portée.

Pour la version 26.4.0

Type de sécurité

- Type de sécurité : Aucun/Ouvert, WEP PSK, WPA/WPA2/WPA3 PSK, WEP 802.1x, WPA/WPA2/WPA3 EAP.
- Phrase secrète : requise pour les types de sécurité basés sur PSK.

Authentification EAP (WEP 802.1x, WPA/WPA2/WPA3 EAP)

- Accepter les types d'EAP : PEAP, TLS, TTLS, SIM, AKA ou PWD, ainsi que Identité (champ obligatoire). Pour PWD, également Mot de passe.
- Pour PEAP et TTLS, également Identité anonyme, Mot de passe et Phase 2 de l'authentification : PAP ou MSCHAPv2.
- Pour TLS, PEAP et TTLS : Type de certificat client ou modèle de certificat (voir Gestion des certificats →) et Version maximale du protocole TLS.

- Vérification du certificat serveur : Certificats CA de confiance, Correspondance des suffixes de domaines (champ obligatoire, Android rejette une liste vide comme non sécurisée), Correspondance avec le nom alternatif du sujet (SAN) et, en option, Sous-chaîne du nom d'objet du certificat des services RADIUS approuvés.
- Activer la mise en cache des clés opportuniste pour une itinérance rapide

---

Randomisation de l'adresse MAC

Mode de randomisation de l'adresse MAC (Matériel/Automatique, par défaut : Automatique) — transmis uniquement aux appareils sous Android 13 ou version ultérieure.

Proxy

Dans la section Paramètres du proxy, Type de proxy définit le type de proxy : Aucun, Manuelle ou Configuration automatique (PAC).

- Avec Manuelle : Hôte et Port pour Proxy HTTP, Proxy HTTPS, Proxy FTP et/ou Proxy SOCKS, au moins un proxy devant être indiqué, ainsi que Contourner le proxy pour (liste d'adresses qui ne sont pas acheminées via le proxy).
- Avec Configuration automatique : URL du PAC.

Pour la version 26.4.0

Un proxy qui s'applique indépendamment du réseau connecté est défini via la configuration Proxy mondial →.

Prise en charge

- Appareils gérés (Device Owner)
- Profil professionnel COPE (Personal Profile Enabled)
- Non disponible pour un profil professionnel pur (BYOD/Profile Owner)

VPN permanent

Cette politique définit quelle application VPN reste en permanence active sur l'appareil.

La politique VPN permanent détermine quelle application VPN déjà installée doit rester en permanence active sur un appareil Android Enterprise. Contrairement aux configurations StrongSwan →, qui équipent une application VPN spécifique de son propre profil, cette politique sélectionne uniquement quelle application fait office de VPN toujours actif – l'application elle-même doit être installée séparément via Gérer les applications →, car elle n'est pas déployée automatiquement par cette politique.

Paramètres

> Les paramètres du VPN toujours actif peuvent être modifiés par l'utilisateur sur l'appareil, sauf si l'option Désactiver la configuration VPN est activée dans les Restrictions →.

- Sélectionner l'application Always-On VPN (obligatoire, bouton Sélectionnez) – l'application qui doit rester en permanence active comme connexion VPN.
- Refuser la mise en réseau lorsque le VPN n'est pas connecté (mode verrouillage) – autorise le trafic réseau exclusivement via la connexion VPN. Tant que le VPN n'est pas connecté, aucun accès réseau n'est possible. Même lorsque le VPN est connecté, tout trafic en dehors du tunnel reste bloqué, sauf si l'application concernée est définie comme exemption de verrouillage →.

> Lorsque le mode verrouillage est activé, l'appareil doit pouvoir se connecter au VPN. Dans le cas contraire, aucune connexion Wi-Fi n'est possible et l'appareil ne peut pas communiquer avec Relution.

Tunnel divisé

La politique VPN permanent détermine uniquement quelle application VPN reste en permanence active. Le trafic acheminé via le tunnel est déterminé par la configuration de l'application VPN ou de la passerelle VPN. Si celle-ci ne limite pas le tunnel à certaines applications ou à certains réseaux de destination, Android achemine l'ensemble du trafic via le VPN.

Pour la version 26.4.0

Le tunnel divisé (split tunneling) est donc également possible en combinaison avec le VPN permanent, à condition que l'application VPN le prenne en charge :

- Configuration de l'application VPN – Si l'éditeur propose une configuration gérée, celle-ci est disponible dans Gérer les applications → via l'action Configuration. Les possibilités de définir des applications ou des réseaux pour le tunnel dépendent du client VPN concerné.
- StrongSwan – Dans le Profil VPN StrongSwan →, la section Applications permet de choisir entre Seules ces applications utiliseront le VPN et Ces applications n'utiliseront pas le VPN (par défaut). Si la liste reste vide avec Ces applications n'utiliseront pas le VPN, toutes les applications utilisent le VPN. La section Tunnel divisé permet en outre de répartir le trafic selon les réseaux de destination : Acheminer uniquement le trafic vers des sous-réseaux spécifiques via le VPN, tout le reste étant acheminé comme s'il n'y avait pas de VPN ou Le trafic vers ces sous-réseaux ne sera pas acheminé via le VPN. En option, Bloquer le trafic IPv4 non destiné au VPN et Bloquer le trafic IPv6 non destiné au VPN bloquent le reste du trafic de la version de protocole concernée.
- Passerelle VPN – Alternativement, la passerelle transmet à l'appareil uniquement les réseaux internes comme routes, au lieu de faire passer l'ensemble du trafic par le tunnel.

Mode verrouillage et exemptions

Pour la version 26.4.0

Lorsque le mode verrouillage est activé, Android bloque tout trafic qui ne passe pas par le VPN. Les applications exclues du tunnel via le tunnel divisé n'ont alors aucune connexion réseau. Il en va de même pour le trafic vers des réseaux de destination pour lesquels le VPN ne fournit pas de route. Un tunnel divisé basé uniquement sur les réseaux de destination n'est donc pas utilisable lorsque le mode verrouillage est activé. Cela vaut également pour la répartition par sous-réseaux dans la section Tunnel divisé du Profil VPN StrongSwan.

Certaines applications peuvent être exemptées du verrouillage. Pour cela, l'option VPN toujours sur l'exemption de verrouillage est définie dans Gérer les applications → via l'action Avancée :

- Non spécifié / Appliquer – l'application est soumise au mode verrouillage.
- Exemption – l'application peut communiquer même sans connexion VPN active. Ce paramètre est pris en charge à partir d'Android 10.

L'option n'est pas disponible pour les applications APK du Relution App Store. Pour celles-ci, Avancée contient uniquement l'option Mode de désinstallation d'application par l'utilisateur.

Une application exemptée continue d'utiliser le VPN tant que l'application VPN l'inclut dans le tunnel. Pour qu'une application communique en dehors du tunnel lorsque le mode verrouillage est activé, elle doit donc être marquée comme Exemption et également être exclue du tunnel dans l'application VPN.

Prise en charge

- Appareils gérés (Device Owner)
- Profil professionnel COPE (Personal Profile Enabled)
- Profil professionnel (Profile Owner/BYOD)

Pour la version 26.4.0

StrongSwan

Ces politiques configurent l'application StrongSwan ainsi que ses profils VPN sur les appareils Android Enterprise.

Relution propose deux politiques complémentaires pour l'application StrongSwan → (`org.strongswan.android`) : Restrictions StrongSwan contrôle le comportement de l'application et référence un profil par défaut, tandis que Profil VPN StrongSwan définit la connexion VPN IKEv2 proprement dite. Via VPN permanent →, l'application StrongSwan peut en outre être définie comme application VPN toujours active. Le profil connecté est déterminé par le paramètre Sélectionner un profil VPN par défaut dans les Restrictions StrongSwan.

Dès qu'une politique contient l'une des deux configurations, Relution installe automatiquement l'application StrongSwan en tant qu'application obligatoire, lui accorde les autorisations demandées et lui permet d'installer des certificats. Une attribution séparée via Gérer les applications → n'est pas nécessaire. Un paramètre défini à cet endroit pour StrongSwan, par exemple un type d'installation différent, est écrasé.

Pour la version 26.4.0

Restrictions StrongSwan

- Permettre aux utilisateurs de créer des profils
- Permettre aux utilisateurs d'importer des profils
- Permettre aux utilisateurs d'utiliser des profils existants
- Permettre aux utilisateurs d'importer des certificats
- Autoriser les utilisateurs à accéder aux paramètres
- Ne pas afficher d'avertissement si l'application n'est pas dans la liste blanche d'alimentation de l'appareil
- Sélectionner un profil VPN par défaut (bouton Sélectionnez) – référence à une configuration Profil VPN StrongSwan de la même version de politique

Profil VPN StrongSwan

Plusieurs profils VPN peuvent être créés et gérés dans le portail. Le formulaire se compose de la zone Profil VPN StrongSwan avec les sections Général, Certificat d'utilisateur et Certificat CA, ainsi que de la zone Paramètres avancés.

Général

- Nom du profil
- Serveur – adresse du serveur VPN. Le port est défini sous Paramètres avancés.
- Type de VPN :
  - IKEv2 EAP (nom d'utilisateur/mot de passe)
  - Certificat IKEv2
  - Certificat IKEv2 + EAP (nom d'utilisateur/mot de passe)
  - IKEv2 EAP-TLS (Certificat)
  - IKEv2 EAP-TNC (nom d'utilisateur/mot de passe)
- Nom d'utilisateur – uniquement pour les types de VPN avec nom d'utilisateur/mot de passe

Certificat d'utilisateur

Cette section n'apparaît que pour les types de VPN avec certificat. Le certificat utilisateur y est défini (voir Gestion des certificats →).

Certificat CA

Certificat CA ou certificat du serveur permettant de vérifier le serveur VPN.

Pour la version 26.4.0

Paramètres avancés

La zone Paramètres avancés est divisée en plusieurs sections.

Général

- Identité du serveur et Identité du client
- Serveurs DNS, MTU de l'appareil du tunnel VPN, Port et Intervalle de maintien NAT-T
- Envoyer des demandes de certificat
- Vérification du certificat via OCSP ou LCR, ainsi que Utiliser un contrôle strict de la révocation
- Utiliser des signatures RSA/PSS et Utiliser les adresses de transport IPv6

Tunnel divisé

- Sous-réseaux à inclure ou exclure
- Bloquer le trafic IPv4/IPv6 non destiné au VPN

Proxy

Hôte, port et Exclure des hôtes du proxy.

Applications

- Seules ces applications utiliseront le VPN – seules les applications listées utilisent le VPN, toutes les autres applications communiquent en dehors du tunnel
- Ces applications n'utiliseront pas le VPN – les applications listées communiquent en dehors du tunnel, toutes les autres applications utilisent le VPN. Si la liste reste vide, l'ensemble du trafic est acheminé via le VPN.

Lorsque le mode verrouillage est activé dans VPN permanent →, les applications en dehors du tunnel ne disposent d'une connexion réseau que si elles sont définies comme exemption de verrouillage.

> Une connexion automatique à la demande (On Demand) n'est pas possible avec Android Enterprise. Le VPN est connecté une fois manuellement dans l'application StrongSwan ; ensuite, le trafic des applications définies passe par le tunnel. Cela vaut aussi avec VPN permanent → : l'utilisateur établit lui-même la connexion initiale.

Algorithmes

Algorithmes IKEv2 et Algorithmes IPsec/ESP.

Prise en charge

Pour la version 26.4.0

- Appareils gérés (Device Owner)
- Profil professionnel COPE (Personal Profile Enabled)
- Profil professionnel (Profile Owner/BYOD)

Usage personnel

Cette politique configure l'usage personnel pour un appareil entièrement géré avec profil professionnel.

La politique Usage Personnel restreint le profil personnel d’un appareil entièrement géré avec profil professionnel (COPE).

Paramètres

- Désactiver la caméra – désactive la caméra dans le profil personnel.
- Interdire les captures d’écran – empêche les captures d’écran dans le profil personnel.
- Types de comptes pour lesquels la gestion est désactivée – empêche l’ajout de certains types de comptes dans le profil personnel.
- Nombre maximal de jours pendant lesquels le mode Travail peut être désactivé – limite la durée pendant laquelle les utilisateurs peuvent suspendre le mode Travail (minimum 3 jours, valeur par défaut 90).
- Autoriser le partage Bluetooth – contrôle si le contenu du profil personnel peut être partagé par Bluetooth. Valeurs : Non spécifié (par défaut, se comporte comme Autorisé), Autorisé, Refusé. Refusé nécessite Android 8 ; une violation de conformité est signalée sur les appareils plus anciens.
- Les utilisateurs peuvent créer un profil d’espace privé – autorise ou empêche la création d’un profil Private Space supplémentaire. Valeurs : Non spécifié (par défaut, se comporte comme Autorisé), Autorisé, Refusé. Avec Refusé, les espaces privés existants sont supprimés.

Pour la version 26.4.0

Play Store personnel

- Type de liste : liste de blocage ou liste d’autorisation
- Apps bloquées ou Apps autorisées – contrôle quelles applications peuvent être installées depuis le Play Store dans le profil personnel.

Prise en charge

- Profil professionnel COPE (appareil entièrement géré avec profil professionnel)

Mot de passe de l’appareil

Cette configuration définit les exigences de mot de passe pour le verrouillage de l’ensemble de l’appareil.

La configuration Mot de passe de l’appareil définit les exigences relatives au verrouillage des appareils Android Enterprise. Les exigences s’appliquent à l’ensemble de l’appareil. Les exigences relatives à un mot de passe distinct pour le profil professionnel sont en revanche définies via la configuration Code secret du profil professionnel →.

Différence avec le mot de passe du profil professionnel

Les deux configurations utilisent le même formulaire pour les exigences de mot de passe, mais leur portée diffère :

26.4.0

	Mot de passe de l’appareil	Code secret du profil professionnel
Portée	Verrouillage de l’appareil (ensemble de l’appareil)	Profil professionnel uniquement
Badges dans le formulaire	aucun	Profil de travail, Profil personnel
Appareils entièrement gérés	appliquée	ignorée par le serveur
Options supplémentaires	aucune	Désactiver les applications de profil professionnel jusqu’à ce que l’utilisateur respecte les exigences, Exiger un code d’accès distinct pour le profil professionnel

Les deux configurations peuvent faire partie de la même stratégie. Relution transmet alors les deux exigences à l’appareil : l’une pour l’appareil, l’autre pour le profil professionnel.

Les appareils entièrement gérés → ne disposent pas de profil professionnel. Une configuration Code secret du profil professionnel ne leur est pas transmise ; le verrouillage de l'appareil y est contrôlé exclusivement via Mot de passe de l'appareil.

Types d'inscription pris en charge

Le formulaire n'affiche aucun badge ; la configuration n'est donc limitée à aucun type d'inscription. Elle est disponible pour tous les types d'inscription Android Enterprise :

- Appareil géré →
- Appareil géré avec profil personnel →
- Appareil avec profil de travail →

Qualité du code d'accès

Complexité minimale à respecter lors de la définition du mot de passe. Pour une nouvelle configuration, Numérique est présélectionné.

Pour la version 26.4.0

Les options suivantes sont disponibles :

- Complexe (fort)
  Le mot de passe doit contenir au moins une lettre, un chiffre et un caractère spécial. Avec cette sélection, les champs obligatoires suivants apparaissent en plus (valeur minimale autorisée entre parenthèses) :
  - Nombre minimum de lettres (1)
  - Nombre minimum de lettres minuscules (0)
  - Nombre minimum de lettres majuscules (0)
  - Nombre minimum de caractères autres que des lettres (0)
  - Nombre minimum de caractères numériques (1)
  - Nombre minimum de symboles (1)

  Les champs sont vides pour une nouvelle configuration. La configuration ne peut être enregistrée qu'une fois tous les champs remplis.

- alphanumériques
  Le mot de passe doit contenir des chiffres et des lettres (ou des symboles).

- Alphabétique
  Le mot de passe doit contenir des lettres (ou des symboles).

- Complexe numérique
  Le mot de passe se compose de chiffres sans séquences répétitives ni ordonnées. Le portail affiche l'indication : « L'utilisateur doit avoir saisi un mot de passe contenant au moins des caractères numériques sans séquences répétitives (4444) ou ordonnées (1234, 4321, 2468). »

- Numérique
  Le mot de passe doit contenir des chiffres.

- Motif
  Malgré son nom, aucun schéma de déverrouillage n'est imposé. Un verrouillage quelconque doit simplement être configuré (par ex. schéma, code PIN ou mot de passe), sans exigence quant à son contenu.

- Biométrique (faible)
  L'appareil doit être protégé au minimum par une méthode de déverrouillage biométrique de faible sécurité. Avec cette sélection, tous les autres champs sont masqués.

> Les options réellement disponibles et applicables dépendent de l'appareil, de la version d'Android et des personnalisations du fabricant.

Pour la version 26.4.0

Longueur minimale du code d'accès

Définit le nombre minimal de caractères du mot de passe. Le champ est obligatoire et prérempli avec `4`. La plus petite valeur autorisée est également `4`.

Âge maximum du code d'accès (en jours)

Nombre maximal de jours avant qu'un nouveau mot de passe doive être défini. Avec la valeur `0`, le mot de passe n'expire jamais. Le champ est obligatoire et prérempli avec `0`.

Historique du code d'accès

Nombre de mots de passe déjà utilisés qui sont enregistrés et ne peuvent pas être réutilisés. Le champ est obligatoire et prérempli avec `0` ; la réutilisation n'est alors pas limitée.

Nombre de tentatives échouées avant l’effacement des données

Le champ Nombre de tentatives de code secret ayant échoué avant que toutes les données ne soient effacées définit après combien de saisies incorrectes les données sont effacées. La plus petite valeur autorisée est `1`. Le champ est facultatif : sans valeur, les données ne sont jamais effacées.

Comportement en cas de non-conformité

Si le mot de passe de l’appareil ne respecte pas les exigences, l’appareil signale une violation de conformité. Le délai au terme duquel l’appareil est alors bloqué puis réinitialisé est défini dans la ligne Code d’accès à l’appareil de la configuration Contrôle de la conformité →. Cette ligne s’applique aux appareils entièrement gérés et aux appareils gérés avec profil personnel. Sur les appareils avec profil de travail, c’est la ligne Code secret du profil professionnel qui s’applique. Sans règle personnalisée, les délais par défaut s’appliquent.

Seule la configuration Code secret du profil professionnel propose une option permettant de désactiver les applications jusqu’à ce que les exigences soient remplies.

Pour la version 26.4.0

Remarques

- La configuration Mot de passe de l’appareil ne peut être ajoutée qu’une seule fois par stratégie.
- Toutes les options ne sont pas disponibles dans la même mesure sur chaque appareil ou chaque version d’Android.
- L’application effective dépend du fabricant, de la version d’Android et du type d’inscription.

Gestion avancée des fonctionnalités du keyguard

Cette configuration désactive certaines fonctionnalités de l’écran de verrouillage sur les appareils gérés.

La configuration Gestion avancée des fonctionnalités du keyguard désactive certaines fonctionnalités de l’écran de verrouillage (keyguard) des appareils Android Enterprise, par exemple la caméra, les notifications ou les méthodes de déverrouillage biométriques. Le verrouillage lui-même est conservé. Les exigences relatives au mot de passe de verrouillage sont définies via la configuration Mot de passe de l’appareil →.

Types d’inscription pris en charge

Le badge Appareil géré du formulaire indique que la configuration est destinée aux appareils d’entreprise :

- Appareil géré →
- Appareil géré avec profil personnel →

La configuration n’est pas prévue pour les appareils avec profil de travail → (BYOD). Elle ne peut être ajoutée qu’une seule fois par stratégie.

Pour la version 26.4.0

Désactivation des fonctionnalités du keyguard

La section Général contient une case à cocher par fonctionnalité. Aucune n’est cochée pour une nouvelle configuration. Chaque case cochée désactive la fonctionnalité correspondante sur les écrans de verrouillage sécurisés.

Option	Effet (texte d’aide du portail)
Désactiver tout	Désactive toutes les personnalisations actuelles et futures du keyguard
Désactiver la biométrie	Désactive toutes les authentifications biométriques sur les écrans de verrouillage sécurisés

Option	Effet (texte d'aide du portail)
Désactiver la caméra	Désactive la caméra sur les écrans de verrouillage sécurisés (par exemple, code PIN)
Désactiver les empreintes	Désactive le capteur d'empreintes digitales sur les écrans de verrouillage sécurisés
Désactivation de la saisie	Désactive la saisie de texte dans les notifications sur les écrans de verrouillage sécurisés
Désactiver le visage	Désactive l'authentification faciale sur les écrans de verrouillage sécurisés
Désactiver l'iris	Désactive l'authentification par iris sur les écrans de verrouillage sécurisés
Désactiver les notifications	Désactive l'affichage de toutes les notifications sur les écrans de verrouillage sécurisés
Désactiver l'état de Trust Agent	Ignore l'état des Trust Agents sur les écrans de verrouillage sécurisés
Désactiver les notifications non expurgées	Masque les contenus sensibles des notifications sur l'écran de verrouillage

Lorsque Désactiver tout est coché, toutes les autres cases sont décochées et désactivées, car elles sont déjà incluses dans cette sélection. Les fonctionnalités individuelles ne peuvent être de nouveau sélectionnées qu'après avoir décoché Désactiver tout.

> La présence effective d'une fonctionnalité sur l'écran de verrouillage (par ex. scanner d'iris ou reconnaissance faciale) dépend de l'appareil.

Différence avec les restrictions

La configuration Restrictions → contient l'option Désactiver le keyguard. Cette option concerne le keyguard dans son ensemble, tandis que Gestion avancée des fonctionnalités du keyguard ne désactive que certaines fonctionnalités de l'écran de verrouillage.

Contrôle de la conformité

Cette configuration définit quand les appareils non conformes sont bloqués et effacés.

La configuration Contrôle de la conformité définit des actions de blocage et d'effacement pour les appareils Android Enterprise qui ne respectent pas certaines exigences d'une stratégie. Pour chaque configuration prise en charge, il est possible de définir après combien de jours de non-conformité l'appareil est bloqué, puis effacé.

La configuration est disponible pour tous les types d'inscription Android Enterprise et ne peut être ajoutée qu'une seule fois par stratégie. Le type d'inscription auquel s'applique une règle dépend de sa ligne (voir ci-dessous).

Comportement par défaut

Sans règle personnalisée, Relution définit des règles par défaut pour les paramètres surveillés : les appareils non conformes sont bloqués après 20 jours et effacés après 30 jours.

Les règles personnalisées ne peuvent que raccourcir les délais : 10 jours au maximum sont autorisés pour le blocage et 30 jours au maximum pour l'effacement.

Pour la version 26.4.0

Vue d'ensemble des configurations

Le tableau du formulaire contient toujours les quatre mêmes lignes, une par configuration dont la non-conformité peut être sanctionnée. Les colonnes affichent les valeurs de la règle correspondante : Bloc après jours, Champ d'application du bloc, Essuyer après quelques jours et Préserver la protection de la réinitialisation d'usine.

Ligne	Paramètres surveillés	S'applique à
Débrayages de sécurité avancés	Politique de cryptage des appareils de Remplacements de sécurité avancés →	tous les types d'inscription

Ligne	Paramètres surveillés	S’applique à
Code d’accès à l’appareil	Exigences de mot de passe de Mot de passe de l’appareil → et Code secret du profil professionnel →	appareils entièrement gérés, appareils gérés avec profil personnel
Code secret du profil professionnel	Exigences de mot de passe de Mot de passe de l’appareil → et Code secret du profil professionnel →	appareils avec profil de travail
Restriction	Méthodes d’entrée autorisées, Services d’accessibilité autorisés et Désactiver le keyguard de Restrictions →	tous les types d’inscription ; Désactiver le keyguard uniquement sur les appareils entièrement gérés

Les lignes Code d’accès à l’appareil et Code secret du profil professionnel portent toutes deux sur l’ensemble des exigences de mot de passe de l’appareil. Seul le type d’inscription détermine laquelle des deux s’applique.

Deux actions sont disponibles dans le menu contextuel d’une ligne :

- Configurer ouvre la boîte de dialogue Configurer la règle.
- Réinitialiser supprime la règle personnalisée de la ligne. La règle par défaut s’applique alors de nouveau.

Pour la version 26.4.0

Configurer la règle

Chaque règle se compose toujours d’une action de blocage et d’une action d’effacement. Un blocage sans effacement ultérieur ne peut pas être configuré.

Action de blocage

Le portail désigne cette section par Action en bloc.

- Bloc après jours
  Nombre de jours de non-conformité avant que l’appareil ou le profil professionnel ne soit bloqué. La valeur préremplie est `10` ; les valeurs de `0` (blocage immédiat) à `10` sont autorisées. La valeur doit être inférieure à Essuyer après quelques jours. Lors du blocage,

une notification s’affiche sur l’appareil et indique, dans la mesure du possible, comment remédier à la non-conformité.

- Champ d’application du bloc
  Définit sur quoi porte le blocage. Le paramètre n’agit que sur les appareils d’entreprise. Non spécifié est présélectionné.
  - Non spécifié — équivaut à Profil de travail.
  - Profil de travail — seules les applications du profil professionnel sont bloquées ; les applications du profil personnel restent utilisables.
  - Appareil — l’ensemble de l’appareil est bloqué, y compris les applications du profil personnel.

Action d’effacement

Le portail désigne cette section par Action d’essuyage.

- Essuyer après quelques jours
  Nombre de jours de non-conformité avant que l’appareil ne soit effacé. La valeur préremplie est `30` ; les valeurs de `0` à `30` sont autorisées. Les appareils d’entreprise sont réinitialisés aux paramètres d’usine ; sur les appareils avec profil de travail (BYOD), le profil professionnel est supprimé.

- Préserver la protection de la réinitialisation d’usine
  Définit si les données de la protection contre la réinitialisation d’usine (Factory Reset Protection, FRP) sont conservées lors de la réinitialisation. Désactivé par défaut. Le paramètre ne s’applique pas aux profils professionnels.

Pour la version 26.4.0

Un clic sur Confirme reprend la règle dans le tableau. Elle n’est enregistrée qu’avec la configuration.

Plusieurs stratégies

Si plusieurs stratégies d’un appareil contiennent la configuration Contrôle de la conformité, la règle de la stratégie ayant la priorité la plus élevée s’applique pour chaque paramètre surveillé. Les paramètres sans règle personnalisée conservent la règle par défaut.

Proxy mondial

Cette configuration définit un proxy HTTP global indépendant du réseau pour les appareils gérés.

La configuration Proxy mondial définit un proxy HTTP qui s'applique indépendamment du réseau connecté. Elle est prévue pour les types d'inscription Appareil géré → et appareil géré avec profil personnel → (COPE), mais pas pour les appareils avec profil de travail → (BYOD).

Le portail affiche l'avertissement suivant dans le formulaire :

> En règle générale, les proxys doivent être configurés par réseau. Toutefois, pour des configurations inhabituelles telles que le filtrage interne général, un proxy HTTP global peut être utile. Si le proxy n'est pas accessible, l'accès au réseau peut être interrompu. Le proxy global n'est qu'une recommandation et certaines applications peuvent l'ignorer.

Un proxy par réseau se définit dans la section Paramètres du proxy de la configuration Wi-Fi →.

Pour la version 26.4.0

Type de proxy

Le champ Type de proxy détermine la manière dont le proxy est défini. Les champs affichés dépendent de la sélection.

- Directe – l'hôte, le port et les exceptions sont indiqués manuellement. Cette option est présélectionnée dans une nouvelle configuration.
- Script PAC – le proxy est configuré automatiquement au moyen d'un script PAC.

Directe

- Hôte proxy (obligatoire) – adresse IPv4 (p. ex. `10.0.0.1`) ou URL avec `http://` ou `https://` et un nom de domaine avec extension en minuscules (p. ex. `http://proxy.example.com`), dans les deux cas sans port ni chemin. Un nom d'hôte sans protocole (`proxy.example.com`) ou sans extension de domaine (`http://proxy`) n'est pas accepté. En cas de saisie non valide, le champ est signalé comme erroné et la configuration ne peut pas être enregistrée.
- Port proxy (obligatoire) – port du proxy ; les valeurs de `0` à `65535` sont acceptées.

- Hôtes pour lesquels le proxy est contourné – liste des hôtes dont les connexions ne passent pas par le proxy. Les noms d'hôte peuvent contenir des caractères génériques tels que `*.example.com`.

> Avec le port proxy `0`, Relution ne transmet aucun proxy global à l'appareil ; la configuration reste alors sans effet.

Script PAC

- URI du script PAC (obligatoire) – URI du script PAC utilisé pour configurer le proxy. Le portail attend une URL valide.

Validation

Lors de l'enregistrement, Relution vérifie qu'un Hôte proxy est indiqué pour le type de proxy Directe et une URI du script PAC pour le type Script PAC. Les champs de l'autre type de proxy ne sont pas transmis à l'appareil.

Pour la version 26.4.0

Connectivité des appareils

Cette configuration gère les paramètres de connectivité des appareils Android Enterprise.

La configuration Connectivité des appareils regroupe les paramètres relatifs à l'accès aux données par USB, au Wi-Fi, au partage de connexion, au partage Bluetooth, au DNS privé, à l'itinérance Wi-Fi, aux points d'accès (APN) et aux services réseau préférentiels. Le portail indique par des badges, au niveau de chaque champ, les types d'inscription et les versions d'Android concernés ; ils sont repris ci-dessous sous Support.

Dans une nouvelle configuration, Non spécifié est présélectionné pour les champs de sélection. Seule exception : la restriction des SSID Wi-Fi, pour laquelle la liste de blocage est présélectionnée.

La configuration remplace les options obsolètes relatives à la configuration Wi-Fi, au transfert de fichiers USB et au partage de connexion de la configuration Restrictions. Si une politique contient les deux configurations, les paramètres de la connectivité des appareils s'appliquent (voir Restrictions →).

Pour la version 26.4.0

Accès aux données par USB

Contrôle les fichiers et/ou les données qui peuvent être transférés via USB. La fonction de chargement n'est pas concernée.

Options :

- Non spécifié
- Autoriser le transfert de données par USB
- Interdire le transfert de données par USB
- Interdire le transfert de fichiers par USB

L'effet de Non spécifié sur le transfert de fichiers par USB est décrit dans Transfert de fichiers via USB →.

Support :

- Profil de travail COPE
- Appareil géré
- Pour Interdire le transfert de données par USB, en plus Android 12+ et USB HAL 1.3+

Configurer le Wi-Fi

Contrôle dans quelle mesure les utilisateurs peuvent configurer eux-mêmes des réseaux Wi-Fi.

Options :

- Non spécifié
- Permettre la configuration du Wi-Fi
- Interdire l'ajout de Wi-Fi – pris en charge à partir d'Android 13 sur Profil de travail COPE et Appareil géré.
- Interdire la configuration du Wi-Fi – pris en charge sur Profil de travail COPE et Appareil géré.

Avec Interdire la configuration du Wi-Fi, le portail affiche l'avertissement « L'appareil ne peut pas utiliser le Wi-Fi, sauf si une configuration Wi-Fi est ajoutée ! ». Les réseaux nécessaires sont alors distribués via la configuration Wi-Fi →.

Paramètres Wi-Fi direct

Pour la version 26.4.0

Contrôle l'utilisation de Wi-Fi Direct.

Options :

- Non spécifié
- Autoriser le Wi-Fi direct
- Désactiver le Wi-Fi direct

Support :

- Profil de travail COPE
- Appareil géré
- Android 13+

Paramètres de connexion

Contrôle dans quelle mesure les utilisateurs peuvent utiliser le partage de connexion (tethering), par exemple via Wi-Fi ou Bluetooth.

Options :

- Non spécifié
- Autoriser toutes les connexions (tethering)
- Désactiver le Wi-Fi tethering – pris en charge à partir d'Android 13 sur Profil de travail COPE et Appareil géré.
- Interdire toutes les connexions (tethering) – pris en charge sur Profil de travail COPE et Appareil géré.

Partage Bluetooth

Contrôle si des contenus peuvent être partagés via Bluetooth.

Options :

- Non spécifié
- Autorisé
- Refusé

Restriction des SSID Wi-Fi

Pour la version 26.4.0

Définit les SSID Wi-Fi auxquels l'appareil peut se connecter. Les réseaux pouvant être configurés sur l'appareil ne sont pas concernés.

Options :

- Interdire la connexion aux SSID Wi-Fi (présélectionné) – liste de blocage. Les SSID sont saisis dans le champ SSID Wi-Fi auxquels il n'est pas possible de se connecter.
- Autoriser la connexion uniquement aux SSID Wi-Fi – liste d'autorisation. Les SSID sont saisis dans le champ SSID Wi-Fi auxquels il est possible de se connecter ; au moins une entrée est obligatoire.

> Pour la liste d'autorisation, le portail signale qu'au moins un SSID Wi-Fi doit être disponible, sinon l'appareil ne pourra pas se connecter à Google ou à Relution.

Support :

- Profil de travail COPE
- Appareil géré
- Android 13+

DNS privé

- Mode DNS privé – mode de configuration des paramètres DNS privé globaux de l'appareil.
  - Non spécifié – par défaut Choix de l'utilisateur.
  - Choix de l'utilisateur – les utilisateurs peuvent configurer eux-mêmes le DNS privé.
  - Automatique – l'appareil tente d'utiliser le serveur DNS fourni par le réseau via une connexion chiffrée avant de recourir au texte clair. Les utilisateurs ne peuvent pas modifier ce paramètre.
  - Hôte spécifié – l'appareil utilise uniquement le serveur DNS indiqué dans le champ Hôte DNS privé. Les utilisateurs ne peuvent pas modifier ce paramètre.
- Hôte DNS privé – nom d'hôte du serveur DNS. Le champ n'est modifiable qu'en mode Hôte spécifié et y est alors obligatoire ; sans nom d'hôte, Relution refuse l'enregistrement.

Support :

- Mode DNS privé : Profil de travail, Appareil géré
- Hôte DNS privé : Appareil géré

Pour la version 26.4.0

Itinérance Wi-Fi

Dans la zone Itinérance Wi-Fi, Ajouter crée un paramètre d'itinérance Wi-Fi par SSID :

- SSID (obligatoire) – nom du réseau auquel le paramètre s'applique. Un seul paramètre est possible par SSID.
- Mode d'itinérance Wi-Fi – Par défaut (présélectionné), Désactivé ou Agressif.

Support :

- Appareil géré
- Profil de travail COPE
- Android 15+

APN

La zone Nom du point d'accès (APN) gère les points d'accès au réseau mobile.

Activer les APN prioritaires

Options : Non spécifié, Désactivé, Activé. Pris en charge sur Appareil géré à partir d'Android 10.

Paramètres APN

Ajouter crée un paramètre APN. Dans la boîte de dialogue, le portail indique que seul le type d’APN Entreprise doit être sélectionné pour utiliser le paramètre dans un profil professionnel. Un paramètre APN portant le même nom ou le même APN qu’un paramètre existant n’est pas accepté.

Champ	Description
Types d’APN	Obligatoire, sélection multiple : Entreprise (Android 13+), Protocole indépendant du support (BIP) (Android 12+), Services à la marque de l’opérateur (CBS), Par défaut, Réseau à distance (DUN), Urgence, Firmware Over-the-Air (FOTA), Haute priorité (HiPri), Pièce jointe initiale (IA), Sous-système multimédia IP (IMS), Service critique de mission (MCX), Système de messagerie multimédia (MMS), Services de communication riches (RCS) (Android 15+), Emplacement sécurisé du plan utilisateur (SUPL), SIM virtuel (VSIM) (Android 12+), Protocole d’accès à la configuration XML (XCAP) (Android 11+)
Nom	Obligatoire, nom d’affichage du paramètre APN
APN	Obligatoire, nom du point d’accès
ID de l’opérateur numérique	Facultatif
ID du transporteur	Facultatif, valeur à partir de `0`
Type d’authentification	Non spécifié, Aucun, PAP, CHAP, PAP ou CHAP
Nom d’utilisateur, Mot de passe	Facultatif
Adresse du proxy, Port proxy	Facultatif, port à partir de `0`
Adresse du serveur (MMSC)	Facultatif

Champ	Description
Adresse proxy MMS, Port proxy MMS	Facultatif, port à partir de `0`
Protocole, Protocole d’itinérance	Non spécifié, IP, IPv4/IPv6, IPv6, Non-IP, Point à point (PPP), Non structuré
Types de réseaux	Sélection multiple : EDGE, GPRS, GSM, HSDPA, HSPA, HSPAP, HSUPA, IWLAN, LTE, NR (New Radio) 5G, TD_SCDMA, UMTS
Activer la session PDU toujours active	Non spécifié, Pas toujours activé, Toujours activé (Android 15+)
Type d’OVNM	Non spécifié, Identificateur de groupe de niveau 1 (GID), Identificateur de carte à circuit intégré (ICCID), Identité internationale d’abonné mobile (IMSI), Nom du fournisseur de services (SPN)
MTU v4, MTU v6	Facultatif, valeur à partir de `0` (Android 13+)

Pour la ve

Services réseau préférentiels

La zone Paramètres de service réseau préférentiel affecte des applications à des tranches réseau dédiées à l’entreprise, par exemple des tranches 5G d’entreprise.

- ID réseau préférentiel par défaut – s’applique aux applications sans configuration propre. Options : Non spécifié (présélectionné), Pas de réseau préférentiel, Réseau préférentiel 1 à Réseau préférentiel 5. Un réseau préférentiel choisi ici doit également figurer dans la liste des configurations.

Sous Configurations de service réseau préférentiel, Ajouter crée une configuration par ID réseau :

- ID réseau préférentiel (obligatoire) – Réseau préférentiel 1 à Réseau préférentiel 5. Chaque ID ne peut être utilisé qu’une seule fois.
- Repli sur la connexion par défaut – indique si l’application peut revenir à la connexion par défaut lorsque le réseau préférentiel n’est pas disponible. Options : Non spécifié, Autorisé,

Refusé.

- Utilisation d’autres réseaux – indique si l’application peut utiliser des réseaux ne correspondant pas aux critères du service réseau préférentiel. Options : Non spécifié, Autorisé, Refusé (Android 14+).

Si Utilisation d’autres réseaux est réglé sur Refusé, Repli sur la connexion par défaut doit également être réglé sur Refusé. Si la liste ne contient aucune configuration, Relution ne transmet rien pour cette zone à l’appareil, pas même l’ID réseau par défaut.

Support :

- Android 13+
- Appareil géré
- Profil de travail

Pour la version 26.4.0

Certificat

Cette configuration installe un certificat CA ou un certificat avec clé privée sur l'appareil.

La configuration Certificat distribue sur les appareils Android Enterprise un certificat issu de la gestion des certificats de Relution, un certificat émis au moyen d'un modèle de certificat ou le certificat utilisateur de l'utilisateur affecté. Une politique peut contenir plusieurs configurations de certificat.

L'installation est effectuée par l'application Relution Companion, à laquelle Relution accorde l'autorisation d'installer des certificats (voir Compagnon & Daemon →).

Général

La zone Général définit le certificat installé.

- Certificat ou modèle sélectionné (présélectionné) – dans le champ Certificat ou modèle de certificat, Sélectionnez ouvre la boîte de dialogue Sélectionnez un certificat ou un modèle de certificat. L'onglet Certificats propose les certificats téléversés, l'onglet Modèles de certificats les modèles de certificats. Les certificats aux formats PKCS#1 et PKCS#12 sont proposés. Sans sélection, la configuration ne peut pas être enregistrée.
- Certificat de l'utilisateur pour le VPN et les applications – au lieu d'un certificat fixe, le certificat enregistré sous VPN et applications dans le profil de l'utilisateur affecté à l'appareil est installé.
    - Nom du certificat – sélectionne un certificat précis par son nom lorsque l'utilisateur possède plusieurs certificats de ce type. Le champ peut contenir des espaces réservés résolus par appareil (voir Espaces réservés avancés →). S'il reste vide, le certificat ayant la plus longue durée de validité est utilisé.

Les certificats au format PKCS#1 sont installés en tant que certificats CA, les conteneurs PKCS#12 en tant que certificats avec clé privée.

Informations sur les sources de certificats :

- Gestion des certificats →
- CA intégré →
- Pool de certificats →

Pour la version 26.4.0

Alias de certificat

L’alias est généré automatiquement dès qu’un certificat, un modèle ou l’option Certificat de l’utilisateur pour le VPN et les applications est sélectionné, et ne peut pas être modifié. L’icône de copie le place dans le presse-papiers.

Le portail en décrit l’usage ainsi : lorsqu’une configuration gérée nécessite un alias de certificat, cette valeur permet de faire référence à cette configuration.

Afin que l’alias reste unique sur l’appareil, Relution le transmet à l’application Companion complété par le numéro de série hexadécimal du certificat entre parenthèses.

Comportement en l’absence de certificat utilisateur

Si l’utilisateur affecté à l’appareil ne possède pas de certificat utilisateur correspondant, Relution transmet tout de même les autres configurations de la politique. Le certificat n’est alors pas installé, et un avertissement est consigné dans le journal du serveur.

Pour la version 26.4.0

Affichage

Cette configuration gère les paramètres d'affichage d'un appareil Android Enterprise géré.

La configuration Affichage détermine si la luminosité et le délai d'attente de l'écran sont choisis par l'utilisateur sur l'appareil ou imposés. Dans le portail, la configuration porte le mode d'enrôlement Appareil géré ; elle s'applique aux appareils entièrement gérés et aux appareils gérés avec profil personnel (COPE), mais pas aux appareils avec profil de travail (BYOD). Elle ne peut être ajoutée qu'une seule fois par politique.

Les deux paramètres se trouvent dans la section Général et comportent chacun deux niveaux : un champ de sélection définit le mode, un champ en retrait en dessous définit la valeur. Le champ de valeur n'est modifiable que si le mode choisi nécessite une valeur.

Luminosité

La luminosité est pilotée par deux champs : le mode et la valeur de luminosité.

Pour la version 26.4.0

Configurer la luminosité

Détermine la manière dont la luminosité de l'écran est pilotée.

Options :

- Configuré par l'utilisateur – La luminosité est réglée sur l'appareil. Cette option est présélectionnée dans une nouvelle configuration.
- Luminosité adaptative – La luminosité est réglée de manière adaptative ; la valeur du champ Luminosité de l'écran est également transmise.
- Luminosité fixe – La luminosité est fixée à la valeur du champ Luminosité de l'écran.

Luminosité de l'écran

Champ obligatoire dès que Luminosité adaptative ou Luminosité fixe est sélectionnée sous Configurer la luminosité. Avec Configuré par l'utilisateur, le champ est verrouillé et aucune valeur de luminosité n'est transmise à l'appareil.

Le texte d'aide du portail indique : « La luminosité de l'écran peut être configurée sur une échelle de 1 à 255, 255 étant la luminosité maximale ». Les valeurs en dehors de cette plage ne sont

pas acceptées ; aucune valeur par défaut n’est préremplie.

Délai d’attente de l’écran

Le délai d’attente de l’écran est également piloté par deux champs : le mode et la durée.

Configurer le délai d’attente de l’écran

Détermine si le délai avant l’extinction de l’écran est imposé.

Options :

- Configuré par l’utilisateur – Le délai est réglé sur l’appareil. Cette option est présélectionnée dans une nouvelle configuration.
- Délai fixe – Le délai est fixé à la valeur du champ Délai d’attente de l’écran.

Durée du délai d’attente

Le champ Délai d’attente de l’écran n’est modifiable qu’avec Délai fixe. Les valeurs disponibles sont 15 secondes, 30 secondes, 1 minute, 2 minutes, 5 minutes et 10 minutes ; 30 secondes est présélectionné.

Pour la version 26.4.0

> Si la politique contient également une configuration Mode kiosque → avec une valeur pour Délai maximum de verrouillage du dispositif, Relution ne transmet le délai d’attente fixe que s’il est plus court que le délai maximum de verrouillage. Dans le cas contraire, seul le mode est transmis, sans valeur de délai.

Prise en charge

- Appareil géré →
- Appareil géré avec profil personnel → (COPE)
- Non disponible pour les appareils avec profil de travail → (BYOD)

Activités préférées

Cette configuration gère l'application à utiliser par défaut pour une opération spécifique.

La configuration Activités préférées attribue une application précise à des opérations Android (intents). Chaque entrée se compose d'une application et, de manière facultative, d'une activité, de catégories et d'actions ; Android utilise ensuite durablement cette application pour les opérations correspondantes. Dans le portail, la configuration ne porte aucun mode d'enrôlement particulier. Elle ne peut être ajoutée qu'une seule fois par politique.

La configuration n'installe pas l'application choisie. L'installation se fait séparément, par exemple via Gérer les applications →. Un cas d'utilisation complet – le Relution Homescreen comme launcher par défaut – est décrit dans l'article Homescreen comme Launcher →. Pour les applications par défaut courantes comme le navigateur ou le téléphone, la configuration Applications par défaut → propose une sélection dédiée.

Pour la version 26.4.0

Liste des applications

La configuration affiche une liste avec les colonnes Nom, Identifiant du bundle, Activité, Actions et Catégories. Les colonnes Actions et Catégories n'affichent que la dernière partie de chaque nom (par exemple `HOME` pour `android.intent.category.HOME`).

Une nouvelle entrée est créée via Ajouter. Le menu contextuel d'une entrée propose Éditer et Supprimer ; plusieurs entrées sélectionnées sont supprimées via le menu contextuel de la liste. Chaque application ne peut figurer qu'une seule fois dans la liste : les applications déjà présentes sont exclues de la sélection dans le Relution App Store, et si une application déjà présente est ajoutée à nouveau par une autre voie, la nouvelle entrée remplace la précédente. Dans une version de politique déjà publiée, la liste est en lecture seule.

Sélection de l'application

La boîte de dialogue Activité crée une entrée en trois étapes. La première étape consiste à choisir la source de l'application :

- Appli Relution App Store – Sélection d'une application dans l'App Store de Relution. Les applications natives et publiques pour Android et Android Enterprise sont proposées.

- Application Google Play Store gérée (Android Enterprise) – Recherche d'une application gratuite dans le Google Play Store géré via Android Enterprise. Cette source n'est disponible que si Android Enterprise est configuré pour l'organisation.
- Ajouter une application manuellement – Saisie manuelle du nom et de l'identifiant du bundle d'une application. Les champs Nom et Nom interne sont obligatoires ; le nom du paquet est saisi comme nom interne (exemple dans le portail : `com.mwaysolutions.relution`).

La deuxième étape consiste à sélectionner l'application ou à saisir les données de l'application manuelle.

Activité, catégories et actions

La troisième étape définit les détails de l'entrée. Lors d'une modification ultérieure via Éditer, seuls ces champs sont affichés ; l'application elle-même reste inchangée.

- Activité – nom de classe facultatif de l'activité au sein de l'application, par exemple `io.relution.homescreen.MainActivity`. Si le champ est renseigné, Relution transmet `nom du paquet/activité` comme cible ; s'il est vide, seul le nom du paquet est transmis.
- Catégories – liste de catégories d'intent, par exemple `android.intent.category.HOME`. La saisie propose les catégories standard d'Android ; des valeurs personnalisées sont possibles.
- Actions – liste d'actions d'intent, par exemple `android.intent.action.MAIN`. Les actions standard d'Android sont également proposées.

Les catégories et les actions ne sont pas obligatoires. Une remarque dans la boîte de dialogue renvoie à la Documentation Google → pour plus de détails sur les catégories et actions standard.

Pour la version 26.4.0

Mode de localisation

Cette configuration définit la manière dont le paramètre de localisation est géré sur un appareil Android Enterprise géré.

La configuration Mode de localisation pilote le paramètre de localisation (services de localisation) de l'appareil. Dans le portail, elle porte le mode d'enrôlement Appareil géré ; elle s'applique aux appareils entièrement gérés et aux appareils gérés avec profil personnel (COPE), mais pas aux appareils avec profil de travail (BYOD). Elle ne peut être ajoutée qu'une seule fois par politique.

L'interaction de ce paramètre avec les autorisations de localisation des applications est décrite dans l'article Services de localisation →.

Paramètre de localisation sur l'appareil

Le champ de sélection Paramètre de localisation sur l'appareil de la section Général est le seul paramètre de la configuration.

Pour la version 26.4.0

Options :

- Choix de l'utilisateur – Le paramètre de localisation n'est pas restreint. Cette option est présélectionnée dans une nouvelle configuration.
- Activer le paramètre de localisation sur l'appareil – Le paramètre de localisation est activé sur l'appareil.
- Désactivé – Le paramètre de localisation est désactivé sur l'appareil.

La valeur sélectionnée est également transmise aux applications Relution de l'appareil (par exemple le Relution Agent).

Remarque sur les profils professionnels

Le portail affiche la remarque suivante dans le formulaire :

Sur Android 11 et versions supérieures, les profils professionnels sur les appareils appartenant à l'entreprise ne peuvent pas imposer directement les services de localisation. La conformité ne peut être restaurée qu'une fois que l'utilisateur a activé ou désactivé manuellement les services de localisation via l'application Paramètres de l'appareil.

Prise en charge

- Appareil géré →
- Appareil géré avec profil personnel → (COPE), sous réserve de la limitation décrite dans la remarque sur les profils professionnels →
- Non disponible pour les appareils avec profil de travail → (BYOD)

Pour la version 26.4.0

Samsung Classroom Management

Cette configuration déploie et configure l'application Samsung Classroom Management pour les cours.

La configuration Samsung Classroom Management met en place l’application du même nom pour les cours sur les appareils Android Enterprise. Dans le portail, elle ne porte aucun mode d’enrôlement particulier. Elle ne peut être ajoutée qu’une seule fois par politique. Samsung Classroom Management nécessite une licence séparée (voir Teacher →).

Comportement sur l’appareil

Lorsqu’une politique contient cette configuration, Relution complète automatiquement la politique de l’appareil :

- L’application Samsung Classroom Management (`com.tabnova.classroomapp`) est déployée en installation forcée ; ses autorisations d’exécution sont accordées. Une configuration gérée de la même application provenant de Gérer les applications → est remplacée par les valeurs de cette configuration.
- Les classes auxquelles appartient l’utilisateur de l’appareil sont transmises à l’application, avec leurs enseignants et élèves. Les classes sont gérées sous `Éducation` → `Classes` (voir Fonction d’éducation →).
- Si l’utilisateur de l’appareil est enregistré comme enseignant dans au moins une classe, l’application Relution Teacher (`io.relution.teacher`) est également déployée en installation forcée.
- Le pays enregistré dans l’adresse de l’organisation est transmis comme pays ; à défaut, `Deutschland` est utilisé.

Général

- Code d’abonnement – obligatoire. Code de l’abonnement Samsung Classroom qui active l’application.
- Nom d’utilisateur – nom sous lequel l’appareil apparaît dans l’application. Prérempli avec l’espace réservé `${user.name}`. L’application n’affiche que les classes contenant un membre portant exactement ce nom ; la valeur doit donc correspondre au nom d’utilisateur Relution. Sous le formulaire, le portail affiche les espaces réservés disponibles pour l’utilisateur et l’appareil (voir Espaces réservés avancés →).

- Nom de l’école – facultatif. Si le champ reste vide, le nom de l’organisation est transmis.
- Appliquer la liste des filtres web par défaut (`https://school.tabnova.com/block.list`) – active la liste de blocage par défaut de Samsung Classroom. Désactivé par défaut.
- URL de la liste de filtres web personnalisés – facultatif. Adresse d’une liste de blocage personnalisée.

Nettoyer après le cours

Cette section définit ce qui est réinitialisé sur l’appareil après le cours.

- Mode de déclenchement – cases à cocher Redémarrez (redémarrage) et Déconnectez-vous (déconnexion) ; les deux peuvent être sélectionnées simultanément. Aucune n’est cochée dans une nouvelle configuration.
- Cookies clairs – supprime les cookies du navigateur. Activé dans une nouvelle configuration.
- Dossiers et fichiers à supprimer – liste de noms de fichiers et de dossiers, par exemple `Downloads` ou `DCIM`.

Apps à effacer

Pour la version 26.4.0

La liste contient les applications dont les données sont effacées ou qui sont désinstallées après le cours. Via Ajouter, des applications publiques gratuites sont sélectionnées dans le Relution App Store ou dans Managed Google Play ; une application déjà présente n’est pas ajoutée deux fois.

Deux cases à cocher sont disponibles par application :

- Effacer les données – les données de l’application sont supprimées.
- Désinstaller – l’application est désinstallée.

Lors de l’ajout d’une application, les deux cases sont cochées. Les applications sélectionnées sont retirées de la liste via Supprimer.

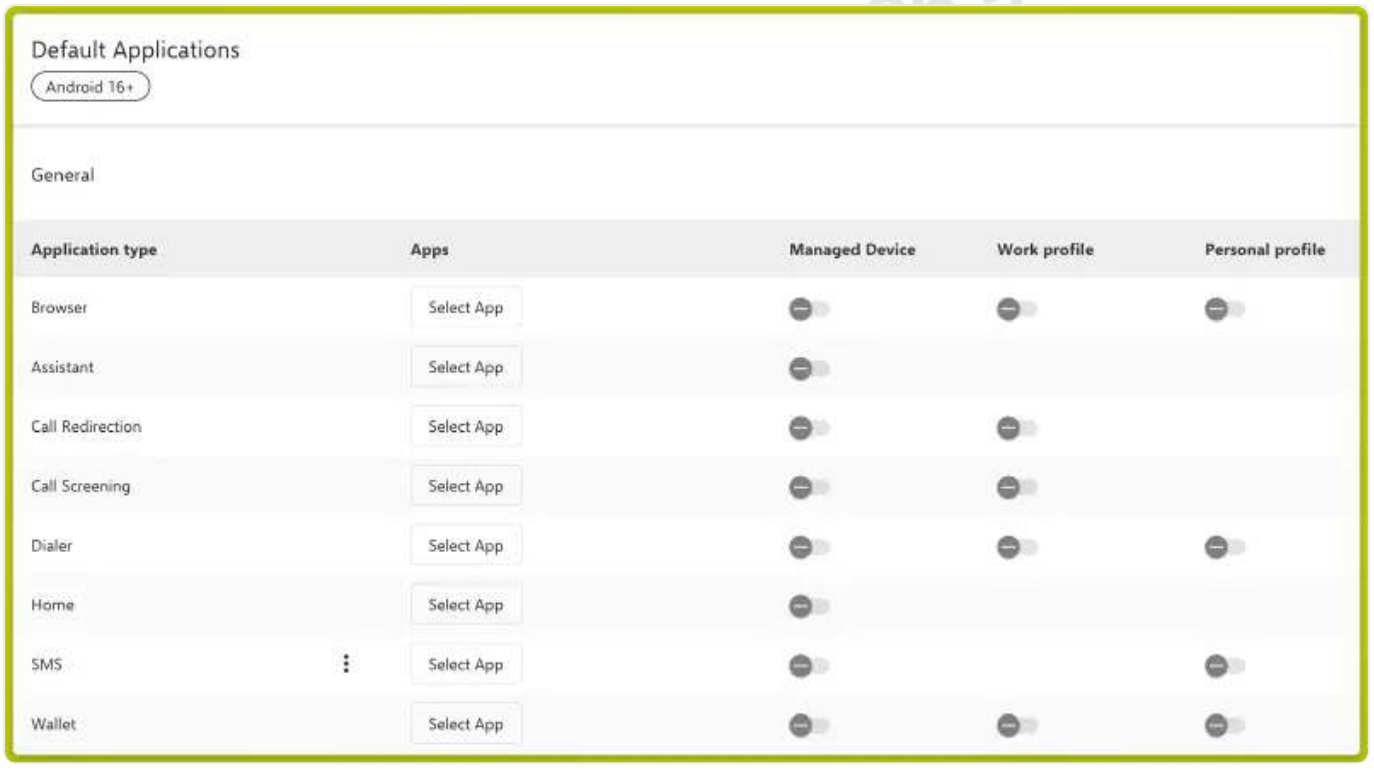
Applications par défaut

Cette politique permet aux administrateurs de définir des applications par défaut pour des fonctions spécifiques sur les appareils Android gérés.

La politique Applications par défaut permet aux administrateurs de configurer des applications par défaut pour diverses fonctions sur les appareils Android. Ces paramètres sont particulièrement utiles pour standardiser l'expérience utilisateur et garantir que seules les applications approuvées sont utilisées.
Cette fonctionnalité est disponible pour les appareils fonctionnant sous Android 16+.

Aperçu des fonctions

Les administrateurs peuvent configurer des applications par défaut pour les fonctions suivantes dans le tableau ci-dessous :



Type d’application	Applications	Appareil géré	Profil de travail	Profil personnel
Navigateur	Brave, Google Chrome	✅		
Assistant	Sélectionner une app			
Redirection d’appel	Sélectionner une app			
Filtrage d’appel	Sélectionner une app			
Composeur	Sélectionner une app			
Accueil	Sélectionner une app			
SMS	Sélectionner une app			
Portefeuille	Sélectionner une app			✅

Pour la version 26.4.0

Options de configuration

- Sélectionner une app : Les administrateurs peuvent choisir l’application par défaut souhaitée pour chaque fonction.
- Appareil géré : Active ou désactive la configuration pour les appareils entièrement gérés.
- Profil de travail : Active ou désactive la configuration pour le profil de travail.
- Profil personnel : Active ou désactive la configuration pour le profil personnel.

> Les applications par défaut définies pour Appareil géré ou Profil de travail et qui ne figurent dans aucune configuration d’application de la politique sont automatiquement mises à disposition par Relution avec le type d’installation Disponible. Elles ne sont donc pas installées automatiquement. Pour garantir l’installation d’une application par défaut, celle-ci est ajoutée en plus via la configuration Gérer les applications, par ex. avec Installé de force. Si l’une des applications par défaut y est définie sur Bloqué, la configuration échoue.

Remarque sur plusieurs applications par défaut

Plusieurs applications peuvent être sélectionnées pour la même fonction, par exemple Brave et Google Chrome comme navigateurs, comme indiqué ci-dessus. Si plusieurs de ces applications sont installées sur l’appareil, Android utilise la première application de la liste. L’ordre déterminant est celui affiché après l’enregistrement et la réouverture de la configuration. Il ne correspond pas nécessairement à l’ordre de sélection et ne peut actuellement pas être modifié manuellement.

Pour la version 26.4.0

Samsung Knox

Relution prend en charge Samsung Knox afin de fournir des fonctionnalités avancées de sécurité et de gestion pour les appareils Samsung.
Les politiques Knox peuvent être appliquées à l'échelle de l'appareil ou dans le profil de travail, en fonction du mode de l'appareil (Propriétaire de l'Appareil ou Profil de Travail).
Le Plugin de Service Samsung Knox est automatiquement déployé sur les appareils où la politique Knox est appliquée.
La configuration s'effectue via ce plugin et propose les fonctionnalités suivantes :

Aperçu des fonctionnalités Knox

Le plugin propose les domaines fonctionnels suivants :

Paramètres de Profil

- Nom et version du profil
- Clé de licence Knox (ex. : Knox Suite, DualDAR)
- Activer/Désactiver le mode de débogage

Pour la Version 26.4.0

Gestion des Applications et Politiques

- Politiques séparées d'applications (Profil de Travail vs Propriétaire de l'Appareil)
- Paramètres de l'appareil (ex. : Caméra, Panneau Rapide, Mises à Jour du Firmware)
- Politiques du Profil de Travail (Propriétaire de Profil)
- Assignations d'applications pour accéder au SDK Knox

Réseau et Sécurité

- Configurations avancées de Wi-Fi *(Premium)*
- Profils APN
- Profils VPN *(Premium)*
- Profils de Firewall
- Profils Proxy (manuel ou PAC)

Certificats et Clés

- Gestion des certificats *(Premium)*
- Déploiement des certificats
- Applications autorisées à accéder aux clés privées *(Premium)*
- Configurations du plugin UCM *(Premium)*

Configuration et Personnalisation de l'Appareil

- Comptes et politiques de l'appareil
- Personnalisation des appareils et des paramètres *(Premium)*
- Mappage des touches pour le lancement d'applications
- Personnalisations DeX *(Premium)*
- Configurations des périphériques
- Liste blanche d'appareils USB

Profils Avancés

- Points de Données NPA *(Premium)*
- Synchronisation des Données RCP *(Premium)*
- Contrôles des permissions des applications

Pour la version 26.4.0

Comportement dans Relution

- La configuration s'effectue dans l'éditeur de configurations d'applications gérées du Plugin de Service Samsung Knox.
- Une configuration Knox est prioritaire sur une configuration du Plugin de Service Samsung Knox dans la configuration Gérer les applications et la remplace.
- Si la configuration Gérer les applications de la même version de politique contient déjà une configuration du Plugin de Service Samsung Knox, celle-ci est reprise lors de la création de la configuration Knox. Le formulaire affiche alors un message d'information.
- Les espaces réservés pour l'utilisateur, l'appareil et les certificats sont pris en charge.
- Si le plugin signale des erreurs, la configuration Knox est affichée dans les détails de l'appareil avec le statut jaune Avis et non comme une violation (Violé). En l'absence d'erreurs, le statut est Résolu. Les retours du plugin y sont consultables.
- Si la configuration Knox est supprimée de la politique, le Plugin de Service Samsung Knox reste installé de force sur les appareils où il est déjà installé et reçoit une configuration vide. Cela s'applique également si le plugin est bloqué dans Gérer les applications.

Remarques

- De nombreuses fonctionnalités ne sont disponibles que sur des appareils Samsung compatibles Knox. La liste des appareils pris en charge est disponible sur la page d’assistance Samsung Knox →.
- Certaines options avancées nécessitent une licence Knox Premium valide.
- Avant le déploiement, il est recommandé de tester avec des appareils pilotes, car les politiques Knox et Android Enterprise peuvent se chevaucher.

Pour la version 26.4.0

Distribution d'applications

Les entreprises décident de plus en plus souvent de soutenir certains processus de travail à l’aide d’une application mobile. Parmi de nombreux autres problèmes conceptuels, la question de la distribution de cette application aux utilisateurs se pose rapidement. Souvent, le cas d’utilisation est que non seulement les employés, mais aussi les personnes externes doivent obtenir l’application - il peut s’agir par exemple de fournisseurs de services, de partenaires ou de clients. Dans la plupart des cas, l’application n’est pas destinée à une large clientèle, mais à des utilisateurs professionnels sélectionnés. Les sections suivantes doivent aider à choisir la meilleure méthode de distribution.

Méthode	Public cible	Compte requis
Apple App Store	grand public	identifiant Apple
Google Play Store	grand public	compte Google
Apple TestFlight	utilisateurs sélectionnés (bêta)	identifiant Apple
Google Alpha-/Beta-Testing	utilisateurs sélectionnés (bêta)	identifiant Google
Magasin d’applications d’entreprise interne	groupe d’utilisateurs connu et défini (par ex. employés, partenaires)	aucun, si distribué via MDM

Distribution via les magasins d’applications publics

Apple et Google proposent chacun une infrastructure de distribution d’applications. Pour Apple, les applications sont mises à la disposition des utilisateurs finaux par l’intermédiaire de l’Apple App Store. Chaque appareil iOS est équipé d’une application App Store préinstallée. La gestion et la publication des applications s’effectuent via le portail des développeurs et App Store Connect. Chez Google, les applications sont mises à la disposition des utilisateurs finaux via le Play Store. L’application PlayStore est préinstallée sur chaque appareil Android. L’administration et la publication des applications se font via le portail des développeurs. Apple et Google définissent le cadre de publication des applications via leurs systèmes.

Si un appareil est géré par un système MDM, l'application du store (App Store ou Play Store) peut également être verrouillée pour l'utilisateur et peut donc ne pas être disponible pour l'utilisateur final.

Distribution via l'Apple App Store

Avantages

- Les applications sont disponibles pour les utilisateurs finaux via le mécanisme standard d'Apple.
- Les applications n'ont pas besoin d'être re-signées et re-provisionnées avec un profil de provisionnement mis à jour après un an.
- Les applications peuvent être activées ou bloquées de manière sélective pour chaque pays.
- Les applications peuvent être proposées à titre onéreux - si on le souhaite - dans des structures définies (Apple prélève à cet effet un pourcentage de commission de 15 %).
- Apple fournit l'infrastructure pour la distribution et la facturation

Inconvénients

- Les utilisateurs ont besoin d'un identifiant Apple sur l'appareil pour installer les applications de l'Apple App Store.
- Pour les entreprises disposant d'appareils gérés, l'Apple App Store peut être bloqué par MDM.
- Toutes les spécifications d'Apple doivent être respectées, comme la prise en charge des nouvelles classes d'appareils telles que l'iPhone X.
- Lors d'un examen, Apple se réserve le droit de ne pas publier l'application ou de la retirer ultérieurement.
- L'examen peut entraîner des retards allant jusqu'à 10 jours (actuellement, la durée moyenne de l'examen est d'environ 3 jours ouvrables).
- Les applications ne peuvent être mises à la disposition de certains groupes d'utilisateurs que de manière très limitée.

Pour la version 26.4.0

Distribution via Google Play Store

Avantages

- Les applications sont disponibles pour les utilisateurs finaux via le mécanisme standard de Google.
- Les applications peuvent être activées ou bloquées de manière sélective pour certains pays.
- Les applications peuvent être proposées à titre onéreux dans des structures définies (Google prélève à cet effet une commission de 15 %).
- Google fournit l'infrastructure pour la distribution et la facturation

Inconvénients

- Les utilisateurs ont besoin d'un compte Google pour installer des applications à partir du Play Store.
- Pour les entreprises disposant d'appareils gérés, le Play Store peut être bloqué par MDM.
- Toutes les spécifications de Google doivent être respectées
- Après l'analyse automatisée des applications, Google se réserve le droit de retirer l'application de la boutique à une date ultérieure.
- En raison des analyses techniques, la publication des applications peut être retardée de quelques heures.
- Les applications ne peuvent être mises à la disposition de groupes d'utilisateurs sélectionnés que dans une mesure très limitée.

Distribution via les programmes bêta des magasins d'applications publics

Apple et Google proposent chacun un programme de test bêta en plus de la distribution d'applications publiques. Chez Apple, les applications sont mises à la disposition des utilisateurs finaux pour des tests bêta via l'application TestFlight. Sur les appareils iOS, cette application peut être installée à partir de l'application Apple Store.

Pour la version 26.4.0

L'administration et la publication des applications se font via le portail des développeurs et App Store Connect dans la zone TestFlight. Sur Google, les applications sont mises à disposition pour les tests alpha ou bêta via le Play Store. Le Play Store est préinstallé sur tous les appareils Android.

L'administration et la publication des applications se font via le portail des développeurs dans la zone Alpha et Beta Testing. Apple et Google définissent le cadre de publication des applications via leurs systèmes.

Distribution via Apple Testflight

Avantages

- Les applications sont mises à la disposition des utilisateurs via un mécanisme fourni par Apple.
- Les applications peuvent être activées de manière sélective pour des utilisateurs individuels.
- Apple fournit l'infrastructure de distribution et de facturation

Inconvénients

- Les utilisateurs ont besoin d'un identifiant Apple pour installer les applications de l'Apple App Store.
- L'installation unique de l'application TestFlight est nécessaire pour installer l'application.
- Apple se réserve le droit de ne pas publier l'application dans une évaluation "réduite".
- L'évaluation peut entraîner des retards pouvant aller jusqu'à 10 jours (actuellement, la durée moyenne d'une évaluation est d'environ deux jours ouvrables).
- La signature de l'application expire après 90 jours

Le service TestFlight est principalement destiné à une courte période de test avant la publication d'une application iOS. Il n'est pas adapté à un fonctionnement permanent en raison de la courte durée de validité de la signature.

Distribution via Google Alpha et Beta Testing

Avantages

- Les applications sont mises à la disposition des utilisateurs via un mécanisme fourni par Google.
- Les applications peuvent être activées de manière sélective pour des utilisateurs individuels.
- Google fournit l'infrastructure de distribution et de facturation

Inconvénients

- Les utilisateurs ont besoin d'un identifiant Google pour installer des applications à partir du Play Store.
- Les clients d'entreprise dont les appareils sont gérés peuvent voir le Play Store bloqué par MDM.

Pour la version 26.4.0

Distribution via le magasin d'applications interne de l'entreprise

Outre la distribution d'applications via leurs magasins publics respectifs, Apple et Google proposent également des mécanismes de distribution d'applications en interne, principalement pour les entreprises. Dans le cas d'Apple, le programme Apple Enterprise et un magasin d'applications d'entreprise tel que Relution sont nécessaires.

Les applications sont mises à la disposition des utilisateurs finaux par le biais d'une application App Store distincte ou d'un site web mobile. Les applications sont gérées via le portail des développeurs.

Les applications sont distribuées par l'intermédiaire du fournisseur de la boutique d'applications de l'entreprise concernée. Chez Google, les applications peuvent être mises à disposition pour le téléchargement et l'installation via un service web.

Pour les appareils spéciaux, tels que Samsung, des mécanismes d'installation et de distribution optimisés peuvent être utilisés. Apple et Google définissent les possibilités de distribution des applications parallèlement à leurs systèmes.

Distribution d'applications iOS via l'App Store d'entreprise

Avantages

- Les applications peuvent être distribuées à des groupes d'utilisateurs sélectionnés, par exemple sous la forme d'un lien profond ou après connexion à l'aide d'un nom d'utilisateur et d'un mot de passe préalablement configurés.
- Les utilisateurs n'ont pas besoin d'un identifiant Apple pour installer des applications à partir d'un App Store d'entreprise interne.
- Il n'est pas nécessaire de satisfaire à toutes les exigences d'Apple
- La publication des mises à jour d'applications n'est pas retardée par un examen d'Apple.
- Certains magasins d'applications d'entreprise (par exemple Relution) peuvent être utilisés sans gestion des appareils (MDM).
- Un système de gestion des utilisateurs existant (ActiveDirectory/LDAP) peut être connecté afin que les utilisateurs n'aient pas besoin de nouvelles informations d'identification.

Pour la version 26.4.0

Inconvénients

- Les applications sont disponibles pour les utilisateurs finaux via un mécanisme spécial approuvé par Apple, mais qui nécessite une configuration initiale de la part de l'utilisateur (voir ici →).
- Les applications doivent être re-signées et re-provisionnées avec un profil de provisionnement mis à jour au bout d'un an. Cependant, cette opération peut être automatisée avec Relution, de sorte qu'il n'y a pas d'inconvénient à cet égard.
- L'infrastructure de distribution peut être fournie sous la forme d'un service en Cloud ou sur site.
- Selon les directives d'Apple, les applications ne peuvent être distribuées qu'aux employés, aux parties intéressées et aux partenaires, mais surtout à un groupe connu d'utilisateurs.

Distribution d'applications Android via l'App Store d'entreprise

Avantages

- Les applications peuvent être distribuées à des groupes d'utilisateurs sélectionnés, par exemple sous la forme d'un lien profond ou après connexion à l'aide d'un nom d'utilisateur et d'un mot de passe préalablement configurés.
- Les utilisateurs n'ont pas besoin d'un identifiant Google pour installer des applications à partir d'une boutique d'applications interne à l'entreprise.
- Il n'est pas nécessaire de satisfaire à toutes les exigences de Google
- La publication des mises à jour d'applications n'est pas retardée par les analyses techniques de Google.
- Certains magasins d'applications d'entreprise (par exemple Relution) peuvent être utilisés sans gestion des appareils (MDM).
- Un système de gestion des utilisateurs existant (ActiveDirectory/LDAP) peut être connecté afin que les utilisateurs n'aient pas besoin de nouvelles informations d'identification.

Inconvénients

- Les applications sont accessibles aux utilisateurs finaux via un mécanisme spécial approuvé par Google, mais qui nécessite une configuration initiale de la part de l'utilisateur.
- L'infrastructure de distribution doit être fournie sous la forme d'un service en nuage ou sur site.

Pour la version 26.4.0

Gérer les apps APK

Il existe trois façons de déployer des applications d'entreprise développées par soi-même sur des appareils Android inscrits via Android Enterprise. La méthode officielle fournie par Google et recommandée par nous est la distribution via le Play Store géré.

Depuis Relution 26.2, les applications APK téléchargées dans le Relution App Store peuvent en outre être distribuées en tant qu'applications personnalisées sur les appareils entièrement gérés, y compris avec profil personnel. Il n'est pas nécessaire pour cela de désactiver les mécanismes de sécurité d'Android Enterprise. Cette méthode n'est pas disponible sur les appareils inscrits en tant que profil professionnel.

La troisième méthode est la distribution directe d'un fichier APK, par exemple via l'application Relution Legacy, le web ou le courrier électronique. Étant donné que divers mécanismes de sécurité d'Android Enterprise doivent être désactivés, cette méthode n'est pas recommandée et n'a de sens que dans des cas exceptionnels.

Pour la version 26.4.0

Distribution via le Play Store

Il existe deux façons de télécharger des applications sur le Play Store. Dans les deux cas, un compte de développeur est nécessaire. Un compte développeur Google coûte 25 $ en une seule fois.

Déployer l'application via la console Play Store (recommandé)

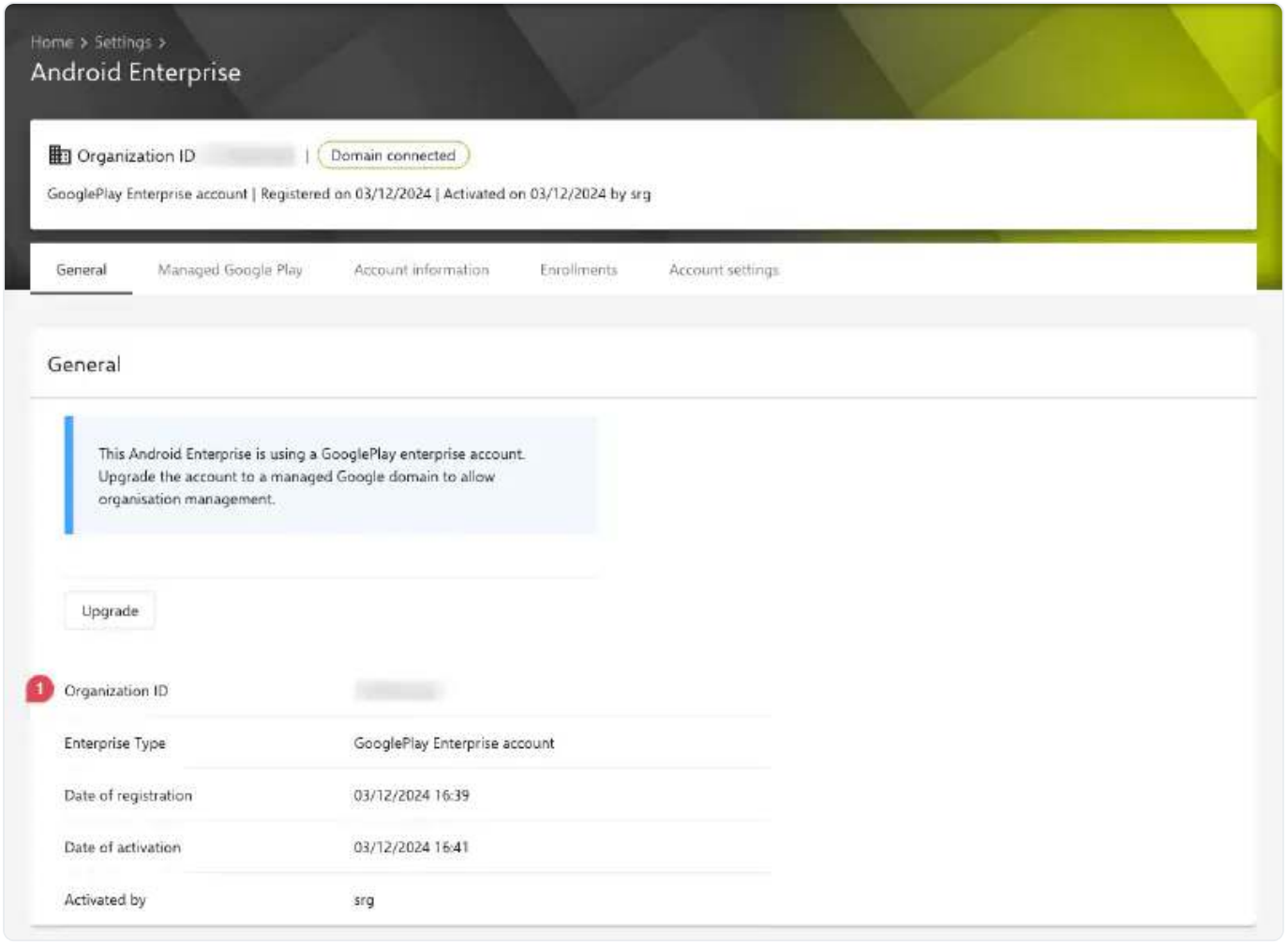
L'application est régulièrement téléchargée sur le Play Store via n'importe quel compte de développeur (Google Play Console →). Nous recommandons d'utiliser un compte d'entreprise officiel à cette fin.

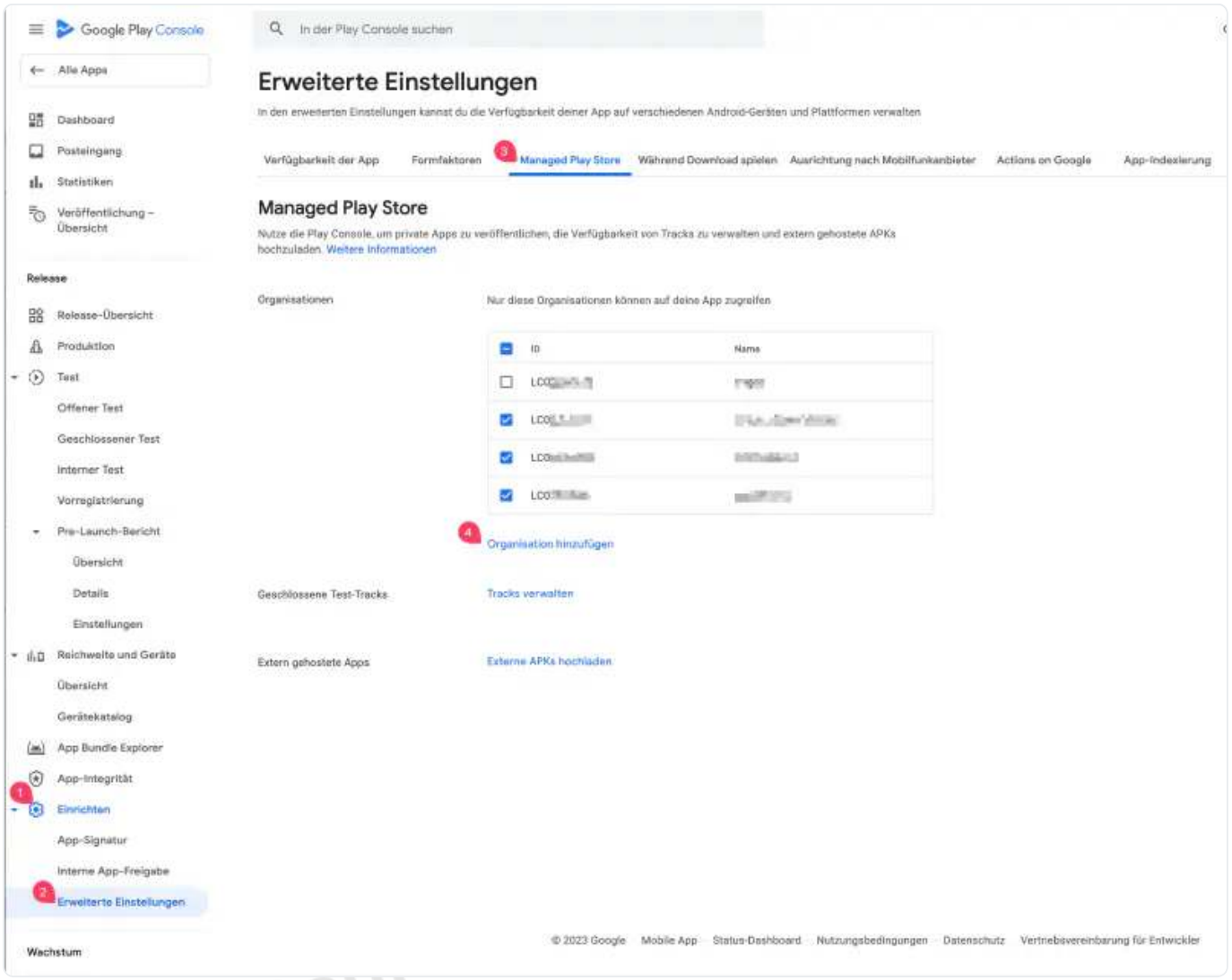
Toutes les options de paramétrage du Play Store y sont disponibles, comme la possibilité de pré-publier des versions de développement de l'application uniquement pour certains groupes de personnes.

Si l'application ne doit pas être accessible au public, sa disponibilité peut en outre être limitée à l'entreprise elle-même. Attention : ce réglage ne peut pas être annulé par la suite. Si l'application doit être proposée au public à l'avenir, elle doit être publiée à nouveau sous un autre nom de paquet.

Le grand avantage est que l'application peut alors être publiée pour d'autres entreprises ou comptes d'entreprise. Cela peut être utile, par exemple, en cas de déménagement du serveur, mais aussi si les données d'accès au compte Google utilisé pour Android Enterprise sont perdues.

Afin de restreindre l'application à l'entreprise elle-même, son ID d'organisation peut être stocké sous `Configuration` → `Paramètres avancés` → `Managed Play Store`. L'ID commence par `LC0...`. Cet ID est visible par exemple dans Relution sous `Paramètres` → `Spécifique à la plateforme de l'appareil` → `Android Enterprise`.





Télécharger via la boîte de dialogue Play Store dans Relution

Au lieu de télécharger l'application via la Google Play Console, il est également possible de la télécharger directement depuis Relution. Cependant, le compte Google utilisé pour configurer Android Enterprise doit être un compte développeur correspondant.

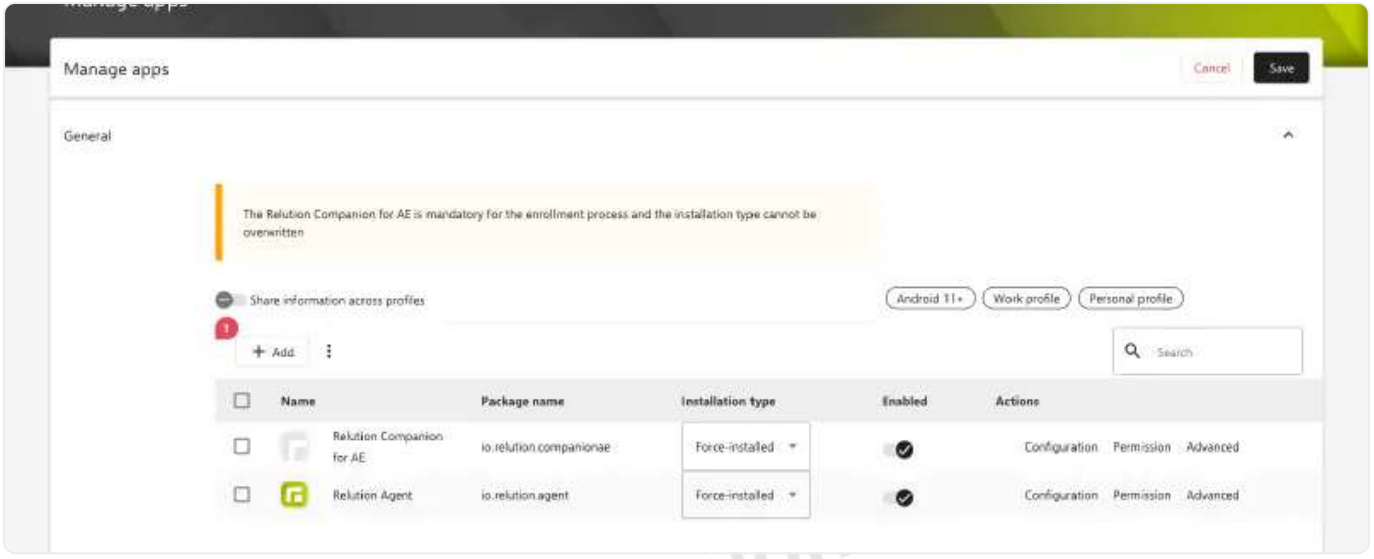
Hormis le nom de l'application, il n'est pas possible d'effectuer d'autres réglages et il n'est pas non plus possible d'activer l'application pour d'autres sociétés ou comptes d'entreprise par la suite. En raison de ces restrictions, nous déconseillons généralement cette option.

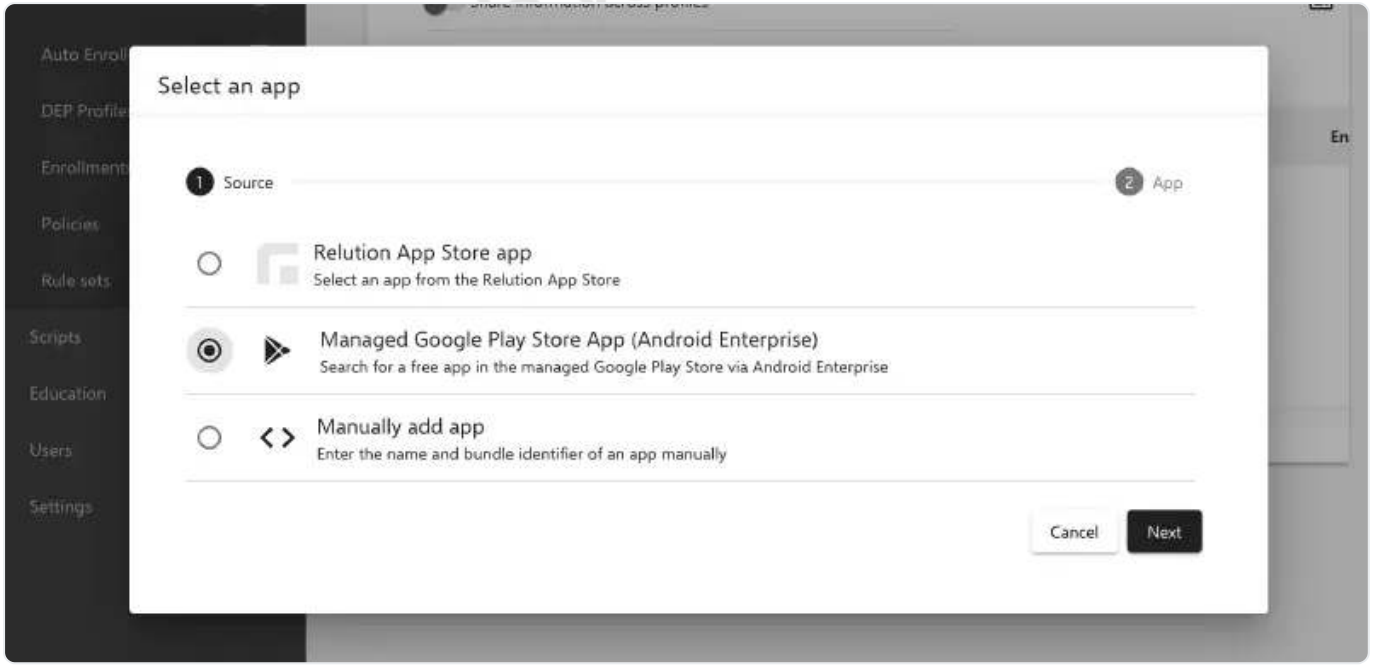
Pour télécharger une application en tant qu'application privée, procéder comme suit :

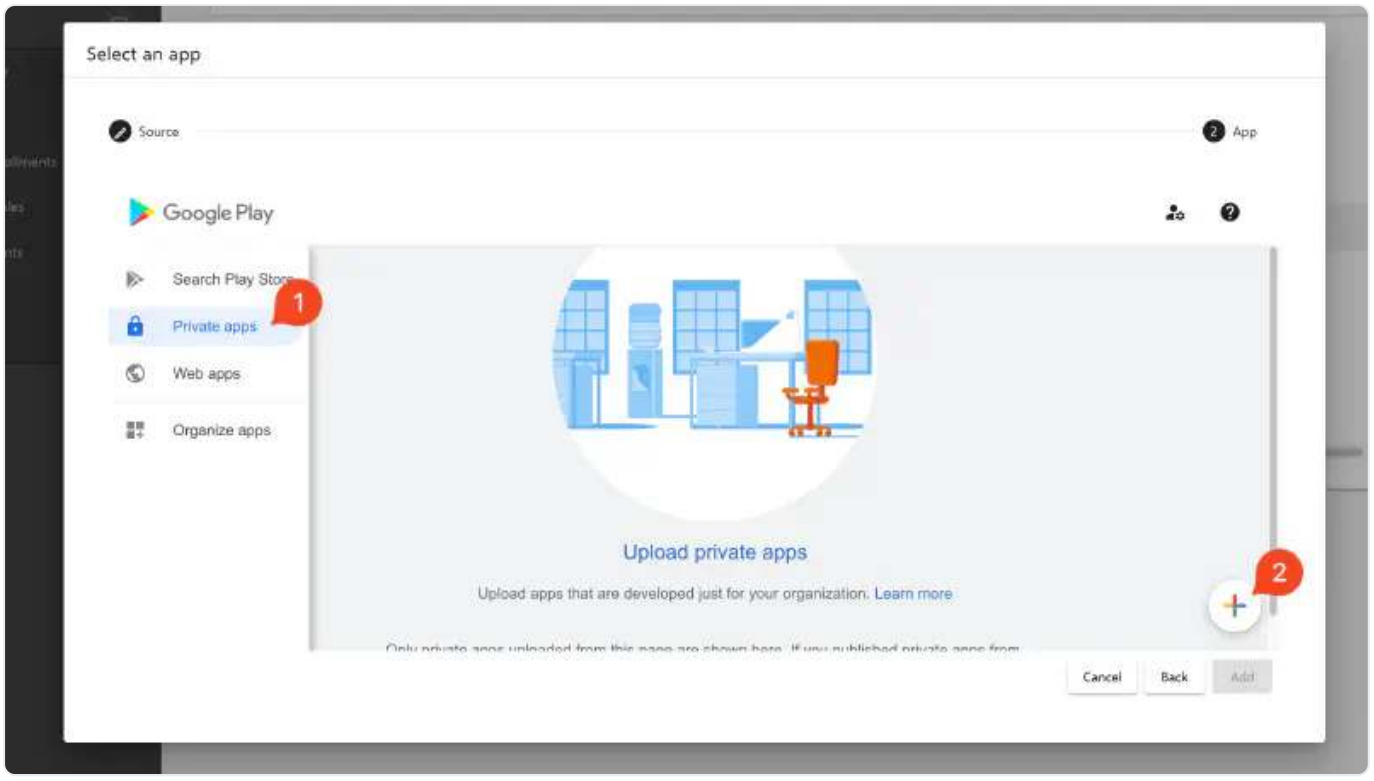
1. Dans Relution, aller dans `Appareils` → `Politiques`.
2. Ouvrir n'importe quelle politique Android Enterprise et ajouter une configuration Gérer les applications.
3. Cliquer sur Ajouter dans la configuration.
4. Sélectionner Application Google Play Store gérée (Android Enterprise).

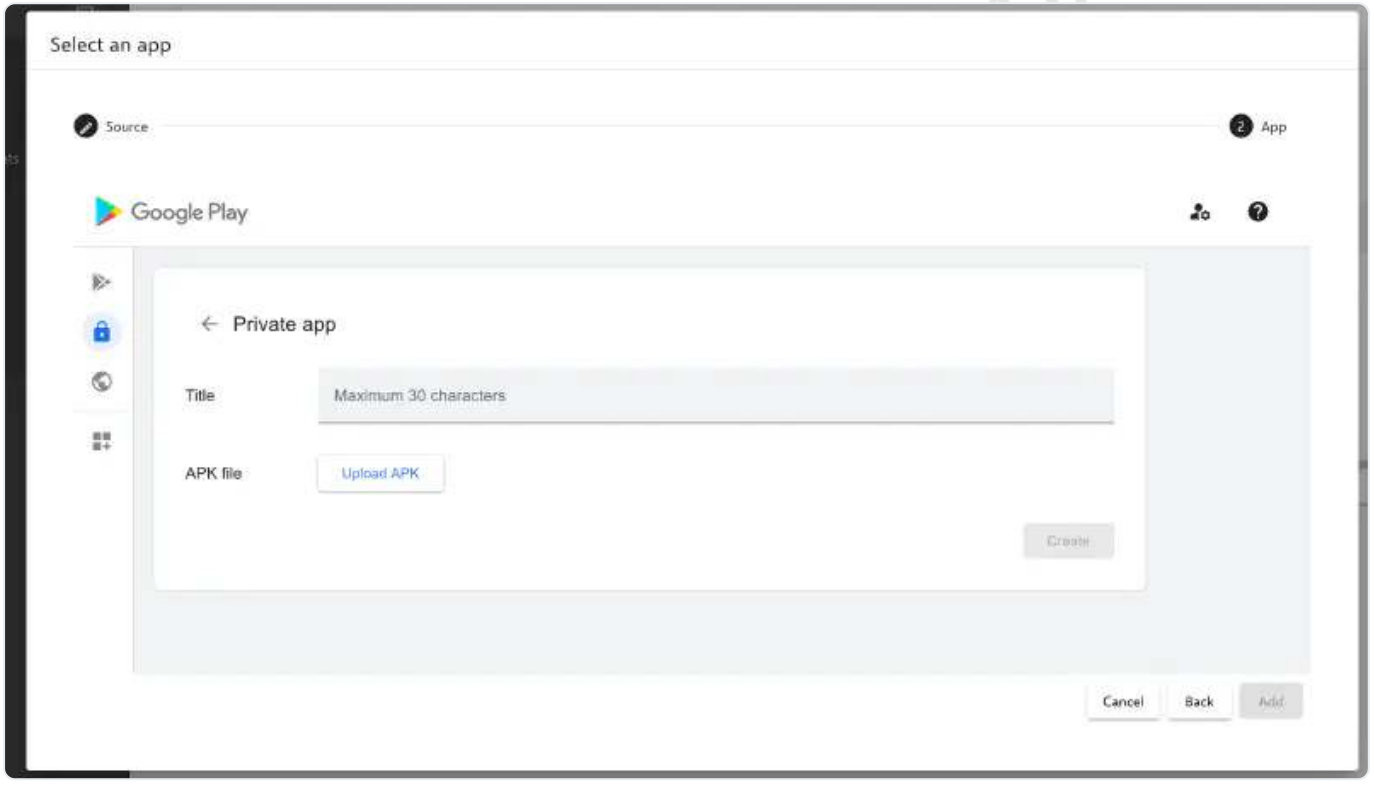
5. Aller sur le lien Apps privées.
6. Cliquer sur + pour ajouter une nouvelle application.

Attention : Le nom du paquet de l'application doit être unique. Si l'application est déjà disponible dans le Play Store, même en tant qu'application privée d'une autre société, elle ne peut pas être téléchargée à nouveau. Nous recommandons donc généralement le téléchargement via le Play Store, qui peut ensuite être utilisé pour déverrouiller l'application pour d'autres identifiants d'organisation.






Select an app
Source
App
Google Play
Search Play Store
Private apps
Web apps
Organize apps
1
Upload private apps
Upload apps that are developed just for your organization. Learn more
2
Cancel
Back
Add


Select an app
Source
App
Google Play
Private app
Title
Maximum 30 characters
APK file
Upload APK
Create
Cancel
Back
Add

Distribution d’un fichier APK

Depuis Relution 26.2, les applications natives téléchargées dans l’App Store de Relution au format `.apk` peuvent être distribuées directement sur les appareils entièrement gérés, y compris avec profil personnel :

- Dans la configuration de politique Gérer les applications via `Ajouter` → `Appli Relution App Store`. L’application est ajoutée avec le type d’installation Sur mesure.
- Via l’action Installer l’application depuis le Relution Store. Les applications natives ne peuvent y être sélectionnées que si seuls des appareils entièrement gérés sont sélectionnés.

Dans les deux cas, Relution doit avoir déterminé les certificats de signature de l’APK. Les assouplissements des paramètres de sécurité décrits ci-dessous ne sont pas nécessaires pour cette méthode.

Sur les appareils inscrits en tant que profil professionnel, les applications personnalisées ne sont pas installées. L’action Sélectionner l’application Play Store dans le Relution Store disponible sur ces appareils ne propose que des applications Play Store.

Pour ces appareils ainsi que pour l’installation de fichiers APK téléchargés (par ex. par courrier électronique ou depuis le web), les paramètres de politique suivants sont nécessaires :

1. Configuration Débrayages de sécurité avancés.
    - L’option Autoriser depuis des sources inconnues doit être réglée sur Autoriser les installations d’applications non fiables sur l’ensemble de l’appareil.

      Cela permet aux utilisateurs d'installer des fichiers APK de n'importe quelle source sur l'appareil !
2. Configuration Gestion du Play Store
    - L’option Activer le Play Store restreint doit être désactivée.

      Si l’option Play Store restreint est active, l’appareil supprimera les applications qui n’ont pas été installées sur l’appareil à l’aide de la configuration Gérer les applications ou qui font partie du système au bout d’environ 10 minutes.

      Cela permet aux utilisateurs d'installer n'importe quelle application du Play Store dans le profil géré.

Pour la version 26.4.0

Une fois ces réglages effectués, il est à nouveau possible d'installer n'importe quel fichier APK sur l'appareil. Étant donné que les utilisateurs peuvent installer des fichiers APK de n'importe quelle source dans ce mode, nous déconseillons généralement d'activer ces paramètres. En outre, il n'existe aucun moyen simple de s'assurer que les applications sont à jour.

Il est également possible d'ajouter manuellement le nom du package de l'application correspondante dans une configuration Gérer les applications afin de l'autoriser. L'application ne devrait alors plus être supprimée automatiquement par l'appareil.

Il existe plusieurs options pour distribuer les fichiers APK, par exemple :

Installation via l'application Relution Legacy.

Pour cela, l'application Relution Legacy est installée sur l'appareil via une configuration Gérer les applications. Ensuite, les utilisateurs peuvent se connecter à l'application et accéder à toutes les applications Android natives stockées dans le Relution Store. Les utilisateurs peuvent télécharger et installer ces applications via l'application Legacy. En fonction de la version d'Android, les utilisateurs doivent également accorder à l'application Relution le droit de demander l'installation d'applications.

Si le Companion (Legacy) est inscrit en plus (nécessite une autre licence d'appareil !), les administrateurs peuvent alternativement installer des applications via une action sur les appareils inscrits en tant que profil professionnel. Selon le type d'appareil, les utilisateurs devront peut-être encore accepter l'installation manuellement. Sur les appareils entièrement gérés, y compris avec profil personnel, cela n'est pas nécessaire : l'action Installer l'application depuis le Relution Store y est disponible sans inscription ni licence d'appareil supplémentaire (voir ci-dessus).

Pour la version 26.4.0

Installation par courriel

Les utilisateurs reçoivent de l'entreprise le fichier APK à installer par courrier électronique.

Installation à partir du web

Les utilisateurs reçoivent le fichier APK à installer via un lien de téléchargement distribué par e-mail, Messenger ou SMS, par exemple.

Liens supplémentaires

Aide Android Enterprise →

Applications auto-hébergées

Les applications Android auto-hébergées permettent aux entreprises et aux organisations de contrôler leurs données et d'accroître leur confidentialité et leur sécurité. En installant et en gérant ces applications sur leurs propres serveurs, elles conservent un contrôle total sur leurs informations sensibles tout en réduisant leur dépendance à l'égard des fournisseurs de services externes.

Cette fonction est disponible à partir de Relution Server 5.23

Conditions préalables

- Il est nécessaire de disposer d'une licence de développeur Android active.
- Les comptes gérés Google Play générés automatiquement ne peuvent pas être utilisés lors du téléchargement d'applications via le Managed Play Store, car ces comptes ne sont pas liés à un compte de développeur Android actif et ne peuvent pas l'être.
- Les applications privées auto-hébergées doivent être configurées dans le compte Google Play avec une licence de développeur Android active.
- Un compte Google doit être lié à Relution `Home` → `Paramètres` → `Android Enterprise`.

Pour la version 26.4.0

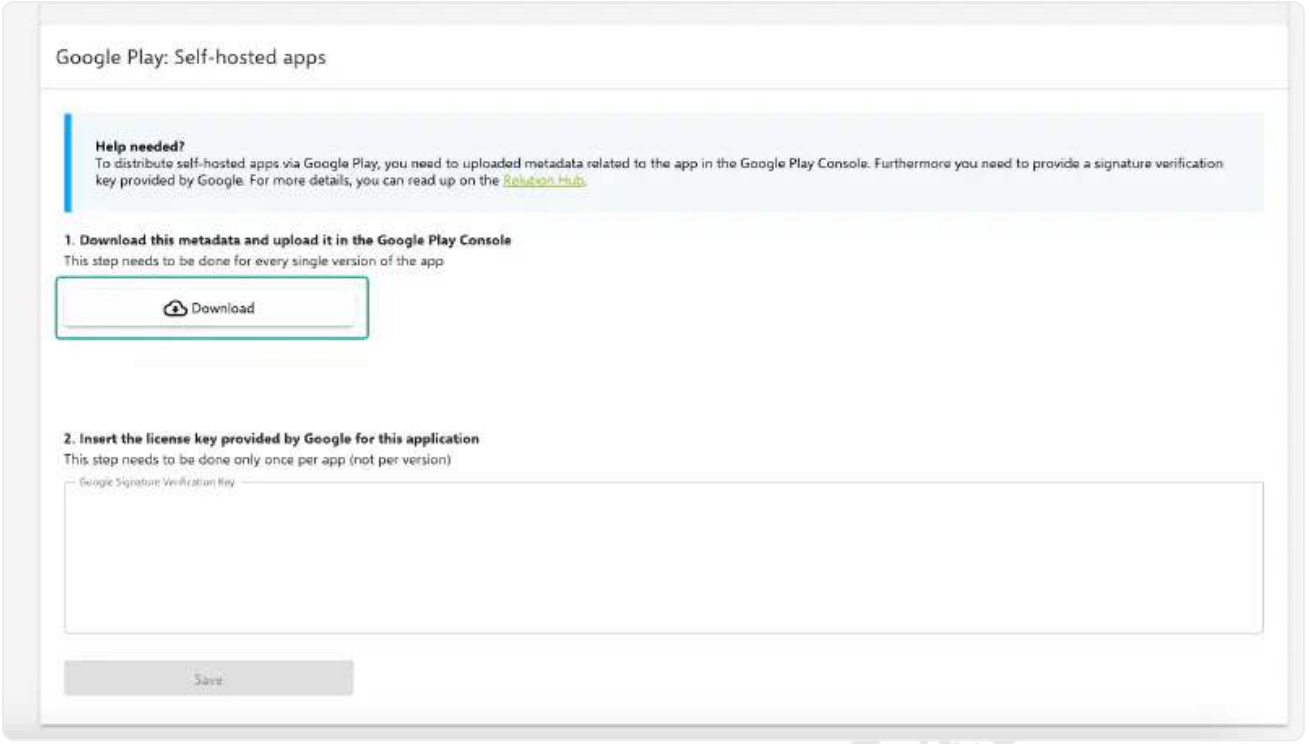
> Elles ne peuvent pas être installées à distance par les administrateurs informatiques sur les appareils avec des profils de travail. Les utilisateurs disposant d'un profil professionnel doivent installer ces applications manuellement via Managed Google Play.

App et métadonnées

1. Le fichier `apk` doit être téléchargé dans Relution sous `Home` → `Apps` → `App Store` → `Ajouter` (boîte de dialogue Ajouter une nouvelle application). Une application existante peut également être utilisée.

   > La version de l'application doit avoir le statut publié dans Relution (Version dans le portail). La section Google Play : applications auto-hébergées n'apparaît dans l'onglet Informations que si la version sous Version y est sélectionnée.

2. Les métadonnées doivent être chargées au format `json` via le bouton Télécharger dans la section Google Play : applications auto-hébergées de l'onglet Informations de l'application.

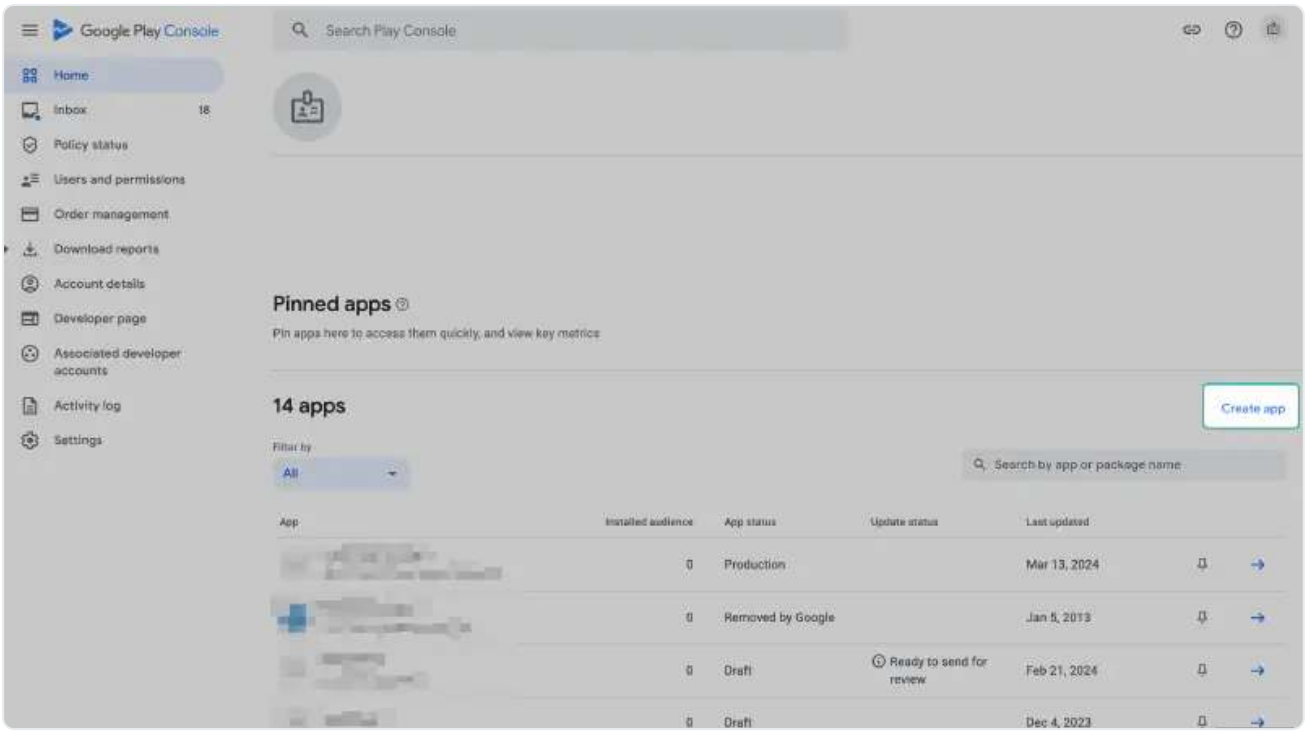


Pour la version 26.4.0

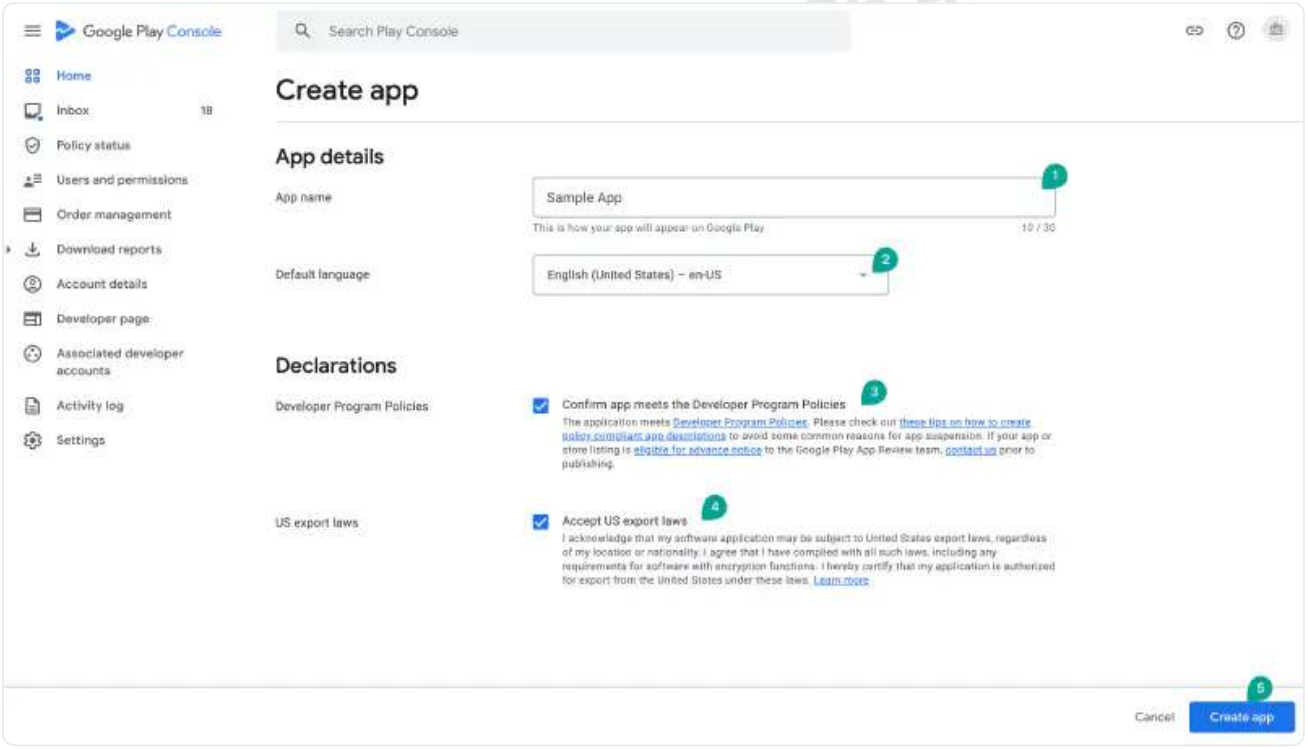
Créer une application

1. Basculer vers Google Play Console →

2. Créer une nouvelle application sous `Create app` (Créer une application)

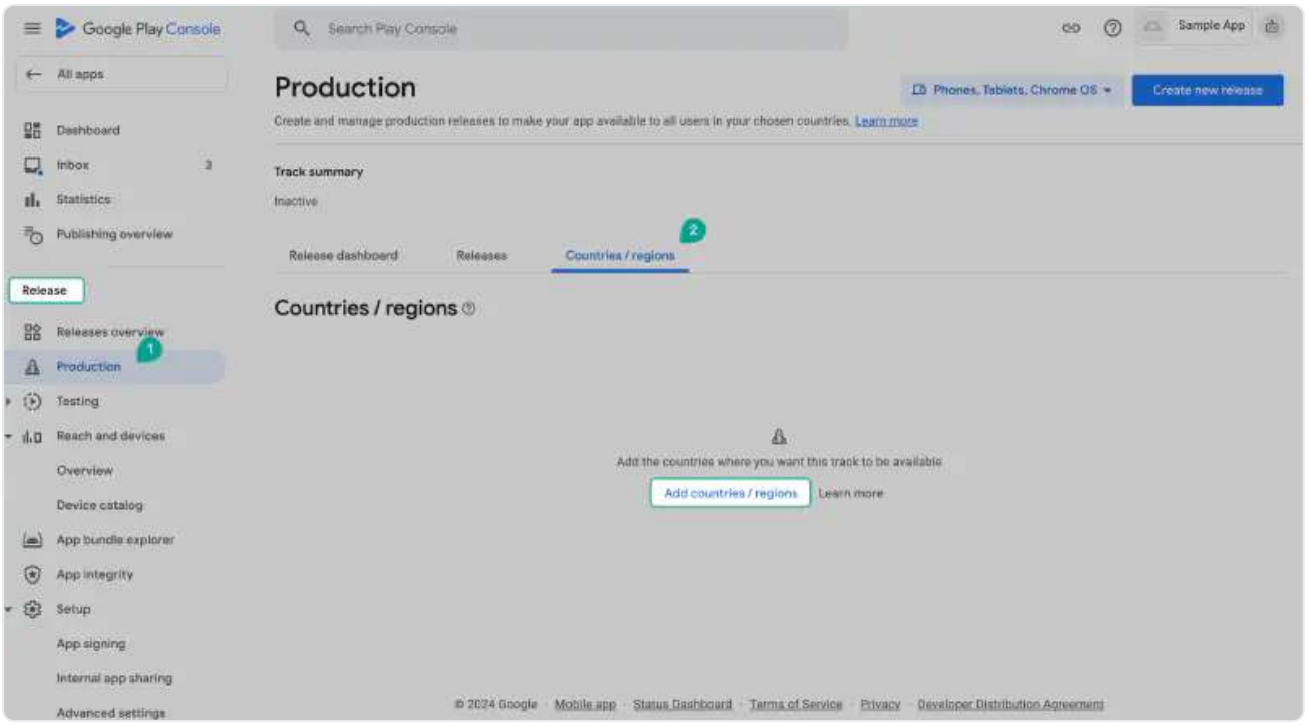


3. Ajouter les détails de l'application

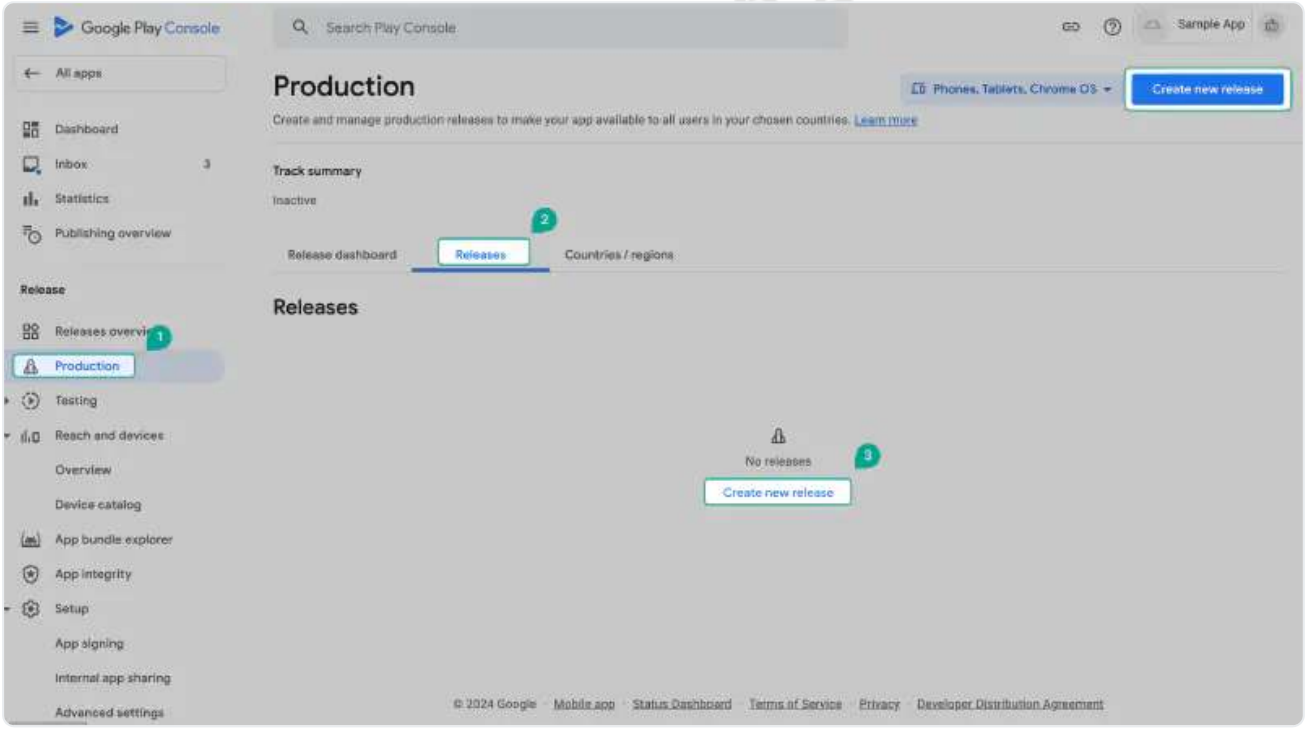


Une icône d'application peut être ajoutée sous Grow > Store presence > Main Store listing dans la section Graphics

4. Ajouter les pays dans lesquels l'application devrait être disponible `Release` → `Production` → `Add countries / regions`

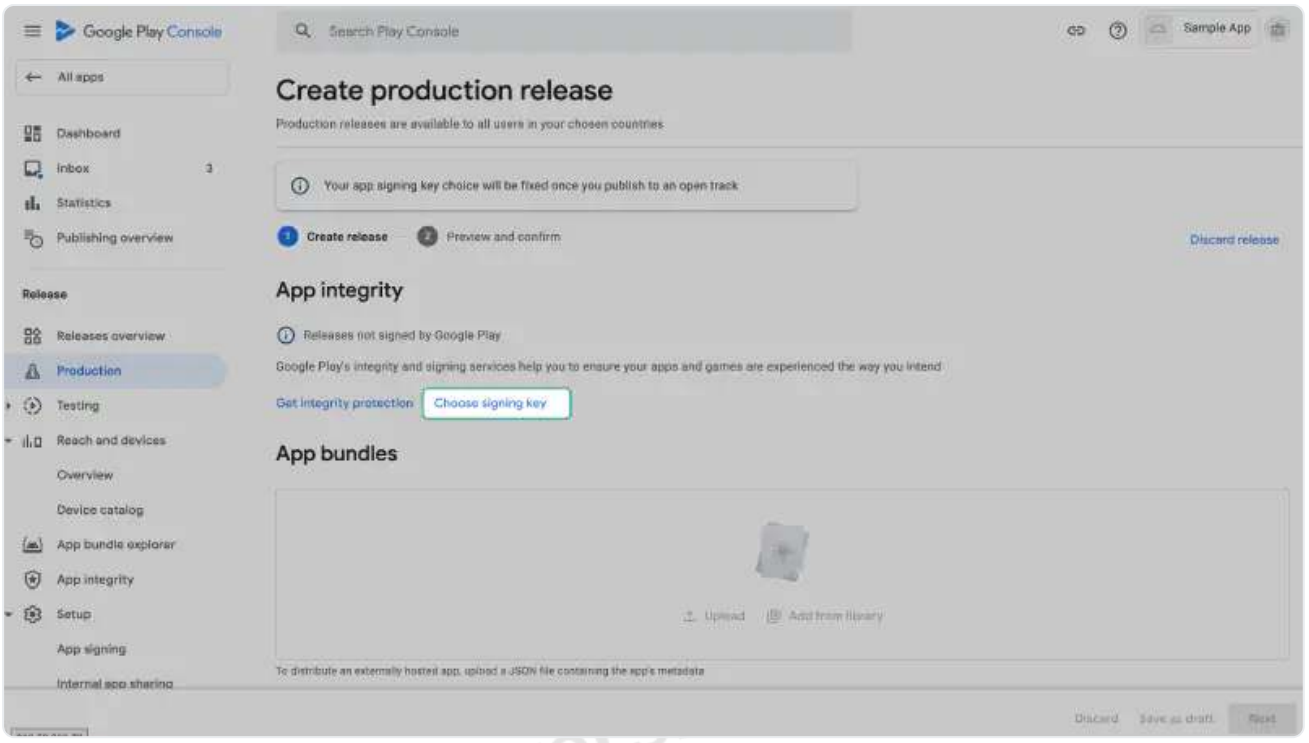


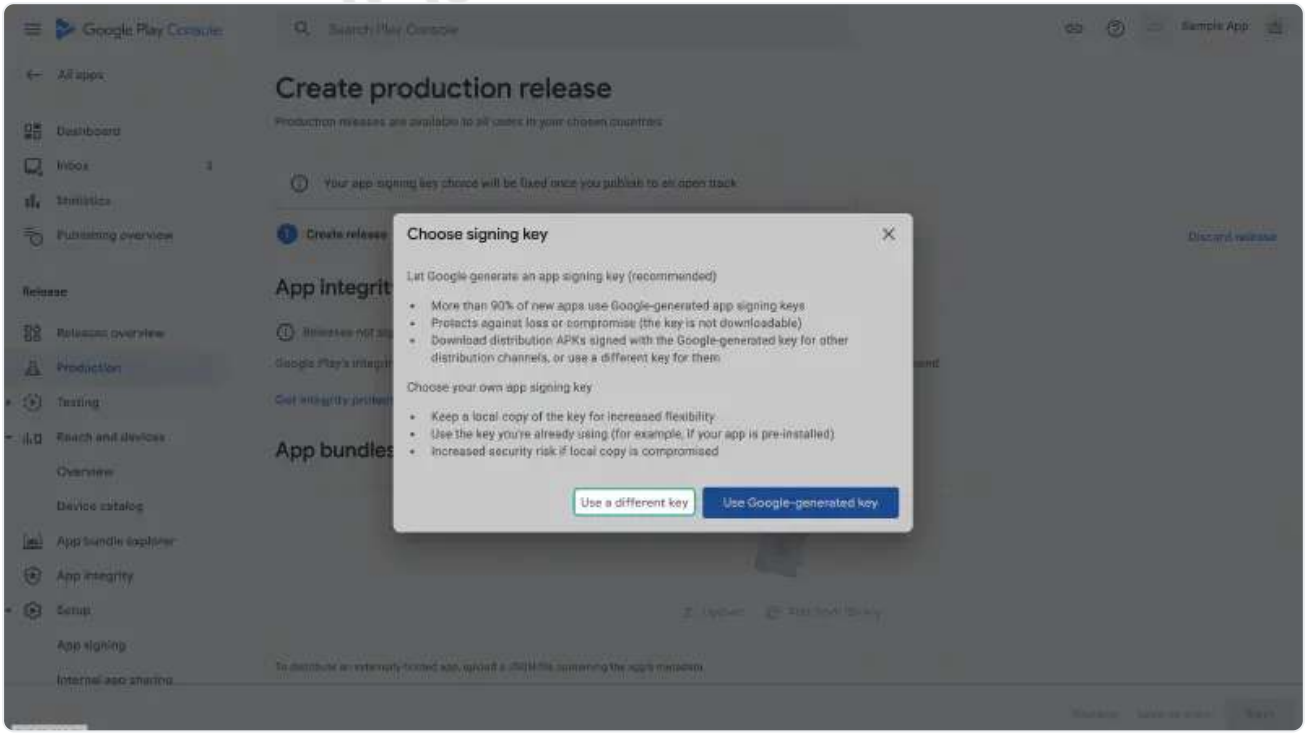
5. Créer une nouvelle version `Release` → `Production` → `Releases` → `Create new release`

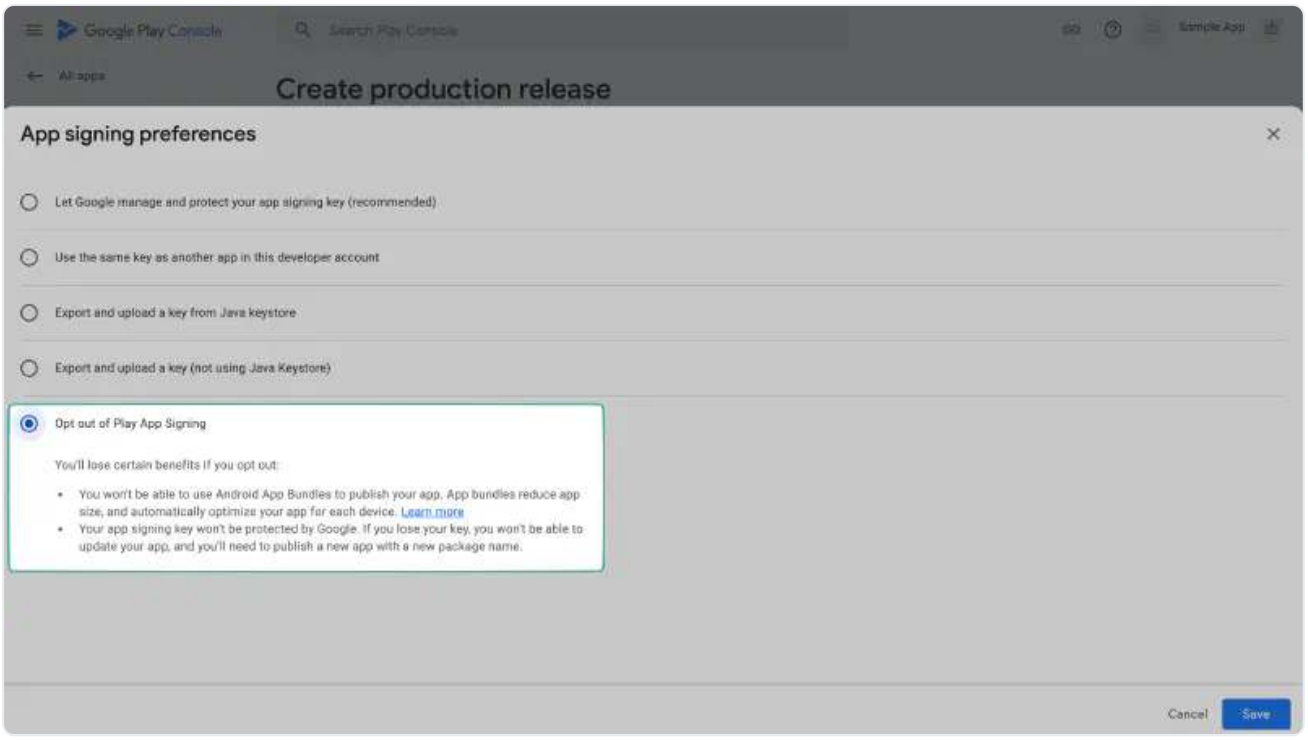


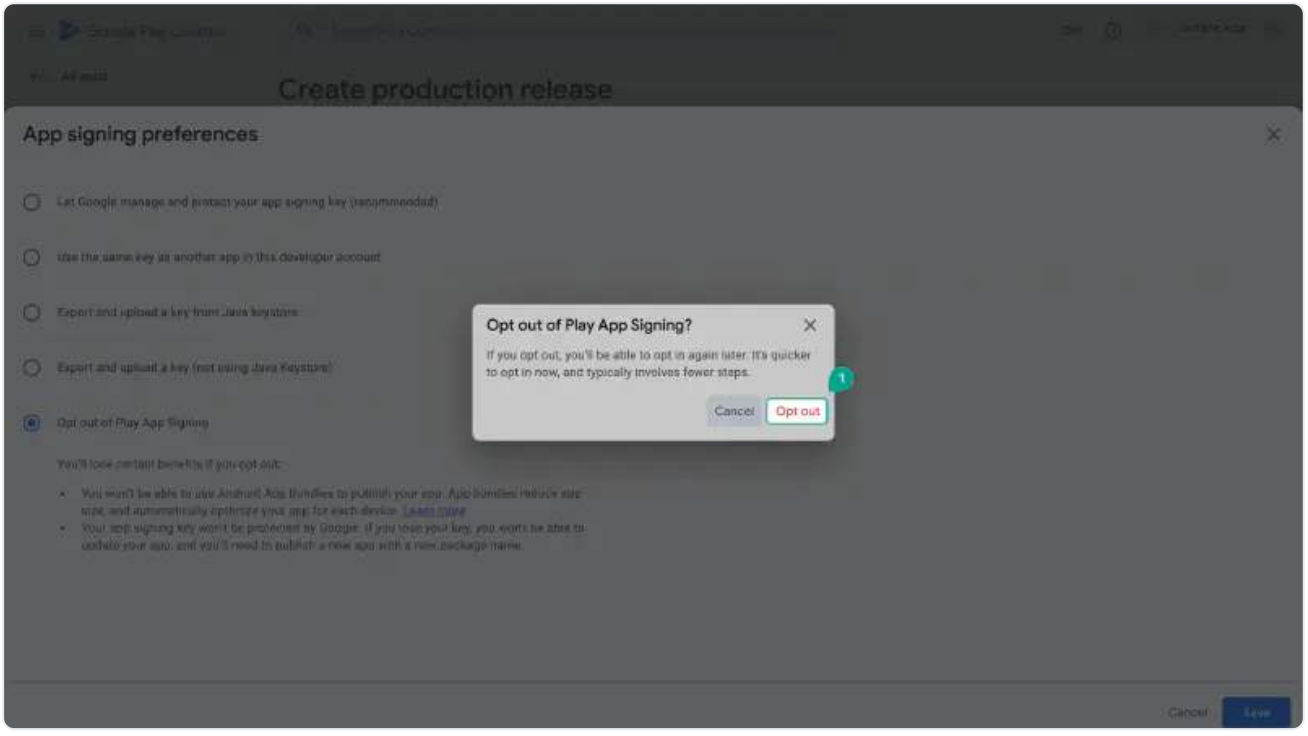
Signature

1. Sélectionner la clé de signature `Use a different Key` → `Opt out of Play App Signing` → `Opt out`

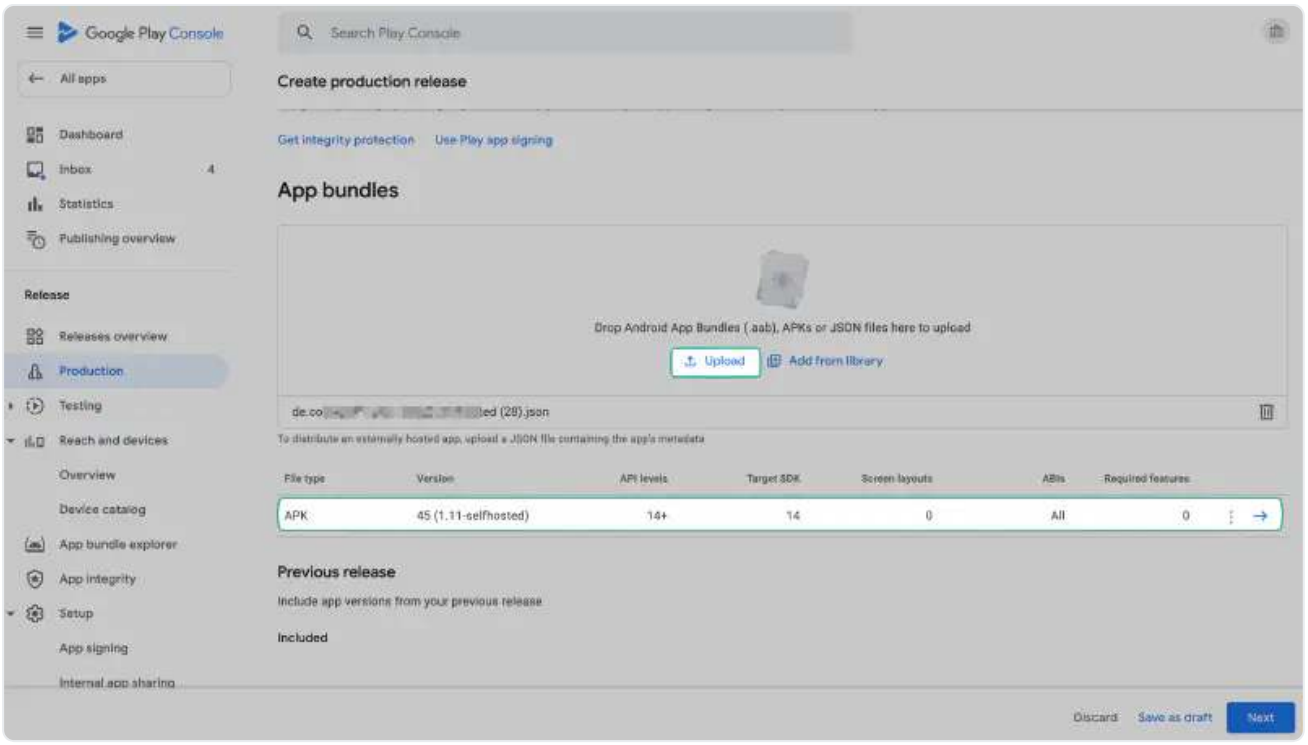




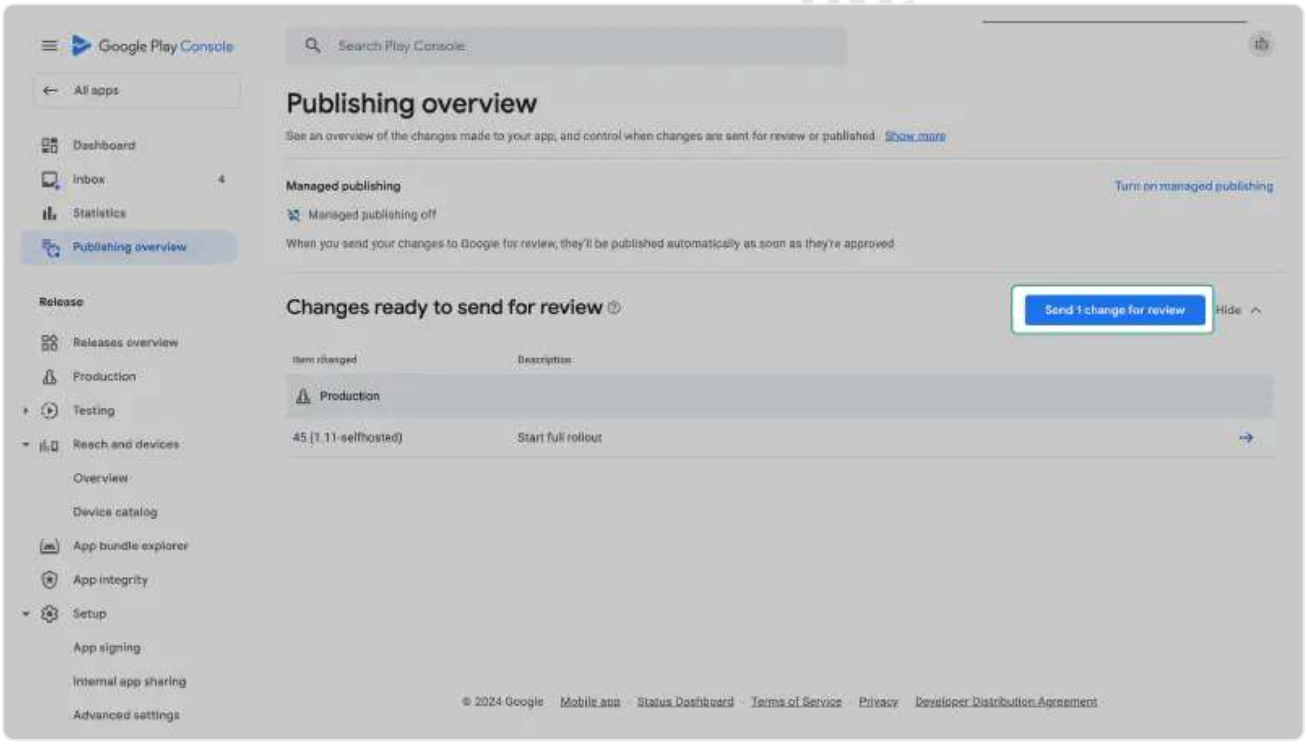




2. Téléverser dans la Google Play Console le fichier de métadonnées `json` obtenu à l'étape 2 de la section « App et métadonnées », puis cliquer sur `Next` et `Save`

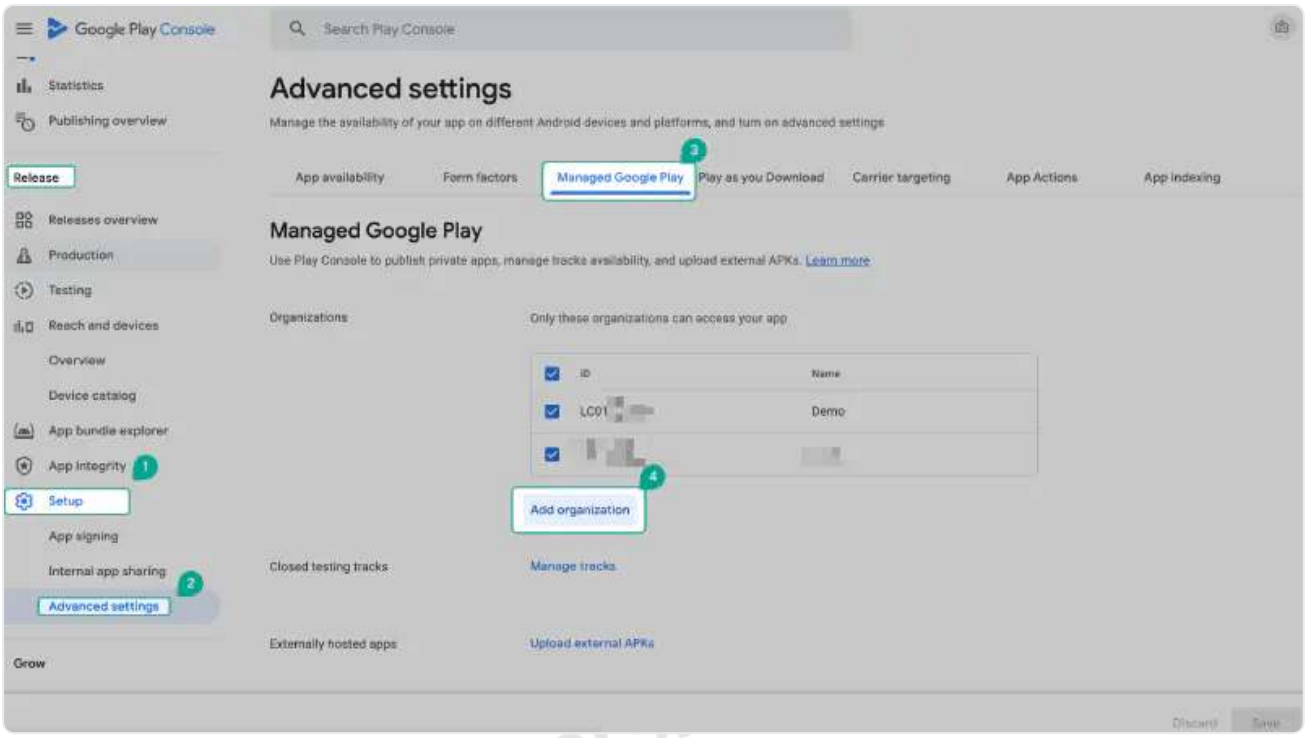


3. Soumettre la modification pour examen via `Send 1 change for review`

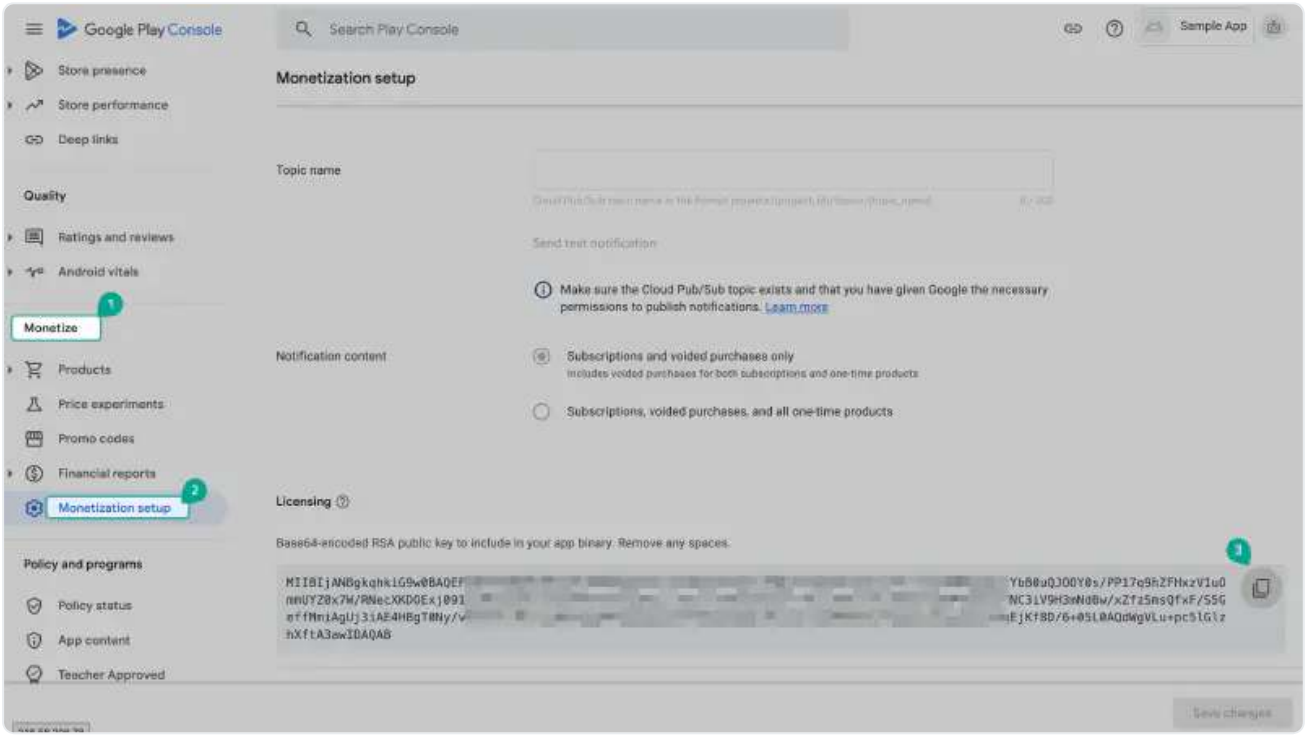


Publication de l’application pour l’organisation

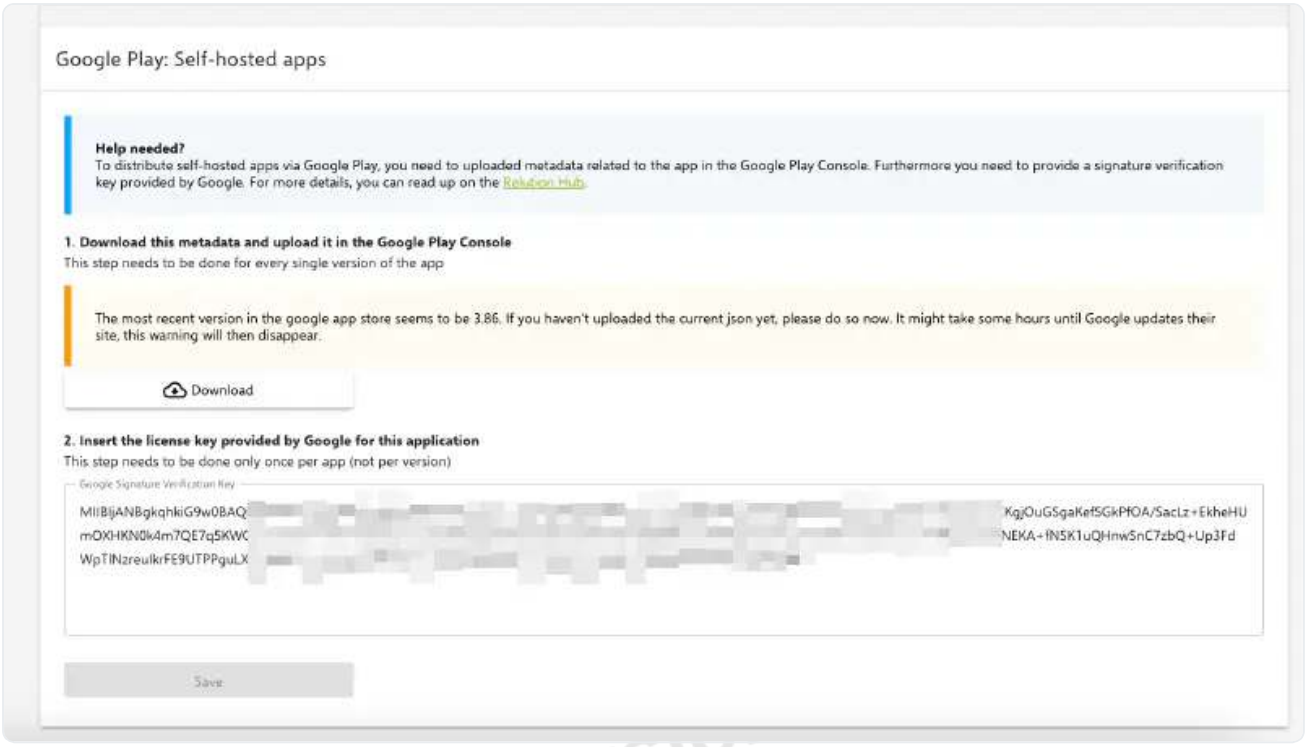
1. Copier le Google OrganizationID depuis le Relution Portal sous `Home` → `Paramètres` → `Android Enterprise` et l’ajouter à la Google Play Console



2. Copier la clé RSA de l’application et l’ajouter à l’application dans Relution `Monétiser` → `Configuration de la monétisation`



3. Coller la clé RSA dans Relution dans le champ Clé de vérification de la signature Google de la section Google Play : applications auto-hébergées, dans l'onglet Informations de la version publiée de l'application, puis l'enregistrer avec Enregistrer. Cette étape n'est nécessaire qu'une seule fois par application, et non par version.



Pour la version

Mettre à jour l'application existante

1. Télécharger la nouvelle version de `apk` dans Relution App Store `Home` → `Apps` → `App Store` → `App`
2. Télécharger les métadonnées `json`

> La version la plus récente dans le magasin d'applications de Google semble être x.xx . Si le json actuel n'a pas encore été téléchargé, le télécharger maintenant. Il peut s'écouler quelques heures avant que Google ne mette à jour son site, cet avertissement disparaîtra alors

3. Créer une nouvelle version de l'application dans la Google Play Console
4. Téléverser dans la Google Play Console les métadonnées `json` de l'application obtenues depuis Relution
5. Envoyer la révision des modifications

Sujets connexes

- Enrôlement Android Enterprise → — Configuration des appareils Android Enterprise.
- Gestion des applications MAM dans Relution → — Notions de base de la gestion des applications.

Fournir des liens web

Des liens web peuvent être fournis sur les appareils Android Enterprise. Contrairement à Apple, les liens web sur les appareils avec l'inscription `Android Enterprise` sont fournis via le `Managed Google Play Store`

Configuration

Ceci nécessite la configuration de politique Gérer les applications :

1. Dans le portail Relution, naviguer vers `Appareils` → `Politiques` et cliquer sur Ajouter.
2. Créer une politique Android Enterprise et lui attribuer un Nom, puis cliquer sur Enregistrer.
3. Après avoir cliqué sur Ajouter, sélectionner l'option Gérer les applications et poursuivre avec Ajouter des détails.
4. À l'étape suivante, cliquer à nouveau sur Ajouter. Dans la boîte de dialogue Sélectionnez une application, sélectionner sous Source l'option Application Google Play Store gérée (Android Enterprise) et cliquer sur Suivant.
5. L'étape App affiche le Managed Google Play Store. Y cliquer sur Web Apps dans le menu de gauche
6. Pour créer une nouvelle Web App, cliquer sur l'icône + dans le coin inférieur droit
7. Dans la boîte de dialogue suivante, il est possible de créer des liens web et d'effectuer leur configuration de base
8. Cliquer sur la Web App nouvellement créée et confirmer avec Sélectionner. La boîte de dialogue se ferme et l'application web apparaît dans la liste de la configuration Gérer les applications
9. Adapter si nécessaire le Type d'installation et appliquer la configuration avec Enregistrer
10. Publier la politique et l'attribuer aux appareils souhaités

Avec le type d'installation par défaut Installé de force, l'application web est installée automatiquement sur les appareils. Avec Disponible, elle est proposée à l'installation dans le Managed Google Play Store sur l'appareil.

Pour la version 26.4.0

Play Store n'affiche aucune app

Sur les appareils Android Enterprise, il peut arriver que le Google Play Store n’affiche aucune application sur l’appareil. Ce comportement survient souvent lorsque certains paramètres ou attributions sont manquants dans le Managed Google Play Store ou dans Relution. Voici un guide étape par étape pour résoudre ce problème :

Trouver et approuver l’application dans le Managed Google Play Store

Tout d’abord, l’application souhaitée doit être trouvée et approuvée dans le Managed Google Play Store.

1. Ouvrir un navigateur web et naviguer vers https://play.google.com/work →.
2. Rechercher l’application souhaitée qui n’apparaît pas sur l’appareil.
3. Approuver l’application pour la rendre disponible pour l’organisation.

Pour la version 26.4.0

Ajouter l’application à une collection dans Relution

Une fois l’application approuvée, elle doit être ajoutée à une collection d’applications dans Relution.

1. Se connecter au Portail Relution.
2. Dans la configuration Gérer l’application, l’ajouter.
3. Sélectionner Application Google Play Store gérée (Android Enterprise).
4. Sélectionner Gérer les applications dans le menu latéral.
5. Créer une collection ou en sélectionner une existante.
6. Sélectionner l’application qui vient d’être approuvée dans le Managed Google Play Store et l’ajouter à la collection.

Rendre l’application **disponible** dans une politique

Enfin, il faut s’assurer que l’application est définie comme disponible dans la politique correspondante. Cela garantit que l’application apparaît sur les appareils attribués.

1. Dans le Portail Relution, naviguer vers la Politique AE.

2. Sélectionner Gérer les applications.
3. Rechercher l’application dans la liste et sélectionner Disponible dans la colonne Type d’installation. Les applications nouvellement ajoutées depuis Managed Google Play sont définies par défaut sur Installé de force. Le bouton Activé doit en outre être activé.

Une fois ces étapes effectuées, l’application devrait apparaître dans le Google Play Store sur l’appareil et pouvoir être installée.

Pour la version 26.4.0

Managed Config Chrome

Les configurations d’application gérées pour Google Chrome peuvent être créées et appliquées dans Relution.

Liste de blocage

`Portail` → `la politique AE` → `Gérer les applications` → `Google Chrome (ajouter si absent)` → `Configuration`

Une fenêtre pop-up s’ouvrira ici. Dans le champ Block access to a list of URLs, la liste suivante doit être saisie. Plusieurs sites Web sont séparés par des virgules.

Liste de blocage →

```
[
  "example.com",
  "https://ssl.server.com",
  "hosting.com/bad_path",
  "https://server:8080/path",
  ".exact.hostname.com",
  "file://*",
  "custom_scheme:*",
  "*"
]
```

Favoris

`Portail` → `la politique AE` → `Gérer les applications` → `Google Chrome (ajouter si absent)` → `Configuration`

Favoris →

Une fenêtre pop-up s’ouvrira ici. Dans le champ Bookmarks, la liste suivante doit être saisie. Plusieurs sites Web sont séparés par des virgules.

```
[
  {
    "toplevel_name": "Company bookmarks"
  },
  {
    "name": "Relution",
    "url": "relution.io"
  },
  {
    "children": [
      {
        "name": "Formations",
        "url": "relution.io/schulungen/"
      },
      {
        "name": "Helpdesk",
        "url": "helpdesk.relution.io"
      }
    ],
    "name": "Internal URLs"
  },
  {
    "name": "Android resources",
    "url": "google.com"
  }
]
```

Client de messagerie géré

Avec Relution Mobile Device Management (MDM), il est possible de configurer de manière centralisée des clients de messagerie courants tels que Google Mail ou Samsung Mail, puis de distribuer ces paramètres à tous les appareils attribués à l'aide d'une politique.

Ce guide décrit comment ajouter l'application de messagerie respective à la politique, puis la configurer avec des variables dynamiques pour une configuration automatique et spécifique à l'utilisateur.

Ajouter l'application Client de Messagerie à la Politique

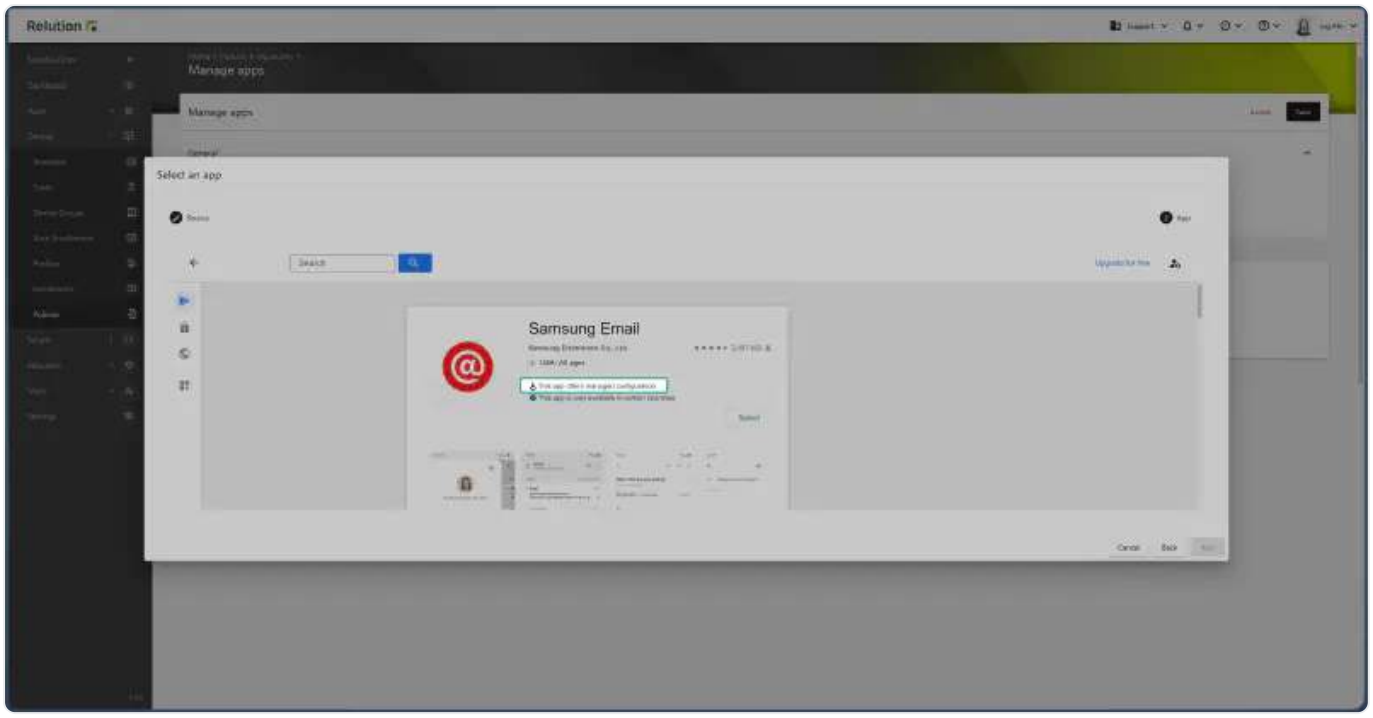
Avant de pouvoir effectuer la configuration, l'application de messagerie souhaitée (Google Mail ou Samsung Mail) doit être ajoutée à la politique Android Enterprise (AE).

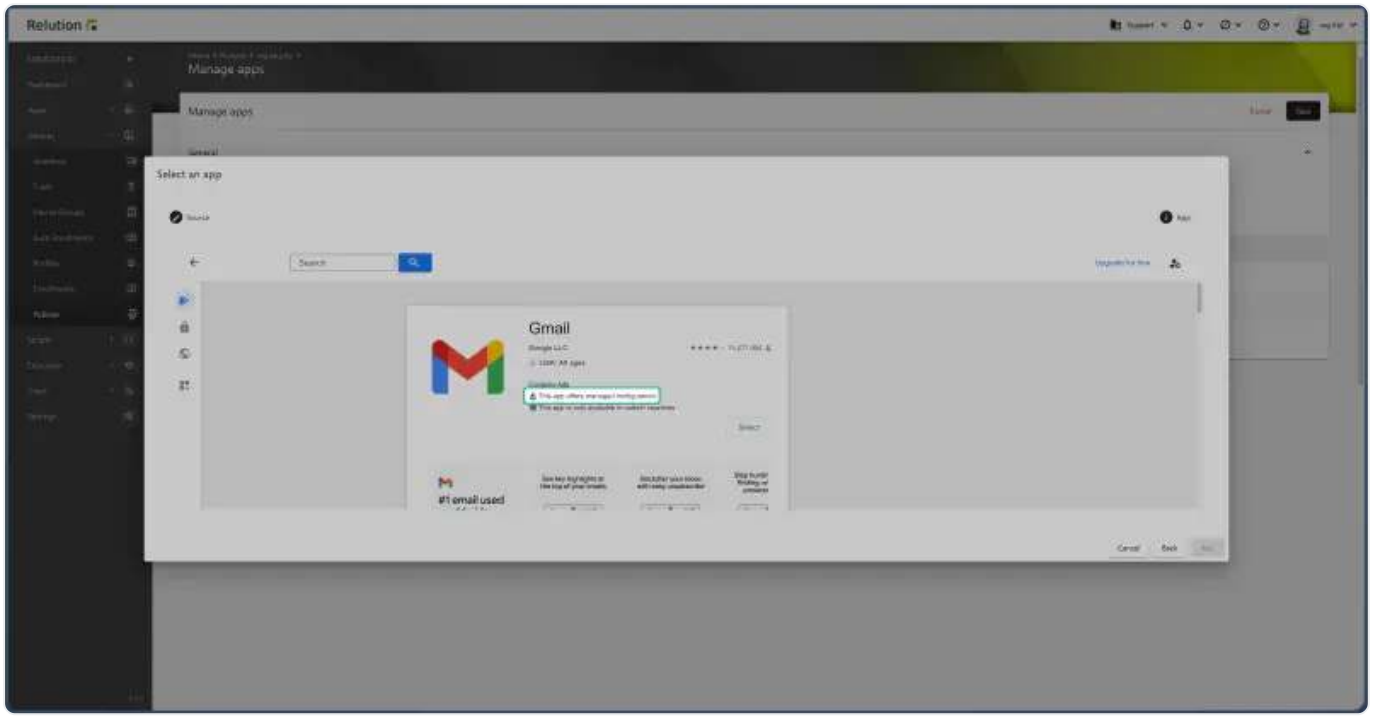
Ajouter l'Application

1. Naviguer dans le Portail Relution jusqu'à la Politique Android Enterprise existante ou nouvelle.
2. Sélectionner la configuration Gérer les applications.
3. Ajouter l'application de messagerie souhaitée (par exemple, Google Mail ou Samsung Mail) depuis le Google Play Store, si elle n'est pas déjà incluse dans la liste.

- Chemin : `Portail` → `Politique AE` → `Gérer les applications` → `Ajouter` → `Application Google Play Store gérée (Android Enterprise)` → `Google Mail/Samsung Mail (ajouter si absent)`

Pour la version 26.4.0





Les applications pour lesquelles des options de configuration gérées (Managed Configs) sont disponibles sont directement identifiables dans la sélection (comme illustré dans les captures d'écran).

À noter : L'étendue de ces configurations est déterminée exclusivement par le fabricant de l'application concernée. Relution n'a aucune influence sur les options fournies.

Démarrer la Configuration

1. Cliquer sur Configuration pour l'application de messagerie ajoutée.
2. Dans la boîte de dialogue, saisir les valeurs souhaitées (voir ci-dessous) et les appliquer avec Confirmer.
3. Enregistrer ensuite la configuration Gérer les applications avec Enregistrer. Confirmer applique les valeurs uniquement à la configuration ouverte ; sans Enregistrer, elles sont perdues en quittant la page.

Les modifications ne sont possibles que dans la dernière version de la politique, non encore publiée. Si celle-ci est déjà publiée, une nouvelle version est d'abord créée.

Configuration d'Application avec Variables (Managed Configuration)

La configuration du client de messagerie s'effectue via la Managed Configuration (Configuration Gérée). Les données utilisateur et les informations de serveur y sont stockées, et des Variables (Placeholders) peuvent être utilisées pour adapter automatiquement les paramètres à l'utilisateur concerné.

Pour une configuration flexible et universelle, les variables Relution peuvent être utilisées (par exemple, `${user.email}`).

- Affichage : Les variables disponibles sont affichées dans la vue de configuration respective.
- Conditions Préalables au Fonctionnement : Pour que ces variables soient correctement résolues, les conditions suivantes doivent être remplies dans le système Relution :

1. Données Valides : Les informations requises (par exemple, une adresse e-mail pour `${user.email}`) doivent être valides et enregistrées pour l'utilisateur.
2. Attribution d'Appareil : L'utilisateur doit être assigné à l'appareil en question.

Pour la version 26.4.0

Pour la version 26.4.0

Résumé et Distribution

Après avoir sauvegardé la Managed Configuration, l’application de messagerie sera automatiquement configurée et distribuée lors de la publication à tous les appareils auxquels la politique est attribuée (par exemple via des groupes d’appareils). Les variables sont alors remplies avec les données de l’utilisateur attribué à l’appareil concerné. Les utilisateurs n’ont qu’à ouvrir l’application, saisir leur mot de passe et peuvent immédiatement consulter leurs e-mails sans avoir à effectuer de réglages manuels de serveur.

> Si les données de la configuration sont ajustées dans Relution mais ne sont pas appliquées sur l’appareil final, l’application correspondante doit être supprimée et la nouvelle configuration appliquée à nouveau.

> Tester d’abord la configuration avec un petit groupe d’appareils afin de s’assurer que toutes les variables et les paramètres de serveur sont correctement pris en compte.

Configuration de Google Mail et Samsung Mail avec Secure Mail Gateway (SMG)

Des ajustements de configuration spécifiques des applications de messagerie sont requis lors de l'utilisation d'une Secure Mail Gateway (SMG). Un guide détaillé pour la mise en œuvre de cette intégration et de ces ajustements se trouve dans la Base de Connaissances : Intégration SMG pour Gmail →

Pour la version 26.4.0

Configurer Gmail pour SMG

Pour utiliser Secure Mail Gateway avec Gmail, certaines configurations sont nécessaires sous Android Enterprise. L'aperçu ci-dessous présente les paramètres qui doivent être configurés. Il est important qu'il n'y ait pas eu de tentatives précédentes de configuration de Gmail sur l'appareil, car sinon des fragments de ces configurations peuvent conduire à des erreurs.

Gmail de Google est particulièrement adapté comme client de messagerie et comme exemple pour cet article, car l'application est généralement disponible pour toutes les versions d'Android et tous les modèles d'appareils.

L'application ne peut pas être configurée manuellement sur l'appareil si la Secure Mail Gateway doit être utilisée.

Ces instructions nécessitent une Secure Mail Gateway fonctionnelle et configurée.

Configuration

Les paramètres de configuration suivants sont nécessaires.

Pour la version 26.4.0

Adresse électronique

Quelle adresse électronique doit être configurée ? Une adresse fixe ou la variable `${user.email}` peuvent être utilisées ici.

Nom d'hôte ou hôte

Le nom d'hôte de l'URL du service SMG définie dans les paramètres de la Passerelle de messagerie → doit être saisi comme nom d'hôte. Selon la configuration, il s'agit du nom d'hôte du serveur Relution ou d'un sous-domaine dédié du service SMG.

> `https://` ne doit pas être indiqué.

Nom d'utilisateur

Le nom d'utilisateur doit être spécifié sous la forme `unique-name-of-relution-organization\username`. Le nom unique de l'organisation peut être consulté sous

`Paramètres` → `Paramètres généraux de l'organisation`.

Identifiant de l’appareil

La variable `${device.exchangeDeviceId}` doit être utilisée ici.

Types d’authentification

L’option d’authentification de base (Allow basic authentication) doit être activée et l’option d’authentification moderne (Allow modern authentication) doit être désactivée.

Pour la version 26.4.0

Configurer Outlook

Dans Relution, Microsoft Outlook pour Android Enterprise peut être préconfiguré via une configuration d'application gérée. Le compte de messagerie est renseigné automatiquement à l'aide de variables (par ex. `${user.email}`), de sorte que seul le mot de passe doit être saisi au premier lancement de l'application.

La configuration minimale d'un compte Microsoft 365 est décrite ci-dessous.

Configuration

`Portail` → `la stratégie AE` → `Gérer les applications` → `Microsoft Outlook (ajouter si absent)` → `Configuration`

Dans la fenêtre contextuelle de configuration, les champs suivants sont renseignés. Toutes les clés partagent le préfixe commun `com.microsoft.outlook.EmailProfile.`.

Clé	Valeur	Description
`ServerHostName`	`outlook.office365.com`	Adresse du serveur Microsoft 365 / Exchange
`EmailUPN`	`${user.email}`	Nom d'utilisateur principal (identifiant de connexion du compte)
`EmailAddress`	`${user.email}`	Adresse e-mail du compte
`EmailAccountName`	`${user.fullname}`	Nom d'affichage du compte
`AccountType`	`ModernAuth`	Méthode d'authentification (authentification moderne)

> Les variables `${user.email}` et `${user.fullname}` sont résolues automatiquement pour chaque utilisateur. D'autres espaces réservés et fonctions sont décrits sous Espaces réservés avancés →.

Séparation des données

Pour séparer les données professionnelles et personnelles sur les appareils Android, trois approches fondamentales sont disponibles : la gestion complète d'un appareil appartenant à l'organisation, l'appareil géré avec profil personnel (COPE) en tant qu'appareil appartenant à l'organisation avec un espace privé séparé, ou le profil de travail en tant que conteneur cloisonné sur un appareil personnel.

Gestion complète de l'appareil (Device Owner, à partir d'Android 9)

Au plus tard depuis Relution 5, l'inscription Android Enterprise en tant qu'appareil entièrement géré (Device Owner) s'est largement imposée pour la gestion des appareils Android dans Relution. Les fonctions MDM sont intégrées dans le système d'exploitation et normalisées. Cela permet une fonctionnalité MDM uniforme et largement indépendante des fournisseurs sur la plateforme Android. Les fonctions Android Enterprise ne sont disponibles que pour les appareils certifiés. Les appareils Samsung peuvent être gérés et sécurisés de manière encore plus approfondie grâce aux fonctions KNOX. L'application Relution Client n'est plus obligatoire pour l'inscription à Android Enterprise.

Pour la version 26.4.0

Par ailleurs, l'inscription classique en tant que Device Administrator reste disponible. Dans ce cas, l'application Relution Client dispose de droits spéciaux sur l'appareil pour pouvoir exécuter les fonctions MDM. Cependant, avec ce type d'inscription, les options d'intervention MDM dépendent fortement de l'appareil Android utilisé.

Un large éventail de configurations et de fonctions est disponible pour la gestion des appareils Android :

- Installation et configuration d'applications (par exemple, client Exchange)
- Managed Google Play Store
- Configuration du WiFi et du VPN
- Enrôlement entièrement automatisé des appareils (KNOX Mobile Enrollment)

Appareil géré avec profil personnel (COPE)

Avec le type d'inscription Configurer un appareil géré avec un profil personnel (Company Owned, Personally Enabled – COPE), un appareil appartenant à l'organisation est remis à des utilisateurs

autorisés à l'utiliser également à des fins privées. En plus de l'espace géré, un profil personnel est disponible, auquel les administrateurs n'ont ni visibilité ni accès. Relution gère l'ensemble de l'appareil et peut par exemple effectuer une réinitialisation d'usine, qui supprime également toutes les données privées.

Profil personnel →

Enrôlement du profil de travail

Android Enterprise offre en outre ce que l'on appelle le profil de travail, qui est destiné aux appareils privés et met en place un conteneur (Travail) sur l'appareil qui peut être géré par Relution. Ce conteneur contient un Managed Play Store, qui ne met à disposition que des applications approuvées pour l'installation. L'installation d'applications à partir du Managed Google Play Store est possible sans compte Google local. En outre, les applications peuvent être configurées via Relution si une configuration d'application gérée est prise en charge par l'application concernée (par exemple, une application de courrier électronique avec une adresse de serveur et un ID utilisateur prédéfinis). Le conteneur peut également contenir son propre carnet d'adresses pour séparer les contacts professionnels des contacts privés.

Relution ne peut pas agir sur ce qui se trouve en dehors du conteneur (Personnel) : l'appareil ne peut par exemple pas être réinitialisé aux paramètres d'usine. Cependant, le conteneur peut être supprimé par Relution, ce qui supprime toutes les données qu'il contient. L'action Dispositif de verrouillage est également disponible pour les appareils dotés d'un profil de travail. Le verrouillage du seul profil de travail ou de l'appareil entier dépend d'Android et des paramètres de verrouillage de l'appareil.

Relution prend en charge le profil de travail au sein d'une organisation parallèlement à la gestion complète des appareils d'Android Enterprise et à l'inscription classique en tant que Device Administrator. Ainsi, Relution permet un fonctionnement mixte avec différents appareils.

Limites fonctionnelles

En outre, les fonctions suivantes dans le conteneur Travail peuvent également être désactivées par restriction :

- App Block/Allowlisting
- Création de nouveaux utilisateurs et profils
- Ajout et suppression de comptes
- Installation d'applications
- Désinstaller des applications
- Utiliser l'appareil photo

Pour la version 26.4.0

- Faire des captures d’écran
- Configurer et utiliser Bluetooth
- Partager des contacts via Bluetooth
- Configurer le réseau mobile
- Configurer le VPN
- Utiliser Android Beam (NFC) pour partager des données d’application
- Montage de supports physiques externes

La configuration des réseaux Wi-Fi et le transfert de fichiers via USB ne peuvent être restreints que sur les appareils gérés et les appareils avec profil personnel (COPE), pas dans le profil de travail des appareils privés.

Pour la version 26.4.0

Homescreen comme Launcher

Relution Homescreen peut être utilisé de deux manières :

1. Mode kiosque → : via la configuration dédiée Relution Homescreen (strictement verrouillée).
2. Lanceur séparé : en le définissant comme application par défaut.

L'utilisation comme lanceur par défaut permet d'afficher les notifications sur l'écran de verrouillage, d'ouvrir le menu système en haut de l'écran et d'afficher les applications système si nécessaire.

Solution

Relution Homescreen peut également être configuré comme une application dans la configuration Gérer les applications. L'inconvénient est que Relution Homescreen n'est pas sélectionné comme lanceur par défaut. Pour cela, il existe la configuration Activités préférées. Elle permet de changer le comportement par défaut d'Android dans certaines situations.

Deux configurations doivent donc être combinées dans une politique : Gérer les applications et Activités préférées.

Pour la version 26.4.0

Gérer les applications

Cette configuration garantit que l’application est présente sur l’appareil et correctement configurée.

- L’application Relution Homescreen (`io.relution.homescreen`) est ajoutée depuis le Google Play Store à la liste des applications via le bouton Ajouter (1).
- Le Type d’installation est défini sur Installé de force (2).
- Les paramètres souhaités pour la disposition et les fonctions de l’écran d’accueil peuvent être définis manuellement via le lien Configuration dans la colonne Actions (3).

Activités préférées

Tous les champs sont décrits dans l’article Activités préférées →.

1. Cliquer sur Ajouter dans la configuration et sélectionner Ajouter une application manuellement.

Pour la version 26.4.0

2. Entrer `Relution Homescreen` comme nom et `io.relution.homescreen` comme nom interne.

Pour la version 26.4.0

3. Remplir les paramètres exactement comme suit :
    - Activité :

```
io.relution.homescreen.MainActivity
```

- Catégories :

```
android.intent.category.DEFAULT
android.intent.category.HOME
```

- Actions :

```
android.intent.action.MAIN
```

Attribution

Une fois les deux configurations enregistrées dans la politique, celle-ci doit être assignée à un groupe d’appareils correspondant. Après la transmission de la politique aux appareils, Relution Homescreen est automatiquement activé comme lanceur par défaut.

Services de localisation

Relution permet de configurer les services de localisation pour les appareils Android Enterprise. L'administrateur peut spécifier les services de localisation de l'appareil et les autorisations de localisation pour les applications individuelles ou laisser l'utilisateur s'en charger.

Services de localisation

Via la configuration Mode de localisation →, les administrateurs définissent dans le champ Paramètre de localisation sur l'appareil si les utilisateurs peuvent activer ou désactiver les services de localisation. Pour ce faire, le champ doit être réglé sur Choix de l'utilisateur. Si aucune configuration n'est définie, Choix de l'utilisateur est la valeur par défaut.

Si les services de localisation sont désactivés, les applications ne pourront pas localiser l'appareil, quelles que soient les autorisations attribuées. Cela concerne toutes les applications, y compris Google Maps ou Waze, par exemple.

- L'option Activer le paramètre de localisation sur l'appareil active le paramètre de localisation sur l'appareil. À partir d'Android 11, les profils de travail sur les appareils appartenant à l'entreprise ne peuvent pas imposer directement les services de localisation ; dans ce cas, l'utilisateur doit activer manuellement les services de localisation dans les paramètres de l'appareil.
- L'option Désactivé désactive et interdit toute modification des paramètres de localisation.

Pour la version 26.4.0

Permissions par défaut de l'application

L'autorisation de localisation de l'agent de Relution et des applications compagnons dépend de ce qui est défini sous `Portail` → `Paramètres` → `Gestion des appareils` → `Inscription` à la ligne Localiser l'appareil. Si la localisation est désactivée pour COD, les deux applications n'obtiendront pas l'autorisation de suivre.

Companion depuis la version 5.18.0 du serveur, Agent depuis la version 5.19.3 du serveur

Permissions individuelles pour les applications

Cette valeur par défaut peut être modifiée individuellement en ajoutant une application à la configuration Gérer les applications. Si l'agent et/ou le compagnon est ajouté ici, les

autorisations de l'application peuvent être définies individuellement. Il est par exemple possible d'accorder à l'utilisateur le droit de définir lui-même toutes les autorisations de l'application.

> Companion depuis la version 5.18.0 du serveur, Agent depuis la version 5.19.3 du serveur

Sans autorisation pour l'Agent, par exemple, l'attribution de politiques en fonction des géofences et des iBeacons ne peut pas être utilisée. Sans autorisation pour le compagnon, l'action Localiser l'appareil ne peut pas être utilisée.

La réponse par défaut pour les demandes d'autorisation est définie comme suit : `Portail` → `la politique AE` → `Gérer les applications` → `Relution Companion for AE` (ajouter si absent) → `Permission` Une fenêtre contextuelle s'ouvrira ici avec l'élément Réponse par défaut pour les demandes d'autorisation.

> Si les services de localisation de Google ont été désactivés lors de la configuration de l'appareil, ils doivent être activés ultérieurement pour la localisation dans Relution Companion

Pour la version 26.4.0

Protection réinitialisation

Pour les appareils Android Enterprise, Relution propose dans les restrictions d'une politique deux paramètres liés à la réinitialisation d'usine. Ils fonctionnent indépendamment l'un de l'autre et peuvent être combinés :

- Le bouton Activer la protection contre la réinitialisation d'usine (FRP) bloque, sur les appareils gérés, la réinitialisation via les paramètres Android. Une réinitialisation via le menu de récupération reste possible.
- Le champ Courriel du compte Google pour le FRP permet d'enregistrer des comptes Google. Après une réinitialisation, une invitation à se connecter avec l'un de ces comptes s'affiche pendant le processus de configuration de l'appareil pour le rendre à nouveau opérationnel. Si aucun compte n'est saisi, la FRP n'est pas active.

Configurer FRP

1. Naviguer vers l'élément de menu `Appareils` → `Politiques` dans le portail Relution et cliquer sur Ajouter.
2. Créer une politique Android Enterprise et lui attribuer un nom, puis cliquer sur Enregistrer.
3. Après avoir cliqué sur Ajouter, sélectionner l'option Restrictions et continuer avec Ajouter des détails.
4. En option, activer le bouton Activer la protection contre la réinitialisation d'usine (FRP) pour bloquer la réinitialisation via les paramètres Android. Une réinitialisation via le menu de récupération reste possible.
5. En option, saisir un ou plusieurs comptes Google dans le champ Courriel du compte Google pour le FRP. Après une réinitialisation, l'un de ces comptes doit se connecter pour déverrouiller l'appareil. Si le champ reste vide, la FRP n'est pas active.
6. Enregistrer la configuration et publier la version actuelle de la politique
7. Pour appliquer la politique aux appareils Android Enterprise, ajouter les appareils souhaités via l'onglet Appareils avec cette stratégie. Les paramètres sélectionnés sont alors automatiquement appliqués aux appareils.

Pour la version 26.4.0

Afficher le portail captif

Pour établir une connexion avec un WLAN, un nom de paquet doit être activé pour Android Enterprise. Il s'agit de `com.android.captiveportallogin` et doit être ajouté manuellement comme Disponible dans la configuration Gérer les applications. L'ajout s'effectue via Ajouter avec la source Ajouter une application manuellement, le nom de paquet étant saisi dans le champ Nom interne. Les applications ajoutées manuellement reçoivent d'abord le type d'installation Installé de force ; la valeur de la colonne Type d'installation est donc ensuite définie sur Disponible.

Il est alors possible d'établir une connexion avec un Wifi qui affiche un portail captif.

Pour la version 26.4.0

Les appels ne s'affichent pas

En mode Kiosque/Homescreen Layout, Android Enterprise n’affiche pas les appels entrants et sortants : l’appareil sonne ou vibre bien, mais aucun overlay d’appel n’apparaît à l’écran. Ceci est dû au fait que, dans ce mode, Android bloque par défaut toutes les applications et overlays qui n’ont pas été explicitement autorisés dans la politique – l’interface d’appel est contrôlée par des paquets système spécifiques à chaque fabricant, qui doivent figurer dans la liste blanche. Les modifications de politique suivantes résolvent ce problème :

Adapter les paramètres de la politique

Pour que la fenêtre d’appel puisse techniquement agir comme un overlay système et s’afficher, il faut utiliser le mode Kiosque à la place du Homescreen Layout.

De plus, les paramètres suivants doivent impérativement être définis dans la configuration Mode kiosque :

- Désactiver les toasts et les superpositions (section Général) : Doit être désactivé (afin que les overlays soient autorisés).
- Barre d’état (section Personnalisation du kiosque) : Doit être définie sur Activé (car la bannière d’appel s’affiche techniquement comme une notification système).

Pour la version 26.4.0

Si le mode Kiosque natif n’est pas suffisamment flexible pour le cas d’usage, un lanceur alternatif tel que le Microsoft Managed Homescreen peut être intégré via l’option Utiliser une application de lancement de kiosque personnalisée au lieu du lanceur par défaut. Celui-ci offre des possibilités de configuration plus étendues pour les scénarios complexes.

> Lors de l’utilisation du Relution Homescreen – aussi bien dans la configuration Kiosque que dans la configuration Layout – ces overlays système ne peuvent pas être imposés et aucun son de notification ne peut être lu, pour des raisons techniques.

Si le Relution Homescreen doit être utilisé, il doit être configuré via Activités préférées →.

Autoriser les noms de paquets requis selon le fabricant

Les applications système nécessaires à la fonction de téléphonie doivent être renseignées avec leur nom de paquet exact dans la configuration Gérer les applications avec la valeur Disponible dans la colonne Type d’installation.

Appareils Samsung

- `com.samsung.android.incallui` — Responsable de la fenêtre d'appel visuelle et du contrôle pendant l'appel.
- `com.android.systemui` — Autorise les notifications head-up (bannière d'appel) lorsque l'écran est actif.
- `com.samsung.android.dialer` — L'application Téléphone Samsung proprement dite (clavier de numérotation).
- `com.samsung.android.smartcall` — Identification de l'appelant Samsung et protection anti-spam au niveau système.

Appareils Google Pixel

- `com.google.android.dialer` — L'application Téléphone Google, incluant l'interface InCall native intégrée.
- `com.android.systemui` — Contrôle la barre de notification et l'affichage de la bannière d'appel supérieure.
- `com.google.android.as` — Android System Intelligence (nécessaire pour le traitement des appels assisté par IA sur les appareils Pixel).

Sons de notification

Pour la version 26.4.0

Outre l'interface d'appel, la lecture des sons de notification dépend également du lanceur utilisé.

Avec les autres lanceurs, les sons de notification sont lus à condition que le paquet `com.android.systemui` soit défini sur Disponible dans la colonne Type d'installation de la configuration Gérer les applications :

- Mode kiosque natif (lanceur par défaut de la configuration Android Enterprise)
- Microsoft Managed Homescreen (via l'option Utiliser une application de lancement de kiosque personnalisée au lieu du lanceur par défaut)

Transfert de fichiers via USB

Le transfert de données/photos via USB n'est plus disponible sur les appareils Android, l'élément de menu correspondant n'apparaît plus sur l'appareil. Ceci est dû au fait que Google ne prend plus en compte un champ de l'API qui régit l'accès USB – la fonction est depuis désactivée par défaut.

Restaurer la fonction

À partir de la version 5.22.4, Relution intègre côté serveur, pour les appareils entièrement gérés et les appareils gérés avec profil personnel (COPE), une nouvelle valeur par défaut qui réactive la fonction :

1. Mettre à jour Relution vers la version 5.22.4 minimum (voir Changelog →).
2. Vérifier la politique, car la valeur par défaut ne s'applique que si la politique ne régit pas elle-même le transfert de fichiers USB :
   - Dans la configuration Restrictions, l'option Désactiver le transfert de fichiers USB ne doit pas être activée (voir Restrictions →).
   - Si la politique contient une configuration Connectivité des appareils → (à partir de Relution 5.24.0), son paramètre Accès aux données par USB s'applique à la place de la valeur par défaut. L'option Autoriser le transfert de données par USB doit y être sélectionnée. Avec la présélection Non spécifié, le transfert de fichiers par USB reste bloqué.
3. Réappliquer les politiques sur les appareils concernés : sous `Appareils` → `Inventaire`, appliquer un filtre sur tous les appareils Android, tout sélectionner, puis réappliquer les politiques via le menu à trois points.

Pour la version 26.4.0

Inscription manuelle

Pour pouvoir gérer les appareils dans Relution, ils doivent être enregistrés. Pour cela, l'administrateur crée une inscription (enregistrement), qui doit ensuite être effectuée sur l'appareil. La création d'une inscription dans Relution est la même pour toutes les plateformes. Le processus d'inscription ultérieur sur les appareils est spécifique à la plateforme `Android Classic / Legacy`.

> À partir du 1er janvier 2025, Relution ne prend en charge qu'Android 10 et les versions ultérieures pour Android Enterprise et Android Classic / Legacy. La prise en charge des versions antérieures d'Android a été interrompue.

> Relution cesse la prise en charge des appareils Samsung équipés d'Android 15+ lorsqu'ils sont gérés via Android Classic. Il est recommandé de passer à Android Enterprise.
>
> Les appareils Samsung équipés d'Android 15 peuvent toujours être gérés via Android Classic. Cependant, les fonctions de base telles que l'installation ou la mise à jour d'applications natives ne seront plus disponibles. Avec Android 16, le mode KIOSK sera également supprimé par Samsung.

Pour la version 26.4.0

Pré-requis pour les inscriptions

- Pour créer des inscriptions, les utilisateurs doivent être assignés au groupe d'utilisateurs `Administrator` ou `Device Manager` de l'organisation.
- Pour effectuer l'inscription sur les appareils, les utilisateurs finals doivent être assignés au moins au groupe d'utilisateurs `User` de l'organisation.
- Les inscriptions sont créées dans l'organisation dans laquelle l'appareil doit être géré. Il n'est pas possible d'inscrire des appareils dans l'organisation globale.
- Connaissances de base sur le type d'inscription utilisé pour chaque plateforme Android : `Android Classic / Legacy` à distinguer de `Android Enterprise`.

Créer des inscriptions manuelles

1. Naviguer vers `Appareils` → `Inventaire` et cliquer sur le bouton d'inscription d'un appareil (libellé S'inscrire dans le portail), ou sur Ajouter sous `Appareils` →

`Inscriptions`.

2. Sélectionner Android comme Plateforme ainsi que la Propriété, par exemple COD - Company Owned Device. Sous Type, Android reste sélectionné. Les autres types sont prévus pour l'inscription d'écrans interactifs, voir Whiteboards →.
3. Cliquer sur Enregistrer pour créer l'inscription.

Facultatif

- Nom de l'appareil et Description de l'appareil : l'appareil et l'inscription seront nommés. La description est affichée avec l'appareil dans l'inventaire. Les deux champs peuvent contenir des espaces réservés utilisateur comme `${user.givenName}`, qui sont remplacés lors de l'inscription à partir de l'utilisateur attribué, voir Espaces réservés avancés →.
- Utilisateur : les utilisateurs Relution peuvent être attribués à des appareils, par exemple pour un équipement 1:1. Un seul utilisateur peut être assigné à un appareil à la fois.
- Groupes d'appareils statiques : après l'inscription, l'appareil est ajouté aux groupes d'appareils → sélectionnés. Les politiques attribuées à ces groupes sont ensuite appliquées à l'appareil. Ce champ n'est visible qu'avec l'autorisation de modifier les groupes d'appareils.
- Inscription à usages multiples : si cette option est activée, plusieurs appareils peuvent être inscrits avec une seule inscription.
- Valable jusqu'au : date après laquelle l'inscription ne peut plus être utilisée. La fin du septième jour suivant la création est préréglée, et la date peut être modifiée selon les besoins. Si le champ reste vide, l'inscription n'expire pas.
- Propriétés personnalisées de l'appareil : champs personnalisables pour des informations supplémentaires.
- Notification : permet de choisir si l'utilisateur doit être informé de l'inscription par courriel ou par SMS. Cette section ne s'affiche que si la notification par courriel ou par SMS est activée sous `Paramètres` → `Notifications`. Le courriel nécessite un utilisateur attribué disposant d'une adresse électronique. Le SMS nécessite un Numéro de téléphone ; si un numéro est enregistré pour l'utilisateur attribué, il est repris automatiquement.

Pour la version 26.4.0

Pour la version 26.4.0

Notes supplémentaires

- Si aucun nom d’appareil n’a été spécifié, le nom de l’appareil est formé à partir du fabricant et du modèle après l’inscription réussie de l’appareil.

- Après l'enregistrement, la vue détaillée de l'inscription affiche le Code d'inscription et le Lien de l'inscription. Les deux peuvent être copiés dans le presse-papiers, par exemple pour transmettre l'inscription sans notification.
- Par défaut, le Code d'inscription comporte 16 caractères (depuis Relution 26.5.2, auparavant 6). La longueur peut être fixée entre 12 et 32 caractères à l'aide de la propriété de configuration globale suivante (nécessite le redémarrage de l'instance) ; les valeurs en dehors de cette plage sont ramenées à la limite correspondante :

```
relution:
  enrollment:
    passcodeLength: 24
```

Effectuer un enrôlement manuel

Les étapes suivantes doivent être effectuées par l'utilisateur de l'appareil Android. En fonction de l'option de notification sélectionnée, l'utilisateur de l'appareil sera notifié par email ou par SMS. Si l'utilisateur de l'appareil est également membre du groupe d'utilisateurs `Device Manager`, le code QR pour l'inscription peut également être scanné directement dans l'organisation. Le code QR s'affiche en cliquant sur l'icône de la colonne Code QR sous `Appareils` → `Inscriptions` (il figure également dans la vue détaillée de l'inscription). Il s'agit généralement de la méthode préférée pour l'inscription d'un appareil Android.

Pour la version 26.4.0

Ensuite les étapes suivantes doivent être exécutées :

1. Il faut s’assurer que l’appareil Android est connecté à l’Internet (WiFi ou réseau mobile).
2. Ouvrir le lien d’inscription :
    - Par courriel : il faut ouvrir l’e-mail sur l’appareil Android et cliquer sur le lien, ou ouvrir l’e-mail sur un autre appareil et scanner le code QR avec l’appareil Android.
    - Par SMS : il faut cliquer sur le lien contenu dans le SMS.
    - Si aucun des deux n’a été reçu : il faut saisir manuellement l’URL de l’inscription dans le navigateur ou contacter l’administrateur compétent.

Pour la version 26.4.0

Pour la version 26.4.0

3. Sur le navigateur de l’appareil Android, cet écran de bienvenue devrait s’afficher. Pour continuer, appuyer sur `Suivant`.

Pour la version 26.4.0

Pour la version 26.4.0

4. Il sera alors demandé de télécharger et d'installer le `Relution Companion` pour Android (également disponible sous forme de *.apk sur notre serveur). Relution Companion APK →

   Une fois l'installation achevée, il faut revenir au navigateur pour continuer à se connecter. Si l'installation échoue, l'installation d'applications de sources inconnues n'est pas autorisée sur l'appareil Android. À partir d'Android 8, cette autorisation est accordée par application, à savoir pour l'application utilisée pour télécharger l'application Relution, par exemple le navigateur (Installer des applis inconnues, selon le fabricant sous `Paramètres` → `Applications` → `Accès spécifiques des applications`). Jusqu'à Android 7, le paramètre se trouve sous `Paramètres` → `Sécurité` → `Sources inconnues`.

Pour la version 26.4.0

Pour la version 26.4.0

5. Appuyer sur le bouton Démarrer l’inscription pour ouvrir le `Relution Companion` pour Android.

Pour la version 26.4.0

Pour la version 26.4.0

6. Accepter l’accord de licence et appuyer sur Get started (le libellé dépend de la langue de l’appareil).

Pour la version 26.4.0

Pour la version 26.4.0

7. L’écran des préférences de confidentialité détermine quelles données facultatives le `Relution Companion` peut transmettre, par exemple les rapports de plantage automatiques. Le choix est enregistré par le bouton d’enregistrement et peut être révoqué ultérieurement dans les paramètres de l’application.

Pour la version 26.4.0

Pour la version 26.4.0

8. Ensuite, il est possible de donner l’autorisation de localiser l’appareil. Si cette autorisation n’est pas accordée, l’administrateur ne pourra pas localiser l’appareil Android en cas de vol ou de perte.

9. Il est également possible d’autoriser Relution à lire l’état de l’appareil pour partager le numéro de téléphone et l’IMEI avec l’administrateur. Ces informations sont transmises de manière cryptée et ne sont jamais partagées avec des tiers.

Pour la version 26.4.0

Pour la version 26.4.0

10. Il sera ensuite demandé d’accorder des droits d’administration à Relution. Cela est nécessaire pour s’assurer que l’appareil Android est conforme aux exigences de l’organisation, telles que les politiques de mot de passe. Si l’option Retirer les anciens appareils Android si l’autorisation de l’administrateur de l’appareil n’est pas accordée est activée sous `Paramètres` → `Gestion des appareils`, la gestion de l’appareil est supprimée lorsque l’autorisation n’est pas accordée ou est révoquée ultérieurement.

Pour la version 26.4.0

Pour la version 26.4.0

11. Il faut appuyer sur Activer pour accorder les autorisations administratives. Selon le fabricant et la version Android de l’appareil, la présentation de l’écran peut différer de la capture d’écran ci-dessus.

Pour la version 26.4.0

Pour la version 26.4.0

12. Sur les appareils Samsung, une boîte de dialogue d’activation de la licence Knox s’affiche également, avec un renvoi à la politique de confidentialité de Samsung Knox. Cette boîte de dialogue doit également être confirmée par Continuer.

Pour la version 26.4.0

Pour la version 26.4.0

13. L’appareil Android va maintenant terminer le processus d’inscription et s’afficher dans l’inventaire des appareils de l’organisation Relution appropriée pour la gestion.

Pour la version 26.4.0

Vue générale

Relution fournit une sélection d'actions pour contrôler et diriger directement les appareils Android Legacy / Classic. L'avantage principal est que ces actions peuvent être appliquées spécifiquement à des appareils individuels.

Une partie de ces actions est également disponible pour les tableaux blancs Android Classic. Les actions proposées dépendent du fabricant et sont indiquées sur la page du fabricant → correspondante. Par exemple, Ajouter un raccourci, Supprimer le raccourci et Localiser l'appareil ne sont disponibles que sur quelques tableaux blancs, et Réinitialiser le code de verrouillage sur aucun. Les actions développées spécifiquement pour les tableaux blancs interactifs se trouvent sous Actions (Tableaux Blancs) →.

Actions disponibles

on 26.4.0

Action	Description
Alerte →	Déclenche une alarme sur l'appareil, même s'il est en mode silencieux
Installer l'application à partir du magasin d'applications Prowise →	Sélectionner une application depuis le Prowise App Store pour l'installer (tableaux blancs Prowise uniquement)
Supprimer l'application →	Désinstalle une application de l'appareil
Envoyer un fichier à l'appareil →	Télécharger un fichier dans un répertoire de l'appareil
Effacer l'appareil →	Réinitialise l'appareil à son état d'usine et efface toutes les données de l'appareil
Redémarrer l'appareil →	Redémarre l'appareil
Localiser l'appareil	Demande la position actuelle de l'appareil. Peut échouer si l'autorisation de localisation n'a pas été accordée sur l'appareil

Action	Description
Verrouiller complètement l'appareil →	L'appareil sera verrouillé avec le mot de passe actuellement défini. Si aucun mot de passe n'est défini, l'appareil pourra être déverrouillé sans mot de passe
Actualiser les informations sur l'appareil →	Met à jour toutes les informations disponibles sur l'appareil, listées dans l'onglet Informations
Envoyer un message →	Affiche un message texte sur l'appareil
Réinitialiser le code de verrouillage	Définit un nouveau mot de passe de l'appareil. Disponible uniquement jusqu'à Android 10 ; sous Android 7 à 10, uniquement si aucun mot de passe n'est actuellement défini sur l'appareil
Installer la mise à jour de Prowise →	Installe la dernière mise à jour du firmware Prowise (tableaux blancs Prowise uniquement)
Déployer l'application Relution Store →	Rechercher une application dans le Relution Store et la distribuer aux appareils
Supprimer le raccourci →	Supprime un raccourci de l'écran d'accueil
Ajouter un raccourci →	Ajoute un raccourci vers un site web sur l'écran d'accueil
Installer une mise à jour →	Installe une mise à jour souhaitée sur l'appareil sélectionné

Déclencher une alarme

L'action Alerte déclenche une alarme sur l'appareil sélectionné, même si l'appareil est réglé en mode silencieux. Cela permet par exemple de localiser plus facilement l'appareil dans une pièce. Le paramètre Durée (en secondes) permet de définir la durée de l'alarme ; par défaut, elle est réglée sur 30 secondes, au maximum 60 secondes.

L'action peut également être déclenchée via des groupes d'appareils, en fonction d'un événement ou selon une planification : Actions de groupes d'appareils →

Supprimer l'application

L’action Supprimer l’application désinstalle une application sélectionnée de l’appareil. L’application peut être choisie parmi quatre sources : Appli Relution App Store, Appli Google Play Store, App installée ou Nom interne d’une application (saisie du nom de package). Plusieurs applications peuvent être sélectionnées simultanément dans les listes.

La liste App installée ne contient que les applications que l’appareil a signalées comme installées lors de sa dernière communication ; les applications système, l’application Relution et les applications en cours d’installation y sont masquées. Si plusieurs appareils sont sélectionnés, seules les applications installées sur tous ces appareils sont affichées.

Si une désinstallation immédiate n’est pas possible, l’utilisateur est à nouveau invité à supprimer l’application toutes les 1440 minutes (une fois par jour).

Il est également possible de supprimer des applications dans les détails de l’appareil, onglet Apps installées, via Désinstaller.

Pour la version 26.4.0

Envoyer un fichier à l'appareil

L’action Envoyer un fichier à l’appareil télécharge un fichier sélectionné dans un répertoire de l’appareil. Le répertoire cible est indiqué par rapport au stockage externe de l’appareil (`/sdcard/`) ; la valeur par défaut est `Download/`. Les archives ZIP sont automatiquement décompressées, sauf si l’option désactivant la décompression des archives ZIP est activée – les fichiers APK, JAR et OBB, en revanche, ne sont jamais décompressés automatiquement. Depuis Android 6.0, la réception du fichier doit en outre être confirmée sur l’appareil.

L’action peut également être déclenchée via des groupes d’appareils, en fonction d’un événement ou selon une planification : Actions de groupes d’appareils →

Effacer l'appareil

L’action Effacer l’appareil réinitialise l’appareil à son état d’usine et efface toutes les données de l’appareil.

L’action est sélectionnée dans les détails d’un appareil sous `Appareils` → `Inventaire`, dans l’onglet `Actions`, via Appliquer l’action. Avant l’exécution, la boîte de dialogue signale que tous les contenus enregistrés sont supprimés définitivement et ne peuvent pas être restaurés après la réinitialisation. Pour les appareils Android Classic, la boîte de dialogue ne propose aucune autre option.

Prérequis

L’action doit être activée sous `Paramètres` → `Gestion des appareils` → `Inscription`, dans la ligne Effacer l’appareil, pour la propriété de l’appareil (COD ou BYOD). Par défaut, elle est activée pour COD et désactivée pour BYOD. Pour les appareils dont la propriété est inconnue, elle est toujours disponible ; ce paramètre ne peut pas être modifié dans le portail. Si l’action est désactivée pour la propriété, Relution ne la propose pas.

L’action n’est pas disponible pour les tableaux blancs Prowise et SMART.

Pour la version 26.4.0

Statut et annulation

Les appareils Android Classic confirment uniquement la réception de l’action. Relution définit donc le statut sur Exécuté dès la remise de l’action ; cela n’indique pas si l’appareil a effectivement été réinitialisé. Une fois créée, l’action ne peut pas être annulée.

Redémarrer l'appareil

L’action Redémarrer l’appareil redémarre l’appareil ou l’éteint. Dans le portail, l’action est signalée par le badge Tableau blanc interactif pour les appareils Android Classic.

L’action est sélectionnée dans les détails d’un appareil sous `Appareils` → `Inventaire`, dans l’onglet `Actions`, via Appliquer l’action. Les options suivantes sont disponibles à l’étape suivante :

- Motif du redémarrage : indication facultative de la raison du redémarrage.
- Mise hors tension (également signalée par le badge Tableau blanc interactif) : l’appareil est éteint au lieu d’être redémarré.

Pour les appareils KION et Newline, ni le motif ni l’option Mise hors tension ne sont disponibles.

Pour la version 26.4.0

Verrouiller complètement l'appareil

L’action Verrouiller complètement l’appareil (Dispositif de verrouillage dans le portail) verrouille l’appareil avec le mot de passe actuellement défini. Si aucun mot de passe n’est défini, l’appareil peut être déverrouillé sans mot de passe.

Pour les appareils Android Classic, il s’agit de la seule action de verrouillage. Aucune autre saisie n’est nécessaire lors de l’envoi.

Tableaux blancs

Sur les tableaux blancs ADVANTouch, CTOUCH, i3-Technologies, Newline, Promethean, Prowise et VS, un mot de passe ou un code PIN doit être défini avant le verrouillage, soit localement sur l’appareil, soit, si disponible, via la configuration.

L’action n’est pas disponible sur les tableaux blancs Clevertouch, heinekingmedia, SMART et ViewSonic.

Pour la version 26.4.0

Déverrouillage

Une action de déverrouillage n’existe que pour les tableaux blancs CTOUCH, i3-Technologies et Newline, voir Déverrouiller l’appareil →. Tous les autres appareils sont déverrouillés directement sur l’appareil avec le mot de passe.

À partir d’Android 7, un mot de passe inconnu ne peut pas non plus être remplacé via l’action Réinitialiser le code de verrouillage : sous Android 7 à 10, elle ne définit un nouveau mot de passe que si aucun mot de passe n’est actuellement défini sur l’appareil ; à partir d’Android 11, elle n’est plus disponible.

Disponibilité selon le type de propriété

L’action n’est proposée que si elle est activée sous `Paramètres` → `Gestion des appareils` → `Inscription` à la ligne Dispositif de verrouillage pour le type de propriété de l’appareil (COD ou BYOD). Par défaut, elle est activée pour les deux.

Actualiser les informations sur l'appareil

L’action Actualiser les informations sur l’appareil actualise toutes les informations disponibles sur l’appareil, affichées dans l’onglet Informations des détails de l’appareil.

Dans les détails d’un appareil sous `Appareils` → `Inventaire`, l’action est déclenchée directement via l’icône Actualiser les informations sur l’appareil dans l’en-tête ; aucune boîte de dialogue ne s’ouvre. Elle est également disponible dans l’onglet `Actions` sous Appliquer l’action.

Relution envoie l’action au Relution Companion sur l’appareil par notification push. Si la remise par push n’est pas possible, l’action reste au statut En attente jusqu’à ce que l’appareil la récupère lui-même lors de sa prochaine connexion. Les informations affichées ne sont actualisées qu’une fois que l’appareil a répondu.

Envoyer un message

Pour la version 26.4.0

L’action Envoyer un message affiche un message texte sur l’appareil. Le titre et le texte du message (Contenu) sont tous deux obligatoires.

Sur les smartphones et tablettes, le message est transmis à l’application Relution par notification push. Si l’envoi réussit, l’action passe directement au statut Exécuté et reçoit en commentaire le titre et le contenu du message transmis. Ce statut confirme la transmission, et non la lecture du message sur l’appareil. Si l’envoi push échoue, l’action reste En attente jusqu’à ce que l’appareil la récupère lui-même. Les écrans interactifs (tableaux blancs) ne reçoivent pas le message par push via l’application Relution, mais, comme les autres actions, via le canal de l’appareil.

Par défaut, les actions de message terminées sont automatiquement supprimées de l’historique des actions au bout de 10 jours.

Déployer une application du Relution Store

L'action Déployer l'application Relution Store permet de rechercher une application dans le Relution Store et de la distribuer à l'appareil. Seules les applications Android natives du Relution Store sont proposées ; une seule application est sélectionnée par action et distribuée dans sa version publiée. L'installation depuis des sources inconnues doit être activée sur l'appareil pour cela.

La boîte de dialogue propose deux options, toutes deux activées par défaut :

- Déployer le mode silencieux si possible : l'installation est tentée en arrière-plan. Si celle-ci n'aboutit pas automatiquement, l'utilisateur est invité sur l'appareil à installer l'application.
- Supprimer l'application sur Enterprise Wipe : l'application est à nouveau supprimée de l'appareil lors d'un Enterprise Wipe.

L'action n'est pas disponible pour les tableaux blancs interactifs Prowise ; les applications y sont installées via Installer l'application à partir du magasin d'applications Prowise →.

Pour la version 26.4.0

Ajouter un raccourci

L'action Ajouter un raccourci ajoute un raccourci vers un site web sur l'écran d'accueil de l'appareil. Les champs obligatoires sont Label (libellé du raccourci) et URL (URL cible valide). Une image personnalisée au format JPEG ou PNG d'une taille maximale de 1 Mo peut être définie de manière facultative via Icône.

Le libellé et l'URL sont également nécessaires pour supprimer ultérieurement le raccourci via l'action Supprimer le raccourci →.

L'action est disponible pour les appareils Android Classic ; parmi les tableaux blancs interactifs, uniquement pour Promethean → et wende.interaktiv → (Wende 8 et Wende 9).

Supprimer le raccourci

L’action Supprimer le raccourci supprime un raccourci de l’écran d’accueil de l’appareil. Le raccourci à supprimer est indiqué à l’aide des champs obligatoires Label et URL ; il n’existe pas de liste de sélection des raccourcis existants. Les valeurs à saisir sont celles avec lesquelles le raccourci a été créé via l’action Ajouter un raccourci →.

L’action est disponible pour les appareils Android Classic ; parmi les tableaux blancs interactifs, uniquement pour Promethean →.

Pour la version 26.4.0

Vue d'ensemble

Une politique est un ensemble d’une ou plusieurs configurations. Chaque politique peut être appliquée à un ou plusieurs appareils en même temps. En outre, une ou plusieurs politiques peuvent être associées à chaque appareil.

Configurations Disponibles

Configuration	Description
ADVANTouch →	Gérer les tableaux blancs interactifs ADVANTouch
Conformité des applications →	Gestion des restrictions spécifiques aux applications
Clevertouch →	Gérer les tableaux blancs interactifs Clevertouch
CTOUCH →	Gérer les tableaux blancs interactifs CTOUCH
Dahua →	Gérer les tableaux blancs interactifs Dahua
EShare →	Configurer l’application EShare
Exchange	Gestion des comptes Exchange
Mise à jour OTA prévue →	Installer à heures fixes les mises à jour du micrologiciel des tableaux blancs Clevertouch, i3 et Newline
Fond d’écran →	Définir le fond d’écran
Hotspot →	Gérer la configuration du hotspot
i3 →	Gérer les tableaux blancs interactifs i3
Configuration du Tableau Blanc Interactif	Gérer les restrictions pour les tableaux blancs interactifs
Mode kiosque →	Paramètres du mode kiosque

Configuration	Description
Configuration du nom du point d’accès	Gérer un nom de point d’accès
Newline	Gérer les tableaux blancs interactifs Newline
Code d’accès	Gestion des politiques de mot de passe pour les appareils Android
Promethean →	Gérer les paramètres Promethean
Restrictions →	Gestion des restrictions de l’appareil
Restrictions du réseau	Gestion des restrictions Wi-Fi
SMART →	Gérer les tableaux blancs interactifs SMART
VPN	Gestion des paramètres VPN
ViewSonic →	Gérer les tableaux blancs interactifs ViewSonic
VS →	Gérer les tableaux blancs interactifs VS
Wi-Fi →	Gestion des paramètres Wi-Fi
Certificat →	Sélectionner un certificat à installer par défaut sur l’appareil

Fond d'écran

À partir de Relution 5.33, la configuration Fond d’écran (Papier peint dans le portail) est disponible pour Android Enterprise et Android Classic/Legacy. Cela permet de définir une image pour l’écran d’accueil qui apparaît sur les appareils après l’application de la politique. La politique permet également d’ajouter du texte (y compris des espaces réservés) pour afficher du texte dynamique sur le fond d’écran.

> Android Enterprise nécessite Relution Companion version 1.18.
>
> Android Classic nécessite Relution Companion version 5.37.

La configuration de fond d’écran définit l’image, mais n’empêche pas les utilisateurs de la modifier sur l’appareil.

Configuration

La section Général contient les champs suivants :

- Texte sur papier peint – texte facultatif placé sur l’image. Les espaces réservés sont résolus par appareil ; les espaces réservés pris en charge sont listés dans le formulaire sous les champs de saisie.
- Couleur du texte – code couleur hexadécimal, par ex. `#ffffff` (par défaut), au choix via le sélecteur de couleur.
- Papier peint – l’image elle-même (champ obligatoire). La taille maximale du fichier est de 3 Mo par défaut ; sur les serveurs auto-hébergés, elle peut être adaptée via le paramètre `relution.wallpaper.max-file-size.android`. Si l’image est plus grande, le portail affiche un message d’erreur et la configuration ne peut pas être enregistrée.

Pour la version 26.4.0

Conformité des applications

Android Classic / Legacy permet de télécharger des Native Apps en tant que fichiers `.apk` dans l'App Store de Relution et de les distribuer aux appareils Android inscrits via une action ou une politique. La distribution via une action est décrite sous Déployer une application du Relution Store →.

> Les applications Google Play ne peuvent pas être installées automatiquement dans Android Classic. Les applications du Google Play Store saisies sous Apps requises doivent être installées par l'utilisateur ; l'option Installation automatique n'est disponible que pour les applications natives de l'App Store de Relution. Pour une distribution gérée des applications Google Play, il convient d'utiliser Android Enterprise (Managed Google Play).

Apk native via une politique

Cette variante ne fournit pas de mise à jour automatique pour les nouvelles versions d'applications.

Tout d'abord, l'application est déployée dans l'App Store de Relution, puis distribuée via une politique avec la configuration Conformité App.

Pour la version 26.4.0

> Une seule politique avec la configuration Conformité App peut être appliquée par appareil. Si une autre configuration de ce type est attribuée à un appareil, elle est ignorée et n'est pas appliquée.

1. Dans le portail Relution, naviguer vers l'élément de menu `Apps` → `App Store` et cliquer sur Ajouter.
2. Sélectionner ensuite l'option Appli native et cliquer sur Suivant.
3. Dans le champ de sélection de fichier, sélectionner le fichier `.apk` souhaité.
4. Sur la page suivante, le statut de publication de l'application doit être changé de Développement (icône bleue) à Production (icône verte, affiché dans le portail sous le libellé « Version »). Cliquer sur Enregistrer.
5. Ensuite, naviguer vers `Appareils` → `Politiques` dans le menu et cliquer sur Ajouter. Créer une politique Android et lui donner un nom. Cliquer sur Enregistrer.
6. Après avoir cliqué sur Ajouter, sélectionner l'option Conformité App et continuer avec Ajouter des détails.
7. Le Type de liste est présélectionné par défaut sur Liste de blocage — Les applications ci-dessous ne sont pas autorisées. Indépendamment de cela, ajouter les applications

souhaitées de l'App Store de Relution sous Apps requises.
8. Enregistrer la configuration et publier la version actuelle de la politique.
9. Pour appliquer la politique aux appareils Android, ajouter les appareils souhaités via l'onglet Appareils avec cette stratégie. Les appareils sont alors affectés à un groupe d'appareils statique existant disposant de cette politique ou à un nouveau groupe d'appareils statique. Les paramètres et applications sélectionnés sont alors automatiquement appliqués ou installés sur les appareils.

Lorsque l'option Installation automatique est cochée, les applications concernées sont installées automatiquement sur les appareils Android. Pour installer les applications, les appareils doivent être attribués à des utilisateurs qui sont membres du groupe d'utilisateurs AppStore User.

Paramètres de la configuration

La configuration Conformité App est divisée en trois sections.

Général

Pour la version 26.4.0

- Appliquer le bloc/liste d'autorisation uniquement en itinérance – la liste de blocage ou d'autorisation n'est appliquée que lorsque l'appareil est en itinérance. Si l'option est désactivée, la liste s'applique indépendamment de l'état d'itinérance.
- Ignorer la liste des blocs/listes d'autorisation sur un réseau sans fil – disponible uniquement si l'option précédente est activée. Lorsque l'appareil est connecté en Wi-Fi, les applications sont autorisées même en itinérance.
- Type de liste – Liste de blocage — Les applications ci-dessous ne sont pas autorisées (par défaut) ou Liste d'autorisation : les applications ci-dessous sont autorisées.

Pour une liste d'autorisation, Apps non autorisées définit le traitement de toutes les autres applications :

- Désinstaller – l'utilisateur est invité à désinstaller l'application de son appareil. L'option n'est pas disponible si Appliquer le bloc/liste d'autorisation uniquement en itinérance est activé.
- Désactiver – l'application reste installée, mais l'utilisateur ne peut plus la lancer.
- Bloquer l'accès Internet – retire l'accès Internet à l'application. L'option est sans effet sur les applications préinstallées et certaines applications peuvent planter ; dans ce cas, Désactiver est préférable.

Applications bloquées ou autorisées

Selon le Type de liste, la section s'intitule Apps bloquées ou Apps autorisées. Les applications peuvent être ajoutées depuis l'App Store de Relution, depuis le Google Play Store ou manuellement via leur nom de package.

L'option Désactiver les applications système tente de bloquer toutes les applications système et préinstallées. Cela inclut l'application Téléphone, de sorte que les appels d'urgence ne sont plus possibles. Si la téléphonie est nécessaire, l'application Téléphone doit être placée sur la liste d'autorisation.

Apps requises

Les applications saisies ici doivent être installées sur l'appareil, sinon l'appareil est considéré comme non conforme. Les applications du Google Play Store doivent être installées par l'utilisateur ; l'Installation automatique n'est possible que pour les applications natives de l'App Store de Relution.

La configuration est refusée lors de l'enregistrement si

- une application figure à la fois sur la liste de blocage et sous Apps requises, ou
- un lien Web est saisi comme application requise.

Pour la version 26.4.0

Restrictions

La restriction ciblée des fonctionnalités de l'appareil et des applications augmente la sécurité lors de l'utilisation d'appareils Android et peut optimiser l'utilisation de l'appareil en le ciblant davantage. Le contrôle des paramètres de l'appareil et la restriction de l'accès empêchent également les applications tierces d'accéder aux données et aux ressources de l'entreprise. La disponibilité des restrictions peut varier en fonction du fabricant de l'appareil et de la version existante du système d'exploitation. Une partie des restrictions n'est disponible que sur les appareils Samsung Knox (groupe Restrictions spécifiques à Knox).

Appliquer des restrictions aux appareils Android

1. Dans le portail Relution, naviguer vers `Appareils` → `Politiques` et cliquer sur Ajouter.
2. Créer une politique Android et attribuer un nom. Cliquer sur Enregistrer.
3. Après avoir cliqué sur Ajouter, sélectionner l'option Les restrictions et passer à Ajouter des détails.
4. Enregistrer la configuration après avoir sélectionné les options souhaitées et publier la version actuelle de la politique.

   Si Appliquer le chiffrement des appareils ou Appliquer le cryptage de la carte SD est activé, la politique doit également contenir une configuration Code d'accès activée. Sinon, la version ne peut être ni publiée ni testée. Pour un chiffrement efficace, une qualité de code d'accès devrait en outre être définie dans la configuration du code d'accès.
5. Pour appliquer la politique aux appareils Android, ajouter les appareils souhaités en utilisant l'onglet Appareils avec cette stratégie. Les appareils sont alors affectés à un groupe d'appareils statique existant disposant de cette politique ou à un nouveau groupe d'appareils statique. Les restrictions sélectionnées sont ensuite automatiquement appliquées sur les appareils.

> De nombreuses options dans les restrictions offrent des explications et des informations étendues via un survol de la souris. Les options réservées aux appareils Samsung Knox sont regroupées dans la section Restrictions spécifiques à Knox.

Pour la version 26.4.0

Restrictions disponibles

La configuration Les restrictions est divisée en trois groupes. L'icône de téléchargement située au-dessus des groupes permet d'exporter toutes les restrictions avec leurs valeurs actuelles dans un fichier CSV.

Restrictions générales

- Appliquer le chiffrement des appareils – chiffre les comptes, les paramètres, les applications et leurs données, les médias et les autres fichiers. Ensuite, un code PIN ou un mot de passe doit être saisi à chaque mise sous tension. Le chiffrement ne peut être supprimé que par une réinitialisation aux paramètres d'usine, qui efface toutes les données. L'opération dure une heure ou plus ; l'appareil doit être chargé et rester branché, car une interruption peut entraîner une perte de données.
- Refuser caméra
- Refuser la caméra/les widgets sur l'écran de verrouillage – l'écran de verrouillage doit être sécurisé par un code PIN, un schéma ou un mot de passe.
- Désactiver la détection racine – les appareils rootés ne sont plus signalés comme non conformes. Les détails de l'appareil continuent d'afficher l'appareil comme rooté.

Pour la version 26.4.0

Roaming

- Activer les restrictions uniquement en itinérance – les restrictions ne sont appliquées que lorsque l'appareil est en itinérance.
- Autoriser en Wi-Fi – disponible uniquement si l'option précédente est activée. Les restrictions ne s'appliquent alors qu'en itinérance, en dehors d'un réseau Wi-Fi.

Restrictions spécifiques à Knox

Ces options ne sont disponibles que sur les appareils Samsung Knox.

Section	Options
Général	Refuser la capture d'écran, Refuser le presse-papiers, Refuser d'activer ou de désactiver le GPS, Refuser de modifier la date et l'heure, Refuser les widgets sur l'écran de verrouillage, Refuser les raccourcis sur l'écran de verrouillage

Section	Options
Stockage	Appliquer le cryptage de la carte SD, Refuser l’accès aux cartes SD, Refuser l’écriture sur carte SD
Débogage	Refuser le débogage USB, Refuser les rapports d’incident
Restrictions USB	Refuser le protocole de transfert multimédia (MTP), Refuser le partage de connexion USB, Refuser le stockage hôte USB
Sauvegarde et réinitialisation	Refuser la sauvegarde, Refuser la réinitialisation, Refuser la mise à jour OTA, Refuser le démarrage en mode sans échec
Restrictions relatives aux applications	Refuser l’installation d’applications autres que Play Store, Refuser Google Play, Refuser YouTube, Refuser le navigateur, Refuser les paramètres, Refuser le numéroteur vocal

Remarques sur certaines options :

- Appliquer le cryptage de la carte SD nécessite un mot de passe alphanumérique sur l’appareil. La politique de code d’accès ne peut être modifiée que lorsque le chiffrement est désactivé.
- Refuser le protocole de transfert multimédia (MTP) bloque tout transfert de fichiers via USB, car Android ne transfère les fichiers que via MTP. Le protocole PTP (Picture Transfer Protocol) est également concerné.
- Refuser le stockage hôte USB empêche le montage de clés USB, de disques durs externes ou de lecteurs de cartes SD comme stockage via USB OTG.
- Refuser le démarrage en mode sans échec empêche le démarrage en mode sans échec, qui permettrait sinon de quitter le mode kiosque.
- Refuser l’installation d’applications autres que Play Store bloque l’installation d’applications en dehors de Google Play ; l’utilisateur ne peut pas l’autoriser dans les paramètres Android. Si l’option est désactivée, l’utilisateur peut autoriser l’installation dans les paramètres Android ; l’option elle-même ne l’active pas.

Pour la version 26.4.0

Mode kiosque

Le mode kiosque transforme les appareils Android en appareils spécialement conçus pour les applications professionnelles. Les utilisateurs finaux ne peuvent donc utiliser que les applications approuvées par l'organisation et les fonctions approuvées sur les appareils fournis avec le mode kiosque activé.

À cette fin, deux modes peuvent être appliqués aux appareils Android : le mode application unique et le mode multi-applications.

Lorsque le mode kiosque est actif, l'appareil affiche le Relution Launcher, dont l'activation doit être confirmée par l'utilisateur ; sur les appareils Samsung avec SAFE, cette confirmation n'est pas nécessaire. L'utilisateur n'a pas accès aux paramètres système.

> En mode kiosque, les appels d'urgence ne sont possibles que si l'application Téléphone fait partie des applications autorisées ou si un Numéro de téléphone d'urgence est défini sous Paramètres de l'appareil.

Pour la version 26.4.0

Kiosque en mode application unique

Le mode application unique est un mécanisme de verrouillage qui limite l'accès de l'appareil à une seule application. Les appareils fonctionnant en mode application unique n'ont qu'un seul but : exécuter une application spécifique avec un minimum de fonctionnalités. L'application se lance d'elle-même, fonctionne au premier plan et est redémarrée même lorsque les appareils sont éteints ou redémarrés. De cette manière, le mode kiosque garantit une utilisation correcte des appareils tout en évitant les distractions inutiles pour les utilisateurs.

1. Dans le portail Relution, naviguer vers `Appareils` → `Politiques` et cliquer sur Ajouter.
2. Créer une politique Android et lui donner un Nom. Cliquer sur Enregistrer.
3. Après avoir cliqué sur Ajouter, sélectionner l'option Mode kiosque et continuer avec Ajouter des détails.
4. Le commutateur Activé/Désactivé reste activé (par défaut). Le champ obligatoire Mot de passe contient le mot de passe permettant de quitter le mode kiosque sur l'appareil (Quitter le mode kiosque →). Sans mot de passe, la configuration ne peut pas être enregistrée.
5. Dans la configuration Mode kiosque, activer Activer le mode application unique et sélectionner exactement une application. L'application sélectionnée doit déjà être installée sur l'appareil, par exemple via l'action Déployer une application du Relution Store →.

6. Enregistrer la configuration après avoir sélectionné des options et des restrictions supplémentaires (Paramètres supplémentaires →) et publier la version actuelle de la politique.
7. Pour appliquer la politique aux appareils Android, ajouter les appareils souhaités en utilisant l'onglet Appareils avec cette stratégie. Les paramètres sélectionnés seront alors automatiquement appliqués aux appareils.

Kiosque en mode multi-applications

Le mode multi-applications limite les appareils à une sélection spécifique d'applications correspondant aux exigences de travail de l'organisation. Les utilisateurs ont la possibilité d'accéder aux applications autorisées et de les utiliser. Le mode kiosque permet un contrôle total de l'utilisation des appareils et garantit que les appareils ne sont utilisés que pour des objectifs spécifiques.

1. Dans le portail Relution, naviguer vers `Appareils` → `Politiques` et cliquer sur Ajouter.
2. Créer une politique Android et lui attribuer un Nom. Cliquer sur Enregistrer.
3. Après avoir cliqué sur Ajouter, sélectionner l'option Mode kiosque et continuer avec Ajouter des détails.
4. Le commutateur Activé/Désactivé reste activé (par défaut). Le champ obligatoire Mot de passe contient le mot de passe permettant de quitter le mode kiosque sur l'appareil (Quitter le mode kiosque →). Sans mot de passe, la configuration ne peut pas être enregistrée.
5. Si l'option Activer le mode application unique est désactivée, il est possible d'ajouter une sélection d'applications. Les applications sélectionnées doivent déjà être installées sur l'appareil. Dès que plus d'une application est sélectionnée, le mode application unique ne peut plus être activé.
6. En outre, des options supplémentaires sont disponibles, dont les suivantes sont particulièrement pertinentes :
    - Activer toutes les applications natives de l'App Store de Relution - activée par défaut. Le kiosque affiche alors, en plus de la sélection, toutes les applications natives du Relution App Store ; les applications non installées sont proposées au téléchargement. Pour n'afficher que les applications sélectionnées, l'option est désactivée.
    - Intervalle d'actualisation App Store - uniquement lorsque l'option précédente est activée ; définit la fréquence à laquelle l'appareil actualise la liste du Relution App Store (1, 2, 4, 6, 12 ou 24 heures ; 12 heures par défaut). Un intervalle plus court fait apparaître

Pour la version 26.4.0

plus tôt les nouvelles applications, mais augmente la consommation de la batterie et le volume de données.
    - Afficher uniquement les applications installées - si cette option est désactivée, toutes les applications disponibles seront affichées et proposées au téléchargement.
    - Afficher les applications installées par un administrateur - les applications installées sur les appareils via l'action Déployer l'application Relution Store apparaissent automatiquement en mode kiosque, même si elles ne sont plus disponibles dans le store.
    - Regrouper les applications par catégorie - range les applications du lanceur dans des dossiers selon leur catégorie. Une application appartenant à plusieurs catégories apparaît dans chacun de ces dossiers.
    - Type d'arrangement d'application - avec Dynamique (par défaut), la grille est calculée automatiquement. Avec Fixe et Fixe et centré (grille à partir du centre de l'écran), le Nombre d'icônes d'application par ligne et le Nombre d'icônes d'application par colonne sont définis (de 1 à 12 chacun).
7. Enregistrer la configuration après avoir sélectionné des options et des restrictions supplémentaires (Paramètres supplémentaires →).
8. Si nécessaire, ajouter la configuration Conformité App à la configuration Mode kiosque.
9. Publier la version actuelle de la politique.
10. Pour appliquer la politique aux appareils Android, ajouter les appareils souhaités en utilisant l'onglet Appareils avec cette stratégie. Les paramètres sélectionnés seront alors automatiquement appliqués aux appareils.

Pour la version 26.4.0

Paramètres supplémentaires

Quel que soit le mode choisi, la configuration propose les paramètres suivants :

- Afficher le nom du périphérique - affiche un nom sur le lanceur. Si le champ Nom de l'appareil est vide, le nom de l'appareil est affiché. Les modifications du nom peuvent prendre plusieurs heures avant d'apparaître sur l'appareil.
- Paramètres de l'appareil - garder l'écran allumé pendant le chargement, Numéro de téléphone d'urgence ainsi que Fond d'écran Homescreen et Papier peint Lockscreen (PNG ou JPEG). Le numéro d'urgence et le fond d'écran de verrouillage apparaissent sur l'écran de verrouillage et nécessitent donc un écran de verrouillage, qui peut être imposé par une configuration Code d'accès. Le numéro d'urgence permet de passer un appel d'urgence même si l'appareil est verrouillé ou si le mode kiosque est actif.
- Restrictions relatives à l'appareil - notamment la barre de navigation, la barre d'état, la barre système, le gestionnaire de tâches et la touche Home, ainsi que des fonctions Samsung

comme Airview, S-Voice, l’écran Edge, les fenêtres multiples et le clip intelligent. La barre de navigation, la barre d’état et son extension, la barre système, le gestionnaire de tâches, la touche Home et l’écran Edge sont autorisés par défaut. Si la barre de navigation ou la barre système est désactivée, l’application gère elle-même la navigation. Les options de suppression des notifications et Effacer les tâches récentes suppriment respectivement les notifications et la liste des applications récemment utilisées.

- Restrictions matérielles - la section de désactivation des touches matérielles permet de bloquer le bouton marche/arrêt, les boutons de volume ainsi que les boutons Accueil, Retour et Menu.

Quitter le mode kiosque

La saisie du mot de passe apparaît sur l’appareil lorsque l’écran est touché rapidement 2 fois, 4 fois, 1 fois puis 3 fois, avec une pause de plus de 0,5 seconde entre chaque groupe. Après saisie du Mot de passe défini dans la configuration, le mode kiosque peut être quitté.

Pour la version 26.4.0

Wi-Fi

La politique Wi-Fi permet de gérer les paramètres Wi-Fi sur les appareils Android Classic. Une politique peut contenir plusieurs configurations Wi-Fi, par ex. pour différents réseaux. Des espaces réservés peuvent être utilisés dans la configuration ; ils sont résolus par appareil lors du transfert. Les espaces réservés disponibles sont affichés dans le formulaire sous les champs de saisie.

Les restrictions d'utilisation du Wi-Fi, par ex. les SSID autorisés ou bloqués et un niveau de sécurité minimal, ne sont pas définies ici, mais via la configuration distincte Restrictions du réseau.

Général

- Le SSID du réseau – nom du réseau (champ obligatoire).
- Priorité – nombre entier à partir de 0. Si plusieurs réseaux sont disponibles, l'appareil se connecte d'abord au réseau ayant la priorité la plus élevée. Par défaut, tous les réseaux ont la priorité 0.
- Ce réseau est masqué – pour les réseaux qui ne diffusent pas leur SSID.
- Type de cryptage – Aucun/Ouvert (par défaut), WEP, WPA/WPA2 PSK ou EAP 802.1x (EAP). Pour WEP et WPA/WPA2 PSK, le champ Mot de passe est obligatoire ; pour WPA/WPA2 PSK, il doit comporter de 8 à 63 caractères.

Pour la version 26.4.0

EAP 802.1x (EAP)

Cette section n'apparaît que pour le type de cryptage EAP 802.1x (EAP). Sous Accepter les types d'EAP, les types PEAP (par défaut), TLS, TTLS et PWD sont disponibles. Selon le type, les champs suivants s'affichent :

- PEAP et TTLS : Phase 2 de l'authentification (Aucun, MSCHAP, MSCHAPv2, GTC ou PAP, par défaut : Aucun), Certificat CA, Identité, Identité anonyme et Mot de passe. Pour PEAP, PAP et MSCHAP sont refusés lors de l'enregistrement.
- TLS : Certificat CA, Certificat d'authentification utilisateur et Identité. Deux options sont disponibles pour le certificat d'authentification utilisateur :
  - Sélectionner un certificat – un certificat avec clé privée (PKCS#12) issu de la Gestion des certificats →.

    - Utiliser un certificat utilisateur – le certificat Wi-Fi du profil de l'utilisateur attribué à l'appareil (voir Certificats utilisateur →). Le champ facultatif Nom du certificat sélectionne un certificat précis par son nom lorsque l'utilisateur possède plusieurs certificats Wi-Fi et peut contenir des espaces réservés. S'il reste vide, le certificat ayant la plus longue durée de validité est utilisé.
- PWD : Identité et Mot de passe.

Les certificats sans clé privée (PKCS1) de la gestion des certificats sont disponibles comme Certificat CA.

> Sur les appareils Samsung Knox, une configuration avec le type d'EAP PEAP, TLS ou TTLS n'est appliquée que si la politique contient également une configuration Code d'accès activée. Si elle est absente ou désactivée, le formulaire affiche un avertissement correspondant.

Type de proxy

- Aucun (par défaut) – pas de proxy.
- Manuelle – l'Hôte (sans protocole) et le Port (1 à 65535) du serveur proxy sont obligatoires. Le champ Contourner le proxy pour reçoit une liste d'adresses qui ne sont pas acheminées via le proxy.
- Configuration automatique – URL du PAC avec l'adresse du fichier PAC (champ obligatoire).

Pour la version 26.4.0

Certificat

La politique Certificat permet de sélectionner un certificat à installer par défaut sur l'appareil. Une politique peut contenir plusieurs configurations de certificat, mais chaque certificat une seule fois.

Prérequis

- Le certificat a été préalablement téléversé sous `Paramètres` → `Certificats` (voir Gestion des certificats →).
- Seuls les certificats de type PKCS1, c'est-à-dire les certificats sans clé privée (par ex. `crt`, `cer`), peuvent être sélectionnés. Les fichiers PKCS#12 (`pfx` / `p12`) n'apparaissent pas dans la sélection.
- Sur les appareils Samsung Knox, le certificat n'est installé que si la politique contient également une configuration Code d'accès activée. Si elle est absente ou désactivée, le formulaire affiche un avertissement correspondant.

Pour la version 26.4.0

Configuration

Dans la boîte de dialogue Ajouter un certificat, le bouton de sélection du champ Certificat de la section Général ouvre la boîte de dialogue de sélection des certificats. Les certificats déjà utilisés dans une autre configuration de certificat de la même politique y sont masqués. Le champ est obligatoire ; Enregistrer n'est actif qu'après la sélection d'un certificat. Le nom de la configuration est repris automatiquement du nom du certificat.

Protection réinitialisation

Les organisations doivent garantir la sécurité et la conformité des appareils Android utilisés pour la prestation de services. Relution peut être utilisé pour minimiser les efforts et augmenter la sécurité en configurant, gérant et surveillant à distance les appareils liés au travail et en corrigeant rapidement toute erreur qui se produit. Un Relution Companion pour Android installé sur les appareils permet l'inscription Android Classic / Legacy des appareils dans Relution. En outre, une réinitialisation d'usine peut être interdite sur les appareils.

L'interdiction de la réinitialisation d'usine est une restriction spécifique à Knox de la configuration Restrictions et n'est disponible que sur les appareils Samsung avec Knox. Sur les appareils d'autres fabricants, l'option n'a aucun effet.

Configurer FRP

1. Dans le portail Relution, naviguer vers `Appareils` → `Politiques` et cliquer sur Ajouter.
2. Créer une politique Android et attribuer un Nom. Cliquer sur Enregistrer.
3. Après avoir cliqué sur Ajouter, sélectionner l'option Restrictions et cliquer sur Ajouter des détails.
4. Sous Restrictions spécifiques à Knox, dans la section Sauvegarde et réinitialisation, s'assurer que l'option Refuser la réinitialisation est activée. Dans les nouvelles configurations de restrictions, l'option est activée par défaut.
5. Enregistrer la configuration et publier la version actuelle de la politique.
6. Pour appliquer la politique aux appareils Android, ajouter les appareils souhaités via l'onglet Appareils avec cette stratégie. Alternativement, la politique est attribuée à des groupes d'appareils entiers via l'onglet Groupes d'appareils avec cette politique. Les paramètres sélectionnés seront alors automatiquement appliqués aux appareils.

> Sur les appareils Samsung avec Knox, le bouton Réinitialiser l'appareil aux paramètres d'usine est ensuite grisé. La réinitialisation via le mode de récupération n'est également plus possible.

Comme l'option est activée par défaut, chaque configuration de restrictions interdit la réinitialisation d'usine tant que l'option n'est pas désactivée. Si un appareil doit être réinitialisé volontairement, l'option Refuser la réinitialisation est désactivée et une nouvelle version de la politique est publiée.

Toutes les autres options de la configuration sont décrites sous Restrictions →.

Pour la version 26.4.0

ADVANTouch

Relution permet de gérer les tableaux blancs interactifs de la marque ADVANTouch.

Gammes et modèles pris en charge

Relution prend en charge les séries de produits ADVANTouch suivantes :

- ADVANTouch PRO 1, 2.0, 2.1 et 3
- ADVANTouch vGAP 2, 3, 4 et 5

La prise en charge s'applique en principe à partir de l'API Android 24 (correspondant à Android 7.0 ou supérieur).

Pour la version 26.4.0

Inscription

Créer une inscription pour la plateforme Android et sélectionner ADVANTouch comme type.

S'assurer que Relution Companion pour ADVANTouch (nom de paquet `com.mwaysolutions.relution.advantouch`) est installé avant l'inscription. Le Relution Companion standard ne peut pas s'inscrire avec une inscription de type ADVANTouch ; le serveur refuse l'inscription.

Ouvrir Relution Companion et saisir l'adresse du serveur et le code d'inscription.

Companion demande plusieurs confirmations. Confirmer les notifications et les demandes d'autorisation affichées. Une fois l'inscription réussie, un écran de confirmation correspondant s'affiche.

L’appareil devrait maintenant être visible dans l’inventaire du portail Relution.

Actions prises en charge

Pour la version 26.4.0

Les actions suivantes peuvent être effectuées sur les tableaux blancs interactifs ADVANTouch via Relution :

Action	Description
Déclencher une alarme →	
Supprimer l’application →	
Envoyer un fichier à l’appareil →	
Effacer l’appareil →	

Action	Description
Redémarrer l’appareil →	Redémarrer ou éteindre (option Mise hors tension)
Verrouiller complètement l’appareil →	Prérequis : un mot de passe ou un code PIN est défini localement sur l’appareil ou via la politique spécifique au fabricant (Activer le code PIN de verrouillage de l’écran)
Actualiser les informations sur l’appareil →	
Envoyer un message →	
Déployer une application du Relution Store →	
Mettre à jour l’OS →	

Pour la version 26.4.0

Politiques prises en charge

Les politiques suivantes sont prises en charge sur les tableaux blancs interactifs ADVANTouch :

Politique	Restrictions
Hotspot →	
Conformité des applications →	
Certificat →	Device Owner

Politique spécifique au fabricant

La politique spécifique au fabricant ADVANTouch propose les paramètres suivants :

Paramètre	Description
Luminosité	Définir la luminosité sur une valeur fixe de 0 à 100
Activer la protection des yeux	
Verrouiller l’entrée tactile	
Source de démarrage	Définir la source active après la mise sous tension de l’écran (Ne pas changer, Android, HDMI 1–3, USB-C 1–2 ou VGA)
Source actuelle	Définir la source actuellement active (mêmes options que Source de démarrage)
Arrêt en l’absence de signal	Mise hors tension si aucun signal n’est reçu après le délai fixé
Délai d’extinction en l’absence de signal	Délai de 1 minute à 1 heure avant la mise hors tension sans signal ; uniquement disponible si Arrêt en l’absence de signal est activé
Réveil à la connexion de la source	
Autoriser les alias de source	Une fois activé, définir des alias pour Android, HDMI1, HDMI2, HDMI3 et USB-C1
Activer Ethernet	
Réveil sur le réseau local	Activer la fonction Wake-on-LAN
Muet	
Volume	Régler le volume sur une valeur fixe de 0 à 100
Activer le code PIN de verrouillage de l’écran	Définir un code PIN de verrouillage de l’écran (exactement 4 caractères)

Paramètre	Description
Activer le verrouillage de l’administrateur	Définir un mot de passe pour le verrouillage de l’administrateur (exactement 4 caractères)
Activer le verrouillage des paramètres	Uniquement disponible si le verrouillage de l’administrateur est activé
Langue	Définir la langue de l’appareil (anglais, allemand ou espagnol)
Activer la mise à jour OTA automatique	
Autoriser l’installation à partir de sources inconnues	Autorise l’installation à partir de sources inconnues, y compris les clés USB
Mise sous tension automatique	Définir les jours de la semaine et l’heure pour la mise sous tension automatique de l’écran
Mise hors tension automatique	Définir les jours de la semaine et l’heure pour la mise hors tension automatique de l’écran
Délai avant que le panneau ne passe en mode veille	Ne pas changer, Jamais, 15 ou 30 minutes, 1, 1,5 ou 2 heures

Pour

Une nouvelle configuration est préremplie avec les valeurs suivantes : luminosité 100, volume 33, langue allemand, veille Jamais ; Activer Ethernet, Autoriser l’installation à partir de sources inconnues et Réveil à la connexion de la source sont activés. La luminosité, le volume et la langue ne proposent pas d’option « Ne pas changer » ; ces valeurs sont donc toujours définies par la politique.

Après la modification du code PIN de verrouillage de l’écran ou du verrouillage de l’administrateur, un redémarrage de l’appareil peut être nécessaire pour que les modifications soient prises en compte.

Activer le propriétaire de l’appareil

Pour activer les fonctions spécifiques au propriétaire de l’appareil, suivre les instructions pour Configuration et connexion d’Android Debug Bridge →.

Une fois l’appareil connecté, activer le mode propriétaire de l’appareil en exécutant la commande suivante :

```
adb shell dpm set-device-owner com.mwaysolutions.relution.advantouch/com.mways
```

Pour la version 26.4.0

Clevertouch

Relution permet de gérer les tableaux blancs interactifs de la marque Clevertouch.

Gammes et modèles pris en charge

Les séries de produits suivantes sont prises en charge :

- IMPACT Lux

Inscription

Créer une inscription pour la plateforme Android et sélectionner Clevertouch comme type. Ouvrir le lien d'inscription sur l'appareil et suivre les instructions sur la page Web.

Le bouton Télécharger affiché permet de télécharger et d'installer Relution Companion pour Clevertouch.

Une fois Companion installé, retourner à la page d'inscription pour lancer le processus d'inscription.

Le Companion s'ouvre alors automatiquement et invite à confirmer plusieurs remarques et autorisations. Une fois l'inscription réussie, un écran de confirmation correspondant s'affiche.

Pour la version 26.4.0

L’appareil devrait maintenant être visible dans l’inventaire du portail Relution.

Actions prises en charge

Pour la version 26.4.0

Les actions suivantes peuvent être effectuées sur les tableaux blancs interactifs Clevertouch via Relution :

Action	Description
Déclencher une alarme →	
Supprimer l’application →	
Envoyer un fichier à l’appareil →	
Effacer l’appareil →	
Redémarrer l’appareil →	Redémarrer ou éteindre (option Mise hors tension)
Actualiser les informations sur l’appareil →	

Action	Description
Envoyer un message →	
Déployer une application du Relution Store →	
Mettre à jour l'OS →	

Politiques prises en charge

Les politiques suivantes sont prises en charge sur les tableaux blancs interactifs Clevertouch :

Politique	Restrictions
Mise à jour OTA prévue →	
Hotspot →	
Wi-Fi →	
Conformité des applications →	

Politique spécifique au fabricant

La politique spécifique au fabricant Clevertouch propose les paramètres suivants :

Paramètre	Description
Luminosité	Définir la luminosité sur une valeur fixe de 0 à 100

Paramètre	Description
Activer la protection des yeux	
Verrouiller l’entrée tactile	
Source de démarrage	Définir la source active après la mise sous tension de l’écran (Ne pas changer, Android, HDMI 1–3, USB-C 1–2 ou VGA)
Source actuelle	Définir la source actuellement active (mêmes options que Source de démarrage)
Arrêt en l’absence de signal	Mise hors tension si aucun signal n’est reçu après le délai fixé
Délai d’extinction en l’absence de signal	Délai de 1 minute à 1 heure avant la mise hors tension sans signal ; uniquement disponible si Arrêt en l’absence de signal est activé
Autoriser les alias de source	Une fois activé, définir des alias pour Android, HDMI1, HDMI2, HDMI3 et USB-C1
Activer Ethernet	
Muet	
Volume	Régler le volume sur une valeur fixe de 0 à 100
Activer le code PIN de verrouillage de l’écran	Définir un code PIN de verrouillage de l’écran (exactement 4 caractères)
Langue	Définir la langue de l’appareil (anglais, allemand ou espagnol)
Activer la mise à jour OTA automatique	
Autoriser l’installation à partir de sources inconnues	Autorise l’installation à partir de sources inconnues, y compris les clés USB
Mise sous tension automatique	Définir les jours de la semaine et l’heure de mise sous tension automatique de l’écran
Mise hors tension automatique	Définir les jours de la semaine et l’heure de mise hors tension automatique de l’écran

Paramètre	Description
Délai avant que le panneau ne passe en mode veille	Ne pas changer, Jamais, 15 ou 30 minutes, 1, 1,5 ou 2 heures

Une nouvelle configuration est préremplie avec les valeurs suivantes : luminosité 100, volume 33, langue allemand, veille Jamais ; Activer Ethernet et Autoriser l’installation à partir de sources inconnues sont activés. La luminosité, le volume et la langue ne proposent pas d’option « Ne pas changer » ; ces valeurs sont donc toujours définies par la politique.

Après la modification du code PIN de verrouillage de l’écran, un redémarrage de l’appareil peut être nécessaire pour que la modification soit prise en compte.

Pour la version 26.4.0

CTOUCH

Relution permet de gérer les tableaux blancs interactifs de la marque CTOUCH.

Gammes et modèles pris en charge

Les séries de produits suivantes sont prises en charge :

- Riva D2

Inscription

Créer une inscription pour la plateforme Android et sélectionner CTOUCH comme type. Ouvrir le lien d'inscription sur l'appareil et suivre les instructions sur la page Web.

Le bouton Télécharger affiché permet de télécharger et d'installer Relution Companion pour CTOUCH.

Une fois Companion installé, retourner à la page d'inscription pour lancer le processus d'inscription.

Le Companion s'ouvre alors automatiquement et invite à confirmer plusieurs remarques et autorisations. Une fois l'inscription réussie, un écran de confirmation correspondant s'affiche.

Pour la version 26.4.0

L’appareil devrait maintenant être visible dans l’inventaire du portail Relution.

Actions prises en charge

Pour la version 26.4.0

Les actions suivantes peuvent être effectuées sur les tableaux blancs interactifs CTOUCH via Relution :

Action	Description
Déclencher une alarme →	
Supprimer l’application →	
Envoyer un fichier à l’appareil →	
Effacer l’appareil →	

Action	Description
Déverrouiller l’appareil →	
Redémarrer l’appareil →	Redémarrer ou éteindre (option Mise hors tension)
Verrouiller complètement l’appareil →	Prérequis : un mot de passe ou un code PIN est défini localement sur l’appareil ou via la politique spécifique au fabricant (Activer le mot de passe pour le verrouillage de l’écran)
Actualiser les informations sur l’appareil →	
Envoyer un message →	
Déployer une application du Relution Store →	Déployer des applications natives via Relution. Autoriser l’installation à partir de sources inconnues doit être activé

Pour la version 26.4.0

Politiques prises en charge

Les politiques suivantes sont prises en charge sur les tableaux blancs interactifs CTOUCH :

Politique	Restrictions
Wi-Fi →	
Conformité des applications →	
Certificat →	Seule l’installation est prise en charge

Politique spécifique au fabricant

La politique spécifique au fabricant CTOUCH propose les paramètres suivants :

Paramètre	Description
Activer le mot de passe pour le verrouillage de l’écran	Définir le mot de passe de l’écran de verrouillage ; une fois activé, le champ Mot de passe de l’écran de verrouillage est obligatoire (au moins 6 caractères)
Réveil sur le réseau local	Activer la fonction Wake-on-LAN (préréglé dans les nouvelles configurations)
Autoriser l’installation à partir de sources inconnues	Autorise l’installation d’applications à partir de sources inconnues ; requis pour Déployer une application du Relution Store
Mise sous tension automatique	Définir les jours de la semaine et l’heure de mise sous tension automatique de l’écran
Mise hors tension automatique	Définir les jours de la semaine et l’heure de mise hors tension automatique de l’écran
Activer la mise à jour OTA	Activer la recherche automatique de mises à jour OTA

Dahua

Relution permet de gérer les tableaux blancs interactifs de la marque Dahua.

Gammes et modèles de produits pris en charge

Les séries de produits suivantes sont prises en charge:

- LPHXX-ST420

Inscription

Créer une inscription pour la plateforme Android et sélectionner Dahua comme type. Ouvrir le lien d'inscription sur l'appareil et suivre les instructions sur la page Web.

Utiliser le bouton Télécharger affiché pour télécharger et installer Relution Companion pour Dahua.

Une fois Companion installé, retourner à la page d'inscription pour lancer le processus d'inscription.

Le Companion s'ouvre alors automatiquement et invite à confirmer plusieurs remarques et autorisations. Une fois l'inscription réussie, un écran de confirmation correspondant s'affiche.

Pour la version 26.4.0

Suivre ensuite les instructions à l'écran jusqu'à ce que l'inscription soit terminée.

L'appareil devrait maintenant être visible dans l'inventaire du portail Relution.

Pour la version 26.4.0

Actions prises en charge

Les actions suivantes peuvent être effectuées sur les tableaux blancs interactifs Dahua via Relution :

Action	Description
Déclencher une alarme →	
Supprimer l'application →	
Envoyer un fichier à l'appareil →	
Effacer l'appareil →	
Redémarrer l'appareil →	Redémarrer ou éteindre (option Mise hors tension)

Action	Description
Verrouiller complètement l’appareil →	
Actualiser les informations sur l’appareil →	
Envoyer un message →	
Déployer une application du Relution Store →	
Mettre à jour l’OS →	

Politiques prises en charge

Les politiques suivantes sont prises en charge sur les tableaux blancs interactifs Dahua :

ersion 26.4.0

Politique	Restrictions
EShare →	
Conformité des applications →	
Ethernet	

Politique spécifique au fabricant

La politique spécifique au fabricant Dahua propose les paramètres suivants:

Paramètre	Description
Luminosité	Régler la luminosité sur une valeur fixe (0 à 100, 100 par défaut)
Activer la luminosité automatique	Régler la luminosité automatiquement (désactivé par défaut)
Délai d’extinction en l’absence de signal (en minutes)	Durée en minutes sans signal d’entrée après laquelle le tableau blanc s’éteint (minimum 1, 5 par défaut)
Source de démarrage	Définir la source active après la mise sous tension de l’écran
Source actuelle	Définir la source actuellement active
Disponibilité de l’USB	Rendre les ports USB disponibles (activé par défaut)
Réveil sur le réseau local (Wake on LAN)	Activer la fonction Wake on LAN (activé par défaut)
Muet	Couper le son (désactivé par défaut)
Volume	Régler le volume sur une valeur fixe (0 à 100, 33 par défaut)
Langue	Définir la langue de l’appareil : anglais, allemand ou espagnol (allemand par défaut)
Fuseau horaire	Définir le fuseau horaire de l’appareil (Europe/Paris par défaut)
Planification de la mise en marche et de l’arrêt de l’alimentation	Jusqu’à 5 plannings de mise sous tension et hors tension automatiques

Pour Source de démarrage et Source actuelle, les options Ne pas changer (par défaut), Android, HDMI 1–3, USB-C 1–2, VGA, OPS, DisplayPort, Composante (YPbPr), AV et Dernière source sont disponibles.

heinekingmedia

Relution permet de gérer les tableaux blancs interactifs de la marque heinekingmedia.

Gammes et modèles pris en charge

Les séries de produits suivantes sont prises en charge:

- Digitale Tafel (DT-86A80-L20HM)
- Digitale Tafel Gen3 (DT-65A11-L30HM)

Inscription

Créer une inscription pour la plateforme Android et sélectionner heinekingmedia comme type. Ouvrir le lien d’inscription sur l’appareil et suivre les instructions sur la page Web.

Utiliser le bouton Télécharger affiché pour télécharger et installer Relution Companion pour heinekingmedia.

Une fois Companion installé, retourner à la page d’inscription pour démarrer le processus d’inscription.

Le Companion s’ouvre alors automatiquement et invite à confirmer plusieurs remarques et autorisations. Une fois l’inscription réussie, un écran de confirmation correspondant s’affiche.

Pour la version 26.4.0

Suivre ensuite les instructions à l’écran jusqu’à ce que l’inscription soit terminée.

L’appareil devrait maintenant être visible dans l’inventaire du portail Relution.

Pour la version 26.4.0

Actions prises en charge

Les actions suivantes peuvent être effectuées sur les tableaux blancs interactifs heinekingmedia via Relution :

Action	Description
Déclencher une alarme →	
Supprimer l’application →	
Envoyer un fichier à l’appareil →	
Effacer l’appareil →	
Redémarrer l’appareil →	Redémarrer ou éteindre (option Mise hors tension)

Action	Description
Actualiser les informations sur l’appareil →	
Envoyer un message →	
Déployer une application du Relution Store →	
Mettre à jour l’OS →	

Politiques prises en charge

Les politiques suivantes sont prises en charge sur les tableaux blancs interactifs heinekingmedia :

ersion 26.4.0

Politique	Restrictions
Mode kiosque →	
Hotspot →	
EShare →	
Conformité des applications →	

Configuration du tableau interactif

La politique Configuration du tableau interactif propose les paramètres suivants pour gérer les tableaux blancs interactifs Heinekingmedia:

Paramètre	Description
Verrouiller les boutons matériels	
Verrouiller la télécommande	
Verrouiller les paramètres	Verrouiller les paramètres de l’appareil. Si l’option est activée, le champ Pin pour déverrouiller les paramètres (chiffres uniquement) doit être renseigné. Le portail réserve ce champ à Prowise et wende.interaktiv, mais la configuration ne peut pas être enregistrée sans lui.
Écran de verrouillage	Disponible uniquement si Verrouiller les paramètres est activé. Activer le verrouillage de l’écran et définir un code PIN numérique (champ obligatoire Code d’accès à l’écran de verrouillage). La désactivation de Verrouiller les paramètres désactive également l’écran de verrouillage.
Verrouiller l’entrée tactile	
Verrouiller les ports USB	
Bloquer l’installation d’applications	
Bloquer la désinstallation d’applications	
Limiter le volume maximal	Définir une valeur pour le volume maximal (champ Volume maximal, en pourcentage, 0 à 100, 100 par défaut)
Luminosité	Définir la luminosité sur une valeur fixe (0 à 100, 100 par défaut). Il n’existe pas d’interrupteur séparé, la valeur est toujours transmise.
Langue	Définir la langue de l’appareil : anglais, allemand, espagnol ou chinois (allemand par défaut)

Paramètre	Description
Fuseau horaire	Définir le fuseau horaire de l’appareil (Europe/Paris par défaut)
Source de démarrage	Définir la source active après le démarrage de l’écran : Android, AV, DisplayPort, HDMI 1–3, OPS, USB-C, VGA ou Dernière source (par défaut)
Sortie HDMI	Définir la résolution et la fréquence d’images : Auto (par défaut), 2k 60Hz, 4k 30Hz ou 4k 60Hz
URL OTA	Adresse des mises à jour OTA (over the air) ; seules les URL HTTPS sont acceptées
Mise sous tension automatique	Après activation de l’interrupteur Désactivé/activé, définir les jours de la semaine et l’heure auxquels l’écran s’allume automatiquement
Mise hors tension automatique	Après activation de l’interrupteur Désactivé/activé, définir les jours de la semaine et l’heure auxquels l’écran s’éteint automatiquement
Verrouiller les applications sélectionnées	Après activation de l’interrupteur Désactivé/activé, verrouiller des applications à l’aide de leurs noms de paquet et définir un code PIN numérique pour les déverrouiller (champ obligatoire Pin pour déverrouiller les applications)
Utilitaires système	Configurer les utilitaires: Effacement de la mémoire, Détection du matériel, Verrouillage des applications, Verrouillage de l’écran, Accueil, Retour, Menu, Écran éteint, Spotlight, WIFI, Source, Tableau blanc, Muet, Volume, Luminosité et Plus. Si l’interrupteur Désactivé/activé est activé, exactement cinq utilitaires doivent être sélectionnés ; sinon la configuration ne peut pas être enregistrée.
Barre de navigation latérale	Configurer les éléments de la barre de navigation latérale: Récent, Source, Contrôle, Paramètres, Gel, Capture d’écran, Heure, Appareil photo, Dossier, Luminosité, Sombre. Si l’interrupteur Désactivé/activé est activé, exactement quatre éléments doivent être sélectionnés ; sinon la configuration ne peut pas être enregistrée.

i3-Technologies

Relution permet de gérer les tableaux blancs interactifs de la marque i3-Technologies.

Gammes et modèles pris en charge

Les séries de produits suivantes sont prises en charge:

- i3TOUCH E-ONE

Inscription

Créer une inscription pour la plateforme Android et sélectionner i3 comme type.

S’assurer que Relution Companion a déjà été installé via l’i3 Store avant de procéder à l’inscription.

Ouvrir Relution Companion et entrer l’adresse du serveur et le code d’inscription.

Companion demande plusieurs confirmations. Confirmer les notifications affichées et les demandes d’autorisation. Une fois l’inscription réussie, un écran de confirmation correspondant s’affiche.

Pour la version 26.4.0

Suivre ensuite les instructions à l'écran jusqu'à ce que l'inscription soit terminée.

L'appareil devrait maintenant être visible dans l'inventaire du portail Relution.

Pour la version 26.4.0

Activer le propriétaire de l'appareil

L'intégration nécessite les autorisations de propriétaire de l'appareil sur l'appareil. Pour activer le propriétaire de l'appareil, suivre les instructions pour Configuration et connexion d'Android Debug Bridge →

Une fois l'appareil connecté, activer le mode propriétaire de l'appareil en exécutant la commande

```
adb shell dpm set-device-owner com.mwaysolutions.relution.i3/com.mwaysolutions
```

Actions prises en charge

Les actions suivantes peuvent être effectuées sur les tableaux blancs interactifs i3-Technologies via Relution :

Action	Description
Déclencher une alarme →	
Supprimer l’application →	
Envoyer un fichier à l’appareil →	
Effacer l’appareil →	
Déverrouiller l’appareil →	
Redémarrer l’appareil →	Redémarrer ou éteindre (option Mise hors tension)
Verrouiller complètement l’appareil →	
Actualiser les informations sur l’appareil →	
Envoyer un message →	
Déployer une application du Relution Store →	
Mettre à jour l’OS →	

Politiques prises en charge

Les politiques suivantes sont prises en charge sur les tableaux blancs interactifs i3-Technologies :

Politique	Restrictions
Mode kiosque →	
Mise à jour OTA prévue →	

Politique	Restrictions
Hotspot →	
Conformité des applications →	

Politique spécifique au fabricant

La politique spécifique au fabricant i3 propose les paramètres suivants:

Paramètre	Description
Activer la luminosité automatique	Régler la luminosité automatiquement
Régler la luminosité	Régler la luminosité sur une valeur fixe. L'activation de cette option déverrouille le champ Luminosité (0 à 100).
Régler le volume	Régler le volume sur une valeur fixe. L'activation de cette option déverrouille le champ Volume (0 à 100).
Activer le code PIN de l'écran de verrouillage	Définir un code PIN pour l'écran de verrouillage dans le champ Code d'accès à l'écran de verrouillage (obligatoire, 4 à 8 chiffres)
Planification de la mise en marche et de l'arrêt de l'alimentation	Jusqu'à 10 plannings de mise sous tension et hors tension automatiques

Promethean

Relution permet de gérer les tableaux blancs interactifs de la marque Promethean.

Gammes et modèles pris en charge

Les séries de produits suivantes sont prises en charge:

- Active Panel 7 et Active Panel 7 Premium
- Active Panel 9 et Active Panel 9 Premium

Inscription

Créer une inscription pour la plateforme Android et sélectionner Promethean comme type.

S’assurer que Relution Companion a déjà été installé via Promethean World avant de procéder à l’inscription.

Si Promethean World ou le Relution Companion ne sont pas disponibles, contacter l’interlocuteur Promethean concerné.

Ouvrir Relution Companion et entrer l’adresse du serveur et le code d’inscription.

Companion demande plusieurs confirmations. Confirmer les notifications affichées et les demandes d’autorisation. Une fois l’inscription réussie, un écran de confirmation correspondant s’affiche.

Pour la version 26.4.0

Suivre ensuite les instructions à l'écran jusqu'à ce que l'inscription soit terminée.

L'appareil devrait maintenant être visible dans l'inventaire du portail Relution.

Pour la version 26.4.0

Actions prises en charge

Les actions suivantes peuvent être effectuées sur les tableaux blancs interactifs Promethean via Relution :

Action	Description
Déclencher une alarme →	
Supprimer l'application →	
Envoyer un fichier à l'appareil →	
Effacer l'appareil →	
Redémarrer l'appareil →	Redémarrer ou éteindre (option Mise hors tension)

Action	Description
Verrouiller complètement l’appareil →	Nécessite un code PIN défini sur l’appareil ou via le paramètre Activ Panel Pin de la politique spécifique au fabricant
Actualiser les informations sur l’appareil →	
Envoyer un message →	
Déployer une application du Relution Store →	
Supprimer le raccourci →	
Ajouter un raccourci →	
Mettre à jour l’OS →	

Politiques prises en charge

Les politiques suivantes sont prises en charge sur les tableaux blancs interactifs Promethean :

Politique	Restrictions
Mode kiosque →	
Wi-Fi →	
Hotspot →	Disponible uniquement pour Active Panel 9 et Active Panel 9 Premium

Pour la version 26.4.0

Politique spécifique au fabricant

La politique spécifique au fabricant Promethean propose les paramètres suivants, dans l'ordre du portail. Lors de la création, les listes de sélection sont réglées sur Ne pas modifier (dans le portail : « Ne changez pas ») ; la valeur du tableau blanc reste alors inchangée.

Paramètre	Description
Luminosité	Régler la luminosité sur une valeur fixe entre 0 et 100
Mode de luminosité	Valeurs possibles : Ne pas modifier, Auto, Économie d'énergie, Protection des yeux, Normal
Extrémité du stylet	Définir le mode de l'extrémité du stylet : Stylo (par défaut) ou Gomme
Contraste	Régler le contraste sur une valeur fixe entre 0 et 100. Disponible uniquement pour Active Panel 7
Délai avant que le panneau ne passe en mode veille	Passage automatique en mode veille après 3 minutes à 4 heures
Temps avant que le panneau ne s'endorme	Passage automatique en mode sommeil après 3 minutes à 8 heures
Activer le capteur de proximité	Activer/désactiver le réveil par proximité. Disponible uniquement pour Active Panel 7 et Active Panel 9 Premium
Activation de la temporisation du détecteur de proximité	Active ou désactive le minuteur de délai du capteur de proximité
Temps de retard du détecteur de proximité	Valeurs possibles : Ne pas modifier, 1 minute, 5 min, 10 min
Activer l'éclairage de l'écran par proximité	Active ou désactive l'éclairage de l'écran lorsqu'un mouvement est détecté
Réinitialiser les minuteries de veille et de sommeil par proximité	Réinitialise les minuteries de veille et de sommeil lorsqu'un mouvement est détecté

Paramètre	Description
Réduire la lumière bleue	Active ou désactive le filtre de lumière bleue
Détection des sources	Configurer la détection automatique des sources. Valeurs possibles : Ne pas modifier, Automatique, Manuel, Off
Source par défaut	Définir la source par défaut, p. ex. la dernière source utilisée, Accueil, HDMI 1–3, AV, DP, OPS, USB-C ou VGA
Mode HDMI EDID	Définir le mode HDMI EDID sur EDID 1.4 ou EDID 2.0
Afficher les paramètres réseau	Afficher ou masquer les paramètres réseau sur l'appareil
Réveil sur le réseau local	Activer la fonction Wake on LAN
Activer la découverte du réseau avec AirPlay	Activer/désactiver le protocole de découverte AirPlay
Activer la découverte du réseau en utilisant Promethean	Activer/désactiver le protocole de découverte propriétaire de Promethean
Activer la découverte du réseau à l'aide de WebRTC	Activer/désactiver le protocole de découverte WebRTC
Activer la découverte du réseau à l'aide de Wi-Fi Direct	Activer/désactiver le protocole de découverte Wi-Fi Direct
Activer le miracast sur l'infrastructure	Activer/désactiver Miracast via infrastructure. Désactiver lorsque Activer la découverte du réseau à l'aide de Wi-Fi Direct est désactivé.
Activer IPv6	Activer/désactiver IPv6. Non disponible sur OPS
Volume	Régler le volume sur une valeur fixe entre 0 et 100. Non modifiable tant que Activer la sourdine est activé
Activer la sourdine	Couper le son
Activer les haut-parleurs du panneau	Active ou désactive les haut-parleurs du panneau
Inclure les haut-parleurs du panneau	Inclure ou non les haut-parleurs du panneau. Ne l'activer que lorsque Mode de sortie de ligne est réglé sur Sortie de ligne et Activer les haut-parleurs du panneau est activé.

Paramètre	Description
Graves	Niveau des graves entre 0 et 100
Équilibre	Balance entre 0 et 100
Aigus	Niveau des aigus entre 0 et 100
Médiums	Niveau des médiums entre 0 et 100
Mode de sortie de ligne	Valeurs possibles : Ne pas modifier, Écouteurs, Sortie de ligne
Activer le subwoofer	Activer/désactiver le subwoofer. Ne l’activer que lorsque Activer les haut-parleurs du panneau est activé.
Mode panneau	Valeurs possibles : Ne pas modifier, Affichage complet, Pas d’affichage, Affichage limité
Activer les utilisateurs et les profils	Activer/désactiver la gestion des utilisateurs locaux sur l’appareil. Disponible uniquement pour Active Panel 7
Activer le menu unifié	Afficher ou masquer le menu unifié
Activer l’onglet du menu d’affichage	Afficher ou masquer l’onglet Menu
Activer la source d’accueil	Activer/désactiver la source Accueil
Activer les applications	Afficher ou masquer les applications non système dans le lanceur
Afficher les paramètres de l’application	Afficher ou masquer les paramètres des applications sur l’appareil
Activer le chargement latéral	Autoriser ou empêcher l’installation d’applications provenant d’autres sources (sideloading)
Activer Google Play	Activer/désactiver Google Play sur l’appareil. Disponible uniquement pour Active Panel 7
Activer la réinitialisation d’usine	Autoriser ou empêcher la réinitialisation d’usine sur l’appareil

Paramètre	Description
Verrouiller les paramètres	Empêcher l’accès aux paramètres du panneau et leur modification sur l’appareil
Activer la mise à jour OTA	Autoriser ou empêcher les mises à jour du micrologiciel par OTA
Activer la mise à jour locale	Autoriser ou empêcher les mises à jour locales du micrologiciel
Redémarrer Screen Share lors de la mise à jour	Si l’option est activée, Screen Share redémarre dès que la découverte du réseau avec AirPlay, Promethean ou WebRTC change. Sinon, Screen Share applique les modifications au prochain lancement
Appliquer Activ Panel Pin	Active la gestion du code PIN. Disponible uniquement pour Active Panel 9 et Active Panel 9 Premium. Si le champ Activ Panel Pin reste vide alors que l’option est activée, le code PIN du tableau blanc est effacé
Activ Panel Pin	Code PIN de 4 à 16 chiffres (uniquement 0 à 9). Modifiable uniquement si Appliquer Activ Panel Pin est activé
Afficher les mots de passe activés	Activer/désactiver l’affichage des mots de passe. Activé par défaut
Masquer le verrouillage du système	Afficher ou masquer le verrouillage du système
L’identité exige que l’utilisateur qui se connecte appartienne à l’organisation inscrite au panel	

Prowise

Relution permet de gérer les tableaux blancs interactifs de la marque Prowise.

Gammes et modèles pris en charge

Les séries de produits suivantes sont prises en charge:

- Touchscreen
- Touchscreen Ultra

Inscription

Pour la version 26.4.0

Créer une inscription pour la plateforme Android et sélectionner Prowise comme type.

S’assurer que Relution Companion a déjà été installé via le Prowise Store avant l’inscription.

Ouvrir Relution Companion et entrer l’adresse du serveur et le code d’inscription.

Companion demande alors plusieurs confirmations. Confirmer les notifications affichées et les demandes d’autorisation. Une fois l’inscription réussie, un écran de confirmation correspondant s’affichera.

Suivre ensuite les instructions à l'écran jusqu'à ce que l'inscription soit terminée.

L'appareil devrait maintenant être visible dans l'inventaire du portail Relution.

Pour la version 26.4.0

Actions prises en charge

Les actions suivantes peuvent être effectuées sur les tableaux blancs interactifs Prowise via Relution :

Action	Description
Déclencher une alarme →	
Installer l'application à partir du magasin d'applications Prowise →	
Supprimer l'application →	
Envoyer un fichier à l'appareil →	
Redémarrer l'appareil →	Redémarrer ou éteindre (option Mise hors tension)

Action	Description
Verrouiller complètement l’appareil →	Nécessite un mot de passe ou un code PIN défini localement sur l’appareil ou, si disponible, via la configuration
Actualiser les informations sur l’appareil →	
Envoyer un message →	
Installer la mise à jour de Prowise →	

Ne sont notamment pas disponibles sur les tableaux Prowise : Effacer l’appareil, Déployer une application du Relution Store, Mettre à jour l’OS ainsi que l’ajout et la suppression de raccourcis. Les applications et les mises à jour sont installées via les deux actions Prowise.

Politiques prises en charge

Les politiques suivantes sont prises en charge sur les tableaux blancs interactifs Prowise :

Pour la version 26.4.0

Politique	Restrictions
Mode kiosque →	
Conformité des applications →	

Configuration du tableau interactif

La politique Configuration du tableau interactif (dans le portail : « Configuration de la carte interactive ») propose les paramètres suivants pour gérer les tableaux blancs interactifs Prowise:

Paramètre	Description
Désactiver les services de partage d’écran	Désactiver Reflect, AirPlay, Chromecast et Miracast. L’interrupteur sélectionne les quatre services ; chaque service peut ensuite être désélectionné individuellement par case à cocher
Verrouiller les paramètres	Verrouille les paramètres du tableau blanc. Si l’option est activée, Pin pour déverrouiller les paramètres est un champ obligatoire qui n’accepte que des chiffres
Écran de verrouillage	Sélectionnable uniquement si Verrouiller les paramètres est activé
Verrouiller les ports USB	
Luminosité	Régler la luminosité sur une valeur fixe entre 0 et 100 (par défaut : 100). La valeur est transmise avec chaque configuration
Verrouiller les applications sélectionnées	L’interrupteur Désactivé/activé verrouille une liste d’applications
Canaux d’entrée désactivés	Liste des entrées vidéo désactivées sur le tableau blanc

SMART

Relution permet de gérer les tableaux blancs interactifs de la marque SMART.

Gammes et modèles pris en charge

Les séries de produits suivantes sont prises en charge:

- MX (IDX55-4)

Inscription

Créer une inscription pour la plateforme Android et sélectionner SMART comme type. Ouvrir le lien d'inscription sur l'appareil et suivre les instructions sur la page Web.

Utiliser le bouton Télécharger affiché pour télécharger et installer Relution Companion pour SMART.

Une fois Companion installé, retourner à la page d'inscription pour démarrer le processus d'inscription.

Le Companion s'ouvre alors automatiquement et invite à confirmer plusieurs remarques et autorisations. Une fois l'inscription réussie, un écran de confirmation correspondant s'affiche.

Pour la version 26.4.0

Suivre ensuite les instructions à l'écran jusqu'à ce que l'inscription soit terminée.

L'appareil devrait maintenant être visible dans l'inventaire du portail Relution.

Pour la version 26.4.0

Actions prises en charge

Les actions suivantes peuvent être effectuées sur les tableaux blancs interactifs SMART via Relution :

Action	Description
Déclencher une alarme →	
Supprimer l'application →	
Envoyer un fichier à l'appareil →	
Redémarrer l'appareil →	Redémarrer ou éteindre (option Mise hors tension)
Actualiser les informations sur l'appareil →	

Action	Description
Envoyer un message →	
Déployer une application du Relution Store →	

Politiques prises en charge

Les politiques suivantes sont prises en charge sur les tableaux blancs interactifs SMART :

Politique	Restrictions
Conformité des applications →	

Pour la version

Politique spécifique au fabricant

La politique spécifique au fabricant SMART propose les paramètres suivants:

Paramètre	Description
Source de démarrage	Définit la source active après la mise sous tension de l’écran : Android, AV, DP, HDMI 1–3, USB-C 1–2, PC ou VGA. Par défaut : Ne pas changer
Activer la luminosité automatique	Activer/désactiver la luminosité automatique
Luminosité	Définir la luminosité sur une valeur fixe entre 0 et 100 (par défaut : 100). La valeur est transmise avec chaque configuration

Paramètre	Description
Délai avant que le panneau ne passe en mode veille	Passage automatique en veille après 1, 5 ou 30 minutes ou 1, 1,5, 2, 5 ou 10 heures ; sinon Jamais
Muet	Couper le son
Volume	Définir le volume sur une valeur fixe entre 0 et 100 (par défaut : 33). La valeur est transmise avec chaque configuration
Langue	Langue du système : Anglais, allemand (par défaut) ou espagnol
Activer l’App Store	Activer/désactiver l’App Store. Activé par défaut
Activer la date et l’heure automatiques	Activer/désactiver la date et l’heure automatiques
Activer le Bluetooth	Activer/désactiver le Bluetooth

Pour la version 26.4.0

ViewSonic

Relution permet de gérer les tableaux blancs interactifs de la marque ViewSonic.

Gammes et modèles pris en charge

Les séries de produits suivantes sont prises en charge:

- CDExx30
- IFP6550-5
- IFP6552-1ANEP

Inscription

Pour la version 26.4.0

Créer une inscription pour la plateforme Android et sélectionner ViewSonic comme type. Ouvrir le lien d'inscription sur l'appareil et suivre les instructions sur la page Web.

Utiliser le bouton Télécharger affiché pour télécharger et installer Relution Companion pour ViewSonic.

Une fois Companion installé, retourner à la page d'inscription pour lancer le processus d'inscription.

Le Companion s'ouvre alors automatiquement et invite à confirmer plusieurs remarques et autorisations. Une fois l'inscription réussie, un écran de confirmation correspondant s'affiche.

Suivre ensuite les instructions à l'écran jusqu'à ce que l'inscription soit terminée.

L'appareil devrait maintenant être visible dans l'inventaire du portail Relution.

Pour la version 26.4.0

Actions prises en charge

Les actions suivantes peuvent être effectuées sur les tableaux blancs interactifs ViewSonic via Relution :

Action	Description
Déclencher une alarme →	
Supprimer l'application →	
Envoyer un fichier à l'appareil →	
Effacer l'appareil →	
Redémarrer l'appareil →	Redémarrer ou éteindre (option Mise hors tension)

Action	Description
Actualiser les informations sur l’appareil →	
Envoyer un message →	
Déployer une application du Relution Store →	
Mettre à jour l’OS →	

Politiques prises en charge

Les politiques suivantes sont prises en charge sur les tableaux blancs interactifs ViewSonic :

Politique	Restrictions
Conformité des applications →	

Politique spécifique au fabricant

La politique spécifique au fabricant ViewSonic propose les paramètres suivants:

Paramètre	Description
Source actuelle	Définir la source actuellement active : Ne pas changer (par défaut), Android, HDMI 1–3, USB-C 1–2 ou VGA
Activer la luminosité	Définir la luminosité sur une valeur fixe (0–100) (CDExx30 uniquement)

Paramètre	Description
Rétro-éclairage automatique	Régler automatiquement le rétroéclairage (IFP6550, IFP6552 uniquement)
Activer le rétro-éclairage	Définir le rétroéclairage sur une valeur fixe (0–100) (IFP6550, IFP6552 uniquement)
Activer Eye Care	
Muet	
Volume	Définir le volume sur une valeur fixe (0–100), 33 par défaut
Activer le code PIN de verrouillage de l’écran	Définir un code PIN de verrouillage de l’écran d’exactement 4 chiffres (obligatoire si l’option est activée)
Verrouiller le menu	
Verrouiller les boutons matériels	
Verrouiller la saisie tactile	
Verrouiller les paramètres	Définir un mot de passe pour déverrouiller les paramètres (champ Mot de passe pour déverrouiller les paramètres, obligatoire si l’option est activée)
Activer la date et l’heure automatiques	
Fuseau horaire	
Langue	
Mise sous tension automatique	Définir les jours de la semaine et l’heure pour la mise sous tension automatique de l’écran
Mise hors tension automatique	Définir les jours de la semaine et l’heure pour la mise hors tension automatique de l’écran
Mode Eco	Active ou désactive le mode d’économie d’énergie de l’écran (Activé, Désactivé). Lorsque le mode Eco est désactivé, l’écran utilise par défaut le niveau d’économie d’énergie 1.

Paramètre	Description
Energy Star	Active ou désactive le mode Energy Star de l’écran (Activé, Désactivé)
Mode veille	Définit le comportement de veille de l’écran : Veille prolongée ou Veille
Veille sans signal	Délai après lequel l’écran passe en veille en l’absence de signal d’entrée : Arrêt, 5, 15 ou 30 minutes

Les paramètres qui ne s’appliquent qu’à certains modèles sont signalés par un badge de modèle dans le portail.

Pour Mode Eco, Energy Star, Mode veille et Veille sans signal, l’option Ne pas changer est sélectionnée par défaut. Le réglage correspondant de l’écran reste alors inchangé.

Pour la version 26.4.0

VS

Relution permet de gérer les tableaux blancs interactifs de la marque VS.

Gammes et modèles pris en charge

Les séries de produits suivantes sont prises en charge:

- VS-S-E1
- VS-S-E3

Inscription

Créer une inscription pour la plateforme Android et sélectionner VS comme type. Un lien d'inscription individuel est généré pour chaque inscription. Ouvrir le lien sur l'appareil et suivre les instructions sur la page Web.

Utiliser le bouton Télécharger affiché pour télécharger et installer Relution Companion pour VS.

Une fois Companion installé, retourner à la page d'inscription pour démarrer le processus d'inscription.

Le Companion s'ouvre alors automatiquement et invite à confirmer plusieurs remarques et autorisations. Une fois l'inscription réussie, un écran de confirmation correspondant s'affiche.

Pour la version 26.4.0

Suivre ensuite les instructions à l’écran jusqu’à ce que l’inscription soit terminée.

L’appareil devrait maintenant être visible dans l’inventaire du portail Relution.

Pour la version 26.4.0

Actions prises en charge

Les actions suivantes peuvent être effectuées sur les tableaux blancs interactifs VS via Relution :

Action	Description
Déclencher une alarme →	
Supprimer l’application →	
Envoyer un fichier à l’appareil →	
Effacer l’appareil →	
Redémarrer l’appareil →	Redémarrer ou éteindre (option Mise hors tension)

Action	Description
Verrouiller complètement l’appareil →	
Actualiser les informations sur l’appareil →	
Envoyer un message →	
Déployer une application du Relution Store →	
Mettre à jour l’OS →	

Politiques prises en charge

Les politiques suivantes sont prises en charge sur les tableaux blancs interactifs VS :

ersion 26.4.0

Politique	Restrictions
Conformité des applications →	

Politique spécifique au fabricant

La politique spécifique au fabricant VS propose les paramètres suivants:

Paramètre	Description
Luminosité	Définir la luminosité sur une valeur fixe (0–100), 100 par défaut
Activer la protection des yeux	

Paramètre	Description
Verrouiller la saisie tactile	
Source de démarrage	Définir la source active après la mise sous tension de l’écran : Ne pas changer (par défaut), Android, HDMI 1–3, USB-C 1–2 ou VGA
Source actuelle	Définir la source actuellement active, mêmes options que pour Source de démarrage
Extinction en l’absence de signal	Éteint l’écran si aucun signal n’est reçu après le délai défini
Délai d’extinction en l’absence de signal	Délai sans signal avant l’extinction (de 1 minute à 1 heure, 5 minutes par défaut) ; uniquement si l’option Extinction en l’absence de signal est activée
Réveil à la connexion de la source	Activé par défaut
Autoriser les alias de source	Une fois l’option activée, des alias peuvent être attribués pour Android, HDMI1–HDMI4, PC et VGA1
Activer Ethernet	Activé par défaut
Réveil sur le réseau local	
Muet	
Volume	Régler le volume sur une valeur fixe (0–100), 33 par défaut
Activer le code PIN de verrouillage de l’écran	Définir un code PIN de verrouillage de l’écran d’exactement 4 caractères (obligatoire si l’option est activée) ; un redémarrage de l’appareil peut être nécessaire pour que la modification soit prise en compte
Langue	Définir la langue de l’appareil, allemand par défaut
Activer la mise à jour OTA automatique	

Paramètre	Description
Autoriser l’installation à partir de sources inconnues	Autorise l’installation à partir de sources inconnues, y compris les clés USB ; activé par défaut
Mise sous tension automatique	Définir les jours de la semaine et l’heure de mise sous tension automatique de l’écran
Mise hors tension automatique	Définir les jours de la semaine et l’heure de mise hors tension automatique de l’écran
Délai avant le passage du panneau en mode veille	Ne pas changer, Jamais (par défaut), 15 minutes, 30 minutes, 1 heure, 1,5 heure ou 2 heures

Pour la version 26.4.0

wende.interaktiv

Relution permet la gestion des tableaux blancs interactifs de la marque wende.interaktiv.

Gammes et modèles pris en charge

La série de produits galneoscreen est prise en charge par Relution:

- galneoscreen V2
- galneoscreen V3
- galneoscreen V4
- galneoscreen V5

Ces modèles sont pris en charge uniquement en combinaison avec les versions Android suivantes:

- Android 8
- Android 9
- Android 11
- Android 14 (fonctionnalités limitées)

Pour la version 26.4.0

Créer une inscription

Pour inscrire un appareil, créer une inscription pour la plateforme Android et sélectionner le type d’inscription Wende. En fonction de la version Android du modèle à inscrire, sélectionner ensuite le sous-type approprié: Wende 8, Wende 9 ou Wende 11.

Le tableau suivant donne un aperçu du sous-type à utiliser pour chaque version Android:

Version Android	Sous-type d’inscription	Fourniture du Relution Companion
Android 8	Wende 8	Relution
Android 9	Wende 9	Relution

Version Android	Sous-type d’inscription	Fourniture du Relution Companion
Android 11	Wende 11	Relution
Android 14	Wende 11	wende.interaktiv

Pour la version 26.4.0

Inscription du tableau blanc interactif

Un lien d’inscription individuel est généré pour chaque inscription. Ouvrir ce lien sur l’appareil et suivre les instructions à l’écran.

Appareils équipés d’Android version 8, 9 ou 11: Pour les appareils équipés d’Android version 8, 9 ou 11, Relution fournit automatiquement la version Companion appropriée en fonction du sous-type d’inscription précédemment sélectionné.

Le bouton Télécharger permet de télécharger Relution Companion pour le modèle de tableau blanc correspondant et de l’installer directement sur l’appareil.

Appareils équipés d’Android version 14: L’inscription d’appareils équipés d’Android 14 nécessite l’installation d’une version spéciale de Relution Companion pour Wende 11.

> Cette version doit être demandée activement auprès de wende.interaktiv avant l’inscription.

Une fois Companion installé, retourner à la page d’inscription pour lancer le processus d’inscription.

Relution Companion démarre alors automatiquement et invite à confirmer plusieurs instructions et autorisations. Une fois l’inscription terminée, un écran de confirmation s’affiche, similaire à celui ci-dessous:

Suivre ensuite les instructions à l’écran jusqu’à la fin du processus d’inscription.

L’appareil devrait maintenant apparaître dans l’inventaire du portail Relution.

Mise à jour de Relution Companion

Selon le type d’inscription et la version Android, Relution Companion est soit mis à jour automatiquement via Relution, soit doit être mis à jour manuellement. Les mises à jour

manuelles peuvent être demandées auprès de wende.interaktiv.

Le tableau suivant indique la méthode applicable:

Sous-type d’inscription	Version Android	Type de mise à jour
Wende 8	Android 8	automatiquement
Wende 9	Android 9	automatiquement
Wende 11	Android 11	automatiquement
Wende 11	Android 14	manuellement (fourni par wende.interaktiv)

La version de Companion que Relution fournit actuellement pour Wende 8, Wende 9 et Wende 11 est indiquée sous `Paramètres` → `Applications client Relution` → `Wende companion`.

Actions prises en charge

Pour la version 26.4.0

Les actions suivantes peuvent être effectuées sur les tableaux blancs interactifs wende.interaktiv via Relution :

Action	Description
Déclencher une alarme →	
Supprimer l’application →	
Envoyer un fichier à l’appareil →	
Effacer l’appareil →	
Redémarrer l’appareil →	Redémarrer ou éteindre (option Mise hors tension)
Localiser l’appareil	

Action	Description
Verrouiller complètement l’appareil →	
Actualiser les informations sur l’appareil →	
Envoyer un message →	
Déployer une application du Relution Store →	
Ajouter un raccourci →	Disponible sur Wende 8 et Wende 9
Mettre à jour l’OS →	

Politiques prises en charge

Les politiques suivantes sont prises en charge sur les tableaux blancs interactifs wende.interaktiv :

Pour la version 26.4.0

Politique	Restrictions
Mode kiosque →	Disponible sur Wende 11
EShare →	
Conformité des applications →	

Configuration du tableau interactif

La politique Configuration du tableau interactif fournit les paramètres suivants pour gérer les tableaux blancs interactifs wende.interaktiv:

Paramètre	Description
Verrouiller les boutons matériels	
Verrouiller la télécommande	
Verrouiller les paramètres	Définir un code PIN (chiffres uniquement) pour déverrouiller les paramètres (champ Pin pour déverrouiller les paramètres, obligatoire si l’option est activée)
Verrouiller la saisie tactile	
Luminosité	Définir la luminosité sur une valeur fixe
Mise sous tension automatique	Définir les jours de la semaine et l’heure auxquels l’écran s’allume automatiquement
Mise hors tension automatique	Définir les jours de la semaine et l’heure auxquels l’écran s’éteint automatiquement
Verrouiller les applications sélectionnées	

Mettre à jour l'OS

L’action Installer une mise à jour (titre de la boîte de dialogue : Mettre à jour le système d’exploitation) permet d’installer une mise à jour logicielle spécifique sur un appareil sélectionné.

L’action est disponible pour les tableaux blancs Android Classic de tous les fabricants, à l’exception de CTOUCH, Newline, Prowise et SMART. Pour les tableaux blancs Prowise, l’action Installer la mise à jour de Prowise → est disponible à la place.

Dans la boîte de dialogue, seule la version est sélectionnée dans la liste Les mises à jour suivantes sont disponibles pour cet appareil :. Seules les mises à jour signalées comme disponibles par l’appareil lui-même peuvent être sélectionnées. Si l’appareil ne signale aucune mise à jour, la liste reste vide et l’action ne peut pas être exécutée.

Si des configurations qui retardent les mises à jour du système d’exploitation sont actives, l’appareil installe la dernière version disponible pour lui, qui peut être plus ancienne que la version sélectionnée. Si un code d’accès est activé, il doit être saisi avant que la mise à jour puisse commencer.

Pour la version 26.4.0

Déverrouiller l'appareil

L’action Déverrouiller l’appareil permet de déverrouiller l’appareil à distance sans saisir de code PIN. Elle sert généralement à lever un verrouillage effectué par l’action Verrouiller complètement l’appareil →.

L’action n’est disponible que pour les tableaux blancs CTOUCH, i3-Technologies et Newline. Tous les autres appareils sont déverrouillés directement sur l’appareil avec le mot de passe.

Installer la mise à jour de Prowise

L’action Installer la mise à jour de Prowise (titre de la boîte de dialogue : Mise à jour du système d’exploitation Prowise) permet d’installer la dernière mise à jour sur un tableau blanc interactif Prowise → sélectionné. L’action n’est disponible que pour les tableaux blancs Prowise et y remplace l’action Installer une mise à jour.

Pour la version 26.4.0

Une date et une heure peuvent être sélectionnées en option pour la mise à jour (champ Mise à jour sur). Si le champ reste vide, la mise à jour est lancée immédiatement.

Si l’action est envoyée à nouveau alors qu’une action antérieure du même type n’a pas encore été transmise à l’appareil, l’action antérieure est annulée. L’action peut également être configurée comme action d’un groupe d’appareils.

Installer l'application à partir du magasin d'applications Prowise

L’action Installer l’application à partir du magasin d’applications Prowise installe une application depuis le Prowise App Store sur un tableau blanc Prowise →. L’action n’est disponible que pour les tableaux blancs Prowise et y remplace l’action Déployer l’application Relution Store.

L’application est identifiée par son nom de paquet. La source est choisie à la première étape, puis une seule application à la deuxième étape :

- Appli Relution App Store : sélection d’une application Android native dans le Relution App Store.
- Appli Google Play Store : recherche dans le Google Play Store public.
- Nom interne d’une application : saisie manuelle du nom de paquet dans le champ Nom interne.

Relution transmet uniquement le nom de paquet au Relution Companion sur le tableau blanc. Le tableau blanc installe ensuite l’application correspondante depuis le Prowise App Store, si elle y est disponible. Si l’application n’existe pas dans le Prowise App Store, elle n’est pas installée.

Pour la version 26.4.0

EShare

EShare est un logiciel multiplateforme permettant le partage d’écran sans fil et la collaboration entre différents appareils. Il permet notamment la duplication d’écran, le transfert de fichiers et le contrôle à distance.

La politique EShare permet de configurer et de gérer les paramètres d’EShare sur les tableaux blancs interactifs. Dans le portail, elle est signalée pour les tableaux blancs de Dahua →, heinekingmedia → et wende.interaktiv →.

Pour la version 26.4.0

Pour la version 26.4.0

Configuration

Les options suivantes sont disponibles pour configurer EShare:

- Nom de l’appareil: définir le nom de l’appareil. Le paramètre fictif `${device.name}` est prédéfini, de sorte que le nom de l’appareil dans Relution est utilisé tant que la valeur n’est

pas modifiée.

- Mode de connexion: choisir Nom de l’appareil, Code Pin (6 chiffres) ou Lettres (8 caractères). Avec Code Pin (6 chiffres) et Lettres (8 caractères), les options suivantes sont également disponibles :
  - Mot de passe: champ obligatoire ; sans mot de passe, la configuration ne peut pas être enregistrée.
  - Intervalle de rafraîchissement du mot de passe: Désactiver, 10 minutes, 30 minutes, 1 heure ou 1 jour.
  - Fenêtre flottante du mot de passe
- Écrans multiples: désactiver ou sélectionner 2, 4, 6 ou 9 écrans.
- Afficher le nom de l’appareil: activer/désactiver l’affichage du nom de l’appareil.
- Activer le plein écran automatique
- Activer AirPlay
- Activer DLNA
- Partager l’écran ou le fichier: désactiver le partage d’écran ou de fichier, autoriser tout ou exiger une autorisation.
- Visualisation, contrôle et annotation sans fil: désactiver toutes les options, autoriser toutes les options, autoriser uniquement l’affichage ou exiger une autorisation.
- Bouton flottant du modérateur: choisir l’option d’affichage: désactiver, toujours afficher, uniquement sur l’écran d’accueil ou automatique.

Pour une nouvelle configuration, le mode de connexion Nom de l’appareil est présélectionné, toutes les cases à cocher sont décochées, et Écrans multiples, Partager l’écran ou le fichier, Visualisation, contrôle et annotation sans fil ainsi que Bouton flottant du modérateur sont réglés sur Désactiver.

Si la configuration ne peut pas être appliquée sur l’appareil, la violation de conformité Configuration d’EShare est affichée pour l’appareil.

Pour la version 26.4.0

Hotspot

La politique Hotspot permet de configurer et de gérer à distance les paramètres du point d’accès Wi-Fi sur les appareils. Dans le portail, elle est signalée pour les tableaux blancs de ADVANTouch →, Clevertouch →, heinekingmedia →, i3-Technologies → et Hikvision.

Configuration

Les options suivantes sont disponibles pour configurer le point d’accès Wi-Fi:

- SSID: nom visible du point d’accès Wi-Fi utilisé pour l’identification par d’autres appareils (champ obligatoire).
- Ce réseau est masqué: désactive la diffusion visible du SSID, empêchant ainsi le hotspot d’apparaître dans la liste des réseaux disponibles. Dans le portail, cette option est signalée uniquement pour Clevertouch et ADVANTouch et elle est désactivée par défaut.
- Authentification: Aucun (réseau ouvert) ou WPA2 (par défaut). ADVANTouch et Clevertouch prennent uniquement en charge WPA2.
- Phrase secrète: mot de passe requis pour accéder au hotspot. Le champ s’affiche uniquement avec WPA2 ; il est alors obligatoire et doit comporter de 8 à 63 caractères.

- Bande de fréquence: la gamme de fréquences du hotspot, 2,4 GHz (par défaut) ou 5 GHz.

Si la configuration ne peut pas être appliquée sur l’appareil, la violation de conformité Configuration du hotspot est affichée pour l’appareil.

Pour la version 26.4.0

Mise à jour OTA prévue

La politique Mise à jour OTA prévue permet d'effectuer automatiquement les mises à jour du micrologiciel des tableaux blancs interactifs en dehors des heures d'utilisation.

La configuration est prise en charge sur les tableaux blancs de Clevertouch →, i3-Technologies → et Newline. Chaque politique peut contenir une configuration de ce type.

Pour la version 26.4.0

Comment ça marche

Le début de la fenêtre de mise à jour est défini dans la section Mises à jour programmées :

- Répète sur : jours de la semaine auxquels la fenêtre de mise à jour commence (sélection multiple, au moins un jour obligatoire). Aucun jour n'est présélectionné dans une nouvelle configuration.
- Heure de début : heure à laquelle la fenêtre de mise à jour commence les jours sélectionnés (par défaut 22:00). L'heure de début s'applique à tous les jours sélectionnés.
- Fuseau horaire : fuseau horaire dans lequel s'applique l'heure de début (par défaut Europe/Paris). C'est ce fuseau horaire qui fait foi, et non l'heure locale de l'appareil ; il convient d'en tenir compte pour les sites répartis sur plusieurs fuseaux horaires.

À l’heure spécifiée, Relution Companion vérifie si une mise à jour du micrologiciel est disponible pour l’appareil. Si une mise à jour est disponible, elle est installée automatiquement et sans intervention de l’utilisateur.

Quand les mises à jour ne sont pas installées

Les mises à jour du micrologiciel ne sont pas installées si l’appareil est éteint à l’heure prévue. Par exemple, si l’appareil n’est pas allumé avant le lendemain matin et que la fenêtre de mise à jour a été manquée, Relution Companion attend la prochaine fenêtre horaire définie pour effectuer la mise à jour. Cela garantit que les mises à jour ne sont effectuées qu’aux heures prévues.

Pour la version 26.4.0

Device Owner (Companion)

La fonction Device Owner pour le Relution Companion offre des possibilités de gestion avancée des appareils Android. Elle comprend les fonctions suivantes :

- Installer et désactiver des applications sans interaction de l'utilisateur (configuration de politique Conformité des applications →).
- Activer le mode kiosque sans interaction de l'utilisateur (configuration de politique Mode kiosque →).
- Action Redémarrer l'appareil →.

Pour les instructions de configuration et de connexion d'Android Debug Bridge, se reporter à : Configuration d'Android Debug Bridge →

Télécharger Relution Companion

Relution Companion →

Pour la version 26.4.0

Installer l'application Relution Companion sur l'appareil

Cela peut être fait manuellement ou via le Android Debug Bridge (ADB).

```
adb install Relution-normal-release.apk
```

Activer le propriétaire de l'appareil après l'installation

```
adb shell dpm set-device-owner com.mwaysolutions.relution/com.mwaysolutions.re
```

Cette commande s'applique au Relution Companion général, dont le nom de paquet est `com.mwaysolutions.relution`. Les variantes du Companion propres à un fabricant utilisent

leur propre nom de paquet (p. ex. `com.mwaysolutions.relution.i3` ou `com.mwaysolutions.relution.advantouch`) ; la commande correspondante figure alors dans l'article du fabricant concerné, par exemple i3-Technologies → ou ADVANTouch →.

Réinscrire l'appareil

L'appareil est ensuite réinscrit dans Relution. Pour cela, une inscription pour la plateforme Android avec le type du fabricant concerné est créée et utilisée dans le Relution Companion sur l'appareil. La procédure est décrite dans la section consacrée à l'inscription de l'article du fabricant concerné, voir Fabricants →.

Pour la version 26.4.0

Configuration d'Android Debug Bridge

Activer le mode développeur sur l’appareil

Ceci peut devoir être demandé au fabricant.

- Ouvrir Paramètres.
- Ouvrir À propos du téléphone (peut varier selon le fabricant).
- Taper 7x sur Numéro de build (active les options pour les développeurs).
- Revenir en arrière et passer à Options pour les développeurs.
- Trouver l’option Débogage USB et l’activer.

Si la politique attribuée à l’appareil contient la configuration Restrictions → avec l’option Refuser le débogage USB activée (présélectionnée pour les nouvelles configurations), le débogage USB peut être bloqué sur l’appareil.

Télécharger et installer Android Debug Bridge (ADB)

Mac →
Windows →
Linux →

Pour la version 26.4.0

Démarrer Android Debug Bridge (ADB)

```
adb start-server
```

Se connecter à l'appareil

```
adb connect <adresse IP>
```

Tout message de confiance affiché par l'appareil doit être confirmé.

Inscrire les appareils EDLA

Avec Relution, il est possible de gérer des tableaux blancs interactifs certifiés EDLA via Android Enterprise.

Inscription

Inscrire l'appareil en tant qu'appareil entièrement géré →. Utiliser la variante par Identifiant DPC → pour l'inscription.

Pour la version 26.4.0

> À partir de Relution 5.33, l'inscription détermine si les applications système préinstallées non essentielles sont désactivées pendant la configuration ou restent activées. Pour cela, l'interrupteur Maintenir les applications système activées est disponible lors de la création de l'inscription sous Options d'inscription, dans la section Conformité. Il est désactivé par défaut. Pour l'inscription des tableaux blancs, cet interrupteur doit être activé.

Relution intègre l'interrupteur exclusivement dans le code QR de l'inscription. L'identifiant DPC ne le contient pas ; lors d'une inscription par identifiant DPC, l'interrupteur n'a donc aucun effet, voir Options d'inscription →. Les applications préinstallées désactivées après l'inscription peuvent être activées ultérieurement, voir Applications préinstallées →.

Extensions EDLA

Pour certains tableaux blancs interactifs, Relution propose des extensions qui complètent la gamme générale de fonctions avec des fonctionnalités spécifiques aux tableaux blancs. Un aperçu de ces extensions est disponible sous Extensions EDLA →.

Plateforme matérielle CVTE

Relution permet de gérer de manière centralisée les tableaux blancs interactifs de la plateforme matérielle CVTE.

Gammes et modèles de produits pris en charge dans la configuration de base

Les fournisseurs et séries de produits suivants sont pris en charge:

- Heinekingmedia DT-75-C10HM

Gammes de produits et modèles pris en charge par Bytello Share

Pour la version 26.4.0

Les fournisseurs et séries de produits suivants prennent en charge la configuration des services de partage d'écran Bytello Share:

- Heinekingmedia DT-75-C10HM

Inscription

L'inscription s'effectue comme décrit dans Inscrire les appareils EDLA →.

Actions prises en charge

Les actions Android Enterprise → sont disponibles, y compris Éteindre l'appareil. Cette action éteint complètement le tableau blanc. Avec Android Enterprise, elle n'est prise en charge que par certains tableaux blancs ; le portail l'identifie par les fabricants pris en charge, dont heinekingmedia (HKM).

Politiques prises en charge

Outre la configuration CVTE OEMConfig, toutes les configurations Android Enterprise sont prises en charge.

Application Relution CVTE OEMConfig

Pour pouvoir utiliser les fonctions supplémentaires des tableaux blancs via Android Enterprise, l'application Relution CVTE OEMConfig doit être installée et configurée sur l'appareil.

Configuration

Créer une politique avec une configuration CVTE OEMConfig pour configurer l'application Relution CVTE OEMConfig.

La configuration installe l'application Relution CVTE OEMConfig sur l'appareil avec le type d'installation Installé de force, la met à jour en priorité élevée et lui accorde les autorisations nécessaires. Les utilisateurs ne peuvent pas supprimer l'application. Une distribution séparée via la configuration Gérer les applications n'est ni nécessaire ni possible : si l'application y figure, la configuration ne peut pas être enregistrée et le portail renvoie à la configuration CVTE OEMConfig.

Pour la version 26.4.0

Des espaces réservés peuvent être utilisés dans les valeurs de la configuration ; le formulaire affiche les espaces réservés disponibles.

L'application transmet en outre des informations supplémentaires sur l'appareil à Relution, par exemple l'adresse IP et MAC, la version du micrologiciel et du système ainsi que l'état d'Ethernet, du point d'accès et de Wake-on-LAN.

Configuration des services de partage d'écran Bytello Share

Ajouter les applications suivantes à la configuration Gérer les applications →:

Nom	Nom interne	Type d'installation
ScreensharePro	com.seewo.screensharepro.server	Pré-installé

Nom	Nom interne	Type d’installation
Bytello ScreensharePro	com.bytello.screensharepro.server	Pré-installé

Options de configuration

L’application Relution CVTE OEMConfig offre les options de configuration suivantes:

Paramètre	Description
Volume	Régler le volume du système (0-100)
Muet	Activer/désactiver la sourdine de la sortie audio
Mode sonore	Sélectionner parmi les modes Standard, Film, Salle de classe, Réunion, Personnalisé
Balance audio	Régler la balance des canaux gauche/droit (0-100)
Basses	Régler les basses fréquences (0-100)
Aigus	Régler les hautes fréquences (0-100)
Luminosité	Régler la luminosité de l’écran (0-100)
Mode image	Standard, Dynamique, Vif, Doux, Personnalisé, Vente au détail
Netteté	Régler la clarté de l’image (0-100)
Contraste	Régler les niveaux de contraste de l’image (0-100)
Teinte	Régler la température de couleur (0-100)
Saturation	Régler l’intensité des couleurs (0-100)
Capteur de lumière automatique	Activer l’adaptation à la lumière ambiante
Filtre de lumière bleue	Réduire la fatigue oculaire dans des conditions de faible luminosité

Paramètre	Description
Activation tactile	Configurer la fonctionnalité de l’écran tactile
Type de barre d’outils	Choisir entre la barre flottante, la barre coulissante ou la barre inférieure du système
Veille automatique	Définir le délai d’inactivité (0-240 minutes)
Veille sans signal	Configurer l’arrêt automatique lorsqu’aucune entrée n’est détectée (0-7200 secondes)
Mode Eye Care	Activer la réduction de la lumière bleue
Réveil sur source	Mise sous tension automatique lorsqu’une entrée est connectée
Wake-on-LAN	Configurer les capacités de réveil réseau
Entrée tactile	Activer/désactiver la fonctionnalité tactile
Verrouillage OEM	Restreindre les modifications non autorisées des paramètres
Ethernet	Gérer la connexion réseau filaire
Point d’accès	Configurer le point d’accès sans fil
Visibilité de l’appareil	Contrôler la découverte du réseau lors du partage
Autorisation requise	Exiger l’autorisation pour les sessions de partage
Chromecast	Activer le protocole de diffusion Google
AirPlay	Activer la duplication d’écran Apple
Miracast	Activer l’affichage sans fil Windows
Webcast	Activer le partage via le navigateur
Démarrage automatique	Lancer le service de partage au démarrage
HID Touch	Activer le contrôle tactile USB
DLNA	Configurer les capacités du serveur multimédia

Paramètre	Description
Nom de l’appareil	Définir un nom de réseau personnalisé
Actualisation du code	Définir la fréquence de mise à jour du code PIN
Taille de la fenêtre	Contrôler la taille du panneau de contrôle flottant
Mises à jour automatiques	Configurer les mises à jour automatiques du micrologiciel
Vérification des mises à jour	Activer les contrôles d’authenticité des mises à jour
Mode débogage	Activer les diagnostics du développeur
Langue	Définir la langue du système (anglais, français, allemand, italien, espagnol, turc)
Calendrier d’alimentation	Créer des calendriers de mise sous/hors tension automatisés avec: récurrence quotidienne/hebdomadaire, paramètres d’heure spécifiques, prise en charge de plusieurs tâches
Alias de source	Renommer les sources d’entrée (HDMI/DP/VGA)
Forcer la source d’entrée	Définir le canal d’entrée au démarrage

Options Bytello Share

L’application Relution CVTE OEMConfig offre également les options de configuration suivantes si Bytello Share est également disponible:

Paramètre	Description
Visibilité du réseau de l’appareil	Activer ou désactiver la visibilité de l’appareil sur le réseau lors du partage.

Paramètre	Description
Autorisation requise	Tous les écrans partagés de l’appareil nécessiteront une autorisation
Activer Chromecast	Activer/désactiver la prise en charge de Chromecast
Activer Airplay	Activer/désactiver la prise en charge d’Airplay
Activer Miracast	Activer/désactiver la prise en charge de Miracast
Activer Webcast	Activer/désactiver la prise en charge de Webcast
Démarrage automatique au démarrage	Démarrer automatiquement le service de partage au démarrage de l’appareil
Commande tactile HID	Activer/désactiver la prise en charge de la commande tactile HID
Activer DLNA	Activer/désactiver la prise en charge DLNA
Nom de l’appareil	Définir le nom de cet appareil
Intervalle de rafraîchissement du code	Définir l’intervalle de rafraîchissement du code (en minutes)
Taille de la fenêtre flottante	Définir la taille de la fenêtre de commande flottante (Normale, Mini, Fermée)
Barre système	Définir la visibilité/l’invisibilité de la barre système.

Newline

Relution permet de gérer de manière centralisée les tableaux blancs interactifs de Newline.

Gammes et modèles de produits pris en charge

- TT-7523QA (Lyra Pro)
- TT-6523QCA+ (Elara Pro)

Inscription

L'inscription s'effectue comme décrit dans Inscrire les appareils EDLA →.

Pour la version 26.4.0

Actions prises en charge

Les actions Android Enterprise → sont disponibles, y compris Éteindre l'appareil. Cette action éteint complètement le tableau blanc. Avec Android Enterprise, elle n'est prise en charge que par certains tableaux blancs ; le portail l'identifie par les fabricants pris en charge, dont Newline.

Application Relution Newline OEMConfig

Pour pouvoir utiliser les fonctions supplémentaires des tableaux blancs via Android Enterprise, l'application Relution Newline OEMConfig doit être installée et configurée sur l'appareil.

Configuration

Créer une politique avec une configuration Newline OEMConfig pour configurer l'application Relution Newline OEMConfig.

La configuration est disponible à partir de Relution 5.34.0.

La configuration installe l’application Relution Newline OEMConfig sur l’appareil avec le type d’installation Installé de force, la met à jour en priorité élevée et lui accorde les autorisations nécessaires. Les utilisateurs ne peuvent pas supprimer l’application. Une distribution séparée via la configuration Gérer les applications n’est ni nécessaire ni possible : si l’application y figure, la configuration ne peut pas être enregistrée et le portail renvoie à la configuration Newline OEMConfig.

Des espaces réservés peuvent être utilisés dans les valeurs de la configuration ; le formulaire affiche les espaces réservés disponibles.

Options de configuration

L’application Relution Newline OEMConfig offre les options de configuration suivantes:

Paramètre	Description
Sortie audio	Définir la sortie audio actuelle
Volume	Définir le volume du système. (0–100)
Muet	Activer/désactiver le mode muet du système.
Réveil sur LAN	Activer ou désactiver le réveil sur LAN
Réveil sur réseau sans fil	Activer ou désactiver le réveil sur réseau sans fil (WoWLAN)
Wi-Fi	Activer ou désactiver la connectivité Wi-Fi.
Ethernet	Activer ou désactiver Ethernet
Point d’accès	Activer ou désactiver le point d’accès
Partage de connexion Ethernet	Activer ou désactiver le partage de connexion Ethernet.
Configuration du proxy	Configurer les paramètres du proxy réseau, notamment les paramètres hôte, port et liste d’exclusion.
Hôte proxy	Nom d’hôte ou adresse IP du serveur proxy

Paramètre	Description
Port proxy	Numéro de port du serveur proxy (1–65535)
Liste d’exclusion du proxy	Liste séparée par des virgules des hôtes à contourner le proxy
Luminosité	Définir la valeur de luminosité. (0-100). Le mode d’image doit être réglé sur CUSTOM/USER.
Mode image	Définir le mode image.
Taille de police	Définir la taille de police.
Source de démarrage	Définir la configuration de la source de démarrage
Commutation automatique de la source	Activer ou désactiver la commutation automatique de la source.
Mise sous tension automatique CEC	Activer ou désactiver la mise sous tension automatique CEC.
Arrêt automatique CEC	Activer ou désactiver l’arrêt automatique CEC.
Type EDID HDMI/DP	Définir la version EDID HDMI/DisplayPort
Réveil de la source du signal	Activer ou désactiver le réveil lors de la détection d’une nouvelle source de signal.
Mode débogage	Activer ou désactiver le mode débogage
Format horaire 24 heures	Activer ou désactiver le format horaire 24 heures
Barre d’outils gauche	Activer ou désactiver la barre d’outils gauche.
Barre d’outils droite	Activer ou désactiver la barre d’outils droite.
Réglages rapides	Activer ou désactiver l’accès aux réglages rapides.
Date/heure de mise sous tension	Configurer l’heure de mise sous tension programmée
Date/heure de mise hors tension	Configurer l’heure de mise hors tension programmée

Paramètre	Description
Durée d’économie d’énergie	Activer pour définir la durée d’économie d’énergie. Désactiver pour ne jamais l’activer.
Durée d’économie d’énergie (minutes)	Durée d’économie d’énergie en minutes. Les valeurs courantes sont 30, 60, 90, 120
Comportement du bouton d’alimentation	Configurer l’action du bouton d’alimentation (veille ou mise hors tension)
Réveil par pression	Activer ou désactiver le réveil de l’écran par pression
Écriture avec protection des yeux	Activer ou désactiver le mode de protection des yeux orienté vers l’écriture
Luminosité adaptative	Activer ou désactiver le réglage automatique de la luminosité pour le confort des yeux
Filtre de lumière bleue	Activer ou désactiver la lumière bleue
Niveau du filtre de lumière bleue	Définir le niveau d’intensité du filtre de lumière bleue (0-100)
Logo de l’appareil	Afficher/masquer le logo du fabricant
Thème de l’interface utilisateur	Choisir entre les variantes de thème Newline Q ou Z
Nettoyage automatique des fichiers	Définir l’intervalle de nettoyage automatique des fichiers
Système d’exploitation Android (avertissement : ne peut être réactivé que dans le menu revendeur)	Activer ou désactiver le système d’exploitation Android (avertissement : ne peut être réactivé que dans le menu revendeur)
Verrouillage USB	Activer ou désactiver le verrouillage du port USB
Verrouillage du menu	Activer ou désactiver l’accès au menu système
Verrouillage des paramètres	Activer ou désactiver la modification des paramètres
Désactiver l’installation d’applications	Activer ou désactiver l’installation d’applications

Paramètre	Description
Verrouillage du bouton d’alimentation avant	Activer ou désactiver la fonctionnalité du bouton d’alimentation avant
Verrouillage des boutons du panneau avant	Activer ou désactiver les boutons du panneau de commande avant
Verrouillage tactile	Activer ou désactiver le verrouillage tactile
Verrouillage tactile de la source du signal	Définir le verrouillage tactile de la source du signal
Verrouillage des paramètres Wi-Fi	Activer ou désactiver les modifications de la configuration Wi-Fi
Verrouillage des paramètres Ethernet	Activer ou désactiver les modifications de la configuration Ethernet
Verrouillage des icônes du lanceur	Activer ou désactiver les modifications des icônes du lanceur
Mot de passe du mode administrateur	Définir le mot de passe du mode administrateur (6 caractères minimum)
Verrouillage du thème et du fond d’écran	Empêcher les modifications des paramètres du thème et du fond d’écran de l’appareil
URL bloquées	Bloquer les URL
OTA local	Activer ou désactiver les mises à jour locales du micrologiciel.
Téléchargement OTA en arrière-plan	Activer ou désactiver les téléchargements OTA en arrière-plan.
Notifications OTA	Activer ou désactiver les notifications de mise à jour OTA.

Applications préinstallées

Pour activer de manière ciblée des applications préinstallées, le nom de package respectif de l'application est nécessaire. Pour obtenir une liste complète de toutes les applications préinstallées qui ne sont plus disponibles après l'inscription dans Android Enterprise, réinitialiser l'appareil aux paramètres d'usine et effectuer le processus complet de configuration de l'appareil sans l'inscrire dans Android Enterprise.

> L'interrupteur Maintenir les applications système activées de l'inscription détermine si les applications système préinstallées non essentielles sont désactivées lors de l'inscription. Relution l'intègre uniquement dans le code QR, pas dans l'identifiant DPC, voir Inscrire les appareils EDLA →.

Une fois l'appareil entièrement configuré et prêt à l'emploi, se connecter à l'appareil via Android Debug Bridge →. Exécuter ensuite la commande suivante pour exporter une liste de tous les packages installés :

```
adb shell cmd package list packages > list1.txt
```

Pour la version 26.4.0

Réinitialiser ensuite l'appareil aux paramètres d'usine et l'inscrire dans Android Enterprise.

Après l'inscription réussie, se connecter à nouveau à l'appareil via ADB et exécuter la commande suivante :

```
adb shell cmd package list packages > list2.txt
```

Il est maintenant possible de comparer les deux fichiers.

Toutes les applications qui apparaissent dans le fichier `list1.txt` mais qui sont absentes du fichier `list2.txt` doivent être ajoutées avec le type d'installation Pré-installé dans la configuration Gérer les applications.

Dans la configuration Gérer les applications, Ajouter ouvre la boîte de dialogue de sélection d'une application. À l'étape La source, sélectionner l'option Ajouter une application manuellement. À

l’étape suivante, indiquer Nom (nom d’affichage de l’application) et Nom interne (nom de package). Le nom interne correspond à l’entrée du fichier `list1.txt` à ajouter – mais sans le préfixe `package:`. Exemple : Si l’entrée `package:io.relution.files` doit être ajoutée, indiquer comme nom interne `io.relution.files`.

Les applications ajoutées manuellement apparaissent d’abord avec le type d’installation Installé de force. Dans la colonne Type d’installation, sélectionner Pré-installé.

Pour la version 26.4.0

Inscription manuelle

À partir de la version 5 de Relution, les appareils Windows 10/11 peuvent être inscrits et gérés sans compte Microsoft ou `Azure AD`. L'inscription nécessite un utilisateur local. Cet utilisateur doit disposer de droits administratifs et ne doit pas être supprimé après l'inscription.

Les appareils doivent être dotés d'un identifiant unique. Lors de l'inscription, Relution identifie un appareil par son identifiant d'appareil Windows et traite une inscription avec un identifiant déjà connu comme une réinscription du même appareil. En particulier lors d'une préconfiguration via une image, il faut donc veiller à ce que les appareils puissent être différenciés par le MDM.

Outre l'inscription manuelle, les appareils Windows peuvent être inscrits via Autopilot → et via l'Inscription en bloc → avec un paquet de provisionnement.

> L'édition Windows 10/11 Home présente diverses restrictions en matière de gestion. Toutes les fonctionnalités de gestion ne sont pas disponibles. Restrictions de l'édition Windows Home →

Pour la version 26.4.0

Versions Windows prises en charge

- Windows 10/11 Home
- Windows 10/11 Professional
- Windows 10/11 Education
- Windows 10/11 Enterprise

Versions de Windows non prises en charge

- Windows 10/11 Enterprise LTSC
- Windows 10/11 IoT Enterprise
- Windows 10/11 IoT Enterprise LTSC

Inscrire manuellement des appareils Windows

Pour inscrire un appareil Windows 10/11, une nouvelle inscription doit être créée dans Relution. L'inscription est créée sous `Appareils` → `Inscriptions` via Ajouter ; l'élément de menu

n’est pas disponible dans l’organisation globale. Dans la section Matériel, Windows est sélectionné sous Plateforme et la Propriété est définie. En option, un nom est indiqué sous Nom de l’appareil (lettres, chiffres et traits d’union uniquement) ; si le champ reste vide, le nom est généré automatiquement. Un utilisateur peut être sélectionné sous Affectation, et une date d’expiration via Valable jusqu’au.

Pour la version 26.4.0

Pour la version 26.4.0

Ensuite, l’inscription est listée sous Inscriptions – avec le statut Envoyé si les informations d’inscription ont été envoyées par e-mail ou SMS, sinon avec le statut Créé. Une fois un appareil

inscrit, une inscription qui n’est pas à usages multiples passe au statut Inscrit et ne peut plus être réutilisée.

Obtenir des informations sur l’inscription

Lors de la création de l’inscription, les informations nécessaires peuvent être envoyées dans le domaine Notification par e-mail, par SMS ou par les deux canaux. Le canal concerné doit être activé sous `Paramètres` → `Les notifications`. L’envoi par e-mail nécessite qu’un utilisateur disposant d’une adresse e-mail soit affecté à l’inscription ; l’envoi par SMS nécessite un numéro de téléphone. Par exemple, les utilisateurs affectés aux appareils à inscrire reçoivent l’e-mail suivant avec toutes les informations pertinentes :

Pour la version 26.4.0

Le lien d’inscription contenu dans l’e-mail permet d’accéder automatiquement à la procédure d’inscription sur l’appareil Windows 10/11.

Pour la version 26.4.0

Effectuer l’inscription sur les appareils Windows 10/11

1. Ouvrir le lien affiché dans l’inscription dans le navigateur de l’appareil à inscrire.

Pour la version 26.4.0

2. Cliquer sur Suivant, puis sur Inscription. Le navigateur va maintenant essayer d’ouvrir l’application de configuration. Cliquer sur Ouvrir.

3. Confirmer toutes les autres boîtes de dialogue. L’appareil est maintenant inscrit et peut être géré avec Relution.

Inscription multiple d’appareils Windows 10/11

Relution prend en charge l’inscription en masse, un moyen efficace d’inscrire un grand nombre d’appareils Windows 10/11 à gérer par un serveur MDM sans avoir besoin de réimager les

appareils.

Pour cela, l’option Inscription à usages multiples est activée lors de la création de l’inscription, dans la section Expiration du domaine Options d’inscription. L’inscription peut alors être utilisée pour plusieurs appareils. L’option seule n’effectue toutefois pas d’inscription en masse : le code d’inscription généré est ensuite intégré dans un paquet de provisionnement (`ppkg`) à l’aide de Windows Configuration Designer. L’inscription en masse est disponible pour Windows 10/11 Professional, Enterprise et Education. Inscription en bloc →

L’action Inscription en bloc du menu contextuel de la liste des inscriptions crée en revanche plusieurs inscriptions individuelles pour des utilisateurs sélectionnés en une seule fois et n’est pas prévue à cet effet.

Pour la version 26.4.0

Pour plus de détails, consulter la documentation Microsoft sur l’inscription en masse :

Windows Provisioning Tool →

> Le compte sur l'appareil avec lequel l'appareil a été inscrit ne doit pas être supprimé.

Inscription en bloc

Lors de l'inscription et de la configuration d'un grand nombre d'appareils Windows 10/11, un processus d'inscription manuel représente une charge de travail non négligeable. L'inscription en masse de Windows (`Windows Bulk Enrollment`) offre un moyen efficace d'inscrire rapidement un grand nombre d'appareils Windows 10/11 sans avoir à compléter l'inscription par le biais des paramètres du système sur chaque appareil individuel. L'inscription en masse d'appareils Windows 10/11 est disponible pour les versions Professional, Enterprise et Education. L'inscription d'appareils individuels est décrite sous Inscription manuelle →.

Windows Configuration Designer (WCD)

L'inscription en masse de Windows nécessite l'outil `Windows Configuration Designer (WCD)`, qui peut être téléchargé à partir du Microsoft Store →. L'outil WCD peut également être téléchargé via le Windows Assessment and Deployment Kit (ADK) → et est alors également disponible dans d'autres langues.

L'outil WCD peut être utilisé pour générer les paquets de provisionnement (`provisioning packages`) nécessaires à l'exécution des inscriptions de masse. Le format de fichier des paquets de provisionnement est un fichier `ppkg`. Il s'agit d'un conteneur pour une collection de paramètres de configuration. L'inscription en masse ne se fait pas avec un compte `Azure AD` ou `Windows Autopilot`. L'inscription se fait via un fichier `ppkg`, qui peut être exécuté avec un compte administrateur après la mise en service de l'appareil. Le fichier `ppkg` peut également être incorporé dans une image Windows ; la procédure est décrite dans le guide suivant (en allemand). Windows Bulk ppkg Image →

> Le ppkg ne doit pas être utilisé comme un auto/unattend.xml sur une clé USB lors de l'installation du système d'exploitation. Lors de l'installation du système d'exploitation, un administrateur temporaire est utilisé, et ce dernier ainsi que l'inscription seraient supprimés au bout d'un certain temps.

Préparation de l'inscription dans Relution

Pour l'inscription en masse d'appareils Windows 10/11, une inscription manuelle doit être créée dans Relution. Elle est créée sous `Appareils` → `Inscriptions` via Ajouter. Dans la section

Pour la version 26.4.0

Matériel, Windows est sélectionné sous Plateforme. Les codes d’inscription d’autres plateformes sont refusés lors de l’inscription Windows.

Pour la version 26.4.0

Les paramètres de l’inscription s’appliquent à tous les appareils inscrits avec le paquet de provisionnement. Si un utilisateur est sélectionné sous Affectation, tous les appareils sont affectés à cet utilisateur ; sans utilisateur, les appareils ne sont affectés à aucun utilisateur.

Dans le domaine Options d’inscription, l’option Inscription à usages multiples est activée dans la section Expiration. C’est la seule façon de pouvoir utiliser l’inscription créée pour plusieurs appareils Windows 10/11. L’option ne peut plus être modifiée après la création de l’inscription. Une date d’expiration peut être définie en option via Valable jusqu’au.

Pour la version 26.4.0

Après l’enregistrement, le Code d’inscription est affiché dans le domaine Informations sur l’inscription de l’inscription avec un bouton de copie ; dans la liste des inscriptions, il figure dans la colonne Code d’inscription. Il est nécessaire dans la suite du processus lors de la création du paquet de provisionnement via l’outil WCD.

Le code d'inscription est intégré de manière fixe dans le paquet de provisionnement. Une fois la date indiquée sous Valable jusqu'au dépassée, les inscriptions avec ce paquet échouent jusqu'à ce que l'inscription soit prolongée dans la liste des inscriptions via l'action Prolonger les inscriptions. Si l'inscription est supprimée, le paquet de provisionnement ne peut plus être utilisé ; il doit alors être recréé avec le code d'inscription d'une nouvelle inscription.

L'action Inscription en bloc du menu contextuel de la liste des inscriptions crée en revanche plusieurs inscriptions individuelles pour des utilisateurs sélectionnés et n'est pas nécessaire pour cette procédure.

Créer des paquets de provisionnement avec Windows Configuration Designer (WCD)

Les étapes suivantes sont effectuées après le téléchargement et l'installation de l'outil WCD pour créer un paquet de provisionnement :

1. Dans l'écran d'accueil, sélectionner la tuile Advanced provisioning.

Pour la version 26.4.0

2. Spécifier un nom de projet et cliquer sur Next.

3. Sélectionner All Windows Desktop Editions et cliquer sur Next.

4. Sauter l’option Import a provisioning package (optional) et confirmer en cliquant sur Finish.

5. Développer l’élément de menu Runtime Settings puis Workplace dans la zone de navigation gauche et cliquer sur Enrollments.
6. Sous Enrollments, saisir et ajouter un UPN au format d’une adresse e-mail. Relution n’évalue pas cette valeur lors de l’inscription. L’organisation et l’affectation de l’utilisateur résultent de l’inscription dans Relution dont le code d’inscription est saisi plus bas comme `Secret`.

Pour la version 26.4.0

Pour la version 26.4.0

7. Développer la nouvelle entrée avec l'UPN dans le volet de navigation gauche et entrer les informations suivantes pour les paramètres restants :
    - `AuthPolicy` — sélectionner `OnPremise`.
    - `DiscoveryServiceFullUrl` — le domaine correspondant au serveur Relution utilisé.
    - `EnrollmentServiceFullUrl` — facultatif.
    - `PolicyServiceFullUrl` — facultatif.
    - `Secret` — le code d'inscription de Relution.

8. Après avoir saisi tous les paramètres, sélectionner `File` → `Save` dans le menu principal.
9. Ensuite, sélectionner `Export` → `Provisioning package` dans le menu principal.

10. Dans la boîte de dialogue suivante, les valeurs du paquet doivent être spécifiées et l'emplacement de la sortie du paquet doit être choisi. Il faut ensuite cliquer sur Create.

Pour la version 26.4.0

Pour la version 26.4.0

Le paquet de provisionnement doit être protégé (chiffré et/ou signé). Cela fournit une couche de protection supplémentaire en cas de perte d’une clé USB ou d’une carte SD. Le chiffrement

protège contre l’accès non autorisé au fichier `ppkg`.

Pour la version 26.4.0

Pour la version 26.4.0

Appliquer les paquets de provisionnement aux appareils Windows 10/11

Il suffit d'ouvrir le fichier `.ppkg` sur l'appareil par un double-clic et de confirmer les boîtes de dialogue. L'appareil est ensuite inscrit automatiquement. Là aussi, l'utilisateur a besoin de droits d'administrateur pour effectuer l'inscription.

Vérification du paquet de provisionnement sur les appareils Windows 10/11 inscrits

Dans les paramètres Windows sous `Access work or school`, la connexion au serveur Relution MDM est visible.

> Le compte utilisé pour inscrire l'appareil ne doit pas être supprimé de l'appareil.

Autopilot

Windows Autopilot est une offre de Microsoft basée sur le cloud qui automatise la configuration de nouveaux appareils Windows 10/11 afin de les préparer à une utilisation en production. Les périphériques Windows 10/11 n'ont pas besoin d'être réinstallés, `Windows Autopilot` utilise l'`image` existante sur les périphériques. Relution supporte l'enrôlement automatique via `Windows Autopilot` et donc les périphériques Windows 10/11 peuvent être rapidement et facilement inventoriés dans Relution via ce chemin.

Conditions requises pour l'utilisation de Windows Autopilot

> Actuellement possible uniquement en utilisant un serveur Relution propre

`Windows Autopilot` peut être utilisé avec Windows 10/11 Professionnel, Entreprise ou Éducation à partir de la version 1709. Son utilisation nécessite un environnement `Microsoft Entra ID`, une licence `Microsoft Entra ID P1 ou P2` ainsi qu'une licence `Microsoft Intune Plan 1`. Pour la configuration dans Microsoft Entra, les utilisateurs doivent disposer de droits d'administrateur, par exemple le rôle `Administrateur général`. Selon la documentation Microsoft, la licence `Microsoft Intune Plan 1` ne devrait pas être nécessaire ; cependant, il s'est avéré qu'Intune n'est pas utilisable sans elle, et c'est uniquement pour cela qu'elle est requise.

Pour la version 26.4.0

Une connexion Internet est impérativement requise lors de la mise en service des appareils Windows 10/11 afin que l'enregistrement et la configuration automatiques puissent être effectués.

Conditions de licence →

Comment cela fonctionne lors du démarrage des appareils Windows 10/11

Lors du démarrage de l'expérience `Out Of The Box Experience` (OOBE) des appareils Windows 10/11, s'il y a une connexion réseau existante, le système détecte automatiquement qu'elle doit être configurée via `Windows Autopilot`. Les appareils soumettent leur identifiant à Microsoft et vérifient s'il a été enregistré dans `Autopilot` pour un environnement `Microsoft Entra ID`. Ensuite, l'utilisateur doit se connecter à la page de connexion de Microsoft avec ses

informations d'identification. La connexion l'inscrira dans Relution et créera un compte utilisateur pour l'utilisateur `Microsoft Entra ID` sur les appareils.

Avantages de Windows Autopilot

Le but de `Windows Autopilot` est d'éviter la tâche fastidieuse de charger individuellement les nouveaux appareils Windows 10/11 avec une `image` créée en interne. Au lieu de cela, les appareils devraient se transformer en appareils préconfigurés de la manière la plus indépendante possible. Cela minimise l'effort requis pour la création de l'image et réduit le temps nécessaire à l'enregistrement physique et à l'approvisionnement des appareils. Microsoft Entra n'a besoin d'être configuré qu'une seule fois pour cela, et l'inscription automatique fonctionne jusqu'à ce que la date de validité définie de la `clé secrète client` expire (voir Lier Microsoft Entra ID →).

Entra Join

Contrairement à `Windows Autopilot`, `Entra Join` ne sert pas à la configuration initiale automatisée d'un appareil, mais à la connexion de l'appareil à l'environnement de l'entreprise. `Windows Autopilot` permet de provisionner et de configurer automatiquement de nouveaux appareils, tandis que `Entra Join` associe l'appareil à l'utilisateur `Microsoft Entra ID`.

Pour la version 26.4.0

Cette alternative à Windows Autopilot, liée à l'utilisateur, permet aux utilisateurs Entra de l'organisation d'enrôler n'importe quel appareil Windows. Pour cela, l'appareil est joint à Entra ID via `Paramètres` → `Comptes` → `Accès Professionnel ou scolaire` → `Connecter` → `Joindre cet appareil à Microsoft Entra ID`, puis la connexion s'effectue avec les identifiants Microsoft. Si les identifiants sont saisis directement dans la boîte de dialogue Connecter, l'appareil est uniquement inscrit dans Entra ID (sans y être joint). Relution ne prend pas en charge ce processus et l'interrompt avec un message d'erreur.

Ajout de l'application MDM dans Entra

L'application MDM est créée dans le cadre de la liaison de Relution avec Entra ID → : sous `Paramètres` → `Gestion des utilisateurs` → `Entra ID`, la première étape Créer une application de l'assistant Relution fournit les informations nécessaires. La liaison se poursuit ensuite à l'étape ID des applications avec l'ID d'application et l'ID de répertoire de cette application.

Il est possible d’utiliser l’application MDM existante dans Microsoft Entra ou d’en créer une nouvelle et de la configurer entièrement avec les informations de l’assistant Relution.

Pour la version 26.4.0

Le domaine du serveur Relution correspondant est ajouté dans `Microsoft Entra ID` sous `Noms de domaine personnalisés`. Cette opération peut prendre un certain temps. Pour plus d’informations, voir la documentation Microsoft.

Documentation Microsoft →

Sous `Mobilité (MDM et MAM)`, l'application MDM souhaitée est ensuite ajoutée et activée :

Pour la version 26.4.0

1. Sélectionner la tuile `On-Premises MDM Application` en bas à droite.
2. Attribuer un nom.
3. Cliquer sur `Add`.

La nouvelle application MDM est maintenant configurée avec les informations de l'assistant Relution :

1. Pour `MDM user scope`, sélectionner le paramètre souhaité.
2. Saisir l'URL des `Conditions d'utilisation MDM` de Relution :

   ```
   https://serverurl/api/device/v1/windows/termsOfUse
   ```

   Microsoft interroge cette URL avant chaque inscription. Aucune page web n'est ouverte.

3. Saisir l'URL de découverte MDM (`MDM discovery URL`) :

   ```
   https://serverurl/api/device/v1/windows/discover
   ```

4. Cliquer sur `Enregistrer`.

pour la version 26.4.0

Vérification des paramètres par défaut d’Entra et finalisation de l’installation

Après avoir lié Entra ID à Relution →, il convient de vérifier si les éléments suivants ont été configurés sous `Devices` → `Device Settings` afin de permettre Entra Join. Cette étape peut être ignorée pour Windows Autopilot.

- Tous les utilisateurs sont autorisés à joindre des appareils à `Microsoft Entra ID`.
- Tous les utilisateurs sont autorisés à inscrire leurs appareils dans `Microsoft Entra ID`.
- Le nombre maximum d’appareils par utilisateur doit être respecté.

Pour la version 26.4.0

Ajout de périphériques Windows 10/11

Ces étapes remplacent les étapes précédemment requises dans le Microsoft Store for Business.

Les nouveaux appareils peuvent être achetés et enregistrés par l'intermédiaire d'un partenaire. De cette manière, les appareils sont automatiquement enregistrés dans le portail Intune et dans `Microsoft Entra ID` et ne doivent pas être saisis manuellement.

Les appareils déjà mis en service peuvent être ajoutés manuellement. Un fichier `CSV` est nécessaire pour cela ; il est généré sur les appareils à l'aide d'un script PowerShell. Le fichier CSV est ensuite téléversé dans le portail Intune → et l'appareil peut ensuite être réinitialisé.

Le fichier peut être créé avec ce script Powershell :

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls1
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 doit être exécuté en tant qu'administrateur.

Le fichier doit ensuite être téléversé sous `Devices` → rechercher `Enrollment` et sélectionner le résultat → faire défiler vers le bas → `Devices` → `Import`.

Les appareils apparaissent ensuite dans la liste des appareils et doivent être associés à un profil configuré.

> Si l'application Entra ID a été créée après le 1er juillet 2026, une adaptation supplémentaire peut être nécessaire lorsque les appareils affichent pendant l'OOBE une erreur indiquant qu'aucune connexion à l'URL des conditions d'utilisation MDM ne peut être établie. Dans ce cas, l'entrée `requestedAccessTokenVersion` du manifeste de l'application est définie sur `null` (`"requestedAccessTokenVersion": null,`).

Préparation de l’Out Of The Box Experience (OOBE) chez Microsoft

Pour la version 26.4.0

Un profil doit maintenant être créé.

Pour ce faire, revenir à l’outil de recherche de fonctions. Cliquer sur `Devices` à gauche → entrer `Enrollment` dans la recherche → faire défiler la liste jusqu’en bas à droite → cliquer sur `Deployment profiles`.

1. Cliquer sur `Créer un profil`.
2. Sélectionner `Windows PC`.
3. Saisir un nom.
4. Cliquer sur `Suivant`.
5. Cliquer sur `Suivant`.
6. Sélectionner `Ajouter des groupes` ou `Ajouter tous les appareils`.
7. Cliquer sur `Suivant`.
8. Cliquer sur `Créer`.

Les appareils sont maintenant connectés au profil.

Synchroniser les appareils Windows 10/11 stockés dans Relution

Sous `Appareils` → `Inscriptions automatiques`, les appareils Windows 10/11 sont ajoutés à Relution via le bouton Synchroniser les appareils. Pour cela, l'option Synchroniser les appareils du pilote automatique (synchronisation des appareils Windows Autopilot) doit être activée dans la liaison Entra ID (étape Services de l'assistant Relution). Les périphériques ne doivent pas être enrôlés pour le moment.

La même étape contient l'option Activer l'inscription au pilote automatique (inscription Windows Autopilot), qui doit rester activée pour Windows Autopilot. Pour une nouvelle liaison, les deux options sont activées par défaut.

En outre, Relution synchronise automatiquement les appareils Autopilot, par défaut toutes les 24 heures. Les appareils qui ne sont plus enregistrés dans Windows Autopilot sont alors retirés des inscriptions automatiques.

Uniquement lorsque les périphériques Windows 10/11 apparaissent dans l'aperçu, un enrôlement automatique via Windows Autopilot peut être effectué.

Enrôlement automatique des appareils Windows 10/11 dans Relution

Pour la version 26.4.0

Après avoir réinitialisé les appareils ou lors du démarrage initial, la connexion réseau est établie dans l'OOBE. Une fois cela fait, les appareils communiquent avec Microsoft et téléchargent le profil `Autopilot`.

L'écran de connexion au compte Microsoft apparaît alors. Une fois que les utilisateurs ont saisi leurs informations d'identification, la communication avec Relution s'établit. Le point de terminaison des conditions d'utilisation est appelé en premier, puis l'inscription à Relution a lieu.

L'enrôlement nécessite qu'il existe dans Relution exactement un utilisateur dont l'adresse e-mail correspond au nom de connexion Entra (UPN), ainsi qu'une inscription automatique pour l'appareil. Si un utilisateur est attribué à l'inscription automatique, seul cet utilisateur peut effectuer l'enrôlement. Ensuite, les appareils Windows 10/11 apparaissent dans l'inventaire des appareils de l'organisation de cet utilisateur et peuvent être configurés davantage par le biais de configurations et d'actions de stratégie Windows.

Si un appareil enrôlé via Windows Autopilot est supprimé dans Relution, il peut être enrôlé à nouveau via la même inscription automatique, même s'il se trouve encore dans la Poubelle.

Ne pas supprimer le compte de l'appareil avec lequel l'appareil a été enregistré.

Pour la version 26.4.0

Actions disponibles

Relution permet aux administrateurs informatiques d'exécuter à distance de nombreuses actions sur les appareils Windows. Ces fonctions facilitent la gestion centralisée, renforcent la sécurité et simplifient le déploiement ainsi que le dépannage en entreprise ou dans l'enseignement. Les actions peuvent être appliquées de manière ciblée à un seul appareil ou, via la sélection multiple dans la liste des appareils, à plusieurs appareils à la fois. Elles peuvent en outre être déclenchées par événement ou de manière planifiée via l'appartenance à des groupes d'appareils : Actions de groupes d'appareils →

La boîte de dialogue des actions s'ouvre sous `Appareils` → `Inventaire` via Appliquer l'action, soit pour les appareils sélectionnés dans la liste, soit dans la vue détaillée d'un appareil. Les actions d'appareil actuellement prises en charge pour les appareils Windows dans Relution sont listées ci-dessous :

Actions disponibles

la version 26.4.0

Action	Description
Supprimer l'application	Fonction : désinstallation des applications sélectionnées de l'appareil. Les applications MSI, EXE et WinGet du Relution Store peuvent être supprimées. Selon l'indication de la boîte de dialogue, la désinstallation ne concerne que l'utilisateur actuellement géré ; les autres utilisateurs peuvent toujours voir et utiliser les applications. Cas d'usage : suppression d'applications obsolètes ou indésirables des appareils Windows gérés de l'entreprise. Prérequis : Relution Companion ; Windows 10 version 1511 ou ultérieure, non disponible pour Windows Home.
Ajouter des comptes	Fonction : ajout de nouveaux comptes d'utilisateurs locaux à l'appareil. Pour chaque compte, un Nom d'utilisateur et un Mot de passe sont indiqués ; l'option Administrateur accorde des droits d'administrateur au compte. Si le mot de passe ne répond pas aux exigences de complexité définies sur l'appareil, le compte n'est pas créé. Cas d'usage : création de profils utilisateurs supplémentaires, par exemple pour des utilisateurs changeants dans les établissements d'enseignement

Action	Description
	ou les entreprises. Prérequis : Windows 10 version 1803 ou ultérieure, non disponible pour Windows Home.
Activer Bitlocker	Fonction : active BitLocker sur un ou plusieurs lecteurs et lance le chiffrement. Pour chaque lecteur, la lettre de lecteur (par exemple `C:`) et le Protecteur sont indiqués : mot de passe de récupération ou TPM (uniquement pour le lecteur du système d'exploitation). Avec Espace utilisé uniquement, seul l'espace occupé est chiffré au lieu de l'ensemble du lecteur. Cas d'usage : protection des données sensibles par le chiffrement des lecteurs. Information complémentaire : si le mot de passe de récupération est choisi comme protecteur, il est généré automatiquement et enregistré dans les détails de l'appareil dans Relution. Prérequis : Relution Companion.
Désactiver Bitlocker	Fonction : désactive BitLocker (chiffrement) sur un ou plusieurs lecteurs. Cas d'usage : supprime la protection de l'appareil en déchiffrant les lecteurs indiqués. Prérequis : Relution Companion.
Effacer l'appareil	Fonction : réinitialisation de l'appareil aux paramètres d'usine et suppression de toutes les données. Cas d'usage : réinstallation d'un appareil avant sa remise ou en cas de problème. Attention : cette opération supprime toutes les données de manière irréversible ! Prérequis : Windows 10 version 1709 ou ultérieure, également pour Windows Home.
Redémarrer l'appareil	Fonction : redémarre l'appareil. Cas d'usage : prise en compte des modifications après des installations ou des configurations, résolution de problèmes.
Localiser l'appareil	Fonction : détermine la position actuelle de l'appareil. Cas d'usage : recherche d'appareils perdus ou volés. Remarque : une connexion Internet active et des services de localisation activés sont nécessaires.

Action	Description
Scanner l'appareil	Fonction : lance une analyse de sécurité de l'appareil avec Microsoft Defender intégré afin de détecter les logiciels malveillants et les menaces. Le Type de balayage est soit Balayage rapide, soit Balayage complet. Cas d'usage : sécurité des appareils de l'entreprise, détection et élimination des menaces potentielles, contrôle du respect des politiques de sécurité. Remarque : Microsoft Defender est le logiciel antivirus intégré à Windows. Prérequis : Windows 10 version 1809 ou ultérieure, également pour Windows Home.
Actualiser les informations sur l'appareil	Fonction : actualisation des informations sur l'appareil enregistrées dans Relution. Cas d'usage : informations à jour sur l'appareil dans Relution.
Déployer Office 365	Fonction : installation d'Office 365 for Business sur l'appareil. Avec Installer la configuration d'Office 365, un fichier Configuration XML créé dans le centre d'administration des applications Microsoft 365 (`config.office.com`) est chargé. L'effacement des données d'installation d'Office supprime les données d'installation sur l'appareil afin qu'une installation échouée puisse être relancée ; la suite Office installée peut alors être désinstallée en option, sans perte de fichiers. Cas d'usage : déploiement simple d'Office 365 sur les appareils de l'entreprise. Prérequis : Windows 10 version 1703 ou ultérieure, non disponible pour Windows Home.
Réinitialiser le mot de passe (Windows)	Fonction : définit un nouveau mot de passe pour un compte d'utilisateur local de l'appareil. Le nom d'utilisateur et le nouveau mot de passe sont indiqués. Cas d'usage : assistance en cas de mot de passe oublié ou bloqué. Prérequis : Relution Companion.
Exécuter le script PowerShell	Fonction : exécution d'un script PowerShell géré dans Relution sur l'appareil. En option, des Arguments de la ligne de commande, des variables d'environnement et un Délai d'attente (en minutes) sont définis. Cas d'usage : automatisation de tâches et de configurations complexes. Remarque : des connaissances en PowerShell sont nécessaires. Prérequis : Relution Companion ; Windows 10 version 1511 ou ultérieure, non disponible pour Windows Home.

Action	Description
Déployer l’application Relution Store	Fonction : installation d’une application du Relution Store sur l’appareil. Les types disponibles sont Déployer l’application Microsoft Store, Installer l’application MSI, Installer l’exe et Déployer l’application winget ; chaque type nécessite sa propre autorisation. Les applications sont installées pour l’ensemble du système, à l’exception des applications WinGet, qui sont installées pour l’utilisateur connecté. Cas d’usage : distribution simple d’applications d’entreprise sur les appareils Windows. Prérequis : Windows 10 version 1511 ou ultérieure, non disponible pour Windows Home. Les applications MSI, EXE et WinGet nécessitent le Relution Companion.

Prérequis

Plusieurs actions sont exécutées exclusivement par le Relution Companion pour Windows → : Supprimer l’application, Activer Bitlocker, Désactiver Bitlocker, Réinitialiser le mot de passe (Windows), Exécuter le script PowerShell ainsi que le déploiement d’applications MSI, EXE et WinGet via Déployer l’application Relution Store.

Certaines actions nécessitent une version et une édition minimales de Windows. La boîte de dialogue des actions signale les éditions prises en charge par des badges. Sous Windows Home, Supprimer l’application, Ajouter des comptes, Déployer Office 365, Exécuter le script PowerShell et Déployer l’application Relution Store ne sont pas disponibles : Limites de Windows Home →

Pour la version 26.4.0

Configurations disponibles

Une politique est un ensemble d'une ou plusieurs configurations. Chaque politique peut être appliquée à un ou plusieurs appareils en même temps. En outre, une ou plusieurs politiques peuvent être associées à chaque appareil.

Configurations disponibles

Configuration	Description
Antivirus	Gestion des paramètres antivirus
Bitlocker →	Configuration du chiffrement des disques (Enterprise et Education à partir de Windows 10 version 1703, Pro à partir de la version 1809, non disponible pour Windows Home)
BranchCache	Configuration de la mise en cache du contenu BranchCache (à partir de Windows 10 version 2004, non disponible pour Windows Home)
Certificat →	Sélection d'un certificat à installer par défaut sur l'appareil
Code d'accès →	Gestion des politiques de mot de passe
Conformité App	Gestion des restrictions spécifiques aux applications (à partir de Windows 10 version 1511, non disponible pour Windows Home)
Contrôle des applications →	Gestion des politiques Windows Defender Application Control (WDAC) (à partir de Windows 10 version 1903, non disponible pour Windows Home)
CSP personnalisé →	Regroupement de paramètres CSP quelconques dans une seule configuration
E-Mail	Ajout de configurations de messagerie pour plusieurs utilisateurs
Exchange →	Gestion des comptes Exchange
Licences Windows	Gestion de la politique de licences Windows

Configuration	Description
Menu Démarrer	Personnalisation du menu Démarrer (à partir de Windows 10 version 1703, non disponible pour Windows Home)
Mise à jour Windows →	Gestion de la politique Windows Update (à partir de Windows 10 version 1607, non disponible pour Windows Home)
Mode kiosque Windows →	Gestion des paramètres du mode kiosque
Nom de l'appareil →	Configuration du nom de l'appareil
Options de sécurité de l'appareil local	Gestion des politiques relatives aux options de sécurité de l'appareil local
Papier peint	Gestion de l'image d'arrière-plan (à partir de Windows 10 version 1709, non disponible pour Windows Home)
Pare-feu Windows →	Gestion des paramètres du pare-feu Windows (à partir de Windows 10 version 1709, non disponible pour Windows Home)
PC partagé →	Gestion de la politique Windows pour les PC partagés
Proxys globaux	Configuration des proxys globaux (à partir de Windows 10 version 1703, non disponible pour Windows Home)
Restrictions →	Gestion des restrictions des appareils
Script →	Gestion de l'exécution automatique de scripts en fonction d'événements ou de calendriers via le Relution Companion
Service de bureau à distance	Gestion du service Bureau à distance
VPN →	Gestion des paramètres VPN (à partir de Windows 10 version 1607, également pour Windows Home)
Wi-Fi →	Gestion des paramètres Wi-Fi
Windows Companion →	Gestion du comportement du Relution Companion pour Windows : journalisation, gestion des applications, communication avec le serveur et changement automatique d'utilisateur de l'appareil
Windows Hello →	Gestion de la configuration Windows Hello

Configuration	Description
Windows Office →	Déploiement de Microsoft Office via un fichier XML de configuration créé en externe (à partir de Windows 10 version 1703, non disponible pour Windows Home)

Les configurations Contrôle des applications, CSP sur mesure, E-Mail, Exchange, Script, VPN, Wi-Fi et Certificat peuvent être ajoutées plusieurs fois à une politique, toutes les autres une seule fois. Si une configuration autorisée une seule fois figure déjà dans la politique, elle n'est plus proposée dans la boîte de dialogue de sélection.

Dans la boîte de dialogue de sélection, des badges indiquent les éditions de Windows prises en charge et la version minimale requise ; les indications entre parenthèses reprennent ces badges. Les autres limites de l'édition Home sont décrites dans Limites de Windows Home →

Les configurations Script et Windows Companion sont appliquées par le Relution Companion pour Windows →.

Pour la version 26.4.0

Contrôle des applications

Avec la version 5.24.0, la configuration Contrôle des applications a été introduite. Grâce à cette fonctionnalité, les politiques de Windows Defender Application Control (WDAC) peuvent être appliquées aux appareils Windows. Ces politiques définissent les applications de confiance, permettant uniquement à ces applications de s'exécuter sur l'appareil. La configuration est prise en charge sur Windows Pro, Enterprise et Education à partir de la version 1903.

Microsoft fournit toutes les informations nécessaires sur les politiques WDAC dans sa documentation →.

Génération de politiques WDAC

Microsoft explique la conception et la création des politiques WDAC dans son guide de conception →.

Il est recommandé de tester minutieusement toute politique WDAC avant de la déployer sur des appareils de production via Relution.

> Il faut s'assurer que l'application *Relution Windows Companion* n'est pas bloquée ou restreinte par les règles définies.

Pour la version 26.4.0

Créer le fichier de politique WDAC nécessaire

Pour la création, il est possible d'utiliser l'Assistant WDAC → et les exemples de politiques de base →.

L'assistant Windows Defender Application Control (WDAC) Policy Wizard génère deux fichiers lorsqu'il est utilisé pour la génération de politiques : un fichier XML et un fichier CIP. L'interface MDM de Microsoft nécessite la politique sous forme de fichier binaire. Le fichier CIP est déjà dans ce format binaire et peut être téléversé directement dans Relution. Le fichier XML doit d'abord être converti en fichier binaire ; ce processus est expliqué dans les sections suivantes.

Fichier Xml

Le fichier xml de la politique WDAC contient deux informations essentielles pour appliquer avec succès la configuration aux périphériques Windows via Relution.

Pour la version 26.4.0

Le `<PolicyID>` est un GUID qui identifie de manière unique cette politique WDAC. Il est donc utilisé pour appliquer, mettre à jour et supprimer la configuration.

Le paramètre `<VersionEx>` est utilisé comme version de la politique WDAC. Par conséquent, `<VersionEx>` doit être augmenté à chaque mise à jour d'une politique WDAC. Si la version est inférieure à la dernière version appliquée, Windows rejette la politique et la mise à jour de la configuration via Relution échoue.

Convertir le fichier xml

Le fichier xml doit être converti en fichier binaire. Ceci peut être fait en utilisant la commande PowerShell ConvertFrom-CIPolicy →.

Exemple :

```
ConvertFrom-CIPolicy -XmlFilePath .\AllowAll.xml -BinaryFilePath .\AllowAll.bin
```

Le fichier binaire résultant peut être téléversé dans Relution dans la configuration Contrôle des applications.

Configuration Contrôle des applications

Pour la version 26.4.0

La configuration Contrôle des applications se compose de deux champs obligatoires :

- Champ ID de contrôle de l'application : Pour que la configuration soit appliquée avec succès à l'appareil, l'ID de contrôle de l'application doit contenir la même valeur que le `<PolicyID>` de la politique WDAC, mais sans les accolades. Un GUID au format `XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX` est attendu ; toute autre saisie est signalée comme non valide.
  - Exemple :
    - PolicyID dans la politique du WDAC : `<PolicyID>{31351756-3F24-4963-8380-4E7602335AAE}</PolicyID>`
    - ID de contrôle de l'application dans la configuration : `31351756-3F24-4963-8380-4E7602335AAE`
  - Il n'est pas possible de modifier l'ID de contrôle de l'application saisi après le premier enregistrement. Cependant, il est possible de créer plusieurs configurations Contrôle des applications (complémentaires) et de les appliquer à un seul appareil.
- Champ Fichier binaire App Control : téléversement de la politique WDAC au format binaire, voir Génération de politiques WDAC →. La remarque dans le formulaire mentionne l'extension `.bin`. Relution ne vérifie toutefois pas l'extension, de sorte que le fichier CIP de l'assistant WDAC peut également être téléversé sans être renommé.

Mise à jour

Pour qu'une nouvelle version de la configuration Contrôle des applications soit appliquée avec succès à l'appareil, le `<PolicyID>` dans la politique WDAC doit avoir la même valeur que l'ID de contrôle de l'application de la configuration et le `<VersionEx>` doit avoir une valeur supérieure à celle de la version précédente.

Supprimer

Pour que la suppression d'une politique WDAC soit appliquée à l'appareil, un redémarrage de l'appareil est nécessaire.

Microsoft recommande une solution de contournement pour que les restrictions de l'application soient supprimées sans redémarrage, voir documentation Microsoft →.

Supprimer une configuration de contrôle d'application non signée

Dans Relution, la suppression sans redémarrage peut être mise en œuvre comme suit :

1. Créer une politique WDAC *Allow-All*.
   - Le `<PolicyID>` doit correspondre à l'ID de contrôle de l'application.
   - La `<VersionEx>` doit être supérieure à la version précédente.
2. Convertir le fichier xml dans le format binaire requis.
3. Créer une nouvelle version de politique dans Relution
   - Téléverser le nouveau fichier binaire de la politique WDAC *Allow-All* dans la configuration Contrôle des applications.
4. Publier la nouvelle version de la politique
   - Cela supprimera les restrictions existantes de l'appareil.
5. Supprimer la politique de l'appareil
   - Cette opération supprime la configuration Contrôle des applications de l'appareil. Toutefois, cette opération n'est active qu'après le redémarrage.

Supprimer une configuration de contrôle d'application signée

La suppression d'une politique WDAC signée (sans nécessiter de redémarrage) peut donc être mise en œuvre dans Relution de la manière suivante :

1. Créer une politique WDAC signée qui autorise les politiques WDAC non signées.
   - Le `<PolicyID>` doit correspondre à l'ID de contrôle de l'application.
   - La `<VersionEx>` doit être supérieure à la version précédente.
2. Convertir le fichier xml dans le format binaire requis.
3. Créer une nouvelle version de politique dans Relution

Pour la version 26.4.0

- Téléverser le nouveau fichier binaire de la politique WDAC signée (autorisant les politiques WDAC non signées) dans la configuration Contrôle des applications.

4. Publier la nouvelle version de la politique
   - Cela permet aux politiques WDAC non signées d'être appliquées sur l'appareil.
5. Supprimer une configuration de contrôle d'application non signée →

Pour la version 26.4.0

CSP personnalisé

L'interface MDM utilise les politiques du fournisseur de services de configuration (CSP) pour gérer les appareils Windows. Celles-ci sont appliquées, supprimées et interrogées sur le dispositif à l'aide du protocole SyncML →, un format XML spécial. La liste des politiques CSP disponibles se trouve dans la documentation officielle de Microsoft MDM →.

Avec la configuration CSP sur mesure, toutes les politiques CSP peuvent être combinées en une ou plusieurs configurations de ce type et appliquées aux appareils Windows. Ainsi, les fonctionnalités applicables via l'interface MDM ne sont limitées que par les politiques CSP disponibles. Microsoft ajoute continuellement de nouvelles politiques CSP. Une vue d'ensemble de celles-ci est disponible ici → dans la documentation officielle de Microsoft.

Notes importantes

Lors de l'utilisation de la configuration CSP sur mesure, celle-ci n'est pas mise en œuvre par Relution ; par conséquent, Relution décline toute responsabilité en cas de dommages éventuels. Vérifier soigneusement les CSP avant de les appliquer à un périphérique, voir Meilleures pratiques →.

Pour la version 26.4.0

Il est possible que les CSP utilisés soient également employés par Relution. Dans ce cas, il peut y avoir des interactions qui pourraient endommager les configurations fournies par Relution.

Fonctionnalité

Les particularités suivantes du protocole SyncML doivent être prises en compte lors de l'utilisation de politiques CSP.

Généralités

Toutes les politiques CSP ne peuvent pas être appliquées à tous les appareils. Elles dépendent de la *version du système d'exploitation* et de la *édition*. Les informations pertinentes peuvent être trouvées dans les politiques CSP respectives. Si un appareil n'est pas pris en charge, le déploiement de cette politique CSP échouera.

Les politiques CSP peuvent être appliquées dans le contexte de l'appareil ou de l'utilisateur →. Il convient de noter que le contexte de l'utilisateur ne s'applique qu'à l'utilisateur qui a effectué

l'inscription. Il est donc recommandé de n'utiliser les politiques CSP que dans le contexte de l'appareil.

Les politiques CSP ne prennent pas en charge toutes les commandes SyncML. Certaines politiques CSP ne peuvent être utilisées que pour l'interrogation (par exemple, la commande *Get*).

Exemple : Pour autoriser ou bloquer Cortana sur un appareil (déjà inclus dans la configuration de Relution *Restrictions*), le CSP suivant peut être utilisé. Politique CSP/Expérience/AllowCortana →

- Cette CSP peut être utilisée pour *toutes les éditions* et à partir de *la version 1507*.
- Seul le contexte de l'appareil est pris en charge.
- Les commandes SyncML suivantes sont autorisées : Ajouter (*Add*), Supprimer (*Delete*), Obtenir (*Get*), Remplacer (*Replace*)

Ajouter et remplacer

SyncML contient diverses spécificités qui doivent être prises en compte pour le déploiement de la configuration.

Certaines politiques CSP doivent être ajoutées avec la commande *Add* lorsqu'elles sont appliquées pour la première fois. Pour tous les déploiements ultérieurs de la configuration (mises à jour), cette commande *Add* peut échouer. Au lieu de cela, une commande *Replace* doit être envoyée, voir aussi Meilleures pratiques →.

Pour la version 26.4.0

Supprimer

La suppression d'une politique CSP peut être effectuée directement sur la politique CSP concernée. Dans certains cas, une commande *Delete* est également possible sur le nœud parent ou *root*. Dans ce cas, toutes les politiques CSP sous le nœud supprimé seront supprimées.

Si la suppression échoue, les politiques CSP contenues restent actives sur le dispositif. L'ajustement du champ Supprimer SyncML est nécessaire, ainsi que la réapplication puis la suppression de la politique.

Atomic et Sequence

La commande `Sequence` permet de regrouper des politiques CSP individuelles et de les exécuter de manière séquentielle. Cependant, si une seule politique CSP échoue, toutes les autres politiques CSP seront toujours appliquées. Cela peut conduire à un comportement indésirable, et la politique CSP défaillante peut devoir être explicitement supprimée.

Si le SyncML est exécuté dans une commande `Atomic`, la commande entière sera annulée si une seule politique CSP échoue. Ainsi, soit toute la configuration est appliquée, soit aucune ne l'est. Par conséquent, la commande `Atomic` est préférable et, pour l'instant, c'est la seule qui soit supportée.

Dans Relution

Pour appliquer une configuration personnalisée à des appareils Windows, la configuration CSP sur mesure est ajoutée à une politique Windows sous `Appareils` → `Politiques`. Après la publication de la politique, la configuration est appliquée aux appareils des groupes d'appareils auxquels la politique est attribuée (voir Politiques →).

La configuration nécessite deux commandes SyncML : dans le champ Installer SyncML, une commande pour l'installation ou la mise à jour de la configuration et, dans le champ Supprimer SyncML, une commande pour la suppression de la configuration. Lors de la publication répétée de la configuration, il convient de s'assurer que la commande dans Installer SyncML a été ajustée en conséquence.

La configuration CSP sur mesure comprend les propriétés suivantes (toutes obligatoires) :

...r la version 26.4.0

Propriété	Description
Nom	Désignation de la configuration (255 caractères maximum)
Installer SyncML	Le SyncML exécuté lorsque la configuration est appliquée à l'appareil
Supprimer SyncML	Le SyncML exécuté lorsque la configuration est supprimée de l'appareil

Pour la version 26.4.0

Relution doit étendre le SyncML spécifié pour appliquer la configuration sur le périphérique, l'évaluer par la suite et afficher un état dans Relution.

- Si le SyncML spécifié contient un élément `<Format>` ou `<Type>`, celui-ci sera étendu avec un *espace de noms* requis. Cela se fait automatiquement après avoir sauvegardé la configuration.

- Un `Atomic` sera enroulé autour du SyncML spécifié. Ceci est nécessaire pour identifier la configuration à laquelle la réponse du dispositif appartient. Cela se produit lorsque la configuration est livrée.
- Le SyncML sera étendu avec `SyncBody`, `SyncHdr` et `SyncML` afin que le SyncML puisse être envoyé à l'appareil d'une manière conforme. Cela se produit lorsque la configuration est livrée.

> Les champs Installer SyncML et Supprimer SyncML ne doivent contenir que les commandes elles-mêmes (par exemple `<Replace>`, `<Add>`, `<Delete>`), sans les éléments `SyncML`, `SyncHdr` ou `SyncBody`. Si le SyncML contient l'un de ces éléments ou s'il ne s'agit pas d'un SyncML valide, la configuration est refusée lors de l'enregistrement. Les messages SyncML complets de la documentation Microsoft doivent donc d'abord être réduits aux commandes.

Des espaces réservés peuvent être utilisés dans les deux champs SyncML, y compris des espaces réservés pour les certificats. Les espaces réservés disponibles sont affichés dans la section Espaces réservés disponibles sous la configuration et sont remplacés lors de la livraison par les valeurs de l'appareil ou de l'utilisateur concerné (voir Espaces réservés avancés →).

À chaque modification des politiques d'un appareil, par exemple après la publication d'une nouvelle version de politique, Relution renvoie le contenu de Installer SyncML de toutes les configurations CSP sur mesure attribuées, même si la configuration elle-même n'a pas changé. Contrairement aux autres configurations Windows, l'état de l'appareil n'est pas interrogé au préalable. Une commande `Add` peut donc échouer lors des livraisons suivantes (voir Meilleures pratiques →).

Pour la version 26.4.0

Si l'application de la configuration échoue sur l'appareil, Relution signale sur l'appareil une violation de conformité du type Configuration personnalisée du CSP.

Exemples

Politique CSP/Expérience/AllowCortana →

- Autoriser Cortana

Installer SyncML :

```
<Replace>
  <CmdID>1</CmdID>
  <Item>
    <Target>
      <LocURI>./Device/Vendor/MSFT/Policy/Config/Experience/AllowCortana</LocU
```

```
    </Target>
    <Meta>
      <Format>int</Format>
    </Meta>
    <Data>1</Data>
  </Item>
</Replace>
```

- Bloquer Cortana

Installer SyncML :

```
<Replace>
  <CmdID>1</CmdID>
  <Item>
    <Target>
      <LocURI>./Device/Vendor/MSFT/Policy/Config/Experience/AllowCortana</LocU
    </Target>
    <Meta>
      <Format>int</Format>
    </Meta>
    <Data>0</Data>
  </Item>
</Replace>
```

- Supprimer la politique CSP *AllowCortana* de l'appareil

Supprimer SyncML :

```
<Delete>
  <CmdID>1</CmdID>
  <Item>
    <Target>
      <LocURI>./Device/Vendor/MSFT/Policy/Config/Experience/AllowCortana</LocU
    </Target>
  </Item>
</Delete>
```

Meilleures pratiques

- Une *mise à jour de la configuration* peut être appliquée par le biais d'une nouvelle version de politique (éventuellement avec un champ Installer SyncML ajusté).
- Si la suppression échoue, les politiques CSP incluses restent actives sur l'appareil. Un ajustement du champ Supprimer SyncML est nécessaire, ainsi qu'une nouvelle application puis une suppression de la politique.
- Il est recommandé d'utiliser *Replace au lieu de Add* à moins qu'il ne soit pas pris en charge pour la politique CSP correspondante.
- Si la commande *Replace* n'est pas autorisée pour le déploiement initial d'une politique CSP, il est recommandé d'appliquer initialement cette configuration à l'aide d'une commande *Add*. Ensuite, mettre à jour le champ Installer SyncML de la configuration (utiliser *Replace* au lieu de *Add*) et l'appliquer sur le dispositif au moyen d'une nouvelle version de la politique.
- Il est recommandé de *tester le comportement souhaité de manière approfondie sur des dispositifs de test appropriés*. Au minimum, les comportements suivants devraient être testés :
  - déploiement initial de la configuration
  - Mise à jour de la configuration
  - Suppression de la configuration

Pour la version 26.4.0

Exemples de politiques

Un exemple complet de politiques personnalisées a été publié sur le Relution Community Board : Forum communautaire Relution - CSP personnalisé →.

Un grand merci à la communauté pour cette contribution précieuse.

Nom de l'appareil

À partir de la version 5.33 du serveur Relution, le nom de l’appareil peut être défini pour les appareils Windows via la politique Nom de l’appareil. Le nom est saisi dans le champ obligatoire Nom de la section Général. Les espaces réservés utilisateur et appareil peuvent être utilisés ; le portail les affiche sous la configuration, dans la zone Espaces réservés disponibles. Une seule configuration de nom d’appareil est possible par politique.

Remarques

> Après avoir ajusté le nom de l’appareil, celui-ci doit être redémarré pour que le nouveau nom prenne effet. Jusqu’au redémarrage, l’ancien nom sera toujours affiché lors de chaque action Actualiser les informations sur l’appareil. Le nom de l’appareil ne peut contenir que des lettres, des chiffres et des tirets. Cela s’applique également aux espaces réservés.

Relution insère d’abord les valeurs des espaces réservés, puis supprime tous les caractères autres que les lettres (a–z, A–Z, sans trémas ni accents), les chiffres et les tirets, y compris dans les valeurs insérées. Les tirets en début et en fin de nom sont également supprimés. Le nom saisi et le nom défini sur l’appareil peuvent donc différer, par exemple `Müller PC_01` devient `MllerPC01`. Après l’insertion des espaces réservés, le nom de l’appareil ne devrait pas dépasser 63 caractères.

D’autres fonctions telles que les sous-chaînes, les valeurs par défaut pour les champs non définis ou le remplacement des trémas sont décrites dans l’article Espaces réservés avancés →.

Si la configuration ou la politique est retirée de l’appareil, le dernier nom d’appareil défini est conservé.

Pour la version 26.4.0

Appliquer des restrictions

Pour s'assurer que les appareils Windows 10/11 ne sont utilisés que conformément aux restrictions spécifiées, des restrictions peuvent être définies dans la configuration de la politique "Restrictions" et appliquées aux appareils Windows inscrits.

Catégories disponibles

La configuration est divisée en groupes suivants :

- Comptes
- Gestion des applications
- Appareil photo
- Connectivité
- Expérience
- Système
- Paramètres
- Wi-Fi
- Alimentation électrique (sections Sur batterie et Branché)
- Confidentialité

Pour la version 26.4.0

À côté de chaque option, le portail indique les éditions de Windows concernées et la version minimale de Windows requise. Les paramètres que l'édition ou la version d'un appareil ne prend pas en charge ne sont pas transmis à cet appareil par Relution. La plupart des restrictions ne s'appliquent qu'à Windows Pro, Enterprise et Education (voir Limites de Windows Home →).

L'icône de téléchargement en haut du formulaire permet d'exporter les valeurs configurées, y compris les modifications non enregistrées, dans un fichier CSV.

Empêcher la suppression de la connexion MDM

Pour s'assurer que les appareils Windows 10/11 (Pro, Enterprise, Education) restent inscrits dans le système et que la connexion à Relution soit maintenue, une restriction permet d'empêcher la suppression du profil MDM par l'utilisateur. L'option de suppression reste affichée, mais n'a plus aucune fonction.

- Autoriser la désinscription de Relution MDM (groupe Expérience) - Si cette option est désactivée, elle garantit que les utilisateurs ne peuvent pas déconnecter manuellement les

appareils connectés du serveur MDM. Une désinscription par le serveur MDM reste possible.
- Autoriser l'utilisateur à réinitialiser l'appareil (groupe Système) - Si cette option est désactivée, elle empêche qu'une réinitialisation aux paramètres d'usine soit effectuée sur les appareils. Cela supprimerait l'enrôlement sur les appareils et la connexion au serveur MDM.

Les deux options sont activées par défaut. La protection ne prend donc effet qu'une fois qu'elles ont été explicitement désactivées dans la configuration.

Les deux options ne s'appliquent qu'à Windows 10/11 Pro, Enterprise et Education. Relution ne les transmet pas aux appareils sous Windows Home : ces appareils peuvent donc toujours être déconnectés du serveur MDM ou réinitialisés aux paramètres d'usine malgré la restriction (voir Limites de Windows Home →).

La combinaison des deux options sécurise le contrôle MDM des appareils Windows 10/11 (Pro, Enterprise, Education) enrôlés ainsi que toutes les configurations et restrictions fonctionnelles.

Pour la version 26.4.0

Windows Hello

Relution permet de configurer Windows Hello Entreprise dans une politique pour les appareils Windows. Windows Hello permet aux utilisateurs de se connecter par code PIN (code confidentiel), reconnaissance faciale ou empreinte digitale au lieu d'un mot de passe.

Configuration

- ID du locataire – ID du locataire Entra ID au format GUID, champ obligatoire.
- Utiliser un module de plateforme sécurisée (TPM) – restreint le déploiement aux appareils disposant d'un TPM utilisable. Activé par défaut.

Règles du code PIN

- Longueur minimale du code PIN et Longueur maximale du code PIN (4 à 127 caractères chacune, par défaut : 4) – la longueur maximale ne doit pas être inférieure à la longueur minimale. Sans modification, la longueur du code PIN est donc fixée à 4 caractères.
- Lettres minuscules dans le code PIN, Lettres majuscules dans le code PIN, Caractères spéciaux dans le code PIN – respectivement Autorisé (par défaut), Requis ou Non autorisé
- Expiration du code PIN et Expiration du code PIN (jours) – impose un changement du code PIN au bout de 1 à 730 jours (à partir de Windows 1511). L'interrupteur est désactivé par défaut, le code PIN n'expire alors pas ; une fois activé, 5 jours sont préréglés.
- Mémoriser l'historique des codes PIN et Taille de l'historique des codes PIN – empêche la réutilisation des 1 à 50 derniers codes PIN (à partir de Windows 1511). Activé par défaut avec 5 codes PIN ; si l'interrupteur est désactivé, aucun historique n'est conservé.

Biométrie et récupération

- Autoriser l'authentification biométrique – active la connexion par visage ou empreinte digitale (à partir de Windows 1511). Activé par défaut.
- Utiliser l'anti-usurpation d'identité améliorée, le cas échéant – protection supplémentaire pour la reconnaissance faciale (à partir de Windows 1511). Activé par défaut.
- Activer la récupération du code PIN – permet de réinitialiser un code PIN oublié (à partir de Windows 1703). Activé par défaut.
- Certificat pour les ressources sur site – Windows Hello Entreprise utilise un certificat pour la connexion aux ressources locales. Si l'option est activée, Windows Hello ne configure le code PIN qu'une fois que l'appareil a reçu un certificat du serveur de gestion, p. ex. via la

Pour la version 26.4.0

configuration Certificats → avec l'Emplacement de la clé de certification Windows Hello pour les entreprises. Activé par défaut. Sans une telle distribution de certificats, aucun code PIN n'est configuré ; dans ce cas, l'option doit être désactivée.

Les options assorties d'une version ne sont transmises qu'aux appareils disposant de la version de Windows correspondante ou d'une version ultérieure.

> Windows Hello Entreprise nécessite une connexion à Microsoft Entra ID. Les exigences minimales exactes en matière de matériel (version TPM) et de version Windows doivent être vérifiées dans la documentation Microsoft →.

Pour la version 26.4.0

Wi-Fi

Relution permet de configurer de manière centralisée des réseaux Wi-Fi sur les appareils Windows, sans que les utilisateurs aient à saisir eux-mêmes les identifiants.

Configuration

- Le SSID du réseau – obligatoire, 32 caractères maximum, sans espace au début ni à la fin, doit être unique au sein de la version de la politique.
- Ce réseau est masqué – pour les réseaux qui ne diffusent pas leur SSID (désactivé par défaut).
- Rejoindre le réseau automatiquement – activé par défaut.
- Type d'authentification : Ouvert (par défaut), WPA personnel, WPA2 personnel, WPA3 personnel, WPA d'entreprise, WPA2 d'entreprise, WPA3 entreprise, WPA3 entreprise 192 bits
- Type de cryptage – pour WPA et WPA2 (personnel ou entreprise), au choix AES (par défaut) ou TKIP ; AES imposé pour WPA3 personnel et WPA3 entreprise, GCMP-256 imposé pour WPA3 entreprise 192 bits ; le champ n'apparaît pas pour Ouvert.
- Mot de passe – clé réseau pour les types d'authentification personnels, 64 caractères maximum. Le portail affiche également le champ pour Ouvert, mais il n'est pas transmis dans ce cas. Si le champ reste vide, aucune clé n'est transmise.
- Mode de transition – uniquement pour WPA3 personnel

Pour la version 26.4.0

Si plusieurs politiques attribuent à un appareil des configurations Wi-Fi avec le même Le SSID du réseau, seule la configuration de la politique ayant la priorité la plus élevée est appliquée.

Authentification Entreprise (EAP)

Pour les types d'authentification entreprise, la section Paramètres de chiffrement s'affiche. Au moins un type EAP doit être sélectionné. Dès qu'un type EAP est sélectionné, la section Confiance s'affiche également avec les noms de serveurs et les certificats approuvés.

- Accepter les types d'EAP – TLS, TTLS et/ou PEAP
- Certificat d'identité – uniquement pour TLS/TTLS ; obligatoire dans ce cas. Deux options sont disponibles :
  - Sélectionner un certificat – un certificat téléversé manuellement (voir Gestion des certificats →) ou un modèle de certificat, par ex. du CA intégré →.
  - Utiliser un certificat utilisateur – le certificat utilisateur du profil de l'utilisateur attribué à l'appareil (voir Certificats utilisateur →). Le champ facultatif Nom du certificat

sélectionne un certificat précis par son nom lorsque l'utilisateur en possède plusieurs et peut contenir des espaces réservés. S'il reste vide, le certificat ayant la plus longue durée de validité est utilisé.

- Type d'authentification interne – pour TTLS : PAP, CHAP, MSCHAP ou MSCHAPv2 (obligatoire) ; dès que PEAP est sélectionné, uniquement MSCHAPv2 (facultatif)
- Authentification interne – champ de texte, uniquement pour TTLS sans PEAP ; obligatoire pour PAP, CHAP ou MSCHAP
- Nom d'utilisateur anonyme – pour TTLS/PEAP, facultatif
- Demander un certificat de serveur à l'utilisateur – uniquement pour PEAP. Si l'option est activée, le certificat du serveur n'est pas validé automatiquement et Windows peut interroger l'utilisateur si l'autorité de certification est introuvable.
- Noms de serveurs approuvés
- Certificats de confiance – sélection multiple de certificats (PKCS#1 ou PKCS#12) depuis la Gestion des certificats →

Pour la version 26.4.0

Windows Update

Relution permet de contrôler de manière centralisée le comportement des mises à jour des appareils Windows. La politique est disponible à partir de Windows 10 version 1607 pour les éditions Pro, Entreprise et Éducation.

Mise à jour automatique

- Comportement des mises à jour automatiques : installation et redémarrage automatiques (par défaut), installation automatique et redémarrage à une heure spécifiée, installation et redémarrage automatiques sans contrôle de l'utilisateur final, installation automatique puis invitation de l'utilisateur à planifier un redémarrage, notification avant le téléchargement, ou désactivation complète des mises à jour automatiques.
- Pour à une heure spécifiée : Fréquence d'installation des mises à jour (à partir de la version 1709) avec Chaque semaine (par défaut) ou une ou plusieurs semaines précises du mois (première à quatrième semaine) ; Chaque semaine exclut la sélection de semaines individuelles. En outre, l'heure (0 à 23 h, par défaut 3 h) et le jour (par défaut : chaque jour) d'installation de la mise à jour.
- Rechercher les mises à jour des applications depuis Microsoft Update (désactivé par défaut)

Pour la version 26.4.0

Général

- Accepter les mises à jour signées par d'autres entités que Microsoft (uniquement depuis un service de mise à jour intranet, signées par un certificat du magasin « Éditeurs approuvés » ; désactivé par défaut)
- Autoriser les téléchargements sur des réseaux à consommation mesurée (à partir de 1709, désactivé par défaut)
- Activer les notifications de redémarrage automatique (désactivé par défaut) et période des rappels (15, 30, 60, 120 ou 240 minutes, par défaut 15 ; à partir de 1703)
- Période des avertissements de redémarrage (2, 4, 8, 12 ou 24 heures, par défaut 4) et des avertissements imminents (15, 30 ou 60 minutes, par défaut 15 ; à partir de 1703 pour les deux)
- Maintenance automatique/réveil (à partir de 1903, activé par défaut)
- Autoriser la double analyse (à partir de 1709, activé par défaut)
- Délai de grâce avant l'échéance (0 à 7 jours, par défaut 2 ; à partir de 1903), pas de redémarrage automatique en dehors des heures d'activité avant l'expiration de l'échéance et

du délai de grâce (à partir de 1903, désactivé par défaut)
- URL du serveur WSUS ainsi qu'une URL alternative ; les deux doivent être des URL `http` ou `https` valides
- Version cible de Windows (à partir de 1803) et version du produit (à partir de 2004, effective uniquement en combinaison avec la version cible) ; pour la version du produit, le portail propose `Windows 10`, `10`, `Windows 11` et `11`

Interface utilisateur

À partir de la version 1809 : autoriser les utilisateurs finaux à accéder à Windows Update ou à suspendre les mises à jour (les deux activés par défaut).

Heures d'activité

- Début et fin des heures d'activité (0 à 23 h, par défaut 8 h à 17 h), plage maximale de 18 heures. Les heures d'activité peuvent s'étendre au-delà de minuit ; si la fin précède le début, elle s'applique au jour suivant.

Mises à jour qualité

Pour la version 26.4.0

- Échéance de redémarrage automatique (2 à 30 jours, par défaut 7 ; à partir de 1703)
- Date de début de pause (à partir de 1703) : les mises à jour qualité sont suspendues pendant 35 jours à compter de la date choisie.
- Échéance en jours (0 à 30, par défaut 7 ; à partir de 1903)
- Période de report en jours (0 à 365 jours)

Mises à jour des fonctionnalités

- Échéance de redémarrage automatique (2 à 30 jours, par défaut 7 ; à partir de 1809)
- Période de désinstallation (2 à 60 jours, par défaut 10 ; à partir de 1803)
- Période de report en jours (0 à 365 jours)
- Échéance en jours (0 à 30, par défaut 7 ; à partir de 1903)
- Date de début de pause (à partir de 1703) : les mises à jour des fonctionnalités sont suspendues pendant 35 jours à compter de la date choisie.

Exchange

Relution permet de configurer de manière centralisée un compte Exchange ActiveSync sur les appareils Windows.

Configuration

La configuration est divisée en sections Général, Paramètres du compte, Paramètres de synchronisation et Paramètres de journalisation. Nom du compte, Adresse électronique, Nom d'utilisateur et Hôte Exchange sont obligatoires ; Domaine Exchange et le mot de passe sont facultatifs.

Général

- Utiliser Secure Mail Gateway : si cette fonction est activée, l'URL et le domaine de la passerelle de messagerie sécurisée → sont distribués aux appareils à la place de l'URL et du domaine Exchange. Ainsi, les appareils communiquent avec le serveur Exchange via la passerelle de messagerie sécurisée. Hôte Exchange et Domaine Exchange sont alors définis automatiquement et ne peuvent pas être modifiés ; le nom unique de l'organisation sert de domaine. Si le nom d'utilisateur contient un `@`, Relution le transmet au format `<domaine>\<nom d'utilisateur>`. L'option n'est disponible que si la passerelle Secure Mail Gateway est configurée et activée dans les paramètres. Si Windows ou une version de Windows est restreinte dans les paramètres de Secure Mail Gateway, le formulaire affiche un avertissement.
- Hôte Exchange – obligatoire, sans protocole (sans `https://`, p. ex. `mail.example.com`).
- Domaine Exchange – facultatif.
- Exchange Server utilise SSL pour l'authentification – activé par défaut.

Paramètres du compte

- Nom du compte – obligatoire.
- Adresse électronique – obligatoire, prend en charge des espaces réservés tels que `${user.email}` ; l'option « Utiliser l'adresse e-mail de l'utilisateur » (dans le portail : Utilisez l'adresse e-mail de l'utilisateur) reprend l'adresse e-mail de l'utilisateur attribué.
- Nom d'utilisateur – obligatoire. Saisi Manuellement ou repris du nom d'utilisateur (`${user.name}`) ou de l'adresse e-mail (`${user.email}`) de l'utilisateur attribué. Le nom d'utilisateur ne peut plus être modifié après la création de la configuration.

Pour la version 26.4.0

- Mot de passe (dans le portail : Mot de) – facultatif, enregistré de manière chiffrée et n'est plus affiché en clair après l'enregistrement.

Si un espace réservé est utilisé, un utilisateur doit être attribué à l'appareil.

Paramètres de synchronisation

- Synchroniser les e-mails, les contacts, le calendrier et les tâches – chacun activable individuellement, tous activés par défaut.
- Période de synchronisation des e-mails : tout, 3 jours, 1 semaine (par défaut), 2 semaines ou 1 mois.
- Intervalle de synchronisation : push (par défaut), manuel, toutes les 15 ou 30 minutes ou toutes les heures.

Paramètres de journalisation

- Journalisation : Désactivée (par défaut), Activée ou Avancée.

Pour la version 26.4.0

Windows Office

Relution permet de déployer de manière centralisée une installation de Microsoft Office sur les appareils Windows à l'aide d'un fichier XML de configuration créé au préalable. La politique est disponible à partir de Windows 10 version 1703 pour les éditions Pro, Entreprise et Éducation.

Configuration

La configuration se compose d'un seul fichier :

- Configuration XML – obligatoire, téléversement d'un fichier XML. Après le téléversement, le formulaire affiche le contenu du fichier pour contrôle.

Ce fichier XML n'est pas créé dans Relution mais généré via l'outil officiel de Microsoft config.office.com →. La licence, le canal de mise à jour ainsi que les applications et langues Office à installer y sont définis.

Pour la version 26.4.0

Installation et désinstallation

L'installation s'exécute de manière asynchrone sur l'appareil. Tant qu'elle est en cours, l'action de modification de politique (Politique de changement dans le portail) reste au statut Pas maintenant.

- Suite Office déjà installée : Relution compare l'ID de produit (`<Product ID="…">`) de l'installation signalée par l'appareil avec l'ID de produit du nouveau fichier XML. S'ils diffèrent, la suite Office existante est d'abord entièrement désinstallée, et la nouvelle configuration n'est installée que lors d'une étape ultérieure. Si l'ID de produit est identique, l'installation est directement répétée sans désinstallation préalable.
- Suppression de la configuration : si la configuration ou la politique est supprimée de l'appareil et que l'appareil signale une installation d'Office, Relution désinstalle Office de l'appareil.
- Erreurs : si l'appareil signale une erreur lors de l'installation, la violation de conformité La configuration de Windows Office n'est pas valide est générée.

L'action d'appareil Déployer Office 365 ne doit pas être utilisée en plus de cette politique. Des informations sur les installations bloquées figurent sous L'installation d'Office est bloquée →.

Code d'accès

La configuration de stratégie Code d’accès définit les exigences auxquelles doit répondre un mot de passe sur les appareils Windows gérés, ainsi que le comportement de l’appareil en cas d’inactivité ou de tentatives de connexion échouées.

Dès que la configuration est attribuée, Relution active le verrouillage de l’appareil par mot de passe. Ce réglage est toujours actif et ne peut pas être désactivé dans la configuration.

> Ces réglages ne s’appliquent pas à tous les types de comptes Windows. La documentation officielle de Microsoft relative au CSP concerné fait foi : CSP DeviceLock →

Options de configuration

- Autoriser les mots de passe simples — Spécifie si les codes PIN ou les mots de passe tels que « 1111 » ou « 1234 » sont autorisés. Activé par défaut.
- Longueur minimale du code d’accès — Nombre minimal de caractères du mot de passe (4–16). La valeur par défaut est 4.
- Qualité du code d’accès — Spécifie si un code d’accès doit être numérique (par exemple « 1042 »), alphanumérique (par exemple « A42B ») ou libre de choix. La valeur par défaut est Alphanumérique.
- Âge minimum du code d’accès (en jours) — Période (en jours) pendant laquelle un mot de passe doit être utilisé avant que l’utilisateur puisse le modifier (0–41). La valeur par défaut est 0 – les modifications sont autorisées immédiatement. Si un âge maximum est défini, la valeur doit être inférieure à l’âge maximum.
- Âge maximum du code d’accès (en jours) — Nombre de jours avant l’expiration du mot de passe (0–730). La valeur par défaut est 0 – les mots de passe n’expirent pas.
- Historique du code d’accès — Nombre de mots de passe récents qui ne peuvent pas être réutilisés (0–24). La valeur par défaut est 0 – le mot de passe actuel peut être remplacé par n’importe quel mot de passe, y compris lui-même. Avec la valeur 1, l’utilisateur ne peut pas réutiliser son mot de passe actuel ; la valeur 5 signifie que ni le mot de passe actuel ni aucun des quatre mots de passe précédents ne peut être réutilisé.
- Temps d’inactivité avant le verrouillage de l’écran — Durée en minutes (0–999) pendant laquelle l’appareil peut rester inactif avant d’être verrouillé ; le code PIN ou le mot de passe doit alors être saisi. La valeur par défaut est 0 – l’appareil ne se verrouille pas.
- Nombre de tentatives de code secret ayant échoué avant que toutes les données ne soient effacées — Nombre de tentatives de connexion échouées après lequel l’appareil est mis en

Pour la version 26.4.0

mode de récupération BitLocker (0–16). Lorsque l’utilisateur atteint cette valeur, l’appareil n’est pas effacé : les données deviennent inaccessibles mais restent récupérables. BitLocker doit être activé. La valeur par défaut est 0 – désactivé.

L’âge minimum du code d’accès est transmis à partir de Windows 10 version 1709, l’âge maximum et l’historique du code d’accès à partir de la version 1511. Sur les versions antérieures, ces valeurs ne sont pas définies.

Qualité du code d’accès

Trois valeurs sont disponibles pour la Qualité du code d’accès :

- Numérique
- Alphanumérique (par défaut)
- Choix de l’utilisateur

Sujets connexes

- BitLocker → — chiffrement de lecteur et clés de récupération.
- Windows Hello → — connexion biométrique et stratégies de code PIN.

Pour la version 26.4.0

Mode kiosque Windows

La configuration de stratégie Mode kiosque Windows limite un appareil à une seule application. La politique est disponible à partir de Windows 10 version 1803 pour les éditions Pro, Entreprise et Éducation. Les cas d'usage typiques sont les bornes d'information, les postes en libre-service et les appareils d'examen.

> L'application sélectionnée et le navigateur kiosque ne sont pas installés automatiquement. Les deux doivent être mis à disposition séparément via la distribution d'applications avant que la configuration ne prenne effet.

Connexion de l'utilisateur

Type de connexion de l'utilisateur détermine quel compte s'exécute en mode kiosque :

- Connexion automatique (par défaut) : l'appareil se connecte automatiquement avec un compte kiosque que Windows met à disposition à cet effet.
- Utilisateur local : le mode kiosque s'applique au compte saisi dans le champ Nom de connexion de l'utilisateur. Ce champ n'apparaît qu'avec cette option et est alors obligatoire. Aucune connexion automatique n'a lieu ; le mode kiosque prend effet dès que le compte se connecte.

Pour la version 26.4.0

Type d'application

Type d'application détermine ce qui est affiché en mode kiosque : Navigateur Microsoft Edge (par défaut), Navigateur de kiosque ou Store App. Les autres champs dépendent de cette sélection et sont décrits dans les sections suivantes. Lors d'un changement de type, Relution supprime de l'appareil les réglages de navigateur du type sélectionné auparavant.

Microsoft Edge

Ces champs apparaissent avec Navigateur Microsoft Edge :

- URL du kiosque Edge – adresse de la page de démarrage, champ obligatoire. Une URL valide doit être saisie.

- Type de mode kiosque Microsoft Edge – Multi-onglets (par défaut) ou Sans onglet.
- Rafraîchir le navigateur après une période d'inactivité – durée en minutes (0 à 1440). Si le champ reste vide, Relution utilise 5 minutes en mode Multi-onglets et 0 en mode Sans onglet.

Navigateur kiosque

Ces champs apparaissent avec Navigateur de kiosque :

- URL de la page d'accueil par défaut – page de démarrage du navigateur kiosque.
- Afficher les boutons d'accueil, Afficher les boutons de navigation et Bouton de fin de session – affichent les boutons correspondants dans le navigateur kiosque.
- Rafraîchir le navigateur après une période d'inactivité – durée en minutes (1 à 1440). Si le champ reste vide, Relution ne définit aucune valeur.
- Autoriser les URLs (max 500) – sans entrée, tous les sites Web sont accessibles dans le navigateur kiosque. Dès qu'au moins une URL est saisie, seules les URL saisies sont accessibles et tous les autres sites Web sont bloqués. Les caractères génériques (`*`) ne sont pas autorisés, chaque entrée doit être une URL valide.

Store App

Avec Store App, le bouton Sélectionner l'application permet de choisir l'application Windows du Relution App Store affichée en mode kiosque (champ obligatoire).

L'application doit déjà être installée sur l'appareil (voir la remarque ci-dessus). Si elle n'est pas installée, la configuration n'est pas appliquée sur l'appareil.

Sujets connexes

- Shared PC → — configurer les appareils Windows pour une utilisation partagée.
- Restrictions → — autres restrictions pour les appareils Windows.

Pour la version 26.4.0

VPN

La configuration de stratégie VPN distribue des profils VPN de manière centralisée sur les appareils Windows gérés. Outre la connexion elle-même, la configuration couvre l’authentification, la résolution de noms, le split tunneling et les réglages de proxy. Windows Home, Pro, Enterprise et Education sont pris en charge à partir de la version 1607.

Le formulaire est divisé en sections Général, Apps, Paramètres DNS, Split tunneling et Configuration du proxy.

> Le nom de profil est l'identifiant univoque d'un profil VPN sur l'appareil. Il doit se distinguer de toute autre configuration VPN au sein de la même version de stratégie ; les majuscules et minuscules ne sont pas distinguées. Si plusieurs stratégies comportant des configurations VPN de même nom de profil s'appliquent à un appareil, seule la configuration de la stratégie de priorité supérieure est appliquée.

Pour la version 26.4.0

Général

Champ	Description
Nom du profil	Obligatoire. Nom du profil VPN sur l’appareil ; sans espace au début ni à la fin
Type de VPN	Automatique (par défaut), L2TP, PPTP ou IKEv2. Le type détermine les types d’authentification proposés
Noms des serveurs	Obligatoire. Au moins un serveur VPN ; plusieurs entrées sont possibles
Connexion automatique	La connexion VPN est établie automatiquement
Mémoriser les informations d’identification	Les informations d’identification de la connexion VPN sont enregistrées sur l’appareil

Authentification

Selon le Type de VPN, le champ Type d’authentification propose les options suivantes. Lors d’un changement de type de VPN, le type d’authentification est réinitialisé.

Option	Disponible avec	Description
Aucun	tous les types	Par défaut. Le profil ne définit aucune méthode d’authentification
EAP	tous les types	Authentification via EAP ; la configuration EAP est saisie dans le champ EAP XML
Clé pré-partagée	L2TP	Le champ Clé pré-partagée apparaît et devient obligatoire ; le bloc Certificat d’identité n’est pas affiché
Certificats d’ordinateur	IKEv2	L’appareil s’authentifie avec un certificat d’ordinateur ; le champ EAP XML n’est pas affiché

Pour la vers

Avec le type de VPN L2TP, une clé pré-partagée ou un certificat d’identité (certificat, modèle de certificat ou certificat utilisateur) est requis. Si les deux manquent, la configuration n’est pas enregistrée.

EAP XML

EAP n’est pas configuré à l’aide de champs individuels, mais sous forme de configuration XML dans le champ de texte EAP XML. Au-dessus du champ, le portail renvoie à la documentation Microsoft sur la structure de cette configuration : Configuration EAP →.

Le champ est disponible pour toutes les combinaisons, sauf IKEv2 avec Certificats d’ordinateur. Le XML n’est transmis à l’appareil qu’avec le type d’authentification EAP ; avec Aucun et Clé pré-partagée, il est ignoré.

Certificat d’identité

Sauf avec le type d’authentification Clé pré-partagée, le bloc Certificat d’identité définit le certificat utilisé pour la connexion :

- Utiliser un certificat utilisateur : utilise le certificat utilisateur. Le champ facultatif Nom du certificat sélectionne un certificat précis par son nom lorsque l'utilisateur possède plusieurs certificats de ce type ; le nom peut contenir des espaces réservés. Si le champ reste vide, le certificat ayant la plus longue durée de validité est utilisé. Un utilisateur disposant d'un certificat utilisateur doit être attribué à l'appareil.
- Sélectionner un certificat : sélection d'un certificat ou d'un modèle de certificat dans la gestion des certificats.

Le certificat n'est installé sur l'appareil avec le profil VPN qu'avec le type d'authentification EAP.

Paramètres IKEv2

Avec le type de VPN IKEv2, les paramètres cryptographiques peuvent également être définis. La valeur par défaut de tous les champs est Non configuré.

- Paramètres IKE SA : Algorithme de chiffrement, Algorithme d'intégrité et Groupe Diffie-Hellman
- Paramètres SA enfant : Algorithme de chiffrement, Algorithme d'intégrité et Groupe Diffie-Hellman (groupe PFS, avec en plus l'option Utiliser le groupe Diffie-Hellman parent)

Soit les six valeurs sont définies, soit aucune ; une saisie partielle n'est pas enregistrée.

Apps

Pour la version 26.4.0

Champ	Description
Apps	Applications dont le lancement établit automatiquement la connexion VPN. Pour les applications de bureau, le chemin d'accès au fichier de l'application est indiqué ; pour les applications universelles (UWP), le nom de la famille de paquets
Limiter la connexion VPN à ces applications	Si l'option est activée, seul le trafic des applications saisies sous Apps passe par le VPN

Paramètres DNS

Le champ DNS suffix reçoit les suffixes DNS ajoutés à la liste de recherche DNS afin que les noms courts soient correctement résolus. Le premier suffixe de la liste est également utilisé comme suffixe DNS principal spécifique à la connexion de l'interface VPN.

Les Règles de la table de politique de résolution des noms (NRPT) définissent la manière dont les noms DNS sont résolus lorsqu'une connexion VPN est établie. Chaque règle indique un domaine et les serveurs DNS ou le serveur proxy web à utiliser pour résoudre ce domaine. Ajouter crée une règle avec les champs suivants :

Champ	Description
Domaine	Obligatoire. Domaine auquel la règle s'applique
Serveurs DNS	Un ou plusieurs serveurs DNS pour ce domaine
Proxy	Serveur proxy web pour ce domaine
Connexion automatique	L'appareil se connecte automatiquement au VPN lorsqu'il se connecte à ce domaine
Persistant	La règle reste active même lorsque le VPN n'est pas connecté

Split tunneling

Le split tunneling est activé à l'aide de l'interrupteur Split tunneling. Ce n'est qu'alors que les entrées de la liste Routes de split tunneling pour cette connexion VPN sont transmises à l'appareil, et seul le trafic vers ces destinations passe par le VPN.

> Si l'interrupteur Split tunneling est désactivé, le profil est configuré en tunnel forcé (force tunnel) : tout le trafic passe par le VPN et les routes saisies sont ignorées.

Chaque route est ajoutée via Ajouter sous forme de Préfixe de destination en notation CIDR, c'est-à-dire une adresse IPv4 ou IPv6 avec longueur de préfixe (par ex. `10.22.0.0/16`). La longueur de préfixe (masque de sous-réseau) doit être supérieure à 0.

Configuration du proxy

Le champ Type de proxy détermine les champs supplémentaires affichés :

Option	Description
Aucun	Par défaut. Aucun proxy n’est configuré pour la connexion VPN
Automatique	Champ obligatoire URL de configuration du proxy : URL valide du script de configuration du proxy
Manuelle	Champs obligatoires Serveur proxy et Port du serveur proxy (valeur 1–65535, préremplie avec 1)

Pour la version 26.4.0

Sujets connexes

- Certificats → — fournir des certificats d’identité et de confiance.
- Wi-Fi → — profils réseau pour les appareils Windows.

Pare-feu Windows

La configuration de stratégie Pare-feu Windows gère le pare-feu Windows sur les appareils gérés. Elle se compose de trois parties : les propriétés globales, les réglages par profil réseau et les règles de pare-feu individuelles.

> Au moins l'une des trois parties doit être configurée avant l'enregistrement — propriétés globales, un profil ou une règle de pare-feu.

> Une configuration de pare-feu peut interrompre la communication entre l'appareil et le serveur MDM. La communication avec le serveur MDM et avec le service de notification Windows (WNS) ne doit pas être bloquée, sinon l'appareil ne peut plus être géré.

Propriétés globales

Pour la version 26.4.0

Les propriétés globales s’appliquent à l’ensemble de l’appareil, tous profils confondus, et se trouvent dans la section Général. Elles sont activées par l’interrupteur Configurer les paramètres globaux ; sans lui, les champs suivants ne sont pas modifiables et ne sont pas transmis. Si l’interrupteur est désactivé, les propriétés globales transmises auparavant sont de nouveau supprimées de l’appareil.

- Bloquer le protocole FTP avec état (File Transfer Protocol)
- Délai d’inactivité des associations de sécurité avant suppression : nombre de secondes sans trafic réseau après lequel une association de sécurité est supprimée (300–3600).
- Encodage de clé pré-partagé
- Exemptions IPSec (sélection) :
  - Aucun
  - Codes de type ICMP IPv6 pour la découverte de voisins (Neighbor Discovery)
  - ICMP
  - Codes de type ICMP IPv6 pour la découverte de routeurs (Router Discovery)
  - Trafic DHCP IPv4 et IPv6
- Vérification de la liste de révocation de certificats (CRL) (obligatoire, par défaut : Désactivé) :
  - Désactivé
  - Échec de la vérification de la LCR uniquement en cas de certificat révoqué
  - Échec de la vérification de la LCR en cas d’erreur
- Correspondance opportuniste du jeu d’authentification par module de saisie de clés
- Activer la file d’attente des paquets (par défaut : Désactivé) :

- Désactivé
- Mettre en file d'attente uniquement les paquets chiffrés entrants
- Mettre les paquets en file d'attente après le déchiffrement pour le transfert uniquement

---

Propriétés de profil

Chaque profil réseau – Réseau de domaine (lieu de travail), Réseau public (non détectable) et Réseau privé (détectable) – dispose de sa propre section avec l'interrupteur Configurer les propriétés du profil. Ce n'est que lorsqu'il est activé que les réglages suivants peuvent être modifiés et sont transmis à l'appareil. S'il est désactivé, les réglages du profil transmis auparavant sont de nouveau supprimés de l'appareil.

- Activer le pare-feu
  - Blindé : sélectionnable uniquement si Activer le pare-feu est défini ; associé au pare-feu, il bloque tout le trafic entrant.
- Autoriser l'action par défaut pour les connexions entrantes (par défaut : activé)
- Autoriser l'action par défaut pour les connexions sortantes (par défaut : activé)
- Désactiver les notifications entrantes
- Désactiver le mode furtif
  - Exemption de paquets sécurisée IPsec avec le mode furtif : sélectionnable uniquement si Désactiver le mode furtif est défini.
- Désactiver les réponses de monodiffusion aux diffusions de multidiffusion
- Règles de pare-feu d'application autorisées du magasin local (par défaut : activé)
- Règles de pare-feu de port globales du magasin local (par défaut : activé)
- Autoriser les règles de pare-feu à partir du magasin local (par défaut : activé)
- Règles IPSec du magasin local (par défaut : activé)

Pour la version 26.4.0

Si les actions par défaut pour les connexions entrantes ou sortantes ne sont pas autorisées, une règle de pare-feu autorisant les connexions avec Relution est nécessaire. Sinon, Relution ne peut plus gérer l'appareil.

Règles de pare-feu

Les règles de pare-feu figurent dans une liste avec les colonnes Nom de la règle, Description de la règle, Direction du trafic et Règle activée. Les boutons Ajouter, Éditer et Supprimer permettent de créer, modifier ou supprimer des règles. Un maximum de 100 règles de pare-feu est possible par configuration.

Pour chaque règle, il est possible de définir l'application, les ports et les types de réseau :

- Nom de la règle (obligatoire)
- Description de la règle
- Règle activée (par défaut : activé)
- Autoriser la connexion pour cette règle (par défaut : activé) : détermine si la règle autorise ou bloque le trafic réseau.
- Paramètre Traversal Edge activé (par défaut : désactivé)
- Direction du trafic : Entrant ou Sortant (par défaut)
- Types de réseaux (obligatoire, sélection multiple) :
  - Tous les ensembles de réseaux existants et tous les futurs ensembles de réseaux (par défaut ; exclut les autres options)
  - Domaine
  - Privée
  - Publique
- Nom de famille du package, Chemin complet du fichier et Service Windows (section consacrée à l'application)
- Plage d'adresses locales et Plage d'adresses distantes (section Adresse IP) : adresses IPv4 ou IPv6, sous forme d'adresse unique ou de plage avec Limite inférieure et Limite supérieure
- Protocole IP : nombre de 0 à 255, avec une liste de suggestions (p. ex. 6 - TCP, 17 - UDP)
- Plage de ports locaux et Plage de ports distants : ports de 1 à 65535, sous forme de port unique ou de plage
- Types d'interface (sélection multiple, par défaut : tous) : Réseau local, Sans fil, Accès à distance
- Liste d'autorisation des utilisateurs locaux : utilisateurs locaux autorisés au format SDDL ; si rien n'est indiqué, la règle s'applique à tous les utilisateurs. Aucune liste n'est possible pour les règles qui ciblent un service Windows.

Pour la version 26.4.0

Un maximum de 20 entrées est possible par liste de plages (Plage de ports locaux, Plage de ports distants, Plage d'adresses locales, Plage d'adresses distantes) ; les plages d'une même liste ne doivent pas se chevaucher. Les plages de ports ne sont disponibles que si 6 - TCP ou 17 - UDP est sélectionné comme Protocole IP.

Sujets connexes

- VPN → — profils VPN pour les appareils Windows.
- CSP personnalisé → — réglages ne disposant pas d'une configuration dédiée.

Installer les certificats

La configuration de politique Certificat pour Windows peut être utilisée pour installer des certificats sur les appareils Windows 10/11 via Relution. Selon le type de certificat, il est possible de définir le magasin de certificats ou l'emplacement du certificat et de sa clé.

Télécharger les certificats vers Relution

Pour pouvoir distribuer des certificats via Relution, ils doivent d'abord être téléchargés dans le magasin de certificats de Relution (voir aussi Gestion des certificats →).

- Pour ce faire, il faut aller dans `Paramètres` → `Certificats`.
- Ensuite, il faut cliquer sur le bouton Ajouter.
- Un nom doit être attribué, le mot de passe doit être saisi pour les fichiers de certificat protégés par mot de passe (par exemple PKCS#12) et enfin, le fichier du certificat doit être sélectionné.
- Confirmer avec Enregistrer.

Pour la version 26.4.0

Appliquer des certificats sur les appareils Windows 10/11

1. Il faut naviguer vers `Appareils` → `Politiques` dans le portail Relution et cliquer sur Ajouter.
2. Une politique Windows doit être créée et un nom doit être attribué. Ensuite, il faut choisir Enregistrer.
3. Après un clic sur Ajouter, l'option Certificat est sélectionnée, puis il faut poursuivre avec Ajouter des détails.
4. Sous Certificat, l'option « Sélectionner un certificat » (dans le portail : Sélectionnez un certificat) est choisie et le certificat chargé dans la section précédente est sélectionné. Les autres options dépendent du type de certificat :
   - Certificat sans clé privée (PEM/DER) : choisir le Magasin de certificats (par défaut : automatiquement).
   - Certificat PKCS#12 (.p12/.pfx), modèle de certificat ou certificat utilisateur : sous Lieu du certificat, choisir Appareil (par défaut) ou utilisateur, définir l'emplacement de la clé du certificat (dans le portail : Emplacement de la clé de certification ; TPM, TPM si disponible, Logiciel ou Windows Hello pour les entreprises ; par défaut : Logiciel) et activer si nécessaire La clé est exportable. Cette option n'est disponible qu'avec Logiciel.

5. La configuration doit être enregistrée et la version actuelle de la politique doit être publiée (Publier).
6. Pour appliquer la politique aux appareils Windows 10/11, il faut ajouter les appareils souhaités via l'onglet Appareils avec cette stratégie. Les certificats sélectionnés seront alors automatiquement installés sur les appareils.

> Pour l'installation de fichiers MSIX, l'option Autorité de certification racine de confiance doit être sélectionnée comme magasin de certificats et un certificat unique exporté du conteneur PKCS#12 (format PEM) doit être utilisé.

Avec automatiquement, Relution choisit le magasin en fonction du certificat : les certificats d'autorité de certification auto-signés sont installés sous Autorité de certification racine de confiance, les autres certificats d'autorité de certification sous Autorité de certification intermédiaire et tous les autres certificats sous Personnel. Si le magasin de certificats d'une configuration existante est modifié, Relution supprime le certificat de l'ancien magasin.

Le certificat d'une configuration existante ne peut plus être modifié par la suite. Un autre certificat nécessite une nouvelle configuration. Les configurations créées avec une version antérieure à Relution 5.25 ne peuvent plus être modifiées et doivent également être recréées.

Pour la version 26.4.0

Distribuer des certificats à partir de modèles de certificats

Depuis Relution 26.0, il est également possible de distribuer des certificats à partir de modèles de certificats directement sur des appareils Windows. Le modèle (par exemple un modèle du CA intégré →) est sélectionné à l'étape 4 via « Sélectionner un certificat » à la place d'un certificat téléchargé. Les options des certificats PKCS#12 (emplacement du certificat et de la clé) s'appliquent alors.

Distribuer des certificats utilisateur

Comme alternative à « Sélectionner un certificat », l'option Utiliser un certificat utilisateur peut être choisie sous Certificat. Le certificat utilisateur du profil de l'utilisateur attribué à l'appareil est alors installé (voir Certificats utilisateur →). Le champ facultatif Nom du certificat sélectionne un certificat précis par son nom lorsque l'utilisateur en possède plusieurs et peut contenir des espaces réservés. S'il reste vide, le certificat ayant la plus longue durée de validité est utilisé. Les options des certificats PKCS#12 s'appliquent également.

PC partagé Windows

Avec la configuration de politique PC partagé (Windows Shared PC), Relution permet d'utiliser les appareils Windows 10/11 pour tous les utilisateurs. Pour garantir une utilisation conforme à la vie privée à tout moment et pour assurer la suppression des données spécifiques à l'utilisateur sur les appareils, le PC partagé permet divers paramètres et restrictions liés aux données.

Cette fonction est particulièrement utile dans les contextes scolaires, éducatifs et de recherche, ainsi que pour les institutions publiques et les entreprises qui souhaitent utiliser des PC partagés dans le respect de la vie privée à tout moment, sans que chaque utilisateur n'ait besoin de son propre ordinateur.

La configuration s'applique à Windows 10/11 Pro, Enterprise et Education. Windows Home n'est pas pris en charge.

Comment configurer la politique de PC partagés de Windows ?

Pour la version 26.4.0

Pour exécuter avec succès Shared PC sur un appareil Windows, une nouvelle politique est d'abord ajoutée sous l'élément de menu `Appareils` → `Politiques`.

Une fois la politique créée, la configuration PC partagé peut être sélectionnée et ajoutée à la politique. Il est également possible de compléter les politiques existantes par la configuration PC partagé.

Les paramètres suivants peuvent être définis dans la configuration :

- Permettre à un seul utilisateur d'être connecté à la fois : Ce commutateur active le mode PC partagé de l'appareil et est activé par défaut. S'il est désactivé, le mode PC partagé est désactivé sur l'appareil.
- Comptes qui peuvent se connecter : Détermine si seuls les comptes de domaine (Domaine) ou également les comptes invités sans mot de passe (Invité et domaine, par défaut) peuvent se connecter aux appareils. Après avoir quitté le mode invité, toutes les données temporaires sont toujours supprimées automatiquement.
- Suppression automatique des comptes après une maintenance ou une déconnexion : Si cette option est activée, Windows supprime les comptes mis en cache afin de libérer de l'espace disque (désactivée par défaut). Spécifier quand les comptes sont supprimés propose les options suivantes :
    - Supprimer immédiatement : Les comptes sont supprimés lors de la déconnexion.

    - Suppression au seuil d’espace disque : Les comptes sont supprimés dès que l’espace disque libre passe sous la valeur indiquée dans Lancer la suppression des comptes lorsque l’espace disque libre est inférieur à la limite fixée. La suppression s’arrête dès que la valeur indiquée dans Arrêter la suppression des comptes lorsque l’espace disque libre est supérieur à la normale est atteinte. Les deux valeurs sont exprimées en pourcentage (0–100, 25 par défaut). Les comptes inactifs depuis le plus longtemps sont supprimés en premier.
    - Suppression au seuil d’espace disque ou d’inactivité (par défaut) : Comme ci-dessus ; en outre, les comptes sont supprimés après le nombre de jours d’inactivité indiqué dans Jours d’inactivité après la suppression du compte (30 par défaut).
- Restreindre l’accès au stockage local : Lorsque ce paramètre est activé, l’utilisateur n’a accès qu’à ses propres données (désactivé par défaut).
- Activer l’environnement éducatif : Les recherches en ligne peuvent être fortement limitées, voire complètement bloquées pour certains sites web (désactivé par défaut).
- Obligation de s’identifier au réveil du mode veille : Si l’appareil est mis en veille alors qu’un utilisateur est connecté, une nouvelle connexion est nécessaire. Le paramètre est activé par défaut.
- Passage en mode veille après un laps de temps déterminé : Afin d’économiser la batterie, le champ Secondes après lesquelles l’appareil passe en mode veille définit au bout de combien de temps l’appareil passe en mode veille (activé par défaut, 300 secondes).
- Heure de la journée à laquelle la maintenance commence : Heure (par défaut 00:00) à laquelle commence la fenêtre de maintenance quotidienne de Windows. Pendant la maintenance, Windows exécute des tâches de maintenance, notamment la suppression des comptes selon l’option de suppression définie.

Pour la version 26.4.0

Sur les appareils Windows Pro, une configuration de fond d’écran nécessite que l’environnement éducatif soit activé. Si une configuration PC partagé dont l’option Activer l’environnement éducatif est désactivée (par défaut) est appliquée à l’appareil, aucun fond d’écran ne peut être configuré. Sans configuration PC partagé, la configuration de fond d’écran active elle-même l’environnement éducatif.

Configuration des scripts Windows

Une configuration de stratégie pour les scripts PowerShell est disponible dans Relution pour les appareils Windows gérés. Dans la sélection, la configuration s'appelle Script et peut être ajoutée aux stratégies Windows comme d'habitude. Elle est exécutée par le Compagnon Windows →, qui doit pour cela être installé sur l'appareil.

Cependant, en préparation, le script PowerShell à distribuer doit être stocké dans le menu sous Scripts.

> Le script n'est pas implémenté par Relution ; aucune garantie n'est donc donnée en cas d'éventuels dommages. Le script doit être soigneusement inspecté avant d'être appliqué à un appareil. En outre, Relution ne peut pas fournir d'assistance pour les erreurs qui peuvent se produire ou pour la création des scripts.

Configuration de la politique

Pour la version 26.4.0

La politique offre, outre la sélection du script souhaité, plusieurs autres options de configuration. Au moins l'un des deux types d'exécution (basée sur les événements ou en fonction du temps) doit être activé.

Script à exécuter

Le script précédemment enregistré doit être sélectionné ici. Il n'est possible de sélectionner qu'un seul script à la fois par configuration ; les scripts PowerShell pour Windows sont disponibles. Les espaces réservés contenus dans le script sont remplacés pour chaque appareil avant la livraison (voir Espaces réservés avancés →).

Exécution basée sur les événements

Le commutateur Exécuter un script pour les événements suivants sur l'appareil fait dépendre l'exécution du script de certains événements sur l'appareil. Au moins l'un des événements suivants doit alors être sélectionné sous Événements liés aux appareils :

- Dispositif démarré
- Utilisateur connecté – le champ facultatif Limiter le déclenchement de la connexion à un utilisateur spécifique limite l'exécution à un utilisateur. Le SID de l'utilisateur ainsi que les

formats `Domain\Username` et `Username` sont pris en charge. Si le champ reste vide, le script est exécuté lors de la connexion de n'importe quel utilisateur.
- Utilisateur déconnecté – lors de l'arrêt, il ne reste que quelques secondes pour l'exécution ; ensuite, l'appareil l'interrompt.

Exécution en fonction du temps

Le commutateur Exécuter le script dans la période de temps suivante permet d'exécuter régulièrement les scripts à des heures précises sur l'appareil cible. Les jours de la semaine sous Répète sur, l'Heure de début (par défaut : 08:00) et le Fuseau horaire (par défaut : Europe/Paris) sont obligatoires.

Restreindre l'exécution

Il est également possible d'empêcher l'exécution du script ou de modifier son comportement dans certaines circonstances. Toutes les options sont désactivées par défaut. Les configurations possibles sont les suivantes :

- Interdire l'exécution en cas de fonctionnement sur piles
- Arrêt de l'exécution lors du passage à l'alimentation par batterie
- Réveiller l'appareil pour l'exécution du script
- Masquer la tâche d'exécution du script sur l'appareil
- Permet de lancer l'exécution du script à la demande

Pour la version 26.4.0

Windows Bitlocker

Avec Relution, le chiffrement BitLocker peut être configuré dans une politique pour les appareils Windows. Les détails sur BitLocker et son fonctionnement sont disponibles dans la documentation Microsoft →.

Configuration

La configuration est divisée en quatre sections : Paramètres de base, Volumes du SE, Disques fixes et Disques amovibles.

Pour les volumes du SE, les disques fixes et les disques amovibles, le Type de cryptage (Complet, Espace utilisé uniquement, Choix de l'utilisateur ou Non configuré) et la Méthode de cryptage (CBC AES 128 bits, CBC AES 256 bits, XTS 128 bits AES ou XTS 256 bits AES) sont définis séparément. La méthode de cryptage doit être définie dans les trois sections ou être réglée sur Non configuré dans les trois, faute de quoi la politique ne peut pas être enregistrée.

Les modifications de la configuration n'ont aucun effet sur les lecteurs déjà chiffrés ou en cours de chiffrement.

pour la version 26.4.0

Paramètres de base

- Cryptage de l'appareil : active le chiffrement complet des lecteurs du système d'exploitation et des disques fixes (par défaut : activé).
- Permettre aux utilisateurs standard d'activer silencieusement le chiffrement bitlocker : autorise le chiffrement silencieux également pour les utilisateurs sans droits d'administrateur. BitLocker doit pour cela être configuré pour le chiffrement silencieux.
- Afficher un avertissement concernant le chiffrement de disque tiers : n'a d'effet que sur les appareils joints à Microsoft Entra ID. L'option est automatiquement désactivée et verrouillée dès que le chiffrement silencieux pour les utilisateurs standard est activé.

Volumes du SE

- Option de récupération avant le démarrage (texte ou URL affichés sur l'écran de récupération avant le démarrage lorsque le lecteur du système d'exploitation est verrouillé) :
  - Message et URL de récupération avant le démarrage par défaut
  - URL de récupération pré-amorçage personnalisée
  - Message de récupération pré-amorçage personnalisé

- Authentification au démarrage : une fois l'option activée, les paramètres suivants sont également disponibles :
  - Longueur minimale du code PIN (dans le portail : Longueur de broche minimale) : 4 à 20 chiffres, 6 par défaut.
  - Module de plateforme sécurisée (TPM) sur des appareils incompatibles : autorise BitLocker sans TPM. Un mot de passe ou une clé de démarrage sur une clé USB est alors nécessaire.
  - Démarrage du TPM, Code PIN de démarrage du TPM, Clé de démarrage TPM et Code PIN et clé de démarrage du TPM : chacun Non configuré, En option, Requis ou Bloqué. Si l'une de ces options est réglée sur Requis, les trois autres doivent être réglées sur Bloqué. Si Module de plateforme sécurisée (TPM) sur des appareils incompatibles n'est pas activé, les quatre options ne peuvent pas être toutes bloquées.
  - Configurer la récupération avec :
    - Autoriser l'agent de récupération de données
    - Créer un mot de passe de récupération
    - Créer une clé de récupération
    - Masquer la page de récupération au cours de l'installation
    - Enregistrer les informations de récupération dans les services de domaine Active Directory (au choix : mot de passe de récupération uniquement, ou mot de passe et clé de récupération)
    - Ne pas activer BitLocker tant que les informations de récupération ne sont pas stockées dans les services de domaine Active Directory

Pour la version 26.4.0

Disques fixes

- Exiger le chiffrement : les disques fixes non protégés par BitLocker sont montés en lecture seule.
- Options de récupération : une fois l'option activée, les paramètres suivants sont disponibles :
  - Autoriser l'agent de récupération de données
  - Créer un mot de passe de récupération
  - Créer une clé de récupération
  - Masquer la page de récupération au cours de l'installation
  - Enregistrer les informations de récupération BitLocker dans les services de domaine Active Directory (au choix : mot de passe de récupération uniquement, ou mot de passe et clé de récupération)
  - Ne pas activer BitLocker tant que les informations de récupération ne sont pas stockées dans les services de domaine Active Directory

Pour la création du mot de passe de récupération et de la clé de récupération, les valeurs Autorisé, Requis (par défaut) et Bloqué sont disponibles. Les mêmes règles s'appliquent aux

volumes du SE et aux disques fixes :

- Le mot de passe et la clé ne peuvent pas être bloqués tous les deux.
- Le mot de passe de récupération ne peut pas être bloqué si les informations de récupération sont enregistrées dans les services de domaine Active Directory.
- Le mot de passe de récupération ne peut pas être réglé sur Requis si la page de récupération est masquée et que l'enregistrement dans les services de domaine Active Directory n'est pas activé.
- La clé de récupération ne peut pas être réglée sur Requis si Exiger le chiffrement est activé pour les disques amovibles.

Disques amovibles

- Exiger le chiffrement : les disques amovibles non protégés par BitLocker sont montés en lecture seule.
- Refuser l'accès en écriture aux appareils configurés dans une autre organisation : seuls les lecteurs dont les champs d'identification correspondent à ceux de l'ordinateur obtiennent un accès en écriture.

Aucune option de récupération n'est disponible pour les disques amovibles.

Pour la version 26.4.0

Informations BitLocker dans les détails de l'appareil

À partir du serveur 5.21, Relution affiche pour chaque lecteur, dans les détails de l'appareil sous Informations sur Bitlocker, les colonnes Volume, État du volume, Statut de protection et Informations supplémentaires. Si un mot de passe de récupération existe pour un lecteur, il y est enregistré avec un horodatage dans la colonne Récupération du mot de passe. Les informations ne sont chargées qu'après un clic sur Afficher.

Chiffrement de l'appareil sans interaction de l'utilisateur

BitLocker peut être activé sur l'appareil sans action de l'utilisateur, sous certaines conditions. Cela s'applique également aux utilisateurs disposant de droits standard.

Les appareils doivent remplir les conditions suivantes :

- Version 1803 ou ultérieure pour les utilisateurs disposant de droits d'administrateur
- Version 1809 ou ultérieure pour les utilisateurs disposant de droits standard
- Appareil joint à Microsoft Entra ou Microsoft Entra hybride, ou activation via l'action Activer Bitlocker dans Relution (nécessite le Relution Companion pour Windows → installé)

- Au moins TPM 1.2
- Mode BIOS : `Native UEFI`

Appareils joints à Microsoft Entra ou Microsoft Entra hybride

Pour les appareils inscrits dans Relution et également joints à Microsoft Entra (par exemple via Autopilot), la configuration BitLocker peut être définie comme suit afin que les appareils soient chiffrés automatiquement dès que la configuration est appliquée.

Paramètres de base :

- Cryptage de l'appareil : Activé
- Permettre aux utilisateurs standard d'activer silencieusement le chiffrement bitlocker : Activé

Volumes du SE :

- Type de cryptage : Complet
- Authentification au démarrage : Activé
- Démarrage du TPM : En option ou Requis
- Code PIN de démarrage du TPM : Bloqué
- Clé de démarrage TPM : Bloqué
- Code PIN et clé de démarrage du TPM : Bloqué
- Configurer la récupération : Désactivé
    - Cette option peut également être activée ; les points suivants doivent alors aussi être configurés :
    - Créer un mot de passe de récupération : Autorisé. Requis ne peut être enregistré que si Enregistrer les informations de récupération dans les services de domaine Active Directory est également activé.
    - Créer une clé de récupération : Autorisé ou Requis. Requis n'est pas admis si Exiger le chiffrement est activé pour les disques amovibles.
    - Masquer la page de récupération au cours de l'installation : Activé

Les autres options de la configuration peuvent être définies selon les besoins. Des paramètres non pris en charge peuvent toutefois entraîner des problèmes lors de l'activation de BitLocker.

Via l'action Activer Bitlocker

Les appareils qui ne sont pas joints à Microsoft Entra ou Microsoft Entra hybride peuvent démarrer le chiffrement BitLocker sans interaction de l'utilisateur via l'action Activer Bitlocker. Cela fonctionne également pour les utilisateurs standard.

Pour la version 26.4.0

L’action est exécutée exclusivement par le Relution Companion pour Windows →, qui doit donc être installé sur l’appareil.

L’action définit, pour chaque lecteur (lettre de lecteur suivie de deux-points, par exemple `C:`), le Protecteur et l’option Espace utilisé uniquement. Les protecteurs disponibles sont TPM (uniquement pour le lecteur du système d’exploitation) et le mot de passe de récupération (dans le portail : Récupération du mot de passe). Le mot de passe de récupération est généré par Windows et apparaît dans les détails de l’appareil sous Informations sur Bitlocker. L’action Désactiver Bitlocker supprime le chiffrement des lecteurs sélectionnés.

Il est toutefois recommandé d’appliquer d’abord une configuration BitLocker sur l’appareil, par exemple pour définir la méthode de cryptage ou d’autres paramètres, même si cela n’est pas obligatoire pour l’activation automatique.

Messages de conformité

Si l’état de l’appareil ne correspond pas à la politique BitLocker, Relution signale sur l’appareil une violation de conformité avec la description `BitLocker Configuration violated. Messages:` suivie de la liste des causes signalées par Windows. Les messages ne sont disponibles qu’en anglais. Les solutions aux messages fréquents sont décrites ci-dessous.

Pour la version 26.4.0

The BitLocker policy requires a TPM protector to protect the OS volume, but a TPM is not used

La politique BitLocker exige un protecteur TPM pour le volume du système d’exploitation, mais aucun TPM n’est utilisé.

- Appliquer la configuration suivante dans la section Volumes du SE :
  - Authentification au démarrage → Activé
  - Module de plateforme sécurisée (TPM) sur des appareils incompatibles → Activé
  - Démarrage du TPM → Requis
  - Code PIN de démarrage du TPM → Bloqué
  - Clé de démarrage TPM → Bloqué
  - Code PIN et clé de démarrage du TPM → Bloqué

The encryption method of the OS volume doesn’t match the BitLocker policy

La méthode de chiffrement du volume du système d’exploitation ne correspond pas à la politique BitLocker.

- Utiliser la commande suivante pour vérifier la méthode de chiffrement de l'appareil :

```
manage-bde -status
```

- Résultat : AES ou XTS avec 128 ou 256 bits
- Configurer en conséquence le champ Méthode de cryptage dans la section Volumes du SE de la politique (par exemple XTS 256 bits AES). La méthode de cryptage doit également être définie dans les sections Disques fixes et Disques amovibles, faute de quoi la politique ne peut pas être enregistrée.

The BitLocker policy requires a TPM-only protector for the OS volume, but TPM protection is not used

La politique BitLocker exige un protecteur TPM seul pour le volume du système d'exploitation, mais la protection TPM n'est pas utilisée.

- Le Type de cryptage de la section Volumes du SE doit être modifié de Complet à Espace utilisé uniquement.

Pour la version 26.4.0

Sujets connexes

- Inscription manuelle → — Inscription manuelle des appareils Windows.

Configurer le Companion

La configuration de politique Windows Companion permet de contrôler le comportement du Relution Companion pour Windows → sur les appareils Windows gérés. La configuration est divisée en quatre sections : Général, Traitement des applications, Communication avec le serveur et Changement d'utilisateur à la connexion.

Niveau d'enregistrement

Définit le niveau de détail des entrées de journal écrites par le compagnon Windows. Les options disponibles sont Aucun, Critique, Erreur, Avertissement, Informations, Débogage et Trace — le niveau de détail augmente à chaque niveau. La valeur par défaut est Informations.

Délai d'action

Définit le temps maximum en minutes pour le traitement d'une action jusqu'à ce qu'elle soit interrompue par le compagnon Windows. La valeur par défaut est de 45 minutes ; les valeurs autorisées vont de 15 à 180 minutes.

Pour la version 26.4.0

Délai d'installation de l'application

Définit la durée maximale en minutes de l'installation d'une application jusqu'à ce qu'elle soit interrompue par le compagnon Windows. La valeur par défaut est de 45 minutes ; les valeurs autorisées vont de 1 à 150 minutes.

Délai de suppression de l'application

Définit le temps maximum en minutes pendant lequel une désinstallation d'application peut être traitée jusqu'à ce qu'elle soit interrompue par le compagnon Windows. La valeur par défaut est de 45 minutes ; les valeurs autorisées vont de 1 à 150 minutes.

Gérer WinGet et ses dépendances

Définit si WinGet et ses dépendances, comme Microsoft VC Redistributable, sont gérés et mis à jour automatiquement par le compagnon Windows. L'option est activée par défaut. Si elle est désactivée, le compagnon ne met plus WinGet à jour, mais installe toujours un Microsoft VC Redistributable manquant afin que les commandes WinGet continuent de fonctionner.

Communication avec le serveur

La communication entre le compagnon Relution et le serveur Relution est nécessaire au bon fonctionnement de Relution. Une communication est initiée soit par :

- le serveur, indiquant au compagnon de commencer à communiquer
- le compagnon, si aucune interaction entre le serveur et le compagnon n'a eu lieu pendant un certain temps

Les paramètres ci-dessous permettent aux administrateurs d'optimiser le comportement de ce mécanisme, bien que cela ne soit généralement pas nécessaire. Après le temps défini par Intervalle de contrôle, le compagnon commencera à communiquer si la dernière communication avec le serveur est plus ancienne que le temps spécifié par Temps écoulé depuis la dernière communication.

Pour la version 26.4.0

Intervalle de contrôle

Définit l'intervalle en minutes dans lequel le compagnon Windows vérifie si une demande au serveur Relution est nécessaire. La valeur par défaut est de 180 minutes ; les valeurs autorisées vont de 15 à 1 440 minutes.

Temps écoulé depuis la dernière communication

Définit la durée minimale en minutes pendant laquelle le compagnon Windows attend avant d'envoyer la demande suivante au serveur Relution. La valeur par défaut est de 120 minutes ; les valeurs autorisées vont de 15 à 600 minutes.

Changement d'utilisateur à la connexion

Depuis la version 26.4, le Relution Companion pour Windows peut mettre à jour automatiquement l'utilisateur de l'appareil défini dans Relution dès qu'une autre personne se

connecte à l'appareil Windows. Cela est particulièrement utile pour les appareils partagés par plusieurs personnes, par exemple dans une salle de classe ou un bureau paysager : l'utilisateur de l'appareil enregistré dans Relution correspond ainsi toujours à la personne réellement connectée sur l'appareil.

Activation

Cette fonctionnalité doit être activée à deux endroits pour prendre effet :

1. Au niveau de l'organisation, sous `Paramètres` → `Applications client Relution` → `Windows companion`, via l'interrupteur Activer le changement d'utilisateur de l'appareil. Ce paramètre n'est disponible que dans les organisations situées sous l'organisation globale et nécessite l'autorisation pour les applications client Relution.

2. En complément, dans chaque politique qui doit utiliser cette fonction, dans la section `Windows Companion` → `Changement d'utilisateur à la connexion` via le Mode de changement d'utilisateur. Si l'interrupteur est désactivé au niveau de l'organisation, la politique ne peut être enregistrée qu'avec le mode Désactivé ; si l'interrupteur est désactivé ultérieurement, les politiques existantes affichent une erreur correspondante à l'ouverture.

Lorsqu'il est activé, le compagnon Windows modifie l'utilisateur attribué à l'appareil dans Relution à chaque connexion Windows. Cela comporte des risques de sécurité : un utilisateur non intentionnel qui se connecte peut déclencher des changements de politique destinés à quelqu'un d'autre, et le jeton d'accès d'un administrateur peut être exposé à d'autres utilisateurs de l'appareil. Chaque politique configurée doit explicitement activer cette option pour qu'elle prenne effet.

Pour la version 26.4.0

Mode de changement d'utilisateur

- Désactivé : aucun changement automatique d'utilisateur.
- Uniquement les utilisateurs du domaine : le changement n'a lieu que si l'UPN de la personne qui se connecte correspond au domaine saisi dans le champ Domaine (sans distinction entre majuscules et minuscules) et si cette personne appartient dans Relution à l'un des fournisseurs sélectionnés sous Fournisseurs d'identité autorisés. Un domaine et au moins un fournisseur d'identité autorisé sont alors requis. Au moins un fournisseur d'identité actif doit exister dans l'organisation ; à défaut, le champ Fournisseurs d'identité autorisés ne peut pas être sélectionné et la politique ne peut pas être enregistrée dans ce mode.
- Tous les utilisateurs : Domaine et Fournisseurs d'identité autorisés sont facultatifs. Si un domaine est indiqué, le changement n'a lieu que si l'UPN y correspond (sans distinction entre majuscules et minuscules) ; si des fournisseurs d'identité sont sélectionnés, la personne doit appartenir à l'un d'eux. Si les deux champs restent vides, aucun filtrage n'est appliqué.

Dans les deux modes actifs, le changement peut en outre être restreint via Utilisateurs et groupes autorisés (bouton Modifier la sélection). Seuls les utilisateurs sélectionnés et les membres des groupes sélectionnés sont alors autorisés. Si le champ reste vide, aucune restriction supplémentaire ne s’applique.

La correspondance se fait à partir du nom de connexion Windows, comparé au nom d’utilisateur dans Relution au sein de la même organisation. Si la personne qui se connecte n’est pas connue dans Relution ou ne remplit pas les conditions configurées, l’utilisateur attribué à l’appareil est supprimé, mais aucune erreur n’est affichée sur l’appareil. À chaque changement, le champ Dernier utilisateur Entra ID connecté est mis à jour dans les détails de l’appareil ; pour les personnes inconnues dans Relution, il affiche le nom de connexion Windows au format `Domaine\Utilisateur`.

Pour la version 26.4.0

Installer une app Windows

Les applications classiques (applications `.msi` et `.exe`) peuvent être téléchargées via le portail dans le Relution App Store, puis installées et désinstallées sur tous les appareils Windows gérés par Relution. L'installation, la détection et la désinstallation sont prises en charge par le Relution Companion sur l'appareil ; celui-ci doit donc être installé sur les appareils cibles : Compagnon Windows →

Les paquets au format `.msix`, `.msixbundle`, `.appx` ou `.appxbundle` sont également téléchargés en tant qu'Appli native, mais ne nécessitent ni règles de détection ni paramètres d'installation : Créer des fichiers MSIX →

Les étapes suivantes doivent être suivies pour une installation réussie :

1. Sous `Apps` → `App Store`, l'option Appli native est sélectionnée via Ajouter.

Pour la version 26.4.0

2. À l’étape suivante, le fichier approprié au bon format (`.msi` ou `.exe`) est téléchargé via la sélection de fichier et le gestionnaire de fichiers natif.

3. Après le téléchargement, la page des détails de l'application s'ouvre. Les paramètres requis doivent être déterminés par l'administrateur et saisis manuellement. Les informations minimales sont le Nom de la version et au moins une règle de détection ; pour les applications `.exe`, les champs obligatoires de l'étape 4 s'y ajoutent. Tant qu'une information obligatoire manque, l'application ne peut pas être enregistrée.

Pour la version 26.4.0

4. Sous Informations sur la version, les paramètres d'installation et de désinstallation sont définis :
    - Pour les applications `.msi`, les champs Paramètres d'installation et Paramètres de désinstallation sont facultatifs. Le champ Paramètres de désinstallation ne peut être modifié qu'une fois une règle de détection MSI ajoutée (voir l'étape 7).

- Pour les applications `.exe`, les champs Paramètres d'installation, Chemin d'accès au désinstallateur (chemin Windows valide vers le programme de désinstallation) et Paramètres de désinstallation sont obligatoires. Au moins le paramètre d'installation silencieuse est requis ; les paramètres peuvent être sensibles à la casse.

Pour que l'installation et la désinstallation s'exécutent en arrière-plan sans intervention manuelle, le paramètre silencieux adapté au programme d'installation est défini, par exemple `/s` ou `/quiet`. Sous les champs, le portail affiche un aperçu de la commande générée, pour les applications `.msi` par exemple `msiexec /i <nom du fichier> <paramètres>` pour l'installation et `msiexec /x {<code produit>} <paramètres>` pour la désinstallation.

Pour la version 26.4.0

5. Par la suite, des règles de détection sont ajoutées pour permettre au Relution Companion pour Windows d’identifier de manière unique l’application sur la machine Windows.

6. Trois types de règles de détection sont disponibles : MSI, Fichier et Registre. Au moins une règle est nécessaire pour détecter le programme sur l'appareil Windows. Pour les fichiers `.msi`, la règle de détection MSI est nécessaire pour pouvoir désinstaller l'application. Pour les fichiers `.exe`, les deux règles de détection Fichier et Registre conviennent. Plusieurs règles de détection peuvent être combinées ; l'application n'est considérée comme installée que si toutes les règles correspondent. Une seule règle de détection MSI est possible par application.

Pour la version 26.4.0

7. Pour la règle de détection MSI, le Code produit MSI de l'application est saisi au format `{AAAAAAAA-BBBB-CCCC-DDDD-EEEEEEEEEEEE}`. Comme il peut y avoir plusieurs versions d'une application, le commutateur vérification de la version permet de vérifier en plus le numéro de version. Pour cela, La version est égale à (=) est sélectionnée dans le champ Opérateur, puis le numéro de version est saisi dans le champ Valeur. Avec La version n'est pas égale à (≠), la règle s'applique lorsqu'une autre version que celle indiquée est installée.

8. La règle de détection Fichier détermine, par la présence d'un fichier ou d'un dossier, si l'application est installée sur l'appareil Windows. Pour cela, les champs Chemin d'accès (par exemple `C:\Program Files\myApp`), Fichier ou dossier (par exemple `myApp.exe`) et Méthode de détection (Le fichier ou le dossier existe ou Le fichier ou le dossier n'existe pas) sont renseignés. Pour les applications 32 bits, le commutateur Application 32 bits est activé ; sur les clients 64 bits, le chemin indiqué est alors ajusté automatiquement, par exemple de `C:\Program Files` à `C:\Program Files (x86)`.

Pour la version 26.4.0

9. La règle de détection Registre vérifie l'existence de l'application sur l'appareil Windows à l'aide d'une clé de registre. Les champs Clé de registre, Nom de la valeur du registre et Méthode de détection sont spécifiés manuellement ; un seul caractère de remplacement (`*`) est autorisé à la fin de la clé de registre. Le nom de la valeur du registre est libre ; `DisplayName` dans la clé de désinstallation de l'application est un choix courant. Pour la Méthode de détection, les options Une valeur avec le nom spécifié existe (par défaut), Une valeur avec le nom spécifié n'existe pas et La valeur est égale à sont disponibles. Le champ Valeur n'est actif qu'avec La valeur est égale à. Afin de détecter l'application de manière unique sur l'appareil Windows, La valeur est égale à est recommandée ; la Valeur requise est obtenue à partir de l'application installée. Le commutateur Application 32 bits adapte automatiquement la clé de registre pour les applications 32 bits sur les clients 64 bits, par exemple de `HKLM\SOFTWARE\Microsoft` à `HKLM\SOFTWARE\WOW6432Node\Microsoft`.

Pour la version 26.4.0

Pour la version 26.4.0

Après avoir ajouté les règles de détection nécessaires, l’application peut être enregistrée.

Ensuite, l’application native peut être installée et désinstallée sur tous les appareils Windows gérés via le Relution App Store.

Désinstallation des applications Windows Store

Les applications Windows Store ne peuvent pas être désinstallées via l'interface graphique. Il est donc nécessaire de les supprimer localement ou via Relution à l'aide d'un script PowerShell. Voici les étapes générales :

Rechercher l'application sur l'appareil

```
Get-AppxPackage -Name *<AppName>* -AllUsers
```

Désinstaller l'application via un script

```
Get-AppxPackage -Name *<AppName>* -AllUsers | Remove-AppxPackage -AllUsers
```

Pour la version

> Le package de provisionnement de l'application peut rester sur l'appareil. Pour supprimer complètement l'application, il faut d'abord interroger le package de provisionnement et déterminer le PackageFullName.

```
Get-AppxProvisionedPackage -Online | Select PackageName
```

Puis le supprimer totalement :

```
Remove-AppxProvisionedPackage -Online -PackageName <PackageFullName>
```

Recommandation : utiliser WinGet

Dans la mesure du possible, il est recommandé d’utiliser WinGet. Il offre un accès à beaucoup plus d’applications et facilite la désinstallation : WinGet →

Pour la version 26.4.0

WinGet

Avec Relution 5.26, il est possible d'utiliser le gestionnaire de paquets WinGet → pour les déploiements d'applications sur les appareils Windows.

> Les sections Limitations et Problèmes connus décrivent des restrictions importantes.

Exigences

1. Le client WinGet doit être installé sur l'appareil. Il est disponible par défaut sur toutes les versions de Windows 11 et sur Windows 10 à partir de la version 2004 (mise à jour de mai 2020).
2. Le Microsoft Visual C++ Redistributable doit être installé sur l'appareil, voir Limitations →.
3. Relution Server version 5.26 ou supérieure.
4. Windows Companion version 1.11 ou supérieure
5. WinGet version 1.6 ou supérieure

Pour la version 26.4.0

Fonctionnalités prises en charge

Avant un déploiement à grande échelle, chaque application WinGet doit être testée sur un appareil de test.

Les sections limitations → et problèmes connus → apportent plus de détails.

- Interroger et ajouter des applications WinGet à l'AppStore de Relution
- Déploiement des applications WinGet via une action, la conformité des applications et les déploiements automatiques
- Afficher les applications WinGet installées dans la liste des applications installées d'un appareil
- Supprimer les applications WinGet via une action
- Mise à jour automatique des applications WinGet sur les appareils

Ajouter les applications WinGet au Relution AppStore

Les applications WinGet doivent être ajoutées au Relution AppStore avant de pouvoir être déployées sur les appareils.

1. Sous `Apps` → `App Store`, le bouton Ajouter ouvre la boîte de dialogue Ajouter une nouvelle application. Sous Source, l'option Winget Store app est sélectionnée.

Pour la version 26.4.0

2. L'application WinGet est recherchée par son nom, sélectionnée et ajoutée au Relution AppStore via Ajouter des détails.

Pour la version 26.4.0

3. Comme les manifestes WinGet ne contiennent pas d’icône, Relution reprend si possible le favicon du site web de l’éditeur comme icône de l’application. Une icône déjà présente, par exemple téléversée manuellement, n’est pas remplacée. Dans les détails d’une application WinGet, seule l’icône est modifiable ; tous les autres champs sont lus automatiquement depuis le store.

Les détails de l’application WinGet peuvent contenir des informations supplémentaires comme l’étendue de l’installation, si elle est fournie pour l’application WinGet.

Déployer les applications WinGet

Une fois que l'application WinGet a été ajoutée à l'AppStore de Relution et qu'elle dispose d'une version au statut de production (Version dans le portail), elle peut être déployée sur les appareils Windows.

Relution doit installer l'application WinGet de manière complètement silencieuse, voir Limitations →. En raison de cette limitation, tous les accords sur les sources et les paquets sont automatiquement acceptés lors de l'installation d'une application WinGet via Relution !

Déployer via une action

Dans la fenêtre d'action d'un appareil Windows, l'option Déployer l'application Relution Store est sélectionnée.

Pour la version 26.4.0

L’application WinGet à déployer est ensuite recherchée et sélectionnée.

Pour la version 26.4.0

Dans l'étape suivante, le déploiement peut optionnellement être ajusté. Ceci n'est actuellement possible que pour l'action de déploiement et non pour la conformité de l'application ou les déploiements automatiques.

- Type d'installateur : Spécifie le type d'installateur à utiliser, voir formats d'installateurs pris en charge →. L'application doit supporter le type d'installateur spécifié ou l'installation échouera.
- Locale : Spécifie la locale à utiliser (format BCP47, 5 caractères au maximum, par exemple `fr-FR`).
- Délai d'attente en minutes : Durée en minutes (1 à 150) après laquelle le Windows Companion interrompt l'installation. Si le champ reste vide, le Délai d'installation de l'application défini dans la configuration de politique Windows Companion → s'applique.
- Forcer l'installation : Exécute la commande et continue avec les problèmes non liés à la sécurité.
- Désinstaller la version précédente lors de la mise à jour : La version précédente de l'application est désinstallée lors de la mise à jour.
- Ignorer la mise à jour si l'application est déjà installée : Ignore la mise à jour si l'application est déjà installée.
- Arguments supplémentaires : Transmet les arguments spécifiés au programme d'installation en plus des paramètres par défaut.

Les options Désinstaller la version précédente lors de la mise à jour et Ignorer la mise à jour si l'application est déjà installée s'excluent mutuellement : l'activation de l'une désactive l'autre.

Pour la version 26.4.0

Pour la version 26.4.0

Après la confirmation de la dernière étape, une action de déploiement d’application est créée.

Déploiement via la conformité de l’application

Les applications WinGet peuvent être ajoutées à l’App Compliance d’une politique Windows.

Déployer via les déploiements automatiques

Les applications Winget peuvent être ajoutées aux déploiements automatiques d’un utilisateur.

Pour la version 26.4.0

Supprimer des applications WinGet par une action

L’action Supprimer l’application permet de désinstaller une application WinGet d’un appareil. Les applications WinGet contenues dans le Relution AppStore sont proposées à la sélection.

Le compagnon Windows exécutera la commande winget uninstall silencieusement, voir Limitations →. En raison de cette limitation, les contrats de source sont automatiquement acceptés lors de la suppression d’une application WinGet de l’appareil.

Pour la version 26.4.0

Mise à jour automatique des applications WinGet sur les appareils

Relution met automatiquement à jour les applications WinGet installées sur les appareils.

Exigences :

- L’application WinGet doit être ajoutée au magasin d’applications de Relution.
- L’application WinGet doit être contenue dans la liste des applications installées sur l’appareil.

Le Relution app store vérifie chaque jour pour chaque application WinGet contenue, si une mise à jour est disponible et rafraîchit les informations de l’application. Lorsque le Windows Companion actualise les informations de l’appareil dans Relution, Relution compare la version de

l'application WinGet installée avec la version au statut de production (Version dans le portail) du magasin d'applications Relution. Seules les entrées de la liste des applications installées dont la source est WinGet sont prises en compte. S'il détecte une version plus récente dans le magasin d'applications Relution, il déclenche une action de déploiement d'application pour cet appareil et l'application est mise à jour. Tant qu'une action de déploiement de l'application est encore ouverte sur l'appareil, aucune nouvelle action n'est créée.

Si la comparaison des versions échoue, la mise à jour automatique n'est pas déclenchée (voir Problèmes connus →).

Limitations

Les restrictions suivantes s'appliquent de manière générale à l'utilisation des applications WinGet dans Relution.

Microsoft Visual C++ Redistributable doit être installé

Le compagnon Windows exécute les commandes WinGet dans le contexte du système. Il faut donc que Microsoft Visual C++ Redistributable soit installé sur l'appareil.

Lorsque le compagnon Windows démarre, il vérifie si cette dépendance est installée. S'il n'est pas installé, le compagnon essaie de le télécharger et de l'installer. S'il n'a pas pu être installé, le compagnon Windows écrit une entrée de journal dans l'observateur d'événements de l'appareil.

Si ce problème survient, les actions WinGet échouent. Le code d'erreur -1073741515 de l'action qui a échoué peut être un indicateur. Dans ce cas, il est possible d'installer manuellement la dernière version de Microsoft Visual C++ Redistributable → en tant qu'application native avec une règle de détection, voir Problèmes connus →.

Le client WinGet doit être installé sur l'appareil

Relution n'installe pas le client WinGet. Si l'option Gérer WinGet et ses dépendances est activée dans la configuration de politique Windows Companion → (par défaut), le Windows Companion met à jour WinGet et ses dépendances, comme Microsoft Visual C++ Redistributable, à son démarrage. Si l'option est désactivée, le Windows Companion ne met pas WinGet à jour ; il installe néanmoins un Microsoft Visual C++ Redistributable manquant. Le client WinGet est disponible par défaut sur toutes les versions de Windows 11 et sur Windows 10 à partir de la version 2004 (mise à jour de mai 2020). Il est intégré à l'AppInstaller, qui peut être installé depuis le Microsoft Store.

Pour la version 26.4.0

Seule l’installation et la désinstallation silencieuses sont prises en charge

L’installation ou la désinstallation de l’application WinGet est exécutée par le Windows Companion. Le compagnon Windows est un processus d’arrière-plan qui ne peut afficher aucune interface utilisateur sur l’appareil. Par conséquent, l’installation ou la désinstallation de l’application échouera si elle ne peut pas être exécutée de manière totalement silencieuse.

Le compagnon Windows ajoutera automatiquement toutes les commandes possibles pour exécuter l’installation ou la désinstallation en silence :

```
winget install --silent --disable-interactivity --accept-package-agreements --
```

```
winget uninstall --silent --disable-interactivity --accept-source-agreements
```

Mais pour certaines applications, même ces commandes n’empêchent pas l’application d’afficher une boîte de dialogue. Un exemple est Mozilla Firefox pendant la désinstallation.

Pour la version 26.4.0

Problèmes connus

Il est recommandé de tester l’installation et la désinstallation de chaque application WinGet sur un appareil de test avant de l’utiliser en production.

Si l’application WinGet doit être utilisée dans le cadre d’une conformité d’application ou d’un déploiement automatique, elle doit figurer dans la liste des applications installées sur l’appareil après son installation et l’actualisation des détails de l’appareil.

Si la mise à jour automatique d’une application WinGet installée est importante, la liste des applications installées doit contenir l’application et avoir une valeur correcte dans la colonne de la version.

Il est impossible d’empêcher certaines applications d’afficher une boîte de dialogue

S’il est impossible d’empêcher une application d’afficher une boîte de dialogue, l’installation ou la désinstallation échouera.

Il peut être possible d’utiliser un installateur différent dans l’action de déploiement de l’application pour contourner ce problème.

Comment savoir

- Ouvrir PowerShell en tant qu’administrateur sur un appareil de test.
- Exécuter la commande `winget install --id <id> --silent --disable-interactivity --accept-source-agreements --accept-package-agreements` en remplaçant `<id>` pour l’installation.
  - Si aucune boîte de dialogue ou invite n’est affichée, l’application peut être installée silencieusement.
  - Sinon, réessayer avec un autre installateur en ajoutant `--installer-type <installer-type>` à la commande, si l’application en supporte plus d’un.
- Exécuter pour la désinstallation `winget uninstall --id <id> --silent --disable-interactivity --accept-source-agreements`
- Si aucune boîte de dialogue ou invite n’est affichée, l’application peut être supprimée silencieusement.

Pour la version 26.4.0

Alternative

Si l’application ne peut pas être installée ou désinstallée, il est recommandé d’utiliser une application native avec des règles de détection à la place.

Certaines applications ne peuvent pas être installées dans le contexte du système

Le client WinGet n’est actuellement pas pris en charge pour être utilisé dans le contexte du système. Mais le Windows Companion s’exécute dans ce contexte et, par conséquent, pour certaines applications, l’installation peut échouer.

Comment savoir

- Tester si l’application peut être installée silencieusement sur un appareil de test, voir Problèmes connus →.
- Retirer à nouveau l’application de l’appareil de test.
- Installer la même application sur le même appareil de test via Relution.

- Si l'installation échoue, il se peut que l'application ne puisse pas être installée via le contexte système.

Alternative

Si l'application ne peut pas être installée ou désinstallée, il est recommandé d'utiliser une application native avec des règles de détection à la place.

Certaines applications n'apparaissent pas dans la liste des applications installées

Certaines applications ne sont pas affichées dans la liste des applications installées, bien que WinGet les reconnaisse comme installées. Ces applications ne devraient pas être utilisées dans une configuration de conformité d'application ou dans des déploiements automatiques, car elles ne peuvent actuellement pas être détectées correctement et cela entraînerait un grand nombre d'échecs des actions de déploiement.

Comment savoir

- Installer une application WinGet sur un appareil de test
- Rafraîchir les détails de l'appareil dans Relution
- L'application devrait apparaître dans les applications installées.

Alternative

Si ce problème survient, il est recommandé d'utiliser une application native avec des règles de détection à la place.

Pour la version 26.4.0

Certaines applications ont des valeurs erronées dans la liste des applications installées

Certaines applications WinGet détectées ont des valeurs erronées dans la liste des applications installées, par exemple pour la version. Ces applications peuvent toujours être utilisées dans la configuration de la conformité des applications, mais si la version est incorrecte, la mise à jour automatique peut ne pas fonctionner.

Comment savoir

- Installer une application WinGet sur un appareil de test.
- Actualiser les détails de l'appareil dans Relution
- L'application est affichée dans la liste des applications installées, mais les valeurs des colonnes sont erronées.

Alternative

Si la mise à jour automatique de cette application n'est pas importante, elle peut être utilisée. Dans le cas contraire, il est recommandé d'utiliser une application native avec des règles de détection.

Détection des doublons dans les applications installées

Si des applications natives avec des règles de détection ont été déployées sur un appareil, l'application peut apparaître deux fois dans la liste des applications installées.

Cela ne signifie pas que l'application est installée deux fois.

Cela signifie simplement que l'application est détectée par la règle de détection et par WinGet.

Comment savoir

- Installer une application avec une règle de détection sur un appareil de test
- Actualiser les détails de l'appareil dans Relution
- L'application apparaît deux fois dans la liste des applications installées. Le nom et les autres informations affichées peuvent ne pas être exactement les mêmes.

Alternative

Actuellement, il n'y a pas d'alternative à ce comportement. Les entrées en double ne peuvent être évitées que si l'application native correspondante avec la règle de détection est supprimée du magasin d'applications de Relution et que l'application WinGet est utilisée à la place.

En raison des limitations → et des problèmes connus → des applications WinGet, il n'est pas recommandé de passer des applications natives avec des règles de détection aux applications WinGet !

Dépendance manquante Microsoft Visual C++ Redistributable

Comme mentionné dans la section limitations → la dépendance *Microsoft Visual C++ Redistributable* est nécessaire pour pouvoir travailler avec les applications WinGet dans Relution.

Par conséquent, le compagnon Windows tente de l'installer sur l'appareil, si elle est manquante. Cette vérification est exécutée lorsque le compagnon Windows est démarré, c'est-à-dire après une nouvelle installation ou un redémarrage de l'appareil.

Il peut arriver que l'installation automatique de Microsoft Visual C++ Redistributable échoue, ce qui entraîne l'échec de toutes les commandes WinGet.

Pour la version 26.4.0

Comment savoir

- Installer une application WinGet via Relution
- L'application n'est pas installée sur l'appareil
- L'action est marquée comme ayant échoué et contient éventuellement le code d'erreur -1073741515.

Alternative

La dernière version de Microsoft Visual C++ Redistributable → peut être installée manuellement en tant qu'application native à l'aide d'une règle de détection.

1. Télécharger le fichier .exe correspondant à l'architecture (x64, arm64, x86) de l'appareil.
2. Ajouter une nouvelle application native
    - Il est suggéré d'ajouter l'architecture dans le nom de l'application pour éviter toute confusion, par exemple *VC Redist x64*.
    - Paramètres d'installation suggérés : `/install /quiet /norestart`
    - Paramètres de désinstallation suggérés : `/uninstall /quiet`
    - Chemin d'accès au programme de désinstallation : doit être déterminé pour chaque version et architecture, voir ci-dessous
    - Règle de détection suggérée :
        - Registre
        - Clé de registre : HKLM\SOFTWARE\Microsoft\VisualStudio\14.0\VC\Runtimes\{x64|x86|arm64}, voir documentation Microsoft →
        - Nom de la valeur du registre : Version
        - Méthode de détection : Une valeur avec le nom spécifié existe
3. Déployer l'application sur les appareils ayant la même architecture
4. L'action doit réussir
5. Actualiser les détails de l'appareil
6. L'application doit figurer dans la liste des applications installées.

Comment détecter le chemin d'accès au programme de désinstallation :

- Ouvrir la clé de registre : HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\
- Rechercher la clé de vc_redist.{x64|x86|arm64}.exe. La clé est un code produit, par exemple *{2d48c97b-0c1e-4160-b3c4-c6dabebde745}*.
- Le chemin d'accès au programme de désinstallation peut être trouvé dans la valeur : QuietUninstallString, par exemple *C:\ProgramData\Package Cache\{2d48c97b-0c1e-4160-*

Pour la version 26.4.0

b3c4-c6dabebde745}\VC_redist.arm64.exe

Échec de la mise à jour WinGet en raison d'un manifeste défectueux

Certaines applications ne peuvent pas être mises à jour avec `winget upgrade`, même lorsqu'une version plus récente est listée dans le magasin d'applications Relution. Si la cause est un manifeste défectueux côté WinGet, la commande de mise à jour se termine avec l'un des codes d'erreur suivants -1978335189 (*no applicable upgrade*), -1978335215 (*package not found*), -1978335192 (*no applicable installer found*) ou -1978335216 (erreur de manifeste/installeur) et l'application peut tout de même être installée via un script.

Comment savoir

- La mise à jour automatique ou une action de déploiement de l'application échoue
- L'action échouée indique l'un des codes d'erreur ci-dessus

Alternative

La mise à jour peut être relancée en tant qu'installation forcée via un script Relution, voir Solution de contournement WinGet Upgrade →.

Pour la version 26.4.0

Créer des fichiers MSIX

Le format MSIX est un format de paquetage d'application Windows utilisé pour créer et distribuer des applications dans Windows 10/11. Ces fichiers MSIX ne sont généralement pas disponibles par simple téléchargement, car ils doivent être certifiés et "repackagés" avant d'être installés sur les appareils Windows.

> Les fichiers MSIX, APPX et les applications Microsoft Store ne peuvent pas être désinstallés des appareils via Relution directement ; seuls les fichiers MSI et EXE ainsi que les applications WinGet peuvent être désinstallés.

Outil d'emballage MSIX

La création de fichiers MSIX nécessite le MSIX Packaging Tool, qui peut être téléchargé depuis le Microsoft Store → et installé sur un appareil Windows.

Pour la version 26.4.0

Création du certificat

L'étape suivante consiste à créer un certificat. Cela peut être fait confortablement via PowerShell. Pour ce faire, changer le nom du certificat et/ou le mot de passe si nécessaire.

```
# Générer un nouveau certificat auto-signé avec le sujet 'CN=Relution', l'algo
# la longueur de clé 2048, l'utilisation de la clé DigitalSignature et le type
# dans le magasin de certificats personnel de l'utilisateur actuel
$Newcert = New-SelfSignedCertificate -Subject 'CN=Relution' -KeyAlgorithm RSA

# Obtenir l'empreinte du certificat nouvellement généré
$thumbprint = $Newcert.Thumbprint

# Récupérer l'objet certificat de la mémoire par son empreinte
$cert = (Get-ChildItem -Path cert:\CurrentUser\My\$thumbprint)

# vérifier si le certificat a été récupéré avec succès
if ($cert -ne $null) {
    # convertir la chaîne de mots de passe en clair en une chaîne sécurisée
    $Secure_String_Pwd = ConvertTo-SecureString "Passw0rd" -AsPlainText -Force

    # Exporter le certificat dans un fichier PKCS#12 sur le bureau de l'utilis
    Export-PfxCertificate -Cert $cert -FilePath $env:USERPROFILE\desktop\MSIXZ

    # Supprimer le certificat de la mémoire
    Remove-Item cert:\CurrentUser\My\$thumbprint
}
```

Le certificat créé doit être stocké dans la catégorie Autorités de certification racines de confiance sur tous les appareils Windows 10/11 où les fichiers MSIX doivent être installés. Cela peut être fait soit avec Relution via la configuration de la politique Certificat, soit manuellement, directement sur les appareils. La chaîne de mots de passe dans l'exemple est Passw0rd. Pour ajouter le certificat manuellement, démarrer la gestion des certificats Manage Computer Certificates en tant qu'administrateur.

Création de fichiers MSIX

Lancer le MSIX Packaging Tool et sélectionner l’option de création d’un nouveau paquetage. Décocher la case Windows Search is active dans la boîte de dialogue suivante.

Pour la version 26.4.0

Dans l’exemple, un fichier MSIX est créé pour Notepad++. Tout d’abord, un fichier d’installation doit être téléchargé. Ensuite, il faut sélectionner un fichier et un certificat dans le MSIX Packaging Tool. La Préférence de signature doit être réglée sur Signer avec un certificat (.pfx).

Les champs appropriés doivent être remplis.

Pour la version 26.4.0

Pour la version 26.4.0

Le programme d’installation de Notepad++ démarre. Il doit être exécuté normalement et les configurations doivent être définies en fonction des besoins.

Dans le MSIX Packaging Tool, cliquer sur Suivant et Oui, continuer lorsque l’installation de Notepad++ est terminée.

L’outil indiquera qu’aucun service n’a été installé et détecté. Dans la dernière boîte de dialogue, l’emplacement du paquet peut être spécifié. Terminer la création en cliquant sur Create.

Pour la version 26.4.0

Pour la version 26.4.0

Déployer le certificat sur d’autres PC Windows

Afin de pouvoir installer le paquet MSIX sur d’autres PC Windows, le certificat doit être fourni sur ces derniers. Pour ce faire, le certificat doit être exporté du conteneur PKCS#12 (`.pfx`) en un fichier de certificat unique (format PEM) à l’aide d’openSSL. OpenSSL doit être installé sur le système. Cela fonctionne avec la commande suivante :

```
openssl pkcs12 -in MSIXZertifikat.pfx -clcerts -nokeys -out MSIXZertifikat.der
```

OpenSSL 3.x et supérieur

```
openssl pkcs12 -in MSIXZertifikat.pfx -clcerts -nokeys -out MSIXZertifikat.der
```

Le certificat PKCS1 qui vient d'être converti peut alors être téléversé dans Relution sous `Paramètres` → `Certificats`. La conversion est nécessaire, car Relution installe un fichier `.pfx` téléversé en tant que certificat client et ne propose le choix du magasin de certificats que pour les certificats individuels (PKCS1).

Enfin, le certificat doit être délivré aux appareils dans une politique pour les appareils Windows. Pour ce faire, la configuration Certificat doit être utilisée et le certificat sélectionné, voir Installer les certificats →.

Il est obligatoire de sélectionner Autorité de certification racine de confiance comme Magasin de certificats. Le réglage par défaut automatiquement placerait le certificat créé dans l'exemple dans Personnel, car il ne s'agit pas d'un certificat d'autorité de certification ; Windows ne ferait alors pas confiance au paquet MSIX.

Téléverser le fichier MSIX dans Relution

Le paquet terminé est téléversé sous `Apps` → `App Store` via Ajouter avec la source Appli native. Relution accepte les formats `.msix`, `.msixbundle`, `.appx` et `.appxbundle`. L'application peut ensuite être distribuée aux appareils Windows sur lesquels le certificat est installé.

Pour la version 26.4.0

Configurer un serveur opsi

Ce guide propose une description détaillée du processus de configuration d'un serveur opsi permettant de déployer efficacement des installations Windows et d'automatiser l'inscription des appareils dans Relution. L'objectif est de mettre en place un serveur opsi fonctionnel, capable d'installer des systèmes d'exploitation Windows sur des appareils clients via le netboot, tout en les intégrant de manière transparente à Relution pour une gestion centralisée.

Ce guide couvre toutes les étapes essentielles, y compris l'installation et la configuration du serveur opsi, ainsi que la préparation des fichiers d'installation de Windows et du Windows Preinstallation Environment (WinPE). Il explique également le processus d'automatisation de l'inscription dans Relution à l'aide de produits opsi locaux.

Glossaire

on 26.4.0

Terme	Explication
Console d'administration	Désigne l'interface utilisateur incluse dans le serveur opsi et accessible sur *https://localhost:4447*.
configed	Désigne l'application Java supplémentaire qui peut être exécutée sur n'importe quel appareil pour se connecter au serveur opsi.
Console de débogage client	Désigne l'interface utilisateur de l'agent opsi, accessible sur *https://<opsi-client-IP>:4441*.

Configuration du serveur opsi

Cette section décrit le processus de configuration du serveur opsi et fournit une description détaillée des configurations, des étapes d'installation et de la préparation des paquets nécessaires.

Installation du serveur

Nous recommandons l'installation basée sur Docker pour mettre en place le serveur opsi dans des environnements Linux. Il convient toutefois de noter que l'installation Docker ne peut pas être utilisée sur des appareils macOS en raison de problèmes de compatibilité avec le serveur TFTP intégré. Pour les systèmes macOS, il convient d'utiliser la VirtualBox préconfigurée →.

Suivre les instructions de la documentation opsi ci-dessous pour configurer le serveur opsi-config. Après l'installation, la console d'administration est accessible sur *https://localhost:4447*. Télécharger également l'application Java → pour `configed`.

Documentation

- Démarrage rapide →
- Installation Docker →
- opsi-WebGui →
- Configuration réseau →

Installation des paquets opsi requis

Ouvrir la console d'administration et accéder à l'onglet Terminal. Dans le terminal, utiliser la commande suivante pour installer les paquets opsi requis :

pour la version 26.4.0

```
opsi-package-updater -v install <nom-du-paquet>
```

Un aperçu de tous les produits locaux et netboot disponibles se trouve dans le dépôt opsi →.

Installer les paquets suivants :

Paquet	Description
opsi-client-agent	Client installé sur l'appareil pour exécuter des commandes
opsi-script	Utilisé par l'agent client pour exécuter des scripts opsi
opsi-uefi-netboot	Requis pour le netboot UEFI afin de modifier l'ordre de démarrage
opsi-winpe	Crée un WinPE sur l'appareil

Paquet	Description
hwaudit (optionnel)	Outil d'inventaire qui collecte des informations sur l'appareil

Inscription des clients

Cette section traite de l'inscription auprès du serveur opsi des appareils sur lesquels un système d'exploitation Windows est déjà installé. L'agent client opsi est installé sur l'appareil pour établir la communication avec le serveur, permettant un contrôle centralisé et l'exécution d'actions.

Pour les clients sans Windows installé, des étapes supplémentaires sont nécessaires pour installer le système d'exploitation via le netboot. Dans ce cas, consulter la documentation officielle d'opsi pour des instructions détaillées sur l'initialisation des clients.

L'agent client opsi peut être téléchargé depuis `https://<opsi-server-ip>:4447/public/opsi-client-agent/`. Après l'installation sur l'appareil, l'adresse du serveur opsi et les identifiants d'un compte administrateur doivent être saisis.

Une fois l'inscription terminée, le client apparaît dans l'inventaire des appareils de `configed`. Pour vérifier la connexion entre le serveur opsi et le client, un message contextuel peut être envoyé (`Menu supérieur` → `Client` → `Envoyer un message contextuel`).

Installer le produit netboot UEFI en définissant l'action demandée sur `une fois`.

L'onglet Fichiers journaux contient des informations détaillées pour dépanner l'agent client opsi et l'image de démarrage Linux. Cela est utile pour déboguer l'installation de produits locaux et netboot.

Pour la version 26.4.0

Documentation

- Installation du client →

Pour la version 26.4.0

Préparation des fichiers d'installation Windows

Cette section fournit des instructions pour obtenir le fichier ISO Windows nécessaire, créer un environnement WinPE compatible et organiser ces fichiers dans la structure de répertoires requise pour les produits netboot. Dans cet exemple, Windows 11 a été installé sur l'appareil.

ISO Windows et WinPE

Pour préparer le serveur opsi au déploiement d'installations Windows, plusieurs composants clés sont nécessaires. Le fichier ISO Windows est d'abord nécessaire pour la version spécifique à installer, par exemple Windows 11. Le fichier ISO peut être téléchargé depuis le site officiel de Microsoft.

Ensuite, un WinPE doit être créé. Le WinPE doit correspondre à la version de l'image Windows déployée. Cela peut être réalisé en utilisant le paquet opsi-winpe, qui nécessite l'installation de Windows ADK et du plugin PE. Alternativement, le WinPE peut être créé directement avec Windows ADK, comme décrit dans la documentation opsi.

La documentation sur les produits netboot → décrit deux options pour créer un WinPE :

1. Utiliser le paquet `opsi-winpe` (Windows ADK et le plugin PE → doivent être installés !)
2. Utiliser Windows ADK.

Configurer la structure de répertoires pour le produit netboot

Installer le paquet wrapper approprié pour l'image Windows depuis le dépôt opsi Netboot → à l'aide du gestionnaire de paquets, par exemple `opsi-local-image-win11-x64_4.3.0.2-13` pour Windows 11.

Un nouveau répertoire est ajouté sur le serveur opsi (par exemple */var/lib/opsi/depot/win11-x64*). Les fichiers de l'image Windows et les fichiers WinPE doivent être placés dans les répertoires correspondants (voir aperçu de la structure de répertoires →).

Fichiers d'installation

Le contenu du fichier ISO Windows doit être déplacé dans le répertoire `installfiles`.

WinPE

Le WinPE doit être déplacé dans le répertoire `winpe`.

> Extraire tous les fichiers des sous-répertoires (*fwfiles*, *media*, *mount*) et les placer au niveau racine. Des problèmes de détection de `setup.exe` peuvent survenir, il convient donc de placer également les répertoires au niveau racine.

Pour la version 26.4.0

À la fin, tous les fichiers et répertoires du WinPE se trouvent au niveau racine du répertoire suivant :

> Afficher l'exemple de configuration complet

Documentation

- Installation du système d'exploitation Windows →
- Produits netboot →

Configurer le serveur DHCP

Pour configurer un serveur DHCP pour le démarrage PXE, des options spécifiques doivent être définies afin de fournir aux clients PXE les informations nécessaires pour localiser le serveur

TFTP et télécharger le fichier de démarrage (bootloader). Ces options sont généralement désignées comme les options DHCP 66 (serveur TFTP) et 67 (fichier de démarrage).

Si le routeur utilisé ne propose pas d'interface pour configurer ces options, par exemple dans le cas d'un serveur DHCP Linux ou Windows, les options suivantes doivent être ajoutées au fichier `dhcpd.conf` :

```
next-server <opsi-server-IP>;
filename "opsi/opsi-linux-bootimage/loader/opsi-netboot.efi";
```

Démarrer le netboot

Pour lancer l'installation d'un produit netboot, accéder à l'onglet Produits netboot dans l'interface Configed. Régler l'action demandée du produit souhaité sur `Setup` et cliquer sur l'icône d'enregistrement dans le coin supérieur gauche.

Une fois l'action envoyée, le processus peut être surveillé en consultant les journaux dans les détails du client de `configed` ainsi que dans la `console de débogage client`. Ces journaux indiquent si le client opsi a bien reçu et traité l'action. Une fois ces étapes terminées, le client Windows recherchera des sources netboot lors du prochain redémarrage et lancera le processus d'installation.

Pour la version 26.4.0

Pour le dépannage, les commandes suivantes permettent d'observer le trafic TFTP sur le serveur opsi :

```
sudo tcpdump -i lo0 port 69
```

```
journalctl -f
```

Documentation

- opsi avec UEFI/GPT →

> Pour les installations de Windows 11, s'assurer que l'appareil prend en charge le TPM 2.0. Vérifier dans le menu du BIOS si l'option est activée. Il est parfois nécessaire de désactiver puis réactiver le TPM, ou de le réinitialiser au prochain redémarrage.

Inscription dans Relution

Cette section décrit le processus d'inscription des appareils dans Relution à l'aide du paquet `relution-enrollment`. Ce produit automatise l'installation d'un paquet de provisionnement via PowerShell, garantissant ainsi une intégration transparente des appareils dans Relution.

Préparer le paquet de provisionnement

Un paquet de provisionnement doit être créé conformément aux instructions relatives à l'inscription en masse Windows →.

> Le paquet doit être nommé relution afin que le script opsi puisse reconnaître le bon fichier.

Installer le paquet opsi pour l'inscription Relution

Le paquet `relution-enrollment` est disponible en version *expérimentale* dans le dépôt opsi public →.

Télécharger le fichier `relution-enrollment_<package-version>.opsi` avec la commande `wget` et exécuter la commande suivante pour installer le paquet opsi afin qu'il soit disponible dans l'interface `configed` :

Pour la version 26.4.0

```
opsi-cli package install relution-enrollment_<package-version>.opsi
```

Après l'installation, le paquet est disponible dans le dossier de dépôt (`/var/lib/opsi/depot/relution-enrollment`). Placer le paquet de provisionnement généré dans ce dossier et exécuter `opsi-set-rights` dans ce répertoire.

```
/var/lib/opsi/depot/relution-enrollment/
├── enrollment.opsiscript
├── relution.ppkg
├── relution-enrollment.files
```

Installer le produit

Pour installer le paquet, sélectionner le client et accéder à l'onglet Produits localboot. Pour le produit `relution-enrollment`, régler l'action demandée sur `une fois`. Enregistrer l'état et déclencher une action `on_demand` (`Menu` → `Client` → `Déclencher l'événement opsiclientd` → `on_demand`).

Comme la commande PowerShell d'installation du paquet de provisionnement marque toujours l'action comme réussie, vérifier les journaux pour repérer d'éventuelles erreurs. L'erreur `Package installation failed, error code -2147024713 (800700B7)` indique qu'un paquet portant le même identifiant est déjà installé.

Si le paquet de provisionnement a déjà été installé, il doit d'abord être supprimé.

Pour la version 26.4.0

Pour la version 26.4.0

Conseils de dépannage

Cette section décrit les problèmes courants pouvant survenir lors de la configuration du serveur opsi et de l'installation netboot, ainsi que des solutions ou des références vers la documentation pertinente pour le dépannage :

- Erreur : Unable to get geometry for disk '/dev/nvme0n1' →
  - Définir le mot de passe de l'utilisateur root en configurant le paramètre hôte `netboot.linux-bootimage.cmdline.pwh`.
  - Si l'erreur survient, appuyer sur `Ctrl + Alt + F3/F4/F5` pour basculer vers le terminal actif.
  - Saisir les identifiants root et le mot de passe.
  - Exécuter la commande `sgdisk --zap-all /dev/nvme0` pour supprimer la partition.
  - Revenir à l'autre terminal et relancer le netboot.
  - Pour plus d'informations, consulter la documentation sur les produits netboot →.
- opsi winPE est vide → : déplacer tous les fichiers des sous-répertoires WinPE (par exemple media) vers le niveau racine.
- L'initialisation de WinPE ne fonctionne pas →

Certificat d'identité

Les appareils Apple et Windows enrôlés dans Relution reçoivent un certificat d’identité. Celui-ci est valable 1 an et est automatiquement renouvelé tant qu’il y a une communication avec l’appareil. Il peut arriver que des appareils soient stockés ou inactifs, et que le certificat d’identité ne puisse pas être renouvelé en conséquence. Pour des raisons de sécurité, Relution refuse toute communication avec un appareil si le certificat d’identité a expiré.

Vérifier et renouveler le certificat d’identité

Les appareils concernés peuvent être vérifiés sous `Navigation` → `Appareils` → `Inventaire` → `[Appareil concerné]` dans l’onglet Informations du bloc Sécurité. Il y a 3 champs pertinents ici :

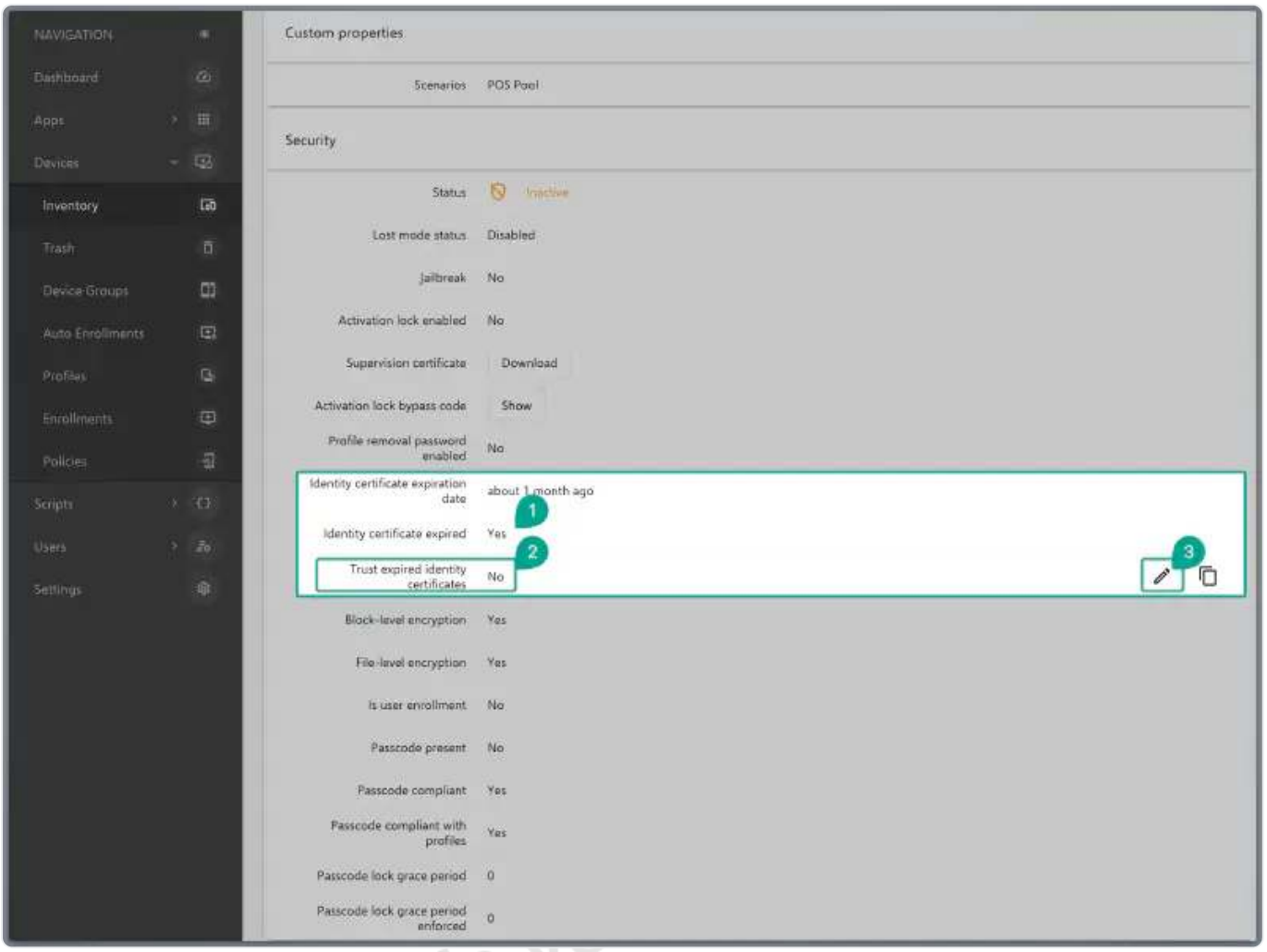
- Date d’expiration du certificat d’identité
- Le certificat d’identité a expiré
- Faire confiance aux certificats d’identité expirés

Pour la version 26.4.0

Si le certificat d’identité a expiré et que Faire confiance aux certificats d’identité expirés n’est pas encore actif, le survol de cette ligne avec la souris fait apparaître le bouton Éditer (icône crayon). Un clic sur ce bouton ouvre une boîte de dialogue de confirmation. Après confirmation, Relution accepte temporairement les messages MDM signés avec le certificat expiré et déclenche le renouvellement : pour les appareils Windows, une action de renouvellement du certificat client est mise en file d’attente ; pour les appareils Apple, le profil MDM est mis à jour. La communication avec l’appareil redevient ainsi digne de confiance et les commandes MDM peuvent être traitées. Dès que l’appareil a reçu un nouveau certificat d’identité, Relution réinitialise automatiquement Faire confiance aux certificats d’identité expirés.

L’action nécessite l’autorisation de modifier les appareils.

> Faire confiance à des certificats expirés présente un risque de sécurité, par exemple lorsque le certificat d'identité a été rendu accessible à des tiers.



Pour la ve

Remarque importante : L'action est disponible dès que le certificat d'identité a expiré et peut également être exécutée lorsque l'appareil est hors ligne. Dès que l'appareil est de nouveau en ligne, il reçoit un nouveau certificat d'identité valide.

Plusieurs appareils concernés peuvent être retrouvés sous `Navigation` → `Appareils` → `Inventaire` à l'aide des filtres Le certificat d'identité a expiré et Faire confiance aux certificats d'identité expirés.

Publier des scripts globalement

Avec Relution `Server Version 5.22`, il est possible de publier des scripts Windows de manière centralisée et de les mettre ainsi à la disposition de toutes les organisations. Cela se fait dans l'organisation globale (jusqu'à la version 5.22 : organisation du magasin).

> Un script créé dans l'organisation globale n'est d'abord visible que dans celle-ci. Ce n'est qu'après Définir la visibilité comme globale qu'il est disponible pour toutes les organisations, y compris celles créées ultérieurement. Cette étape ne peut pas être annulée. Le script ne peut ensuite être modifié ou supprimé que dans l'organisation globale.

Ajouter un script

Une fois la connexion à l'organisation globale établie, la section Scripts est accessible via la navigation sur le côté gauche. Il est alors possible d'y créer de nouveaux scripts à l'aide du bouton Ajouter. La création est divisée en 3 points.

Pour la version 26.4.0

Général

- Nom - Le nom d'affichage global du script (obligatoire, 255 caractères maximum)
- Description - Une description supplémentaire du script (4000 caractères maximum)
- Plateforme - Pour les scripts Windows, Windows est sélectionné (obligatoire, présélectionné). Les fichiers `*.ps1` et le champ Arguments ne sont proposés que pour Windows. La plateforme ne peut plus être modifiée après l'enregistrement et est également verrouillée tant qu'un fichier script est chargé.

> Les modifications ultérieures d'un script disponible globalement s'appliquent à toutes les organisations. Sur les appareils dont la politique utilise le script, celui-ci est mis à jour automatiquement.

Contenu

- Fichier script - Un fichier local `*.ps1` peut être chargé via Sélectionnez (ou par glisser-déposer). Son contenu est repris dans le champ Contenu.
- Contenu - Le script peut également être saisi directement dans le champ de texte. Dès que le champ contient du texte, Fichier script est masqué.

Exécution

- Délai d'attente (en minutes) - Après l'expiration de la période de temps spécifiée, l'exécution du script est interrompue de force. Valeur par défaut : 5 minutes, plage autorisée : 1 à 30 minutes.
- Arguments - Les arguments et les valeurs qui leur sont attribuées sont insérés au début du script lorsqu'il est exécuté sur l'appareil (512 caractères maximum). Chaque affectation, sauf la dernière, doit se terminer par un point-virgule. Les arguments peuvent être utilisés dans le script par leur nom.

Exemple :

```
# Arguments (champ « Arguments »)
$arg1=10; $arg2='text'

# Utilisation dans le script
Write-Host $arg1

# Exécution sur l'appareil : ./test.ps1
# Résultat de l'exécution : 10
```

Pour la v

Placeholders disponibles

Les placeholders disponibles peuvent être utilisés aussi bien directement dans le contenu du script (point Contenu) que dans les Arguments sous Exécution. Les placeholders disponibles dans le formulaire sont affichés sous les champs de saisie. Exemple d'argument : `$serial='${device.serialnumber}'`. D'autres fonctions, comme les sous-chaînes ou les valeurs par défaut, sont décrites dans l'article Espaces réservés avancés →.

Rendre un script disponible globalement

Après l'enregistrement, le script n'est visible que dans l'organisation globale. Pour le mettre à la disposition de toutes les organisations, le script est sélectionné dans la liste sous Scripts, puis Définir la visibilité comme globale est choisi dans le menu contextuel (menu à trois points de la ligne ou de la barre d'actions). La boîte de dialogue qui suit liste les scripts concernés ; Publier applique la modification. La fonction nécessite l'autorisation de modifier les scripts.

Pour la version 26.4.0

Cette action ne peut pas être annulée.

Dans les autres organisations, le script apparaît ensuite en lecture seule dans l'onglet Depuis Mondial de la liste des scripts. Il peut y être utilisé dans une politique avec la Configuration des scripts Windows → ou via l'action Exécuter le script PowerShell. Tant que le script est utilisé dans une politique publiée d'une organisation quelconque, il ne peut pas être supprimé, pas même dans l'organisation globale.

Dans une méta-organisation, la même fonction est disponible sous le nom Définir la visibilité à méta ; le script est alors visible dans les organisations de cette méta-organisation.

L'installation d'Office est bloquée

Avec la version 5.21 de Relution Server, il est possible d'installer Microsoft Office sur les appareils Windows gérés à l'aide d'un fichier de configuration (XML). Avec la version 5.22, une configuration correspondante et une extension de l'action ont été ajoutées. L'installation est possible via la configuration de politique Windows Office → ou via l'action Déployer Office 365 et est prise en charge sur Windows Pro, Enterprise et Education à partir de la version 1703, mais pas sur Windows Famille (Home).

Cette installation peut échouer pour de nombreuses raisons.

En principe, l'action Déployer Office 365 ne doit pas être utilisée si l'installation a déjà été configurée dans la politique. Un redémarrage doit être évité pendant l'installation.

Cas de problème

1. L'action de modification de politique (Politique de changement dans le portail) a le statut Pas maintenant.
2. Office ne s'installe pas, bien qu'aucune erreur ne soit visible dans la liste des actions.

Pour la version 26.4.0

Dans les deux cas, il est toujours utile de jeter un coup d'œil au gestionnaire des tâches de l'appareil. Souvent, des activités en arrière-plan sont en cours d'exécution, ce qui indique une installation en cours, ou la carte réseau affiche un trafic de téléchargement.

Cas 1 - Pas maintenant

L'action de modification de politique pour une politique avec la configuration Windows Office reste dans le statut Pas maintenant. Ce statut n'apparaît que lors de l'installation d'Office via une politique, lorsqu'une installation est encore en cours sur l'appareil ou qu'une autre suite Office doit d'abord être désinstallée. L'action Déployer Office 365 ne reçoit jamais ce statut.

1. Une action Actualiser les informations sur l'appareil est envoyée à l'appareil.
2. L'installation peut contenir de grandes quantités de données qui doivent être téléchargées et traitées. En fonction de la connexion et du matériel utilisés, cela peut prendre beaucoup de temps. Il convient d'attendre au moins une heure si ce statut apparaît.
3. Une fois l'heure écoulée, une nouvelle action Actualiser les informations sur l'appareil est envoyée à l'appareil. Si l'action de modification de politique a été délivrée il y a au moins 60 minutes, Relution poursuit l'application de la politique, même si l'appareil signale encore une installation en cours. Sans cette actualisation, cela ne se produit qu'à la prochaine

actualisation automatique des informations de l'appareil ou lorsque l'appareil signale la fin de l'installation d'Office.

4. Si le statut ne change toujours pas, l'installation peut être réinitialisée à l'aide de l'action Déployer Office 365, en choisissant l'option d'effacement des données d'installation d'Office. Le commutateur Désinstaller la suite Office 365 actuelle permet en outre de supprimer la suite Office installée. Si aucune donnée d'installation n'est présente sur l'appareil et que le commutateur n'est pas activé, l'action échoue.
5. Il convient d'attendre au moins cinq minutes avant de relancer l'installation.

Cas 2 - Office ne semble pas s'installer sans raison

Ce cas peut se produire lors de l'utilisation de la configuration de la politique. Dans ce cas, la politique doit toujours être réappliquée en premier lieu (Réappliquer les politiques) et le comportement ultérieur doit être observé.

Si cela ne fonctionne pas non plus, l'installation d'Office, qui peut être bloquée, peut être réinitialisée comme décrit dans le cas 1, étape 4 (action Déployer Office 365 avec l'option d'effacement des données d'installation d'Office).

La politique doit ensuite être de nouveau réappliquée (Réappliquer les politiques).

Si l'appareil signale une erreur lors de l'installation via la politique, l'action de modification de politique passe au statut Erreur et la violation de conformité La configuration de Windows Office n'est pas valide est générée. L'action Déployer Office 365, en revanche, signale déjà un succès dès que l'appareil a accepté la commande ; un échec ultérieur de l'installation n'y est pas visible.

Pour la version 26.4.0

Compagnon Windows

Le Relution Companion pour Windows est un service Windows qui est installé sur tous les appareils Windows gérés par Relution, à l'exception des appareils sous Windows Home et des appareils dont l'édition n'est pas reconnue. Il ne s'agit pas d'une application ordinaire disponible dans le Windows App Store ou le Relution App Store. Relution Companion pour Windows dispose de droits d'administration, est destiné aux administrateurs uniquement et s'exécute entièrement en arrière-plan. Il n'interagit pas avec les utilisateurs finaux.

Installation

Avec la version 5.15 de Relution Server, le Relution Companion pour Windows est automatiquement installé sur tous les appareils Windows nouvellement inscrits, sauf sous Windows Home. Si l'appareil Windows est déjà géré par Relution, le Relution Companion pour Windows sera également installé automatiquement. Sous Windows Home, le Companion n'est pas disponible, pas plus que les scripts PowerShell ou l'installation de paquets MSI et EXE : Limites de Windows Home →

Sur l'appareil Windows, sous Paramètres, l'inscription Relution Connecté à Relution est affichée. Dans le sous-menu Info, il est visible que le Relution Companion pour Windows a été installé avec succès.

Pour la version 26.4.0

Pour la version 26.4.0

Tant que le Companion ne s’est pas manifesté auprès du serveur après l’installation, l’appareil affiche l’avis de conformité « Le Companion Windows n’est pas installé ! ». Si un Companion installé ne répond plus, cet avis devient une violation de conformité et le Companion est réinstallé. Lorsqu’une version plus récente du Companion est disponible sur le serveur, le Companion est automatiquement mis à jour sur l’appareil.

Si un appareil Windows n’est plus géré par Relution, le Relution Companion pour Windows est automatiquement supprimé de l’appareil.

Objectif du Relution Companion pour Windows

Par défaut, la configuration des périphériques Windows enrôlés dans Relution utilise ce que l'on appelle les fournisseurs de services de configuration (Configuration Service Providers, CSP), qui permettent d'accéder à certains paramètres du système Windows. Les possibilités de configuration sont cependant limitées. Grâce au Relution Companion pour Windows, les options de configuration sont considérablement élargies.

Options supplémentaires

Avec le Relution Companion pour Windows, des scripts PowerShell supplémentaires à usage unique basés sur Windows peuvent être exécutés sur les appareils Windows enrôlés via les actions Relution.

Un autre avantage de Relution Companion pour Windows est l'installation et la désinstallation d'applications classiques dans le contexte de l'appareil. Cela permet d'installer et de désinstaller les fichiers `.msi` et `.exe` sur les appareils Windows inscrits via l'App Store de Relution.

Par ailleurs, les fonctions suivantes passent exclusivement par le Companion : l'installation d'applications WinGet, l'exécution régulière de scripts via la Configuration des scripts Windows → ainsi que les actions Réinitialiser le mot de passe (Windows), Activer Bitlocker et Désactiver Bitlocker. Le comportement du Companion lui-même est piloté par la politique Configurer le Companion →.

Pour la version 26.4.0

Application de scripts Powershell aux appareils Windows

Les scripts PowerShell sont des fichiers texte contenant au moins une commande PowerShell qui est exécutée par Windows lorsque le fichier est ouvert. Les processus, tant sur l'ordinateur que chez Relution, peuvent s'en trouver grandement facilités. Les fichiers de script sont écrits par l'administrateur lui-même et enregistrés sous l'extension `.ps1`. Seuls les scripts PowerShell ne nécessitant aucune interaction de la part de l'utilisateur peuvent être exécutés, puisque le Relution Companion pour Windows fonctionne entièrement en arrière-plan. Pour réinitialiser des mots de passe utilisateur oubliés, l'action dédiée Réinitialiser le mot de passe (Windows) est désormais disponible.

Depuis Relution 5.16, les scripts PowerShell sont gérés de manière centralisée dans Relution. Un script n'est donc plus téléversé dans l'action, mais créé au préalable sous `Scripts` → `Scripts` via Ajouter. Les valeurs par défaut de Délai d'attente (en minutes) et Arguments y sont également définies. La sélection d'un script dans l'action nécessite le droit de lecture des scripts ; sans ce droit, aucune liste de scripts n'est affichée.

Pour exécuter avec succès un script PowerShell sur un appareil Windows, les étapes suivantes doivent être effectuées :

1. Dans l'inventaire des appareils, appeler l'appareil Windows désiré et, sur la page de détails de l'appareil, sous l'onglet Actions, cliquer sur le bouton Appliquer l'action.
2. Sélectionner ensuite l'action Exécuter le script PowerShell.

3. Sélectionner le script PowerShell souhaité dans la liste des scripts gérés.

Pour la version 26.4.0

4. À la deuxième étape, Définir les paramètres d'exécution des scripts, les valeurs du script sélectionné sont préremplies et peuvent être adaptées pour cette exécution :
    - Le champ obligatoire Délai d'attente (en minutes) (de 1 à 30) définit après combien de minutes l'exécution du script est interrompue de force.
    - Le champ Arguments accepte des affectations de variables au format `$arg1=10; $arg2='text'` (512 caractères au maximum ; chaque affectation, sauf la dernière, se termine par un point-virgule). Elles sont insérées au début du script avant son exécution, et le script peut utiliser ces variables par leur nom, par exemple `Write-Host $arg1`.

5. Le script PowerShell exécuté est listé sur la page de détails de l’appareil, sous l’onglet Actions.

Un script peut aussi être lancé directement sous `Scripts` → `Scripts` via Exécuter sur l’appareil. L’état d’exécution ainsi que le résultat et la sortie d’erreur de chaque exécution sont consultables dans l’historique du script concerné sous `Scripts` → `Scripts` (Afficher le résultat, Afficher la sortie d’erreur).

Pour la version 26.4.0

Limites de Windows Home

L'édition Windows Home est limitée en termes de possibilités d'administration par rapport aux autres éditions. Les fonctions qui ne sont pas disponibles peuvent souvent être reconnues dans l'interface web par le fait qu'elles ont des badges indiquant quelles éditions sont prises en charge. Par conséquent, l'édition Windows Home n'y figure pas. Toutes les fonctions concernées ne portent cependant pas un tel badge.

Les appareils sous Windows Home peuvent être retrouvés dans la liste des appareils via la colonne ou le filtre Édition OS (valeur Accueil, qui désigne Windows Home dans le portail).

Les restrictions concernent notamment les fonctions suivantes :

Installation d'applications

L'API Microsoft MDM (CSP) pour l'installation des applications MSIX et Microsoft Store n'est pas disponible sur Windows Home. Relution n'est donc pas en mesure d'installer ces applications. Par conséquent, les politiques qui en dépendent (conformité des applications) ne sont pas non plus disponibles.

Pour la version 26.4.0

Cette restriction affecte également l'installation automatique de Relution Companion pour Windows. Par conséquent, l'installation des paquets MSI et EXE n'est pas non plus disponible sur Windows 10/11 Home, puisque cette fonction nécessite un Companion installé/configuré.

Ainsi, les actions suivantes ne sont pas disponibles sur Windows 10/11 Home :

- Déployer l'application Relution Store (y compris l'installation d'applications MSI, EXE et WinGet)
- Supprimer l'application
- Déployer Office 365
- Effacer les données d'installation d'Office 365

De plus, la politique suivante n'est pas disponible :

- Conformité App

Exécution de scripts PowerShell

L'exécution de scripts PowerShell nécessite l'installation du Relution Companion pour Windows. En raison de la restriction concernant l'installation des applications, il n'est pas possible d'installer le Companion. Par conséquent, il n'est pas non plus possible d'exécuter des scripts PowerShell via le Companion sur les appareils fonctionnant sous Windows Home Edition.

Ainsi, l'action suivante n'est pas disponible sur Windows 10/11 Home :

- Exécuter le script PowerShell

Autres fonctions du Companion

Le Relution Companion pour Windows → n'est jamais déployé sous Windows Home ; il en va de même pour les appareils dont Relution ne reconnaît pas l'édition (Édition OS Autres). Outre les scripts PowerShell et l'installation d'applications, toutes les autres fonctions qui passent par le Companion sont donc également indisponibles, par exemple les actions Réinitialiser le mot de passe (Windows), Activer Bitlocker et Désactiver Bitlocker ainsi que l'exécution régulière de scripts via une politique.

Pour la version 26.4.0

Autres actions et politiques

Les actions suivantes ne sont pas non plus prises en charge sous Windows Home :

- redémarrage de l'appareil (Appareil de redémarrage dans le portail)
- Ajouter des comptes

Les politiques suivantes ne sont pas appliquées sous Windows Home :

- Bitlocker
- Mise à jour Windows
- Pare-feu Windows
- Mode kiosque Windows
- PC partagé
- Windows Office
- Options de sécurité de l'appareil local
- proxys globaux (Proxies mondiaux dans le portail)
- BranchCache
- Papier peint

- Contrôle des applications

Dans les restrictions (Les restrictions dans le portail), de nombreux paramètres individuels ne sont pas non plus pris en charge sous Windows Home.

Restent notamment disponibles sous Windows Home les actions Effacer l'appareil (à partir de la version 1709) et analyse de l'appareil (Périphérique de balayage dans le portail, à partir de la version 1809) ainsi que les politiques VPN et Antivirus (partiellement).

Afficher les applications installées

L'API Microsoft MDM (CSP) pour interroger les applications modernes installées (Microsoft Store/MSIX) n'est pas disponible sur Windows 10/11 Home. Ainsi, Relution ne peut pas découvrir les applications installées pour les appareils inscrits et par conséquent ne peut pas les afficher dans les détails d'un appareil sous Apps installées.

La découverte des applications installées via EXE / MSI nécessite l'installation d'un Relution Companion pour Windows. En raison de la limitation concernant l'installation des applications, il n'est pas possible d'installer le Companion. Par conséquent, il n'est pas non plus possible de détecter les applications installées via le Companion sur les appareils fonctionnant sous Windows Home Edition.

Pour la version 26.4.0

Ainsi, les informations suivantes ne sont pas disponibles sur Windows 10/11 Home :

- Affichage des applications installées.

Mise à niveau vers une édition supérieure

La politique Licences Windows permet de mettre à niveau un appareil sous Windows Home vers une édition supérieure à l'aide d'une clé de produit, voir Configurations disponibles →. Une mise à niveau effectuée de cette manière ne peut pas être annulée en supprimant la politique.

URL pour Microsoft Store

Les appareils Windows gérés qui utilisent le Microsoft Store pour acquérir, installer ou mettre à jour des applications doivent avoir accès à ces points de terminaison via les ports TCP 80 et 443 du pare-feu.

API Microsoft Store (AppInstallManager):

- `displaycatalog.mp.microsoft.com`
- `purchase.md.mp.microsoft.com`
- `licensing.mp.microsoft.com`
- `storeedgefd.dsx.mp.microsoft.com`

Au moment de la création de ce document, ce sont les points de terminaison actuellement requis.
La documentation complète est fournie par Microsoft ici :
Documentation Microsoft →

Pour la version 26.4.0

Contournement WinGet Upgrade

Certaines applications WinGet ne peuvent pas être mises à jour par `winget upgrade`, bien qu'une version plus récente soit listée dans le magasin d'applications Relution. La cause est presque toujours un manifeste défectueux côté WinGet — la commande de mise à jour échoue alors avec *no applicable upgrade*, *package not found*, *no applicable installer found* ou une erreur apparentée.

La solution de contournement proposée par Microsoft consiste à réinstaller l'application avec le drapeau `--force`. Le script ci-dessous automatise cette récupération pour une application WinGet unique et peut être exécuté sur les appareils avec l'action Exécuter le script PowerShell.

> Il s'agit d'une solution de contournement. Elle ne devrait être utilisée que pour les applications dont la mise à jour normale est connue pour échouer. Une installation forcée remplace les fichiers de paquet existants et peut masquer d'autres problèmes d'installation.

Script

Pour la version 26.4.0

Le script est créé en tant que script PowerShell sous `Scripts` → `Scripts` via Ajouter, puis exécuté sur les appareils avec l'action Exécuter le script PowerShell ou, dans la liste des scripts, via Exécuter sur l'appareil. Il est exécuté par le compagnon Windows dans le contexte de l'appareil (SYSTEM). Au début du script, la variable `$AppIdentifier` doit être définie sur l'identifiant WinGet exact de l'application à réparer (par exemple `Nextcloud.NextcloudDesktop`).

L'identifiant peut aussi être transmis dans le champ Arguments (par exemple `$AppIdentifier='Nextcloud.NextcloudDesktop'`), de sorte qu'un même script puisse servir pour plusieurs applications. Dans ce cas, la première ligne du script doit être supprimée, car elle écraserait sinon la valeur transmise.

Par défaut, les scripts ont un Délai d'attente (en minutes) de 5 minutes. La mise à jour et l'installation forcée d'applications volumineuses pouvant durer plus longtemps, la valeur devrait être augmentée en conséquence lors de la création du script ou dans l'action (30 minutes au maximum).



Fonctionnement

1. Le script recherche `winget.exe` dans `C:\Program Files\WindowsApps\Microsoft.DesktopAppInstaller_*` — l'installation utilisée par le Windows Companion dans le contexte système.
2. Il appelle `winget list --id <AppIdentifier> --exact` pour vérifier si l'application est déjà installée. Si ce n'est pas le cas, le script se termine sans rien faire.
3. Il appelle `winget upgrade --id <AppIdentifier> --exact` avec les paramètres silencieux obligatoires → de Relution. Les paramètres sont étalés avec `@SilentFlags` afin que PowerShell transmette chaque élément comme argument distinct — nécessaire pour que WinGet les analyse correctement. Si la mise à jour réussit, le script se termine.
4. Si la mise à jour se termine avec l'un des codes d'erreur WinGet récupérables, le script réessaie en tant que `winget install --id <AppIdentifier> --exact --force` avec les mêmes paramètres silencieux. Les codes reconnus sont :
   - `-1978335189` — *no applicable upgrade*
   - `-1978335215` — *package not found*
   - `-1978335192` — *no applicable installer found*
   - `-1978335216` — erreur de manifeste/installeur observée en pratique
5. Tout autre code de sortie WinGet est transmis tel quel.

La détection repose uniquement sur les codes de sortie de WinGet. La sortie texte dépendrait de la langue de l'appareil et différerait entre les installations Windows en anglais et en allemand.

L'état d'exécution ainsi que le résultat et la sortie d'erreur du script (par exemple les messages de `Write-Host`) sont consultables dans l'historique du script sous `Scripts` → `Scripts` (Afficher le résultat, Afficher la sortie d'erreur).

Si la réparation doit être exécutée régulièrement, le script peut aussi être exécuté de manière planifiée ou sur événement via la configuration de politique Configuration des scripts Windows →.

Pour la version 26.4.0

Code d'erreur WinGet

Erreur WinGet -1073741515

L’installation d’applications WinGet via Relution échoue avec le code d’erreur suivant : `-1073741515` (`0xC0000135`)

Cause

Lors de l’installation d’applications via WinGet, une erreur peut survenir si le redistribuable Microsoft Visual C++ n’est pas installé sur la machine cible.

Solution

Le compagnon Windows installe lui-même un redistribuable Microsoft Visual C++ manquant, même si l’option Gérer WinGet et ses dépendances est désactivée dans la politique Configurer le Companion →. Si l’erreur persiste, une installation manuelle permet d’y remédier.

La description complète de la cause, ainsi que la solution consistant à installer manuellement une application native avec une règle de détection, incluant les chemins de registre requis et la détermination du chemin du désinstallateur, est décrite dans l’article WinGet →, dans la section Problèmes connus.

Pour la version 26.4.0

Erreur WinGet -1978335230

L’installation d’applications WinGet via Relution échoue avec le code d’erreur suivant : `-1978335230` (`0x8A150002`)

L’un des messages d’erreur suivants s’affiche :

```
Argumentname wurde für den aktuellen Befehl nicht erkannt: --disable-interacti
```

```
Argument name was not recognized for the current command : --disable-interacti
```

Cause

La version de WinGet installée est trop ancienne et ne prend pas encore en charge l'argument requis `--disable-interactivity`.

Solution

WinGet doit être installé au moins en version 1.6.

Si l'option Gérer WinGet et ses dépendances est activée dans la politique Configurer le Companion → (valeur par défaut), le compagnon Windows met à jour WinGet et ses dépendances à son démarrage.

Si l'option est désactivée ou n'est pas disponible, WinGet doit être mis à jour manuellement. Une mise à jour est disponible dans le Microsoft Store (paquet App Installer).

Les versions de WinGet antérieures à 1.6 ne peuvent pas encore se mettre à jour elles-mêmes.

Pour la version 26.4.0

Sur demande

En cas d'intérêt pour la gestion des appareils Linux, envoyer un message à l'adresse sales@relution.io →.

CA intégrée

Relution permet d'utiliser des certificats intégrés. Ces certificats sont utilisés dans de nombreux domaines, par exemple le chiffrement SSL/TLS, la sécurité du courrier électronique, les connexions VPN et Wi-Fi et la signature.

Les instructions suivantes décrivent la création d'une autorité de certification intégrée (CA) et d'un modèle de certificat avec des variables pour l'affectation. Une politique incluant la configuration du certificat est ensuite créée et assignée aux appareils appropriés. Cela permet de générer le certificat pour les appareils finaux.

Créer une autorité de certification intégrée

Dans Relution, une autorité de certification intégrée est créée sous `Paramètres` → `Autorités de certification` → `Ajouter`. Dans la section Général, un Nom est saisi (éventuellement une Description) et l'option Intégré est sélectionnée dans le champ Type d'autorité. Le type d'autorité ne peut plus être modifié après l'enregistrement.

Pour la version 26.4.0

Dans la section Paramètres du certificat, le bouton Générer du champ Certificat crée un nouveau certificat racine. Le bouton Sélectionner permet également d'utiliser un certificat PKCS#12 existant, téléversé au préalable sous `Paramètres` → `Certificats` (voir Gestion des certificats →). L'autorité de certification est ensuite créée avec Enregistrer.

L'option Intégré n'est disponible qu'avec l'autorisation de lire les certificats, et le bouton Générer uniquement avec l'autorisation de créer des certificats.

Générer un certificat racine intégré

Générer ouvre la boîte de dialogue Générer un certificat racine intégré. Confirmer crée le certificat racine et le reporte dans le champ Certificat.

Champs obligatoires

- Nom : Nom du certificat.
- Mot de passe : Mot de passe du certificat racine.
- Nom commun (CN) : Généralement le nom de domaine.
- Expire le : Une durée de validité de 10 ans est présélectionnée. La date la plus proche pouvant être choisie est le lendemain.

Champs facultatifs

- Organisation, Unité d'organisation, État fédéral, Localité : Informations supplémentaires sur le titulaire, reprises dans le nom distinctif (Distinguished Name) du certificat racine.
- Pays : L'Allemagne est présélectionnée.

Modèle de certificat

Le modèle de certificat `Paramètres` → `Modèles de certificats` → `Ajouter` est utilisé pour définir les paramètres du certificat.

Champs obligatoires

- Nom : Nom du modèle.
- Autorité de certification : L'autorité de certification intégrée créée précédemment est choisie via Sélectionner.
- Nom du sujet : par exemple, `CN=MyUseCase-${user.email}`. Des variables telles que `${user.name}`, `${device.serialnumber}` ou `${user.email}` peuvent être utilisées, voir Espaces réservés avancés →. Les caractères spéciaux sont échappés par une barre oblique inverse placée devant (par exemple `CN=John\, Doe`).

Le texte libre dans `CN=MyUseCase` doit être choisi en fonction du cas d'utilisation, par exemple VPN ou Wi-Fi.

Pour la version 26.4.0

Options supplémentaires

- Type de modèle de certificat : Ne peut plus être modifié après l'enregistrement.
  - Certificat (par défaut) : Relution génère la clé et le certificat et les met à disposition via la politique.
  - SCEP sur l'appareil : Pour iOS, macOS et tvOS, le modèle est converti en configuration SCEP. L'appareil génère lui-même la clé et demande le certificat à Relution via SCEP. Les paramètres correspondants (par exemple Réessais, Retard de nouvelle tentative, accès à la clé privée) se trouvent dans la section Configuration de SCEP.
- Noms alternatifs des sujets : Noms supplémentaires dans le certificat, chacun avec l'un des types suivants (pour SCEP sur l'appareil, uniquement E-mail, DNS, Nom principal et URI) :
  - Nom du répertoire
  - DNS
  - E-mail
  - Adresse IP
  - Nom principal (UPN)
  - URI
- Algorithme de clé : RSA (par défaut) ou EC. EC n'est proposé que pour une autorité de certification intégrée avec le type de modèle Certificat.

- Longueur de la clé : 4096 bits sont présélectionnés. Pour le type de modèle Certificat, 3072 et 4096 bits sont disponibles pour RSA, et 256, 384 et 521 bits pour EC ; pour SCEP sur l'appareil, 2048 et 4096 bits. Les modèles déjà enregistrés conservent une longueur de clé choisie auparavant jusqu'à ce qu'elle soit modifiée.
- Utilisation des clés de certification : Sélection multiple, par exemple Signature, Chiffrement des clés, Chiffrement des données ou Non répudiation.
- Utilisations des clés étendues des certificats : Sélection multiple, par exemple Authentification du client ou Authentification du serveur.
- Activer le renouvellement automatique : Les certificats émis sont renouvelés automatiquement. L'interrupteur est désactivé par défaut. Les deux champs suivants ne sont modifiables que lorsqu'il est activé :
  - Période de renouvellement automatique (en jours) : Un certificat est renouvelé automatiquement lorsque sa date d'expiration se situe dans cette période. La valeur par défaut est de 1 jour. Elle doit être inférieure à la Période d'expiration du certificat (en jours).
  - Comportement lors du renouvellement des certificats : Les anciens certificats restent valables (par défaut) ou Invalider directement les anciens certificats.
- Période d'expiration du certificat (en jours) : Un certificat n'est plus valide après cette période. La durée présélectionnée est de 365 jours.

Politique avec configuration du certificat

Pour la version 26.4.0

Pour que les étapes prennent effet et qu'un certificat soit créé, une politique avec une configuration de certificat doit être créée dans Relution. Voici un exemple pour iOS :

Sous `Appareils` → `Politiques` → `Ajouter`, la plateforme (ici iOS) est choisie dans la section Général, un nom est attribué à la politique et celle-ci est enregistrée.

Dans la politique créée, la configuration Certificat est ajoutée. Après la saisie d'un nom, le bouton Sélectionner du champ Certificat ouvre la boîte de dialogue de sélection d'un certificat ou d'un modèle de certificat. Le modèle de certificat créé précédemment y est choisi dans l'onglet Modèles de certificats, puis appliqué avec Confirmer.

De même, le modèle de certificat peut être utilisé pour les configurations VPN et WLAN.

Validation

L'entrée suivante doit être créée dans l'historique de l'appareil dans Relution après la distribution :

`Un certificat pour le modèle de certificat $Template a été émis par l'utilisateur de l'appareil $User.`

De plus, le nouveau certificat peut être trouvé sur la carte Certificats installés dans les informations de l'appareil (appareils Apple et Linux, à condition que les informations de l'appareil soient à jour).

Une vue d'ensemble de tous les certificats émis via des modèles de certificats, avec possibilité de révocation, est disponible sous `Paramètres` → `Certificats délivrés` (voir Gestion des certificats →).

Pour la version 26.4.0

Gestion des certificats

En plus de la CA intégrée → pour les certificats émis automatiquement, Relution propose deux autres vues pour la gestion des certificats : Certificats pour les certificats téléversés et les certificats enregistrés par Relution, et Certificats délivrés pour un aperçu des certificats émis ou attribués aux appareils par une politique de certificat.

Certificats

Sous `Paramètres` → `Certificats`, il est possible de téléverser et de gérer des fichiers de certificats existants (par ex. `crt`, `cer`, `der`, `pem`, `p12` / `pfx`).

Champs obligatoires lors du téléversement

- Nom : Nom du certificat.
- Fichier de certificat : Le fichier de certificat à téléverser.

Optionnel

- Mot de passe : Mot de passe du fichier de certificat, si celui-ci est chiffré.

Pour la version 26.4.0

Un certificat téléversé peut ensuite être sélectionné dans de nombreuses configurations de politiques comme certificat générique — de manière similaire à un modèle de certificat de la CA intégrée, mais sans émission automatique par appareil. Les cas d'usage typiques incluent les configurations VPN, Wi-Fi (EAP-TLS) et Exchange/e-mail, ainsi que les configurations de certificats Windows et Android Enterprise.

Outre les certificats téléversés (utilisation Générique), la liste affiche par défaut les certificats enregistrés par Relution, par exemple le certificat racine de la CA intégrée (Certificat racine PKI intégré), les certificats (Certificat de pool intégré) issus d'un pool de certificats → ainsi que les certificats push et de signature. Les filtres Utilisation, Type (`PKCS1` / `PKCS12`) et État permettent de restreindre l'affichage. Le fichier de certificat d'une entrée peut être téléchargé via le bouton de téléchargement de la liste.

Un certificat supprimé n'est pas effacé définitivement, mais reçoit l'état Supprimé. Comme le filtre État n'affiche par défaut que Créé, les certificats supprimés ne deviennent visibles qu'après modification du filtre ; ils peuvent être restaurés via l'action Certificat de restauration.

Certificats délivrés (Device Certificates)

Sous `Paramètres` → `Certificats délivrés`, un aperçu de tous les certificats émis ou attribués automatiquement à un appareil par une politique de certificat (CA intégrée, SCEP/Microsoft ADCS ou pool de certificats →) est disponible — incluant le certificat, l'appareil, le modèle de certificat utilisé, l'autorité de certification, ainsi que les dates d'émission, d'expiration et, le cas échéant, de révocation. Les certificats révoqués sont masqués par défaut et s'affichent via le filtre Certificats révoqués ; la liste peut en outre être filtrée par Modèle de certificat. Pour les certificats révoqués, les colonnes Révoqué par et Motif de la révocation indiquent qui a révoqué le certificat et pour quel motif.

L'émission manuelle n'est pas possible depuis cette vue — les certificats ne sont créés que suite à un processus d'inscription ou de politique. Deux actions sont disponibles :

- Supprimer : Retire l'entrée de Relution. Si un appareil demande à nouveau le certificat, un nouveau certificat est émis. Les certificats non encore expirés et associés à une liste de révocation (CRL) gérée par Relution ne peuvent pas être supprimés, mais uniquement révoqués. Cela vaut également après une révocation, jusqu'à l'expiration du certificat.
- Révoquer : Révoque le certificat via la liste de révocation de certificats (CRL) de l'autorité de certification associée. Un motif doit être sélectionné dans le champ obligatoire Motif de la révocation : non spécifié, compromis essentiel (compromission de la clé), Compromis CA, changement d'affiliation, remplacé, cessation d'activité, retrait du privilège ou Compromis AA.

Pour la version 26.4.0

La révocation n'est possible que pour les certificats émis par une CA intégrée, car Relution ne gère une liste de révocation que pour ceux-ci. Les certificats d'une autorité de certification SCEP ou Microsoft ADCS ainsi que les certificats issus d'un pool de certificats ne peuvent pas être révoqués dans Relution, mais uniquement supprimés ; leur révocation s'effectue auprès de l'autorité de certification émettrice. Les certificats déjà révoqués ou expirés ne peuvent pas non plus être révoqués.

> Important : La révocation est une véritable opération PKI : Relution génère ensuite une liste de révocation (CRL) mise à jour et signée. Les systèmes qui vérifient le certificat (par ex. un serveur RADIUS ou une passerelle VPN) la récupèrent via le point de distribution CRL enregistré dans le certificat ou interrogent le statut via OCSP. Cette action est irréversible.

Pool de certificats

Outre la CA intégrée →, qui émet elle-même les certificats, Relution prend en charge les autorités de certification de type Pool de certificats. Dans ce cas, une PKI externe existante sert de source : les certificats qui y sont émis sont importés dans Relution sous forme d'archive et conservés sous forme de pool. Lorsqu'un certificat est nécessaire pour une configuration, il est attribué à partir de ce pool au lieu d'être généré.

Créer une autorité de certification de type Pool de certificats

La création s'effectue sous `Paramètres` → `Autorités de certification` → `Ajouter`. Dans le menu déroulant Type d'autorité, l'entrée Pool de certificats est sélectionnée. Ce type n'est disponible que dans les organisations standard, et non dans l'organisation globale ou une méta-organisation.

Pour la version 26.4.0

Champs obligatoires

- Nom : Nom de l'autorité de certification dans Relution.

Les indications relatives à l'émission des certificats — par exemple un mot de passe pour le certificat racine, un common name ou une date d'expiration — ne sont pas nécessaires, car un pool de certificats ne signe pas lui-même de certificats.

Importer des certificats dans le pool

L'importation s'effectue en modifiant l'autorité de certification enregistrée précédemment ; le champ Importer le pool de certificats n'apparaît qu'après le premier enregistrement. Une archive ZIP contenant les fichiers de certificats émis en externe y est téléversée. En dessous, Relution liste les certificats déjà contenus dans le pool.

Un sous-type peut être défini en option dans le champ Sous-type de certificat par défaut. Il détermine la fonction pour laquelle les certificats seront disponibles par la suite. Les options disponibles correspondent aux fonctions des certificats utilisateur : Certificat général, Wi-Fi, Exchange, VPN et applications, Cryptage S/MIME et Signature S/MIME (voir Certificats utilisateur →). Si un sous-type est sélectionné, il s'applique à tous les certificats de l'archive ; la colonne `#Zertifikatstyp` du fichier CSV est alors ignorée et peut être absente. Avec le réglage par

défaut Aucun, le sous-type est lu ligne par ligne dans la colonne `#Zertifikatstyp` ; les lignes sans sous-type valide sont signalées comme erreurs.

Structure de l’archive

L’archive ZIP contient les fichiers de certificats émis en externe ainsi qu’exactement un fichier CSV (UTF-8) qui indique pour chaque certificat un identifiant et le mot de passe d’importation. Sont acceptés comme fichiers de certificats les conteneurs PKCS#12 (`.p12` ou `.pfx`) ainsi que les fichiers PEM (`.pem` avec clé privée, certificat et chaîne de certificats). Le séparateur est le point-virgule, la ligne d’en-tête est la suivante :

```
#E-Mail-Adresse;#P12-Passwort;#Zertifikatstyp
```

Colonne	Contenu
`#E-Mail-Adresse`	Identifiant du certificat, repris comme nom du certificat — doit correspondre au nom du fichier de certificat correspondant dans l’archive
`#P12-Passwort`	Mot de passe d’importation du fichier de certificat correspondant
`#Zertifikatstyp`	Fonction du certificat : `GENERAL_CERTIFICATE`, `WIFI`, `EXCHANGE`, `VPN`, `SMIME_ENCRYPTION` ou `SMIME_SIGNING` ; n’est évaluée que si aucun Sous-type de certificat par défaut n’est sélectionné lors de l’importation

Les colonnes sont associées via la ligne d’en-tête, leur ordre est donc libre. Une ligne par certificat, par exemple :

```
#E-Mail-Adresse;#P12-Passwort;#Zertifikatstyp
max.mustermann@example.com;motDePasseSecret;WIFI
```

La correspondance entre la ligne CSV et le fichier de certificat s’effectue par le nom de fichier : le fichier de certificat contenu dans l’archive porte comme nom l’identifiant de la colonne `#E-Mail-`

`Adresse`, dans l'exemple `max.mustermann@example.com.p12`. Si le nom du fichier diffère de l'identifiant, le certificat ne peut pas être associé. Les fichiers de certificats sans ligne CSV correspondante sont ignorés.

> Aucune attribution aux comptes utilisateur
>
> La colonne `#E-Mail-Adresse` sert uniquement d'identifiant ; les certificats ne sont pas attribués à des comptes utilisateur. Lors de la distribution, chaque appareil reçoit du pool un certificat valide, non encore attribué, du sous-type requis, de préférence celui dont la date d'expiration est la plus proche. Un pool de certificats ne convient donc pas aux scénarios dans lesquels le certificat doit contenir une identité utilisateur précise.

Après le téléversement, le formulaire affiche le résultat : nombre de certificats importés, de doublons ignorés et d'erreurs. Les identifiants concernés sont listés sous Importations échouées. Les lignes erronées n'interrompent pas l'importation ; les autres certificats sont tout de même importés. Un certificat est considéré comme doublon si son numéro de série existe déjà dans le pool de l'organisation.

Certificats importés dans la gestion des certificats

Les certificats importés apparaissent ensuite sous `Paramètres` → `Certificats` avec l'utilisation Certificat de pool intégré, chacun avec le sous-type choisi lors de l'importation ou indiqué dans le fichier CSV — Wi-Fi dans le cas décrit ici. Cette vue permet de consulter et de gérer les certificats comme tous les autres certificats enregistrés, voir Gestion des certificats →.

Modèle de certificat pour un pool de certificats

Pour que les certificats du pool puissent être utilisés dans les configurations de politiques, un modèle est créé sous `Paramètres` → `Modèles de certificats` → `Ajouter`.

Si un pool de certificats est sélectionné comme autorité de certification, les champs relatifs à la génération de certificats sont masqués (Nom du sujet, Noms alternatifs des sujets, Algorithme de clé, Longueur de la clé, Utilisation des clés de certification, Utilisations des clés étendues des certificats). Sont affichés :

- Nom : Nom du modèle.
- Type de modèle de certificat et Description (facultatif).
- Autorité de certification : L'autorité de certification de type Pool de certificats créée précédemment.

Pour la version 26.4.0

- Activer le renouvellement automatique avec Période de renouvellement automatique (en jours) : Si la date d'expiration d'un certificat attribué est comprise dans cette période, il est remplacé par un certificat libre du même sous-type issu du pool. L'ancien certificat est marqué comme supprimé et n'est plus attribué.
- Comportement lors du renouvellement des certificats et Période d'expiration du certificat (en jours) (champ obligatoire, valeur par défaut 365).

Le sous-type requis découle de la configuration dans laquelle le modèle est utilisé, par ex. Wi-Fi pour une configuration Wi-Fi. Si le pool ne contient plus de certificat libre de ce sous-type, aucun certificat ne peut être attribué et Relution signale une violation de conformité ; le pool doit alors être complété par d'autres certificats. Si seul un renouvellement est dû, l'ancien certificat reste attribué jusqu'à son expiration et Relution génère une notification de conformité.

Validation

La configuration est complète lorsque

- l'autorité de certification de type Pool de certificats est créée,
- l'importation de l'archive ZIP (dans l'exemple avec le sous-type Wi-Fi) s'est terminée sans doublons et sans erreurs,
- les certificats importés sont listés sous `Paramètres` → `Certificats` avec le sous-type Wi-Fi, et
- le modèle de certificat de l'autorité de certification de type Pool de certificats s'affiche sans champs relatifs à la génération de certificats, mais avec les options de renouvellement et d'expiration.

Pour la version 26.4.0

L'utilisation ultérieure du modèle dans une politique correspond à la procédure décrite pour la CA intégrée, voir CA intégrée →.

Fail2Ban – blocage d'IP

À partir de la version 5.19 de Relution, un paramètre de serveur global permet de définir si une adresse IP est bloquée en cas de tentatives de connexion incorrectes. Les paramètres se trouvent dans l'organisation globale sous `Paramètres` → `Sécurité du système`. Dans la configuration, il est possible de définir après combien de tentatives de connexion infructueuses une adresse IP est bloquée et si le blocage est levé automatiquement après un délai défini. De plus, l'administrateur du système a la possibilité d'autoriser ou de bloquer de façon permanente les connexions depuis une adresse IP ou une plage entière d'adresses IP (Règles d'accès IP).

Configurer le blocage d'IP

La section Général propose les options suivantes :

- Activé : Active le blocage d'IP (par défaut : désactivé).
- Nombre maximal d'échecs de connexion (10 par défaut) : Si les échecs de connexion d'une adresse IP dépassent cette valeur, l'adresse IP est bloquée. Une connexion réussie depuis cette adresse IP remet le compteur à zéro.
- Effacer les adresses IP bloquées après une durée déterminée avec Déblocage après (en minutes) (60 par défaut) : Lève automatiquement le blocage après le délai défini. Si cette option n'est pas activée (par défaut), l'adresse IP reste bloquée jusqu'à ce que l'entrée soit supprimée manuellement dans les Règles d'accès IP ou que l'adresse IP y soit autorisée.

Pour la version 26.4.0

Règles d'accès IP

Le tableau Règles d'accès IP répertorie les adresses IP enregistrées et bloquées automatiquement (avec Bloqué depuis). Ajouter une adresse IP permet d'ajouter des adresses IPv4 individuelles ou des plages entières (Adresse IP ou CIDR) avec un statut : Autorisé, Bloqué, Autorisé en permanence ou Blocage permanent. Les entrées sélectionnées peuvent être modifiées collectivement pour les bloquer, les autoriser ou les bloquer de façon permanente (actions Sélection des blocs, Autoriser la sélection de façon permanente et Bloquer définitivement la sélection).

> Les règles d'accès IP, y compris les entrées avec le statut Blocage permanent ou Autorisé en permanence, ne s'appliquent que si l'interrupteur Activé est activé dans la section Général.

La signification des statuts, des exemples CIDR et des recommandations pour éviter un verrouillage accidentel sont décrits sous Optimisation de la sécurité →.

Blocage de l’utilisateur après des tentatives de connexion infructueuses

Indépendamment du blocage d’IP, chaque organisation peut définir sous `Paramètres` → `Gestion des connexions`, dans la section Échec des tentatives de connexion, avec Désactivation de l’utilisateur en cas d’échec des tentatives de connexion consécutives et Nombre maximal de tentatives de connexion échouées (10 par défaut), si un utilisateur est bloqué après des tentatives de connexion échouées consécutives, et après combien.

L’utilisateur est désactivé dès que le nombre maximal de tentatives échouées est atteint. Il peut être réactivé par l’administrateur. Seules les tentatives de connexion des utilisateurs qui se connectent avec un mot de passe enregistré dans Relution sont comptées ; les utilisateurs qui s’authentifient exclusivement de manière externe (par exemple via LDAP) ne sont pas bloqués. Une connexion réussie remet à zéro le compteur des tentatives échouées.

Détails : Gestion des connexions →

Pour la version 26.4.0

Organisation globale

Avec la version `5.23.x`, l'organisation globale a été introduite dans Relution. Elle combine l'organisation du magasin et l'organisation du système. Jusqu'à la version 5.22, l'organisation du magasin devait être activée manuellement. Avec la version 5.23, cette activation est automatique.

Identification de l'organisation globale

La nouvelle organisation porte le nom de Global. Les comptes ayant l'autorisation des administrateurs système et les comptes ayant l'autorisation de l'ancienne organisation Store y ont accès.

Dans le sélecteur d'organisation en haut à droite, l'organisation globale est reconnaissable à l'icône de globe. Les organisations Meta portent une icône de structure, les sous-organisations une icône propre et les organisations autonomes une icône de bâtiment.

Sélecteur d'organisation

Nouveau dans 26.4

Cliquer sur le nom de l'organisation en haut à droite de l'en-tête ouvre le sélecteur d'organisation. Depuis la version 26.4, l'organisation Global est désormais toujours affichée fixe en haut de la liste. Il est également possible d'épingler certaines organisations comme favorites à l'aide de l'icône d'épingle, afin qu'elles apparaissent au-dessus de la liste complète des organisations pour un accès plus rapide.

Pour la version 26.4.0

Fonctionnalité

L’ensemble des fonctions est disponible pour les utilisateurs disposant d’une autorisation d’administrateur système. De nouvelles organisations peuvent également être créées dans cette organisation. Cela est possible via le nouvel élément de menu Organisations.

Les utilisateurs sans autorisation d’administration d’organisation, c’est-à-dire les utilisateurs qui ont été transférés à partir d’une organisation de magasin existante, ont accès à la gamme typique de fonctions de l’organisation de magasin.

Aucun appareil ne peut être inscrit dans l’organisation globale elle-même. Les appareils sont inscrits et gérés dans les organisations subordonnées.

Les applications, politiques et scripts peuvent en outre être mis à disposition au niveau d’une organisation Meta pour ses sous-organisations (Organisations Meta →).

Utilisateurs globaux

Les utilisateurs peuvent être créés de manière centralisée au niveau de l’organisation globale, puis être affectés à différents tenants avec des rôles ou des permissions spécifiques.

Cette structure permet une gestion flexible des identités : par exemple, un utilisateur global peut agir en tant qu’administrateur dans le Tenant A, tout en n’occupant que le rôle d’enseignant dans le Tenant B.

Pour la version 26.4.0

Plus d’informations sur les permissions →

Inscription automatisée des appareils à l’échelle du système

Via Apple School Manager ou Apple Business Manager, les appareils destinés à l’Inscription automatisée des appareils (ADE, DEP dans le portail) peuvent être affectés à l’organisation globale. Un profil DEP dans l’organisation globale pour lequel l’option Nom d’utilisateur + Mot de passe est sélectionnée sous Authentification utilisateur attribue les appareils Apple à l’organisation de l’utilisateur connecté.

Une organisation cible peut également être définie pour une inscription automatique de l’organisation globale dans la section S’inscrire à l’organisation. L’appareil est alors inscrit dans cette organisation, même sans authentification de l’utilisateur. Si Nom d’utilisateur + Mot de passe est sélectionné en plus, l’utilisateur connecté doit appartenir à l’organisation cible. Le même procédé est possible via les organisations Meta.

DEP →

Il est toujours possible d’ajouter des jetons DEP à d’autres organisations.

Pour la version 26.4.0

Distribution et versionnement des applications natives

Les applications natives peuvent être distribuées via une politique avec la configuration Conformité App. L’attribution de la version peut être définie dans l’organisation globale au sein de l’application, dans l’onglet Attributions de version.

Publier des politiques ou les copier dans des organisations

Pour la version 26.4.0

Les politiques créées dans l’organisation globale peuvent être distribuées de deux façons :

- Copier vers une ou plusieurs organisations (libellé du portail : Copie à l’organisation (s)) : copie la politique dans une ou plusieurs organisations. Disponible uniquement pour les politiques iOS et tvOS.
- Définir la visibilité comme globale : met la politique à la disposition de toutes les organisations. Disponible pour les politiques publiées de toutes les plateformes.

Les politiques rendues globales sont en lecture seule dans les organisations subordonnées ; les modifications ne sont possibles que dans l’organisation globale. Lors de la priorisation, les politiques globales sont prioritaires.

Pour la version 26.4.0

Politiques générales →

Mise à disposition globale de scripts

Les scripts créés dans l’organisation globale (scripts PowerShell pour Windows et scripts shell pour macOS) peuvent être mis à disposition en lecture seule dans toutes les organisations

subordonnées. Cela fonctionne de la même manière que la publication de politiques ou d'applications. Pour ce faire, le menu à trois points de l'entrée du script dans le tableau est ouvert et la fonction Définir la visibilité comme globale est sélectionnée.

Publier des scripts globalement →

Configuration LDAP à l'échelle du système

La configuration LDAP → peut être effectuée ici dans les Paramètres et un mappage spécifique à l'organisation peut être réalisé. L'avantage est que le fournisseur LDAP ne doit être configuré qu'une seule fois de manière centralisée.

Cette configuration peut être établie pour les comptes d'utilisateurs, les groupes, les classes, les comptes d'enseignants et d'étudiants ainsi que les groupes d'enseignants et d'étudiants dans la zone Associer des objets à des organisations. Les filtres de mappage ne répartissent que les objets déjà couverts par les filtres d'importation de la configuration LDAP.

L'option Synchroniser les objets non mappés avec cette organisation détermine le sort des objets auxquels aucun mappage ne s'applique : si elle est activée (par défaut), ils sont synchronisés dans l'organisation qui contient la configuration LDAP. Si elle est désactivée, ils ne sont pas importés et sont signalés comme erreurs de synchronisation.

Pour la version 26.4.0

Déplacer des appareils vers d'autres organisations

Via le bouton de déplacement (libellé du portail : Passer à) dans la liste des appareils de l'organisation globale, les appareils iOS/iPadOS, tvOS, macOS, Windows et Android Legacy peuvent être déplacés vers d'autres organisations. Cela n'est pas possible pour les autres plateformes (notamment Android Enterprise, ChromeOS, Linux, visionOS, watchOS).

Le déplacement supprime de l'appareil les données spécifiques à l'utilisateur et à l'organisation, notamment l'utilisateur assigné, les groupes d'appareils et les certificats. Seules les politiques qui ont été rendues globales via l'organisation globale seront conservées sur les appareils.

Déplacer un appareil vers une organisation →

Applications globales

À partir de la version `5.29`, il est possible de distribuer des applications natives à d'autres organisations via l'organisation globale. En termes simples, cela implique la création d'un lien vers l'application dans les organisations enfants. Cela permet d'économiser des ressources de base de données/mémoire et simplifie considérablement le déploiement de l'application.

Les applications créées via un compte Apps et livres (VPP dans le portail) de l'organisation globale remplacent automatiquement les applications existantes dans d'autres organisations.

Exigences

1. Pour distribuer l'application souhaitée, l'accès à l'organisation globale doit être possible. Elle est reconnaissable à l'icône de globe dans le sélecteur d'organisation en haut à droite, en général également au nom Global.
2. Une application native téléchargée ou une application Google, Apple ou Windows Store qui n'a pas encore été distribuée globalement :
   - iOS : .ipa
   - macOS : .pkg, .dmg
   - Android : .apk
   - Windows : .msix, .msixbundle, .appx, .appxbundle, .msi, .exe
3. L'application dispose d'au moins une version publiée (statut de production, libellé du portail : Version). Sinon, la fonction Définir la visibilité comme globale est désactivée, avec l'indication que la sélection contient des applications non publiées.
4. L'application ne doit pas être déjà disponible au niveau global.

Pour la version 26.4.0

Exécution

1. Dans la navigation latérale à gauche, sous `Apps` → `App Store`, survoler l'application native désirée avec la souris.
2. Cliquer sur le menu à 3 points à côté du nom de l'application.
3. Sélectionner Définir la visibilité comme globale.
4. Pour les applications qui sont déjà (partiellement) attribuées, une fenêtre de dialogue avec des conflits et des notes peut apparaître.

> Cette action ne peut pas être annulée. Les applications suivantes existent déjà dans d'autres organisations. Si elles sont rendues globales, les applications des autres

organisations seront remplacées et supprimées. Sélectionner les applications qui doivent être rendues globalement disponibles.

Ce processus peut prendre un certain temps.

5. L’application apparaît ensuite comme Partagé dans la colonne Portée. Dans les organisations enfants, elle apparaît comme Depuis Mondial (provenant de l’organisation globale).

Pour la version 26.4.0

Gestion des connexions

Pour sécuriser davantage les connexions dans Relution, une variété de paramètres peut être configurée pour l'organisation concernée sous `Paramètres` → `Gestion des connexions`. Les options pour la complexité des mots de passe, l'authentification multifactorielle (MFA) ainsi que les tentatives de connexion échouées y sont décrites.

Politique de mot de passe

- Mot de passe simple (par défaut : désactivé) : Lorsque l'option est activée, un mot de passe simple peut correspondre au nom d'utilisateur, par exemple, nom d'utilisateur test et mot de passe test. Lorsqu'elle est désactivée, le mot de passe ne doit correspondre ni au nom d'utilisateur ni au nom de l'organisation.
- Longueur minimale du mot de passe : 3 à 72 caractères, 8 par défaut.
- Âge maximum du mot de passe en jours : Lorsque cet âge est dépassé, un nouveau mot de passe doit être défini lors de la prochaine connexion. La valeur par défaut `0` signifie que les mots de passe n'expirent pas.
- Nombre minimum de chiffres
- Nombre minimum de lettres minuscules
- Nombre minimum de lettres majuscules
- Nombre minimum de symboles : Tout caractère qui n'est ni une lettre ni un chiffre est considéré comme un symbole.
- Désactiver la réinitialisation du mot de passe oublié

Pour la version 26.4.0

Les nombres minimums de chiffres, de lettres minuscules et majuscules et de symboles sont de `0` par défaut.

Désactiver la réinitialisation du mot de passe

La fonctionnalité Mot de passe oublié peut être désactivée sous `Paramètres` → `Gestion des connexions` avec l'option Désactiver la réinitialisation du mot de passe oublié. Lorsqu'elle est désactivée, il n'est plus possible de réinitialiser un mot de passe sans l'intervention d'un administrateur. Pour les comptes locaux dont le mot de passe est perdu, un administrateur doit réinitialiser directement le mot de passe.

L'effet dépend du niveau de l'organisation :

- Dans l'organisation globale, la désactivation s'applique à toutes les organisations.

- Dans une méta-organisation, elle remplace le paramètre pour les organisations de cette méta-organisation.
- Dans une organisation, elle ne s'applique qu'à l'écran de connexion de cette organisation.

Si l'option est définie dans une organisation parente, l'interrupteur est en lecture seule ; le portail indique alors que le lien a été désactivé par l'organisation mère.

Avant de désactiver cette option, au moins un compte administrateur avec un mot de passe connu et récupérable devrait exister.

Authentification multi-facteurs (MFA)

- Authentification par e-mail (par défaut : activée)
- Délai d'expiration du code à usage unique : de 30 secondes à 1 heure, 10 minutes par défaut.
- Applications d'authentification (TOTP) (par défaut : activées)

Si les deux facteurs sont désactivés, le portail indique que tous les utilisateurs peuvent se connecter sans MFA.

MFA →

Pour la version 26.4.0

Tentatives de connexion échouées

- Désactivation de l'utilisateur en cas d'échec des tentatives de connexion consécutives (par défaut : désactivée)
- Nombre maximal de tentatives de connexion échouées (10 par défaut, au moins 1)

Lorsqu'un utilisateur atteint le nombre maximal, il est désactivé et doit être réactivé par un administrateur. Une connexion réussie remet le compteur à zéro. La désactivation ne s'applique qu'aux utilisateurs Relution locaux ; les utilisateurs qui s'authentifient exclusivement de manière externe (par exemple via LDAP) ne sont pas comptés.

Le blocage d'adresses IP après des tentatives de connexion échouées est décrit sous Fail2Ban – blocage d'IP →.

Authentification multifactorielle

L’authentification multifactorielle, ou MFA en abrégé, est un mécanisme de sécurité qui exige des utilisateurs qu’ils fournissent au moins deux facteurs de vérification indépendants pour s’identifier de manière unique lorsqu’ils accèdent à une application.

L’accès non autorisé est rendu nettement plus difficile par la méthode d’authentification supplémentaire ; le niveau de sécurité est donc considérablement accru.

MFA et Relution

Relution permet aux utilisateurs LDAP et locaux d’activer les méthodes d’authentification supplémentaires Courriel (jeton par e-mail) et Application Authenticator dans le portail Relution en plus de spécifier le nom d’utilisateur et le mot de passe.

Avec la version 5.16, l’exigence de l’Office fédéral allemand de la sécurité des technologies de l’information (BSI) pour les fournisseurs MDM d’implémenter la fourniture d’un niveau de sécurité supplémentaire est prise en compte.

pour la version 26.4.0

Comment le MFA est-il configuré dans Relution ?

Sous `Paramètres` → `Gestion des connexions`, un administrateur d’organisation ou système définit dans la section Authentification multifactorielle quelles méthodes MFA sont disponibles dans l’organisation. Par défaut, l’authentification par e-mail (Authentification des e-mails) et Applications d’authentification (TOTP) sont activées. Le paramétrage de l’organisation à laquelle appartient l’utilisateur fait foi.

Pour l’authentification par e-mail, le Délai d’expiration du code à usage unique est défini : 30 secondes, 1, 2, 5, 10, 15 ou 30 minutes, ou 1 heure (par défaut : 10 minutes). Applications d’authentification (TOTP) permet la connexion avec un code temporel issu d’une application d’authentification. Chacune des deux méthodes peut être désactivée individuellement ; les deux peuvent aussi être actives en parallèle.

Si les deux méthodes sont désactivées, Relution ne demande plus de second facteur lors de la connexion – ni pour les rôles avec MFA imposée, ni pour les utilisateurs ayant déjà configuré des jetons MFA.

Pour la version 26.4.0

Forcer la connexion MFA

Le système de permission de Relution a été étendu avec la possibilité d’authentification multifactorielle. Il est possible de définir pour un rôle si la connexion MFA est requise ou non.

Si le rôle avec la connexion MFA activée est assigné à un utilisateur ou à un groupe, une connexion MFA est obligatoire lors de la connexion.

Si aucune méthode MFA n’a encore été configurée, l’utilisateur doit le faire lors de sa première connexion.

Forcer la MFA pour un groupe

Pour que la connexion MFA s’applique à tous les membres d’un groupe, un rôle avec MFA activée est créé et attribué au groupe. Les rôles des groupes parents sont également pris en compte.

1. Sous `Utilisateurs` → `Permissions`, un nouveau rôle est créé via Ajouter, ou un rôle personnalisé existant est ouvert.

2. Dans la section Authentification multi-facteurs, l’option Appliquer l’authentification multifactorielle pour le rôle est activée et validée avec Enregistrer.
3. Sous `Utilisateurs` → `Groupes`, le groupe souhaité est ouvert.
4. Via Gérer les autorisations, le rôle est sélectionné et validé avec Enregistrer.

La section Authentification multi-facteurs n’apparaît dans le rôle que si au moins une méthode MFA est activée sous `Paramètres` → `Gestion des connexions`. Les rôles standard de Relution ne peuvent pas être modifiés ; un rôle personnalisé est donc nécessaire pour la MFA. L’attribution est également possible pour les groupes synchronisés via LDAP. De plus amples informations sur les rôles figurent dans l’article Permissions →.

Jeton d’e-mail

Chaque utilisateur peut activer la MFA pour lui-même dans le portail Relution, indépendamment d’un administrateur. Dès qu’un jeton MFA est configuré, le second facteur est demandé à chaque connexion, même sans rôle imposant la MFA.

Dans le portail Relution, le menu utilisateur en haut à droite ouvre l’entrée Profil. Dans l’onglet Jetons MFA, le bouton Ajouter ouvre la boîte de dialogue Ajouter un nouveau jeton MFA. L’onglet n’existe que si au moins une méthode MFA est activée sous `Paramètres` → `Gestion des connexions`. Après la sélection de Courriel, l’adresse e-mail est saisie à l’étape suivante.

Pour la version 26.4.0

Il est possible de stocker dans le système des adresses électroniques privées ou propres à l’utilisateur, ce qui est utile dans le contexte scolaire.

Après la saisie, un code de vérification à usage unique est envoyé à l’adresse électronique enregistrée. Ce code est valable pour la période définie par l’administrateur. Dès que le Code de vérification à six chiffres reçu par e-mail est saisi, l’authentification multifactorielle est configurée. Si la configuration est interrompue auparavant, le jeton apparaît avec le statut Inachevé et ne compte pas comme facteur MFA.

Pour la version 26.4.0

Il est possible de stocker un nombre quelconque de facteurs d’authentification multifactorielle dans le portail Relution. Si plusieurs jetons e-mail sont configurés, le code est envoyé à toutes les adresses enregistrées lors de la connexion. En plus de la variante e-mail, l’utilisation de diverses “Apps Authenticator” est supportée.

Si la deuxième variante Application Authenticator est sélectionnée dans la boîte de dialogue Ajouter un nouveau jeton MFA, un code QR s’affiche ; il est scanné avec une application d’authentification préalablement installée sur l’appareil.

Il est également possible d’utiliser une clé de configuration pour la vérification.

Pour la version 26.4.0

Pour la version 26.4.0

Si plusieurs applications Authenticator sont utilisées sur plusieurs appareils en même temps, la validité d’au moins une application est vérifiée pour une connexion correcte. Lors de l’utilisation des deux méthodes d’authentification multifactorielle, c’est l’application Authenticator qui est principalement interrogée ; la variante e-mail enregistrée sert de solution de secours. Lors de la connexion, le bouton Utiliser le courrier électronique (sous Vous n’avez pas accès à l’application Authenticator ?) permet de passer à la variante e-mail ; Renvoyer l’e-mail demande un nouveau code.

Pour la version 26.4.0

Si seule l’application Authenticator est utilisée, il n’y a pas de solution de secours par email.

Supprimer les tokens MFA manuellement

Les jetons MFA peuvent être supprimés manuellement par l’utilisateur dans Profil, onglet Jetons MFA.

Si toutes les variantes MFA ont été supprimées manuellement, mais que la MFA est imposée par un rôle, l’authentification multifactorielle doit être stockée à nouveau la prochaine fois que l’utilisateur se connecte au Relution Portal.

Que se passe-t-il si le MFA est perdu ?

Si l'utilisateur n'a pas accès à l'email et/ou à l'application Authenticator alors que la MFA est activée, la connexion au portail Relution n'est plus possible - il est obligatoire d'aller voir l'administrateur.

Sous `Utilisateurs` → `Utilisateurs`, l'utilisateur concerné peut être ouvert et le jeton supprimé dans la section Jetons MFA. L'autorisation de supprimer des utilisateurs est requise. Avec l'autorisation de créer des utilisateurs, des jetons MFA peuvent également y être ajoutés pour l'utilisateur.

La colonne MFA de la liste des utilisateurs indique si un utilisateur a configuré la MFA ; le filtre du même nom distingue Configuré et Non configuré.

Pour la version 26.4.0

Configuration de confiance TLS

La configuration de confiance TLS regroupe les paramètres côté serveur pour l'établissement de connexions TLS de confiance. Elle se trouve sous `Paramètres` → `Configuration de confiance TLS` et se divise en deux zones : les certificats de confiance pour les connexions sortantes et l'épinglage de certificats pour l'inscription Apple. La configuration de confiance TLS n'est disponible que dans l'organisation globale et s'applique à l'ensemble du serveur, pour toutes les organisations. Les modifications des deux zones sont appliquées ensemble via Enregistrer dans la partie supérieure de la page.

Certificats de confiance

Relution accepte ces certificats CA en plus du magasin de confiance par défaut du système lors de l'établissement de connexions TLS sortantes. Via Ajouter, des certificats CA préalablement téléversés sous `Paramètres` → `Certificats` sont sélectionnés (voir Gestion des certificats →). La boîte de dialogue de sélection n'affiche que les certificats identifiés comme autorité de certification (CA) ; les conteneurs de certificats tels que `pfx` / `p12` ne peuvent pas être sélectionnés. L'aperçu indique pour chaque entrée le Nom, le Type et la date d'expiration (Expire le) ; les entrées sélectionnées sont retirées via Supprimer.

Les certificats utilisés ici comme certificat de confiance ou comme certificat d'ancrage ne peuvent pas être supprimés dans la gestion des certificats tant qu'ils sont référencés.

Pour la version 26.4.0

Épinglage de certificats (inscription Apple)

Nouveau dans 26.5

Lorsque le commutateur Activer l'épinglage de certificats de la zone Général est activé, la connexion TLS vers le serveur MDM est validée avec les certificats d'ancrage sélectionnés au lieu du magasin de confiance du système. Cela rend plus difficiles les attaques de type man-in-the-middle et l'utilisation d'autorités de certification non autorisées. Lors de l'inscription des appareils Apple, l'épinglage est repris dans le profil MDM et s'applique ensuite à l'ensemble de la communication de l'appareil avec le serveur MDM, y compris le check-in. Si l'épinglage est désactivé, l'appareil vérifie la connexion par rapport au magasin de confiance du système.

Les certificats à vérifier sont sélectionnés dans la zone Certificats d'ancrage via Ajouter parmi les certificats CA enregistrés dans la gestion des certificats ; l'aperçu indique pour chaque entrée le

Nom, le Type et la date d’expiration (Expire le). Au moins un certificat d’ancrage est requis pour activer l’épinglage. Le commutateur Exiger la vérification de révocation des certificats impose en outre une vérification de l’état de révocation des certificats. Si Activer l’épinglage de certificats est désactivé, Relution vide la liste des certificats d’ancrage et réinitialise la vérification de révocation ; après réactivation, les certificats d’ancrage doivent être sélectionnés à nouveau.

L’épinglage est enregistré dans le profil MDM

L’épinglage est intégré au profil MDM au moment de l’inscription. Les modifications effectuées ici concernent les nouvelles inscriptions. Relution ne transmet la configuration modifiée aux appareils déjà inscrits que lors de la mise à jour de leur profil MDM (action Mettre à jour le profil MDM ou renouvellement automatique avant l’expiration du certificat d’identité). Une configuration erronée peut priver les appareils de toute communication MDM ; un appareil qui ne peut plus se connecter au serveur MDM en raison d’un épinglage erroné ne reçoit plus non plus de mise à jour de profil et doit être réinscrit. Seuls des certificats CA à longue durée de vie devraient être épinglés ; lors de la rotation d’une CA, l’ancien et le nouveau certificat d’ancrage restent sélectionnés.

N’activer la vérification de révocation qu’avec des informations de révocation

L’option Exiger la vérification de révocation des certificats ne doit être activée que si le certificat TLS du serveur fournit des informations de révocation (URL du répondeur OCSP). En l’absence de cette information, les appareils peuvent refuser la connexion.

Pour la version 26.4.0

Comportement lors de l’inscription

Lorsque l’épinglage est activé, la connexion de l’appareil au serveur MDM est vérifiée par rapport aux certificats d’ancrage sélectionnés pendant l’inscription. Si la chaîne de certificats TLS du serveur remonte à l’un des certificats d’ancrage, l’inscription réussit. Cette vérification s’applique également à la communication MDM ultérieure de l’appareil inscrit. En cas de divergence, la connexion est rejetée et l’inscription échoue.

Si l’épinglage est activé mais qu’aucun certificat d’ancrage n’est configuré ou ne peut être chargé, Relution génère les profils MDM sans épinglage.

Les appareils dont la version du système d’exploitation est inférieure à la version minimale requise pour l’épinglage continuent d’être inscrits sans épinglage ; l’inscription y reste fonctionnelle.

Notifications relatives aux certificats d’ancrage

Relution vérifie les certificats d’ancrage épinglés toutes les heures ainsi qu’après chaque enregistrement et signale les problèmes dans le centre de notifications afin d’éviter à temps le blocage des appareils. Les notifications sont reçues par les utilisateurs de l’organisation globale autorisés à consulter la configuration de confiance TLS. Sont notamment signalés :

- un certificat d’ancrage qui expire dans moins de 90 jours ou qui a déjà expiré,
- un certificat d’ancrage qui ne peut pas être chargé ou qui n’est pas un certificat CA,
- un épinglage inefficace, par exemple lorsqu’aucun certificat d’ancrage n’est configuré ou qu’aucun ne correspond à la chaîne de certificats TLS du serveur.

Pour la version 26.4.0

Configuration LDAP

À partir de la version `5.18.0` de Relution, les fournisseurs LDAP pour l'importation d'utilisateurs, de groupes et de classes peuvent être configurés directement via le portail Relution. Le formulaire contient les paramètres de configuration habituels, qui peuvent être vérifiés à l'aide de plusieurs tests fonctionnels. Un redémarrage du service Relution n'est pas nécessaire avec la configuration via le portail ; les modifications et reconfigurations n'interrompent donc pas l'exploitation. Pour la configuration de la synchronisation LDAP, des connaissances en la matière ainsi qu'un navigateur LDAP capable d'afficher correctement les attributs sont recommandés. Pour Windows, le Softerra LDAP Browser et pour Linux ou macOS l'Apache Directory Studio ont fait leurs preuves. Ces deux outils sont gratuits.

> La configuration de fournisseurs LDAP via le portail Relution nécessite une licence payante incluant la fonctionnalité Connexions à l'interface utilisateur LDAP. Sans cette licence, la configuration ne peut pas être enregistrée, et les utilisateurs, groupes et classes ne sont pas synchronisés.

Pour la version 26.4.0

Principes de base

La configuration LDAP s'effectue sous `Paramètres` → `Synchronisation LDAP`. Plusieurs fournisseurs LDAP peuvent être configurés par organisation. Les adresses e-mail des utilisateurs dans Relution doivent être uniques. Dans le cas contraire, des erreurs peuvent se produire et certains comptes d'utilisateurs ne peuvent pas être créés. Un nouveau fournisseur LDAP est créé via Ajouter.

Une synchronisation manuelle peut être lancée à tout moment : dans cette liste via Démarrer la synchronisation pour le fournisseur sélectionné, ainsi que dans les listes des utilisateurs, des groupes et des classes via Synchronisation LDAP ponctuelle. La page de détails d'un fournisseur affiche, pour chaque type (utilisateurs, groupes, classes), le résultat de la dernière synchronisation.

Configuration de base

Le formulaire de configuration est divisé en plusieurs niveaux. Tous les paramètres ne sont pas toujours nécessaires selon le cas. Certains champs contiennent déjà des exemples qui suggèrent la syntaxe.

Synchronisation LDAP

Pour la version 26.4.0

Un nom est d'abord attribué au fournisseur LDAP. Un nom court et significatif est recommandé.

> Ce nom ne peut pas être modifié par la suite.

Paramètres du serveur

- URL du serveur LDAP : L'URL du serveur LDAP est saisie et confirmée par la touche `Entrée`.

Si LDAPS est utilisé et que le serveur ne dispose pas d'un certificat de confiance, le certificat peut être enregistré sous Certificats de serveur de confiance afin que Relution le classe comme fiable. Il est également possible, avec Faire confiance à tous les certificats, d'accepter n'importe quel certificat de serveur. Le portail signale alors le risque de sécurité ; il est préférable d'enregistrer explicitement les certificats.

La connexion est vérifiée avec Tester la connexion au réseau. La tentative de connexion doit être réussie avant de poursuivre la configuration.

Pour la version 26.4.0

Pour la version 26.4.0

Authentification

- Bind DN pour l'utilisateur : Nom d'utilisateur disposant de droits de lecture dans le LDAP. Idéalement, le Distinguished Name (DN) est utilisé ici.
- Mot de passe Bind : Le mot de passe correspondant.

Les informations d'identification sont vérifiées avec Test d'authentification.

Base DN

Après un Test d'authentification réussi, les DN de base signalés par le serveur sont proposés dans la sélection DNs de base découverts ; la première entrée est présélectionnée. Utiliser le DN de base découvert comme DN de base reprend l'entrée sélectionnée dans le champ Base DN. Les modifications nécessaires peuvent être apportées à tout moment.

Pour la version 26.4.0

Critères de recherche pour les utilisateurs

- Base de recherche des utilisateurs (unité organisationnelle) : La base de recherche pour les utilisateurs, relative au DN de base, par exemple `OU=users`.
- Filtre de recherche des utilisateurs : Les filtres de recherche LDAP conventionnels sont utilisés ici. Relution utilise toujours l'espace réservé `%v` pour la saisie de l'utilisateur. Par exemple, un filtre de recherche simple pour les utilisateurs pourrait être `(&(cn=%v)(objectClass=person))`.
- Champ de recherche de l'utilisateur : Définit la profondeur du chemin à parcourir pour rechercher des comptes d'utilisateurs avec le filtre de recherche correspondant. La sélection de Sous-arbre peut entraîner un grand nombre de résultats.

Mappage manuel pour les utilisateurs

Après l'établissement de la connexion, Relution vérifie de quel type de LDAP il s'agit, par exemple OpenLDAP ou un Active Directory. Les champs appropriés sont ensuite préconfigurés par un mappage automatique. Cette fonction peut être partiellement ou totalement remplacée en activant Mappage manuel des attributs de l'utilisateur.

Par exemple, il est recommandé de définir une clé étrangère. Cela s'avère utile lorsque les utilisateurs changent de nom : le compte utilisateur reste identifiable, et le nom et l'adresse e-mail sont simplement mis à jour sans créer un nouveau compte dans Relution.

Pour la version 26.4.0

> Le champ objectSID ne convient pas ici. Il provoque des erreurs car il contient parfois des caractères ininterprétables.

Synchronisation des utilisateurs

Le bouton Tester l'importation d'utilisateurs permet de vérifier si les utilisateurs peuvent être importés et si les filtres renvoient les bons résultats.

- Il est également possible d'activer Importation périodique des utilisateurs. Il s'agit d'une synchronisation automatique qui s'exécute toutes les 24 heures à l'heure sélectionnée (Temps de synchronisation). Si l'importation périodique est désactivée, les utilisateurs correspondant au filtre de recherche sont tout de même importés lors de la connexion ou lors de l'affectation à une inscription.

- Une synchronisation manuelle peut être lancée à tout moment (voir Principes de base →).
- Groupe synthétique : Il s'agit d'un groupe créé automatiquement par la synchronisation LDAP. Tous les utilisateurs importés via le fournisseur LDAP – lors de la synchronisation planifiée ou lors de la première connexion – deviennent membres de ce groupe.
  - Le nom du groupe se compose du Nom unique de l'organisation en majuscules et de la valeur saisie. Avec la valeur par défaut `LDAP`, on obtient par exemple le groupe `MYORG LDAP`.
  - Si le champ reste vide, aucun groupe synthétique n'est créé.
  - Comme des permissions peuvent être attribuées aux groupes LDAP, le groupe synthétique permet d'attribuer un rôle commun à tous les utilisateurs LDAP, par exemple pour l'Authentification multifactorielle →.
- L'option Lorsqu'un utilisateur LDAP n'est pas trouvé n'est modifiable que si Importation périodique des utilisateurs est activée (par défaut : Ne rien faire). Elle s'applique également lorsqu'un utilisateur existe encore dans le LDAP mais ne remplit plus les critères de recherche. Trois réactions sont disponibles :
  1. Ne rien faire : L'utilisateur reste dans Relution. Cependant, il ne peut plus être utilisé pour la connexion car le fournisseur LDAP refuse l'authentification.
  2. Désactiver l'utilisateur dans Relution : C'est le paramètre recommandé, car les comptes d'utilisateurs restent associés aux appareils et aucune donnée n'est perdue si les comptes ne sont accidentellement plus trouvés, par exemple après le renommage d'un groupe dans le LDAP qu'un filtre ne trouve alors plus.
  3. Supprimer l'utilisateur de Relution : Les utilisateurs qui ne sont plus trouvés par l'importateur sont supprimés directement de la base de données, sans tenir compte des liens avec les appareils, les groupes ou les classes.

> Attention : La suppression est irréversible — les utilisateurs concernés sont immédiatement supprimés de la base de données, sans tenir compte des liens avec les appareils, les groupes ou les classes.

Critères de recherche pour les groupes

- Base de recherche du groupe (unité d'organisation) : La base de recherche pour les groupes, relative au DN de base, par exemple `OU=groups`.
- Filtre de recherche de groupe : Les filtres de recherche LDAP conventionnels sont utilisés ici. Relution utilise toujours l'espace réservé `%v` pour la saisie de l'utilisateur. Par exemple, un

Pour la version 26.4.0

filtre de recherche simple pour les groupes pourrait être `(&(cn=%v)(objectClass=groupOfNames))`.

- Champ de recherche du groupe : Définit la profondeur du chemin à parcourir pour rechercher des groupes avec le filtre de recherche correspondant. La sélection de Sous-arbre peut entraîner un grand nombre de résultats.

Pour la version 26.4.0

Mappage manuel pour les groupes

Le mappage manuel (Mappage manuel des attributs de groupe) se comporte pour les groupes de la même manière que pour les utilisateurs. Souvent, le champ `entryUUID` est utilisé pour la Clé étrangère (UID) et le champ `member` pour Membre. Les attributs peuvent être vérifiés avec l'un des outils LDAP recommandés ci-dessus ou via la console avec `ldapsearch`.

Synchronisation des groupes

Le test de l'importation des groupes (bouton Importation d'un groupe d'essai) permet de vérifier si les groupes sont trouvés.

Pour que des groupes LDAP soient importés, Importer des groupes d'utilisateurs importés doit être activé. Relution importe alors tous les groupes dont des utilisateurs synchronisés sont membres et qui correspondent au filtre de groupe, y compris les groupes auxquels ces groupes appartiennent à leur tour. Si l'option est désactivée, seuls des groupes synthétiques sont créés.

Il est également possible d'activer Importation de groupes périodiques : toutes les 24 heures, à l'heure sélectionnée (Temps de synchronisation), tous les groupes correspondant au filtre de

groupe sont importés, même sans membres importés. Importation de groupes périodiques et l'heure ne peuvent être réglées que si Importer des groupes d'utilisateurs importés est activé.

L'importation part toujours des utilisateurs : les groupes n'entraînent pas l'importation d'utilisateurs supplémentaires. Les membres d'un groupe ne sont importés que s'ils correspondent eux-mêmes aux critères de recherche des utilisateurs.

> Les groupes qui ne sont plus trouvés lors d'une synchronisation réussie, par exemple après une modification du filtre de groupe, sont supprimés dans Relution.

Éducation

La synchronisation LDAP peut également être utilisée pour créer des classes qui sont affichées dans la section Éducation du menu et qui peuvent être utilisées pour la Relution Teacher Console ou dans Apple Classroom. Les classes à créer dans Relution sont des objets de groupe dans le LDAP. Elles doivent contenir au moins un enseignant ou un groupe d'enseignants et au moins un élève ou un groupe d'élèves.

Pour la version 26.4.0

Critères de recherche pour les classes

La configuration est ici similaire à celle des utilisateurs et des groupes : une base de recherche contenant les classes et un filtre de recherche correspondant sont définis. L'étendue de la recherche est configurée comme d'habitude via le menu déroulant.

La configuration peut être vérifiée avec le test de l'importation des classes (bouton Importation de la classe de test). Les classes ne sont créées ultérieurement que si elles contiennent au moins un enseignant ou un groupe d'enseignants et au moins un élève ou un groupe d'élèves. Les groupes ne sont pris en compte que s'ils sont trouvés via les critères de recherche pour les groupes d'enseignants et d'élèves.

Critères de recherche pour les enseignants et les élèves

Ici, la configuration consiste également en une base de recherche et un filtre correspondant. Souvent, les types d'utilisateurs individuels sont définis par l'appartenance à un groupe. Les filtres de recherche peuvent se présenter comme suit, par exemple :

- Enseignants : `(&(memberOf=CN=all-teachers,OU=groups,DC=school,DC=local)(objectClass=person))`

- Élèves : `(&(memberOf=CN=all-students,OU=groups,DC=school,DC=local)(objectClass=person))`

Les filtres peuvent être vérifiés avec Test d'importation d'enseignants et Tester l'importation d'élèves.

Critères de recherche pour les groupes d'enseignants et d'élèves

À partir de la version 5.31 de Relution, les groupes peuvent être importés en tant que membres de classes. Pour cela, un filtre est configuré pour les groupes d'enseignants et un autre pour les groupes d'élèves. Ces filtres peuvent être utilisés en complément des filtres pour les enseignants et les élèves ou à leur place. Si l'importation automatique des données d'éducation est activée, au moins l'un des deux filtres (filtre d'utilisateurs ou de groupes) doit être défini pour chaque rôle. Les filtres de recherche peuvent par exemple se présenter comme suit :

- Enseignants : `(&(cn=teacher*)(objectClass=groupOfNames))`
- Élèves : `(&(cn=students*)(objectClass=groupOfNames))`

Les filtres peuvent être vérifiés avec les tests d'importation des groupes d'enseignants et d'élèves (boutons Importation d'un groupe d'enseignants pour un test et Tester l'importation de groupes d'étudiants).

Pour la version 26.4.0

Synchronisation des données d'éducation

L'importation automatique des données d'éducation est également configurée ici : avec Importation périodique d'éducation, les classes sont synchronisées toutes les 24 heures à l'heure sélectionnée (Temps de synchronisation). Les classes qui ne sont plus trouvées lors d'une synchronisation réussie sont supprimées dans Relution.

Mappage des organisations (Global et méta)

Dans l'organisation globale et dans les méta-organisations, il est possible de configurer des fournisseurs LDAP et de synchroniser des utilisateurs, des groupes et des classes dans des organisations individuelles via des mappages (Associer des objets à des organisations). Pour chaque organisation cible, des filtres peuvent être définis pour les utilisateurs, les groupes, les classes, les enseignants, les groupes d'enseignants, les élèves et les groupes d'élèves, chacun sous forme de filtre LDAP ou de filtre DN. Le résultat peut être vérifié avec le test du mappage (bouton Cartographie des organisations de test).

Les filtres d’un mappage ne répartissent que les objets déjà trouvés via les filtres d’importation. Par défaut, seuls les objets correspondant à un mappage sont synchronisés ; tous les autres ne sont pas importés et sont signalés comme erreurs de synchronisation. Si l’option Synchroniser les objets non mappés avec cette organisation est activée sous Paramètres de mappage de l’organisation, les objets restants sont placés dans l’organisation dans laquelle le fournisseur est créé. Si un objet correspond aux filtres de plusieurs organisations, il est ignoré avec une erreur.

Pour la version 26.4.0

Organisations Meta

Les organisations Meta forment une hiérarchie sous l'organisation globale. Une organisation Meta regroupe plusieurs sous-organisations qui héritent des éléments qu'elle partage, comme les applications, les politiques et les scripts. La création d'organisations en général est décrite sous Créer des organisations →.

Type d'organisation

Lors de la création d'une organisation dans l'organisation globale, le Type d'organisation est défini :

- Autonome : une organisation autonome est créée directement sous l'organisation globale. Elle peut être attribuée ultérieurement à une organisation Meta.
- Meta : une organisation Meta est créée directement sous l'organisation globale. D'autres organisations peuvent lui être attribuées après la création et héritent des éléments qu'elle partage.
- Sous-organisation : une sous-organisation est attribuée à l'organisation Meta sélectionnée et hérite des éléments qu'elle partage. L'organisation Meta est choisie via Sélectionner Meta comme organisation parente ; ce choix est obligatoire. Cette attribution ne peut pas être annulée.

Pour la version 26.4.0

Le choix du type d'organisation n'est proposé que lors de la création dans l'organisation globale. Les organisations créées au sein d'une organisation Meta deviennent automatiquement ses sous-organisations. Le type d'une organisation existante ne peut pas être modifié lors de sa modification. Une organisation autonome ne peut être rattachée ultérieurement à une organisation Meta que via Assign to Meta Organization (voir ci-dessous).

Les restrictions suivantes s'appliquent en outre aux organisations Meta :

- Une organisation Meta ne peut pas être reconvertie en organisation autonome.
- Les organisations Meta ne peuvent pas être imbriquées : une organisation Meta ne peut pas être rattachée à une autre organisation Meta.
- L'organisation globale ne peut pas être une organisation Meta.
- Une organisation Meta à laquelle des sous-organisations sont rattachées ne peut pas être supprimée.

Héritage vers les sous-organisations

Les sous-organisations reprennent les éléments que l'organisation Meta partage avec toutes ses sous-organisations, par exemple les applications, les politiques, les scripts, les groupes d'appareils et les rôles. Dans l'organisation Meta, ces éléments sont marqués Partagé ; dans les sous-organisations, ils sont marqués Depuis Meta. Dans les listes, ils se trouvent dans l'onglet Partagé (Meta) ou Depuis Meta. Les éléments marqués Local uniquement restent limités à l'organisation Meta. Les éléments hérités ne peuvent être modifiés que dans l'organisation Meta.

Si des applications déjà présentes dans d'autres organisations sont rendues disponibles à l'échelle Meta, le portail signale ce conflit. Pour les applications sélectionnées, les applications existantes dans les autres organisations sont remplacées et supprimées.

Attribuer une organisation existante

Une organisation autonome peut être rattachée ultérieurement à une organisation Meta. Cette action n'est disponible que dans l'organisation globale et nécessite l'autorisation de modifier les organisations. Elle n'est pas disponible dans une organisation Meta.

Sous `Organisations`, une ou plusieurs organisations autonomes sont sélectionnées, puis Assign to Meta Organization est choisi dans le menu contextuel (le libellé n'est pas encore traduit dans le portail français). L'action est également disponible dans la vue détaillée d'une organisation autonome. Dans la boîte de dialogue, l'organisation Meta cible est d'abord sélectionnée. Après Suivant, la boîte de dialogue affiche l'organisation Meta choisie et, sous Nouvelles sous-organisations, les organisations à attribuer ; le bouton Confirmer effectue l'attribution.

> L'attribution à une organisation Meta est permanente et ne peut pas être annulée. Seules les organisations autonomes peuvent être attribuées.

Pour la version 26.4.0

Lier Microsoft Entra ID

En liant `Microsoft Entra ID` à Relution, la base des intégrations basées sur Microsoft au sein de l'organisation est mise en place. Cela comprend, par exemple, la connexion d'appareils Windows ainsi que l'utilisation d'autres services Microsoft en association avec Relution.

Les utilisateurs et groupes de `Microsoft Entra ID` peuvent ainsi être synchronisés avec Relution. Cela permet de gérer les comptes utilisateurs de manière centralisée dans Microsoft et de les provisionner automatiquement dans Relution.

Pour que les utilisateurs synchronisés puissent ensuite se connecter via Relution, il faut également configurer l'authentification OIDC →. Si les accès doivent être sécurisés via l'accès conditionnel →, la liaison de `Microsoft Entra ID` et la configuration d'OIDC → sont toutes deux nécessaires.

Les paramètres nécessaires à cet effet sont configurés en partie dans Relution et en partie dans le centre d'administration Microsoft Entra.

Pour la version 26.4.0

Prérequis

Pour lier `Microsoft Entra ID` avec Relution, les conditions suivantes doivent être remplies si seuls des utilisateurs de `Microsoft Entra ID` doivent être synchronisés avec Relution :

- un environnement `Microsoft Entra ID` existant
- des autorisations suffisantes dans Microsoft Entra, en général le rôle `Administrateur général`
- un serveur Relution accessible
- une inscription d'application dans Microsoft Entra

Si `Windows Autopilot` ou `Entra Join` doit également être utilisé, les conditions supplémentaires suivantes sont requises :

- l'URL du serveur Relution, qui sera enregistrée ultérieurement dans Microsoft Entra
- une application MDM créée

Ouvrir la configuration de la liaison dans Relution

Dans le portail Relution, la zone de configuration se trouve sous `Paramètres` → `Gestion des utilisateurs` → `Entra ID`.

Un assistant accompagne la configuration et la liaison avec Microsoft Entra. Il comprend les étapes Créer une application, ID des applications, Permissions, URI de redirection et Services.

Pour la version 26.4.0

Créer l’application

La première étape, Créer une application, indique que la connexion nécessite une application dans le portail Entra. Le bouton Ouvrir Entra ID ouvre la zone `Mobilité (MDM et MAM)` dans Microsoft Entra. En dessous, l’assistant Relution affiche les valeurs à saisir dans l’application MDM :

Pour la version 26.4.0

- Portée de l'utilisateur MDM : requise uniquement pour Windows Autopilot ou l'accès conditionnel. `Aucun` ignore la portée, `Tous` inclut tous les utilisateurs du locataire, `Certains` cible uniquement des utilisateurs sélectionnés. Si plusieurs solutions MDM partagent le même locataire avec Autopilot ou l'accès conditionnel, chaque utilisateur doit être assigné à une seule solution MDM.
- URL des conditions d'utilisation MDM : `https://<host>/api/device/v1/windows/termsOfUse`
- URL de découverte MDM : `https://<host>/api/device/v1/windows/discover`

L'application MDM est nécessaire pour `Windows Autopilot` et `Entra Join` et, selon la remarque du portail, également pour l'accès conditionnel. Sa création et sa configuration (application MDM locale, domaine personnalisé, URL) sont décrites dans l'article Windows Autopilot →.

Pour synchroniser uniquement des utilisateurs et des groupes de Microsoft Entra avec Relution, une inscription d'application standard suffit et cette étape est ignorée avec Suivant. L'inscription

d’application peut être créée via le lien suivant : Nouvelle inscription d’application dans Entra →

Configurer les paramètres de l’application

À l’étape ID des applications, les informations suivantes de Microsoft Entra sont transférées dans l’assistant Relution. Elles s’appliquent aussi bien à l’application MDM qu’à une inscription d’application standard :

1. ID de l’application (client)
2. ID d’annuaire (locataire)
3. la valeur de la Clé secrète client (dans Relution, champ Secret du client)

Vérifier dans la ligne Vérifier la configuration permet de tester immédiatement si Relution peut se connecter à Microsoft Entra avec ces informations.

Si l’accès conditionnel est déjà configuré pour l’organisation, Relution signale lors de la modification de l’ID d’annuaire (locataire) que le nouveau locataire s’applique également au paramètre d’accès conditionnel. L’ID d’application et le secret de ce paramètre doivent ensuite être vérifiés.

Uniquement pour une application MDM (Windows Autopilot, Entra Join) : l’URI de l’ID d’application est ensuite sélectionné dans les paramètres locaux de l’application MDM pour être modifié. Pour une inscription d’application standard, cette étape et la suivante sont supprimées.

Dans la vue suivante, l'URL du serveur correspondante est saisie comme `URI de l'ID d'application`.

Pour la version 26.4.0

Ensuite, une Clé secrète client est ajoutée sous Certificats et secrets :

1. Dans l'onglet Clés secrètes client, cliquer sur Nouvelle clé secrète client.
2. Dans la fenêtre de dialogue `Ajouter une clé secrète client`, indiquer une description et la durée de validité.
3. Cliquer sur Ajouter.

Lorsque la période de validité a expiré, la connexion n'existe plus et Relution ne peut plus communiquer avec Microsoft Entra. Dans ce cas, une nouvelle `Clé secrète client` doit être créée pour l'application dans Microsoft Entra et de nouveau enregistrée dans Relution.

Pour la version 26.4.0

La nouvelle entrée est ensuite affichée dans l'aperçu sous l'onglet `Clés secrètes client`.

La `Valeur` correspondante n'est affichée qu'une seule fois et doit donc être copiée immédiatement et transférée dans Relution.

Configurer les autorisations API

À l'étape suivante, Permissions, les autorisations API sont configurées. Un bouton de l'assistant ouvre directement les autorisations API de l'application dans Microsoft Entra :

Pour la version 26.4.0

Selon les fonctionnalités Microsoft utilisées ultérieurement, il peut être nécessaire d'ajouter d'autres autorisations plus tard.

Les paramètres suivants doivent être effectués dans Microsoft Entra :

1. Cliquer sous `Autorisations API` → `Autorisations configurées` sur Ajouter une autorisation.
2. Dans la fenêtre de dialogue Demander des autorisations API, sélectionner Microsoft Graph sous API Microsoft.

3. À l’étape suivante, sélectionner la vignette Autorisations d’application.

Pour la version 26.4.0

4. Sélectionner l’autorisation `User.Read.All` pour User.

5. Sélectionner l’autorisation `Group.Read.All` pour Group.

Pour la version 26.4.0

6. Sélectionner l’autorisation `Device.ReadWrite.All` pour Device et confirmer la sélection avec Ajouter des autorisations.

Pour les autorisations API nouvellement ajoutées, un point d’exclamation est d’abord affiché comme statut. Pour que l’application reçoive les autorisations, les administrateurs doivent les confirmer une fois via Accorder un consentement d’administrateur pour « ». Le statut est ensuite affiché avec une coche verte pour `Accordé`.

Pour la version 26.4.0

Vérifier dans la ligne Vérifier les autorisations contrôle si les autorisations ont été accordées. Sans consentement, la vérification signale Permission non accordée.

Définir l’URI de redirection

À l’étape URI de redirection, l’assistant Relution affiche l’`URI de redirection` qui est ensuite saisie dans Microsoft Entra pour la plateforme `Web`. Un bouton de l’assistant ouvre la page correspondante de l’application dans Microsoft Entra :

Pour la version 26.4.0

1. Cliquer sous Authentification sur Ajouter une plateforme.
2. Dans la fenêtre de dialogue Configurer les plateformes, sélectionner la vignette Web.

3. Dans la section Web, saisir l’URL du serveur sous Ajouter une URI de redirection.
4. Désactiver la case Jetons d’ID.
5. Cliquer sur Enregistrer.

Pour la version 26.4.0

Vérifier dans la ligne Vérifier les URI de redirection contrôle si l’URL du serveur est enregistrée dans l’application. L’URI saisie doit correspondre exactement à l’URL du serveur affichée, sinon la vérification signale que l’URI de redirection n’est pas présente.

La configuration dans Microsoft Entra est ainsi terminée.

Choisir les options de service Relution et terminer la configuration

L’étape Services définit les services utilisés par Relution. Quatre commutateurs sont disponibles : l’activation de l’inscription Autopilot, la synchronisation des appareils Autopilot, Synchroniser les utilisateurs d’Entra ID et Synchroniser les groupes Entra ID. Pour une nouvelle connexion, les quatre commutateurs sont déjà activés. Si seuls les utilisateurs et les groupes doivent être synchronisés (sans `Windows Autopilot` ni `Entra Join`), les deux commutateurs Autopilot sont désactivés.

En cliquant sur Enregistrer, la configuration et la liaison de `Microsoft Entra ID` dans Relution sont terminées.

Gérer et synchroniser la connexion

Après l’enregistrement, `Paramètres` → `Gestion des utilisateurs` → `Entra ID` affiche l’aperçu de la Connexion Entra ID avec l’ID de l’application et l’ID d’annuaire. Les fonctions suivantes y sont disponibles :

- Modifier la connexion : rouvre l’assistant, par exemple pour saisir une nouvelle valeur dans le champ Secret du client après l’expiration de la clé secrète client.
- Vérifier la connexion : vérifie en une seule étape la connexion, les autorisations et l’URI de redirection.
- Supprimer la connexion : supprime la liaison avec Microsoft Entra.

- Section Services : les quatre commutateurs de la configuration peuvent être modifiés ici ultérieurement et appliqués avec Enregistrer.

La section Synchronisation affiche pour chaque synchronisation la Dernière synchronisation, les Nouvelles entrées, les éventuelles erreurs et la Synchronisation suivante. Par défaut, les utilisateurs et les groupes sont synchronisés une fois par jour et les appareils Autopilot toutes les 24 heures.

Une synchronisation peut également être lancée manuellement :

- La synchronisation des appareils Autopilot récupère les appareils enregistrés dans Windows Autopilot.
- Synchronisation des utilisateurs et des groupes (dans le menu de la barre d'actions) n'est disponible que si la synchronisation des utilisateurs et celle des groupes sont toutes deux activées. La boîte de dialogue propose un Mode de synchronisation : Modifications uniquement (Recommandé) ne récupère que les utilisateurs et groupes modifiés depuis la synchronisation précédente. Synchronisation complète réimporte tous les utilisateurs et groupes et peut durer très longtemps. Elle n'est utile que si la synchronisation des modifications ne donne pas le résultat attendu.

Dans l'organisation globale, la liaison s'applique à l'ensemble du système, dans une méta-organisation à l'ensemble de la méta-organisation. L'aperçu l'indique sous Étendue du compte. Le mappage d'organisation permet alors d'associer des groupes Entra ID à certaines organisations. Dans ce cas, les commutateurs de synchronisation des utilisateurs et des groupes sont couplés et sont toujours activés ou désactivés ensemble.

Pour la version 26.4.0

Résumé

Une fois ces étapes terminées, `Microsoft Entra ID` est lié à Relution. Les utilisateurs et groupes de Microsoft Entra ID peuvent ainsi être synchronisés avec Relution, et d'autres fonctionnalités liées à Microsoft peuvent être utilisées.

Pour la connexion des utilisateurs synchronisés à Relution, il faut également configurer l'authentification OIDC →. Cela s'applique également à l'utilisation de l'`accès conditionnel`.

OIDC avec Entra

OpenID Connect `OIDC` est un protocole d'identité basé sur OAuth 2.0 qui permet une authentification et une autorisation sécurisées pour les applications web et mobiles. Il permet aux utilisateurs de se connecter en toute sécurité à divers services, tandis que les fournisseurs de services peuvent simultanément accéder à des informations d'identité vérifiées. Cet article explique, étape par étape, comment configurer OIDC dans Relution à l'aide de Microsoft Azure.

> Lors de la connexion via OIDC, aucune classe ni aucun groupe n'est synchronisé. Un utilisateur n'est créé dans Relution qu'à sa première connexion réussie, et seulement si Créer des utilisateurs inconnus dans Relution est activé. Relution ajoute automatiquement les utilisateurs nouvellement créés au groupe `<Nom du prestataire> Users` et crée ce groupe dans l'organisation si nécessaire. Ce groupe permet d'attribuer des autorisations.

Paramètres dans Relution

OpenID Connect `OIDC` peut être configuré dans le portail Relution sous `Paramètres` → `Gestion des utilisateurs` → `OpenID Connect`. Les captures d'écran suivantes montrent une configuration fonctionnelle avec Microsoft Azure.

Pour la version 26.4.0

Pour la version 26.4.0

Pour la version 26.4.0

Détails de la configuration

Nom du prestataire : Champ obligatoire. Sera affiché sur le bouton de connexion dans le portail Relution et ne peut plus être modifié après l'enregistrement. Créer des utilisateurs inconnus dans Relution : Active la création automatique de nouveaux utilisateurs inconnus lors de leur première connexion à Relution. Le commutateur est désactivé par défaut. Dans ce cas, seuls les utilisateurs déjà présents dans Relution peuvent se connecter. Vérifier la configuration : Vérifie avant l'enregistrement si la configuration est valide.

Si une connexion est effectuée avec un utilisateur inconnu sur l'organisation du magasin avec la configuration OIDC activée, celui-ci est automatiquement créé dans l'organisation du magasin. En

cas de plusieurs mandants avec configuration OIDC, la connexion doit se faire via l'URL de l'organisation afin que l'utilisateur inconnu soit créé dans l'organisation correspondante. Cette URL est affichée dans le portail au niveau des connexions OIDC.

Pour la version 26.4.0

Détails du client

Identifiant du client : Correspond dans Azure à l'ID de l'application. Secret du client : Correspond dans Azure à la clé secrète client de l'ID de l'application. Lors de la modification d'une configuration enregistrée, le champ reste vide. Si aucune nouvelle valeur n'est saisie, le secret existant reste inchangé.

URI du serveur

Utiliser le point de terminaison de découverte : Si le fournisseur le prend en charge, une configuration automatique des URI nécessaires est effectuée Configurer manuellement les points d'extrémité : Nécessaire dès que la découverte automatique ne fonctionne pas.

Avec Microsoft Azure, les points de terminaison doivent être saisis manuellement.

- URI d'autorisation
  `https://login.microsoftonline.com/$-votre-ID-de-mandant/oauth2/v2.0/authorize`
- JWK Set URI
  `https://login.microsoftonline.com/common/discovery/keys`
- Token URI
  `https://login.microsoftonline.com/$-votre-ID-de-mandant/oauth2/v2.0/token`
- Point de terminaison de fin de session (champ Point de terminaison de la session, facultatif, pour la déconnexion auprès de l'IdP, voir Vérification de la déconnexion)
  `https://login.microsoftonline.com/$-votre-ID-de-mandant/oauth2/v2.0/logout`

Pour la version 26.4.0

Configuration étendue

Attribut du nom d'utilisateur du fournisseur OIDC : Attribut du fournisseur OIDC qui contient le nom d'utilisateur unique de l'utilisateur authentifié (par défaut : `email`).

Attribut du nom d'utilisateur de Relution : Définit la propriété utilisateur Relution (Nom d'utilisateur, Adresse e-mail, UUID ou Clé étrangère (UID) ; par défaut : Adresse e-mail) avec laquelle la valeur de l'attribut du fournisseur OIDC est comparée. Avec UUID, les utilisateurs inconnus ne sont pas créés, même si Créer des utilisateurs inconnus dans Relution est activé.

Authorization Grant Type : Définit par quel mécanisme OAuth l'application obtient l'accès (par défaut : `authorization_code`).

Portée : Détermine en tant que scope OAuth quelles informations ou ressources peuvent être demandées par Relution via OIDC (par défaut : `openid`, `email`, `profile`).

Options avancées

Déconnexion de l'utilisateur de l'OIDC lors de la déconnexion de Relution : Lors de la déconnexion de Relution, le navigateur est également redirigé vers le point de terminaison de déconnexion de l'IdP (par défaut : désactivé). Les détails figurent sous Vérification de la déconnexion.

Créer une nouvelle inscription d'application

1. Connexion au portail Azure, puis accès à Microsoft Entra ID

2. Créer une nouvelle `Inscription d'application` → `Nouvelle inscription` pour OIDC

3. Nommer l’application, sélectionner le type de compte Comptes dans cet annuaire d’organisation uniquement et l’enregistrer

Pour la version 26.4.0

Pour la version 26.4.0

La seule connexion via OIDC ne nécessite aucune autorisation API supplémentaire ni consentement d'administrateur. Les autorisations d'application pour Microsoft Graph (p. ex. `User.Read.All`) ne sont nécessaires que pour la liaison avec Microsoft Entra ID → et y sont configurées.

Ajouter une clé secrète client (Client Secret) sous Certificats et secrets

1. La clé secrète client requise est créée sous Ajouter un certificat ou un secret

2. Via Nouvelle clé secrète client, la Description et la durée de validité Valide jusqu'au peuvent être définies

Pour la version 26.4.0

3. La clé client peut être copiée directement

> Important : la clé client n’est affichée qu’une seule fois ! Une fois la période de validité expirée, la connexion n’existe plus et Relution ne peut plus communiquer avec Azure. Dans ce cas, une nouvelle clé secrète client doit être créée pour l’application dans Azure et retransférée dans Relution.

Pour la version 26.4.0

Ajouter l’URI de redirection

Nouveau dans 26.4

L’URI de redirection sera affiché dans le portail Relution une fois la connexion configurée et enregistrée.

Pour la version 26.4.0

Remarque de migration — URI de redirection avec portée (à partir de 26.4.0). Avec 26.4.0, le schéma des URI de redirection a changé : les callbacks de connexion sont désormais scopés, afin de pouvoir être sécurisés par chemin sur le reverse proxy à l'avenir. Les URI de redirection à enregistrer dépendent de la configuration OIDC concernée : les configurations créées à partir de 26.4 utilisent toujours les URI de redirection scopées. Les configurations créées avant 26.4 continuent d'utiliser l'URI de redirection précédente (`/login/oauth2/code/`) jusqu'à leur conversion aux chemins scopés (voir Convertir les configurations existantes).

> À partir de 26.5.0, les connexions effectuées pendant un enrôlement d'appareil (`enrollment`), dans le Relution Agent (`agent`), dans Relution Assets (`assets`) et dans le portail libre-service (`selfService`) passent en outre par des portées dédiées. Si la configuration utilise les chemins scopés et que ces connexions sont utilisées avec OIDC, les URI correspondantes doivent être enregistrées auprès du fournisseur d'identité.

Où les trouver : les URI de redirection de l'instance concernée sont affichées dans le portail Relution sous `Paramètres` → `Gestion des utilisateurs` → `OpenID Connect`, dans la section URLs OIDC scopées de la configuration, dès que la connexion a été enregistrée, et peuvent y être copiées. Le portail n'affiche toutefois que les entrées URL de redirection (management), URL de redirection (device) et, avec une licence Education, URL de redirection (teacher). Il n'affiche actuellement pas les URI pour l'enrôlement des appareils (`/api/enrollment/`), le Relution Agent (`/api/agent/`), Relution Assets (`/api/assets/`), le portail libre-service (`/api/selfService/`) et Relution en tant que fournisseur d'identité → (`/api/idp/`). Elles sont ajoutées manuellement selon le schéma ci-dessous, dans la mesure où la fonction concernée est utilisée avec OIDC.

Chemins précédents (configurations créées avant 26.4, une seule URI de redirection) :

```
https://<host>/login/oauth2/code/<registrationId>
```

Chemins scopés (configurations créées à partir de 26.4 ou converties, enregistrer toutes celles qui s'appliquent) :

```
https://<host>/api/management/login/oauth2/code/<registrationId>       # porta
https://<host>/api/enrollment/login/oauth2/code/<registrationId>       # enrôl
https://<host>/api/teacher/login/oauth2/code/<registrationId>          # licen
https://<host>/api/agent/login/oauth2/code/<registrationId>            # Relut
https://<host>/api/assets/login/oauth2/code/<registrationId>           # Relut
https://<host>/api/selfService/login/oauth2/code/<registrationId>      # porta
https://<host>/api/idp/login/oauth2/code/<registrationId>              # Relut
https://<host>/api/device/login/oauth2/code/<registrationId>           # 26.4.
```

`<registrationId>` est l'UUID de configuration OIDC affiché dans Relution.

URL de déconnexion : le portail affiche en outre deux URL de déconnexion dans la même section. Il ne s'agit pas d'URI de redirection :

- URL de déconnexion du canal frontal (front-channel) : `https://<host>/api/management/v1/logout/connect/front-channel/<registrationId>`
- URL de déconnexion du canal arrière (back-channel) : `https://<host>/api/management/logout/connect/back-channel/<registrationId>`

Convertir les configurations existantes

Les configurations créées avant 26.4 continuent d'utiliser l'URI de redirection précédente après la mise à jour. Une telle configuration affiche en outre la section URLs OIDC héritées avec l'URL de redirection actuellement active et l'URL de déconnexion back-channel précédente. La conversion s'effectue en deux étapes :

1. Toutes les URI scopées applicables sont ajoutées à l'inscription d'application Entra existante. L'URI précédente reste enregistrée pour le moment.
2. Dans Relution, la configuration est ouverte sous `Paramètres` → `Gestion des utilisateurs` → `OpenID Connect`, puis Activer les chemins OIDC scopés est cliqué dans la section URLs OIDC héritées et la boîte de dialogue suivante est confirmée.

> La conversion est irréversible. Ensuite, Relution n'utilise plus que les URI scopées pour cette configuration. S'il en manque une auprès du fournisseur d'identité, les connexions concernées échouent.

Pour la version 26.4.0

Les configurations nouvellement créées n'affichent pas cette section, car elles utilisent les URI scopées dès le départ. L'URI précédente est obsolète et pourrait être supprimée dans une future version.

URI de redirection pour l'enrôlement des appareils

Nouveau dans 26.5

À partir de Relution 26.5.0, toutes les connexions effectuées pendant un enrôlement passent par une portée dédiée `enrollment`. Cela concerne l'Inscription automatisée des appareils (ADE, DEP dans le portail) d'Apple, Apple Account-Driven User Enrollment, l'enrôlement Android Enterprise ainsi que la connexion dans le DPC Android Enterprise. Pour les configurations avec chemins scopés, ces connexions ne fonctionnent que si l'URI `/api/enrollment/` indiquée ci-dessus est enregistrée auprès du fournisseur d'identité. Les configurations avec les chemins précédents continuent d'utiliser l'URI précédente, y compris pour les enrôlements.

Symptôme en cas d'URI manquante : la connexion au portail Relution continue de fonctionner, car elle utilise l'URI `/api/management/`. Seul l'enrôlement de l'appareil échoue, par exemple

l’enrôlement ADE d’un Mac avec le message `AADSTS50011: The redirect URI ... does not match`. Si cette erreur apparaît lors d’un enrôlement avec une configuration utilisant les chemins scopés, l’URI `/api/enrollment/` manque dans l’inscription d’application Entra.

Backchannel Logout

Relution prend en charge le Backchannel Logout à partir de la version serveur 5.32.0

Scénario d’exemple : Un utilisateur est connecté simultanément à un service SSO central et à plusieurs applications. Lors de la déconnexion du service SSO, le Backchannel Logout garantit que les sessions dans toutes les autres applications sont également terminées, même si elles fonctionnent en arrière-plan.

Prérequis pour les utilisateurs Entra pour OIDC

> Pour que la connexion via OIDC avec un utilisateur Entra fonctionne, une adresse e-mail doit obligatoirement être renseignée pour l'utilisateur Entra.

Pour la version 26.4.0

Vérification de la déconnexion

Avant la mise en service, les voies de déconnexion sont vérifiées :

- Déconnexion auprès de l'IdP lors de la déconnexion de Relution : un clic sur Déconnexion dans Relution révoque la session. Le navigateur n'est redirigé en plus vers le point de terminaison de déconnexion de l'IdP que si le commutateur Déconnexion de l'utilisateur de l'OIDC lors de la déconnexion de Relution est activé sous Options avancées et qu'un point de terminaison de fin de session est connu. Comme les points de terminaison sont configurés manuellement pour Entra, le champ Point de terminaison de la session doit être renseigné à cet effet.
- Déconnexion front-channel : lorsque l'utilisateur se déconnecte auprès de l'IdP, l'IdP appelle l'URL de déconnexion du canal frontal affichée dans le portail et Relution révoque la session. Cette URL doit pour cela être enregistrée auprès de l'IdP.
- Déconnexion back-channel : l'IdP envoie une notification de déconnexion à l'URL de déconnexion du canal arrière — la session est révoquée sans intervention de l'utilisateur.

Le test de ces voies permet de s'assurer qu'une fin de session initiée par l'IdP (par ex. via la console d'administration de l'IdP) est correctement transmise à Relution.

Pour la version 26.4.0

Relution en tant que fournisseur d'identité

À partir de la version 26.5.0, Relution peut agir comme son propre fournisseur d'identité OpenID Connect / OAuth2 : les applications clientes sont enregistrées directement dans Relution, ce qui permet aux utilisateurs de se connecter avec leur compte Relution existant à toutes les applications connectées.

La configuration se trouve sous `Paramètres` → `Fournisseur d'identité`. La page n'est visible qu'avec l'autorisation de lecture des clients IdP ; l'enregistrement, la modification et la suppression de clients nécessitent les autorisations correspondantes.

> Cette fonctionnalité est actuellement en phase bêta et est susceptible d'évoluer. Les retours, questions et suggestions sont les bienvenus.

> Seuls les clients OIDC confidentiels sont pris en charge actuellement – les clients publics (par exemple les applications monopages ou les applications natives sans secret client, comme celles utilisées par Zammad) suivront dans une version ultérieure.

Pour la version 26.4.0

Fonctionnalités

- Flux de connexion OIDC standard via le flux Authorization Code avec PKCE ; les jetons de rafraîchissement (refresh tokens) sont pris en charge.
- Scopes configurables par client (`profile`, `email`, `phone`, `relution`), avec un écran de consentement affiché aux utilisateurs. Le scope `relution` fournit des données spécifiques à Relution (par exemple l'appartenance à une organisation). Le scope `phone` peut être activé, mais ne fournit actuellement aucun claim supplémentaire (par exemple aucun numéro de téléphone).
- Déconnexion unique (Single Sign-Out) : la déconnexion initiée par l'application connectée (RP-initiated logout) ainsi que le Back-Channel Logout OIDC 1.0 sont pris en charge.
- Clés de signature (JWK) : Les clés utilisées pour signer les jetons sont gérées automatiquement par Relution et renouvelées régulièrement (une clé active est remplacée par une nouvelle au bout de quatre mois) – aucune action n'est nécessaire.

Rotation et révocation des clés de signature

Les clés de signature sont gérées dans la section Clés de signature de la page `Paramètres` → `Fournisseur d'identité`. Cette section n'est disponible que dans l'organisation globale ; elle

n’est pas affichée dans les méta-organisations et les sous-organisations.

La rotation automatique couvre entièrement le fonctionnement normal. Pour les cas exceptionnels (par exemple en cas d’incident de sécurité), deux interventions manuelles sont disponibles :

- Rotation des clés : Une nouvelle clé active est créée et la clé précédente est retirée (statut En retrait). Les jetons déjà émis restent valides jusqu’à leur expiration. Une nouvelle rotation n’est possible qu’au plus tôt cinq minutes après la dernière.
- Révoquer : La clé sélectionnée est immédiatement supprimée du jeu de clés publié. Il convient de noter que les applications connectées (relying parties) peuvent conserver la clé précédente en cache pendant un certain temps, de sorte que les jetons signés avec celle-ci peuvent ne pas être reconnus comme invalides avant l’expiration de ce cache.

Pour la version 26.4.0

Points de terminaison pour l’intégration

Dans la section Fournisseur en haut de la page `Paramètres` → `Fournisseur d'identité`, l’URL de l’émetteur (Issuer URL), le Document de découverte (`.well-known/openid-configuration`) et l’URI JWKS sont affichés et peuvent être copiés directement. Les autres points de terminaison techniques (par exemple le point de terminaison de jeton) peuvent être consultés au besoin dans le document de découverte.

Chaînage de fournisseurs d’identité (IdP chaining)

Relution peut également être chaîné derrière un fournisseur d’identité en amont (par exemple Microsoft Entra ID → Relution → application connectée).

Enregistrement d’un client

Pour la version 26.4.0

Un client dédié est créé pour chaque application connectée via Enregistrer un client :

- Nom du client : Choisi librement, affiché aux utilisateurs sur l’écran de consentement, et utilisé par les administrateurs pour distinguer plusieurs clients.
- Identifiant du client et Secret du client : Générés automatiquement et requis par l’application connectée (relying party). L’application s’authentifie avec ceux-ci via `client_secret_basic` ou `client_secret_post`. Le secret du client n’est affiché qu’une seule fois, directement après la création du client, et doit être copié à ce moment-là ; il ne peut plus être consulté ensuite. En cas de perte, un nouveau secret peut être généré dans la liste Clients enregistrés via Régénérer le secret (également affiché une seule fois). L’ancien secret devient alors invalide et tous les jetons existants du client sont révoqués.
- Activé : Un client désactivé refuse les nouvelles connexions ainsi que le renouvellement des jetons par jeton de rafraîchissement.
- Exiger PKCE : Activé par défaut. Si l’application connectée ne prend pas en charge PKCE, l’option peut être désactivée pour le client concerné.
- URI de redirection : Fournies par l’application connectée et doivent être renseignées en conséquence.

- URI de redirection après déconnexion : Adresses vers lesquelles l'application peut rediriger le navigateur après une déconnexion initiée par l'application (RP-initiated logout).
- URL de déconnexion back-channel : Si elle est renseignée, Relution notifie l'application en arrière-plan dès que la session du client se termine. Elle reste vide si l'application ne prend pas en charge la déconnexion back-channel.
- TTL du jeton d'accès et TTL du jeton de rafraîchissement : Durée de validité des jetons émis. Pour les nouveaux clients, le formulaire est prérempli avec 5 minutes et 1 jour respectivement ; les valeurs autorisées vont de 1 à 60 minutes pour les jetons d'accès et de 1 à 90 jours pour les jetons de rafraîchissement.
- Autorisations (scopes) : Chaque scope est réglé sur Désactivé, Facultatif ou Obligatoire. Par défaut, `profile` et `email` sont obligatoires, `phone` et `relution` désactivés. `openid` est toujours actif (Toujours accordé). L'activation d'un scope le rend seulement disponible ; l'application connectée doit également le demander lors du flux de connexion. Si la demande ne contient pas `openid` ou un scope obligatoire, la connexion est refusée avec l'erreur `invalid_scope`. Les scopes facultatifs ne sont accordés que si l'application les demande et qu'ils ne sont pas refusés sur l'écran de consentement.
- Donner le consentement administrateur pour tous les utilisateurs (Admin Consent) : Le consentement pour l'ensemble des scopes d'un client peut être approuvé au préalable par les administrateurs (en bloc, et non scope par scope) – les utilisateurs ne sont alors plus invités à les accepter sur l'écran de consentement lors de leur première connexion à l'application. Lorsque cette option est activée, les scopes ne peuvent plus être configurés que comme Désactivé ou Obligatoire. Les scopes réglés auparavant sur Facultatif sont automatiquement réinitialisés à leur valeur par défaut (`profile` et `email` : Obligatoire ; `phone` et `relution` : Désactivé).

Les clients qui ne sont plus nécessaires sont supprimés dans la liste Clients enregistrés.

Pour la version 26.4.0

Pour la version 26.4.0

Pour la version 26.4.0

Visibilité selon le niveau d’organisation

Le niveau d’organisation auquel un client est enregistré détermine quels utilisateurs peuvent s’y connecter :

- Global : Tous les utilisateurs du système peuvent se connecter.
- Méta-organisation : Tous les utilisateurs de la méta-organisation ainsi que de ses sous-organisations peuvent se connecter.
- Sous-organisation : Seuls les utilisateurs de cette sous-organisation peuvent se connecter.

Aperçu du jeton

Un aperçu des claims du jeton résultant peut être consulté pour la configuration de scopes actuelle d’un client – ce qui permet de vérifier au préalable quelles informations une application connectée recevrait dans le jeton.

Les scopes fournissent les claims suivants :

Scope	Claims
`openid`	`sub` (ID de l'utilisateur), `amr` (méthode d'authentification), en plus `idp` avec un fournisseur d'identité en amont
`profile`	`name`, `given_name`, `family_name`, `preferred_username`, `locale`, `updated_at`
`email`	`email`
`relution`	UUID, nom et nom unique de l'organisation de l'utilisateur
`phone`	aucun actuellement

Pour la version 26.4.0

Consentements accordés

Dans leur profil, les utilisateurs voient dans l'onglet Applications autorisées à quelles applications ils ont accordé quelles autorisations, et peuvent y révoquer l'accès. Les administrateurs disposant de l'autorisation correspondante trouvent la même section dans les détails d'un utilisateur. La révocation supprime également les autorisations existantes de l'application pour cet utilisateur, de sorte que l'application ne peut plus obtenir de nouveaux jetons via le jeton de rafraîchissement ; le consentement est de nouveau demandé lors de la prochaine connexion.

Journalisation

Les connexions via le fournisseur d'identité sont enregistrées à la fois dans le journal d'audit (audit log) et dans l'historique de connexion de l'utilisateur concerné. Dans l'historique de connexion, la colonne Client IdP indique par quel client la connexion a été effectuée.

OIDC avec Workspace

OpenID Connect `OIDC` est un protocole d'identité basé sur OAuth 2.0 qui permet une authentification et une autorisation sécurisées pour les applications web et mobiles.
Il permet aux utilisateurs de se connecter en toute sécurité à divers services, tandis que les fournisseurs de services peuvent simultanément accéder à des informations d'identité vérifiées.

Ce guide explique la configuration d'OIDC dans Relution à l'aide de l'exemple de Google Workspace.

> Lors de la connexion via OIDC, aucune classe ni aucun groupe n'est synchronisé. Les utilisateurs ne sont créés dans Relution qu'à leur première connexion réussie, et uniquement si le commutateur Créer des utilisateurs inconnus dans Relution est activé dans la configuration OIDC. S'il est désactivé (par défaut), seuls les utilisateurs déjà présents dans Relution peuvent se connecter. Relution ajoute automatiquement les utilisateurs nouvellement créés au groupe `<Nom du prestataire> Users`, qui permet d'attribuer des autorisations.

Pour la version 26.4.0

Configuration du projet et du client (Google Cloud Console)

Tout d'abord, une application doit être enregistrée dans la Google Cloud Console afin d'obtenir les identifiants nécessaires.

1. Se connecter sur console.cloud.google.com →.
2. Créer un nouveau projet ou en sélectionner un existant.

3. Dans le menu, accéder à `APIs & Services` → `OAuth consent screen` et configurer cet écran si nécessaire.

4. Passer à Credentials, cliquer sur Create Credentials et sélectionner OAuth client ID.

Pour la version 26.4.0

5. Sélectionner `Web application` comme Application type.

6. Renseigner l’URL du serveur sous Authorized JavaScript origins (par ex. `https://support.relution.io`). *Remarque : laisser pour l’instant le champ Authorized redirect URIs vide ou y renseigner provisoirement l’URL ; il sera mis à jour plus tard avec les URI de redirection provenant de Relution.*

Pour la version 26.4.0

7. Après l’enregistrement, le Client ID est affiché. Le copier.

8. Modifier à nouveau le client nouvellement créé pour consulter les détails.

Pour la version 26.4.0

9. Copier le Client Secret. Conserver l’ID et le secret en sécurité pour une utilisation ultérieure dans Relution.

Configuration du SSO (Google Admin Console)

Pour la version 26.4.0

Parallèlement, le profil Single Sign-On (SSO) doit être enregistré dans la console d'administration Google.

1. Accéder à la Google Admin Console →.
2. Créer un nouveau profil OIDC sous `Security` → `Authentication` → `SSO with third-party IdP`.

3. Saisir le Client ID et le Client Secret obtenus au chapitre précédent.
    - Utiliser l’URL du serveur Relution (par ex. `https://support.relution.io`) pour l’Issuer URL ainsi que pour la Change password URL.

Pour la version 26.4.0

Configuration d’OIDC dans Relution

Les données rassemblées sont maintenant saisies dans Relution afin d’établir le lien avec Google.

1. Ouvrir dans Relution les paramètres OIDC sous `Paramètres` → `Gestion des utilisateurs` → `OpenID Connect`.

Pour la version 26.4.0

Pour la version 26.4.0

Pour la version 26.4.0

2. Sous Nom du prestataire, saisir un nom unique (p. ex. « Google Workspace »). Le nom apparaît sur le bouton de connexion et ne peut plus être modifié après l’enregistrement.
3. Si nécessaire, activer Créer des utilisateurs inconnus dans Relution afin que les nouveaux utilisateurs soient créés automatiquement lors de leur première connexion.
4. Saisir le Client ID et le Client Secret de la Google Cloud Console dans les champs Identifiant du client et Secret du client.
5. Dans la section URI du serveur, sélectionner l’option d’utilisation du point de terminaison de découverte (discovery endpoint), puis saisir `https://accounts.google.com` dans le

champ URI de l'émetteur.

6. Enregistrer brièvement la configuration puis la rouvrir pour voir les champs générés.
7. Dans la section URLs OIDC scopées, copier toutes les entrées URL de redirection affichées (une pour `management` et une pour `device`, plus `teacher` avec une licence Education).

Pour la version 26.4.0

8. Retourner sur la Google Cloud Console →.
9. Modifier le client OAuth et ajouter sous Authorized redirect URIs toutes les URL qui viennent d'être copiées depuis Relution. Ajouter également les URI de redirection que le portail n'affiche pas, au minimum celle pour l'enrôlement des appareils (`/api/enrollment/`), voir URI de redirection scopées.

La section Configuration étendue définit comment Relution associe l'utilisateur connecté : l'Attribut du nom d'utilisateur du fournisseur OIDC (par défaut : `email`) est comparé à la propriété utilisateur sélectionnée sous Attribut du nom d'utilisateur de Relution (Nom d'utilisateur, Adresse e-mail, UUID ou Clé étrangère (UID) ; par défaut : Adresse e-mail). Avec UUID, aucun utilisateur inconnu n'est créé. La Portée est par défaut `openid`, `email`, `profile`. Vérifier la configuration permet de valider la configuration avant l'enregistrement.

Pour la version 26.4.0

URI de redirection scopées

Nouveau dans 26.4

Remarque de migration — URI de redirection avec portée (à partir de 26.4.0). Avec 26.4.0, le schéma des URI de redirection a changé : les callbacks de connexion sont désormais scopés, afin de pouvoir être sécurisés par chemin sur le reverse proxy à l'avenir. Les URI de redirection utilisées dépendent de l'utilisation, ou non, des chemins précédents par la configuration OIDC : les configurations créées à partir de 26.4 utilisent toujours les URI de redirection scopées. Les configurations créées avant 26.4 continuent d'utiliser l'URI de redirection précédente (`/login/oauth2/code/`) jusqu'à leur conversion aux chemins scopés (voir Convertir les configurations existantes).

À partir de 26.5.0, les connexions effectuées pendant un enrôlement d'appareil (`enrollment`), dans le Relution Agent (`agent`), dans Relution Assets (`assets`) et dans le portail libre-service (`selfService`) passent en outre par des portées dédiées. Si la

configuration utilise les chemins scopés et que ces connexions sont utilisées avec OIDC, les URI correspondantes doivent être enregistrées auprès du fournisseur d'identité.

Où les trouver : les URI de redirection de l'instance concernée sont affichées dans le portail Relution sous `Paramètres` → `Gestion des utilisateurs` → `OpenID Connect`, dans la section URLs OIDC scopées de la configuration, dès que la connexion a été enregistrée, et peuvent y être copiées. Le portail n'affiche toutefois que les entrées URL de redirection (management), URL de redirection (device) et, avec une licence Education, URL de redirection (teacher). Il n'affiche actuellement pas les URI pour l'enrôlement des appareils (`/api/enrollment/`), le Relution Agent (`/api/agent/`), Relution Assets (`/api/assets/`), le portail libre-service (`/api/selfService/`) et Relution en tant que fournisseur d'identité → (`/api/idp/`). Elles sont ajoutées manuellement selon le schéma ci-dessous, dans la mesure où la fonction concernée est utilisée avec OIDC.

Chemins précédents (configurations créées avant 26.4, une seule URI de redirection) :

```
https://<host>/login/oauth2/code/<registrationId>
```

Chemins scopés (configurations créées à partir de 26.4 ou converties, enregistrer toutes celles qui s'appliquent) :

Pour la version 26.4.0

```
https://<host>/api/management/login/oauth2/code/<registrationId>       # porta
https://<host>/api/enrollment/login/oauth2/code/<registrationId>       # enrôl
https://<host>/api/teacher/login/oauth2/code/<registrationId>          # licen
https://<host>/api/agent/login/oauth2/code/<registrationId>            # Relut
https://<host>/api/assets/login/oauth2/code/<registrationId>           # Relut
https://<host>/api/selfService/login/oauth2/code/<registrationId>      # porta
https://<host>/api/idp/login/oauth2/code/<registrationId>              # Relut
https://<host>/api/device/login/oauth2/code/<registrationId>           # 26.4.
```

`<registrationId>` est l'UUID de configuration OIDC affiché dans Relution.

URL de déconnexion : le portail affiche en outre deux URL de déconnexion dans la même section. Il ne s'agit pas d'URI de redirection :

- URL de déconnexion du canal frontal (front-channel) : `https://<host>/api/management/v1/logout/connect/front-`

`channel/<registrationId>`
- URL de déconnexion du canal arrière (back-channel) : `https://<host>/api/management/logout/connect/back-channel/<registrationId>`

Convertir les configurations existantes

Les configurations créées avant 26.4 continuent d'utiliser l'URI de redirection précédente après la mise à jour. Une telle configuration affiche en outre la section URLs OIDC héritées avec l'URL de redirection actuellement active et l'URL de déconnexion back-channel précédente. La conversion s'effectue en deux étapes :

1. Toutes les URI scopées applicables sont ajoutées au client OAuth Google existant. L'URI précédente reste enregistrée pour le moment.
2. Dans Relution, la configuration est ouverte sous `Paramètres` → `Gestion des utilisateurs` → `OpenID Connect`, puis Activer les chemins OIDC scopés est cliqué dans la section URLs OIDC héritées et la boîte de dialogue suivante est confirmée.

> La conversion est irréversible. Ensuite, Relution n'utilise plus que les URI scopées pour cette configuration. S'il en manque une auprès du fournisseur d'identité, les connexions concernées échouent.

Les configurations nouvellement créées n'affichent pas cette section, car elles utilisent les URI scopées dès le départ. L'URI précédente est obsolète et pourrait être supprimée dans une future version.

Pour la version 26.4.0

URI de redirection pour l'enrôlement des appareils

Nouveau dans 26.5

À partir de Relution 26.5.0, toutes les connexions effectuées pendant un enrôlement passent par une portée dédiée `enrollment`. Cela concerne l'Inscription automatisée des appareils (ADE, DEP dans le portail) d'Apple, Apple Account-Driven User Enrollment, l'enrôlement Android Enterprise ainsi que la connexion dans le DPC Android Enterprise. Pour les configurations avec chemins scopés, ces connexions ne fonctionnent que si l'URI `/api/enrollment/` indiquée ci-dessus est enregistrée auprès du fournisseur d'identité. Les configurations avec les chemins précédents continuent d'utiliser l'URI précédente, y compris pour les enrôlements.

Symptôme en cas d'URI manquante : la connexion au portail Relution continue de fonctionner, car elle utilise l'URI `/api/management/`. Seul l'enrôlement de l'appareil échoue, avec un message signalant une URI de redirection invalide (`invalid_redirect_uri`, chez Google `Error 400: redirect_uri_mismatch`). Si cette erreur apparaît lors d'un enrôlement avec une

configuration utilisant les chemins scopés, l'URI `/api/enrollment/` manque dans le client OAuth Google.

Backchannel Logout

Relution prend en charge le Backchannel Logout à partir de la version serveur 5.32.0.

Scénario : Un utilisateur est connecté simultanément à plusieurs applications via SSO. Dès que la déconnexion du service SSO central a lieu, le Backchannel Logout garantit que les sessions dans Relution et les autres applications connectées en arrière-plan sont également terminées de manière sécurisée.

Vérification de la déconnexion

Avant la mise en service, les voies de déconnexion sont vérifiées :

- Déconnexion auprès de l'IdP lors de la déconnexion de Relution : un clic sur Déconnexion révoque la session dans Relution. Si le commutateur de déconnexion OIDC lors de la déconnexion de Relution est activé sous Options avancées (par défaut : désactivé) et qu'un point de terminaison de fin de session est connu (saisi manuellement dans le champ correspondant ou communiqué par l'IdP via la découverte), le navigateur est en outre redirigé vers le point de terminaison de déconnexion de l'IdP.
- Déconnexion front-channel : lorsque l'utilisateur se déconnecte auprès de l'IdP, l'IdP appelle l'URL de déconnexion du canal frontal affichée dans le portail et Relution révoque la session. Cette URL doit pour cela être enregistrée auprès de l'IdP.
- Déconnexion back-channel : l'IdP envoie une notification de déconnexion à l'URL de déconnexion du canal arrière — la session est révoquée sans intervention de l'utilisateur.

Le test de ces voies permet de s'assurer qu'une fin de session initiée par l'IdP (par ex. via la console d'administration de l'IdP) est correctement transmise à Relution.

Pour la version 26.4.0

Configuration de l'heure creuse

Dans les versions 5.23 et suivantes, la configuration Off-Time de Relution permet aux utilisateurs disposant des autorisations nécessaires (par défaut les rôles Administrator et Device Manager d'une organisation) d'entrer les calendriers des vacances scolaires pour les Länder allemands et d'ajouter leurs propres dates, soit manuellement, soit en téléversant un fichier de calendrier existant. Les politiques dans lesquelles l'Off-Time est activée sont désactivées pendant ces périodes.

Configuration

La configuration Off-Time se trouve dans une organisation sous `Paramètres` → `Configuration de l'heure creuse`. Elle n'est pas disponible dans l'organisation globale.

Synchroniser les calendriers des vacances scolaires

La synchronisation est activée via le commutateur Synchroniser le calendrier des vacances scolaires (uniquement pour l'Allemagne) et la sélection de l'État fédéral, puis appliquée avec Enregistrer. Les vacances de l'année en cours et de l'année suivante sont reprises ; ensuite, le serveur met à jour les entrées automatiquement. Le bouton à côté de Dernière synchronisation de l'heure d'arrêt permet de lancer la synchronisation manuellement. Si la synchronisation est désactivée, toutes les entrées synchronisées sont supprimées.

Pour la version 26.4.0

Pour la version 26.4.0

Les calendriers des vacances scolaires ne sont disponibles que pour l'Allemagne.

Ajouter ou importer des périodes personnalisées

Ajouter ouvre la boîte de dialogue Configurer les congés. À l’étape Type de vacances, le choix se fait entre Manuel et Importation :

- Manuel : un Nom et la période personnalisée (champ Période d’usage hors temps) avec date de début et date de fin sont saisis.
- Importation : un fichier de calendrier est téléversé. Les formats suivants sont pris en charge : `.ical`, `.ics`, `.ifb`, `.icalendar`. Seuls les événements d’une journée entière avec un titre sont repris ; le titre devient le nom de l’Off-Time.

Pour chaque entrée, la liste affiche le nom, la date de début, la date de fin et la source (manuelle, importée avec le nom du calendrier ou Synchronisé pour un Land). Les entrées passées sont grisées. Les entrées peuvent être modifiées et supprimées ; le menu contextuel permet d'exporter les Off-Times sous forme de fichier iCalendar (Exporter les heures creuses vers iCalendar) ou au format CSV. Par défaut, les Off-Times expirées sont supprimées automatiquement deux ans après leur fin.

Pour la version 26.4.0

Application dans les politiques

Lors de la création ou de la modification d'une politique, le commutateur Configuration du temps mort peut être activé. Lorsqu'il est activé, la politique est désactivée pendant toutes les périodes définies dans la configuration Off-Time (p. ex. vacances scolaires) et n'est pas appliquée aux appareils. Cela vaut aussi lorsqu'aucune planification basée sur le temps n'est configurée. Les périodes sont évaluées dans le Fuseau horaire de la politique, qui peut être défini même sans planification basée sur le temps lorsque l'Off-Time est activée ; à défaut, le fuseau horaire du serveur s'applique.

Pour la version 26.4.0

La configuration Off-Time a une priorité plus élevée qu'une politique basée sur le temps : pendant une Off-Time, la politique reste désactivée même dans sa plage horaire.

Certificats d'organisation

Pour fonctionner avec le service Apple APNS — responsable des notifications push et de la soumission des profils aux appareils Apple inscrits — Relution a besoin d’un certificat MDM push signé. Si aucun certificat APNS n’est configuré, l’inscription des appareils Apple est désactivée et le centre de notifications signale Certificat APNS manquant. Avant et après l’expiration du certificat, les avis Le certificat APNS expirera bientôt et Le certificat APNS a expiré s’affichent.

Pour la version 26.4.0

> Un certificat APNS existant devrait toujours être renouvelé plutôt que recréé. Si un certificat avec un topic push différent est téléversé, les appareils déjà inscrits conservent leur ancien certificat ; une fois celui-ci expiré, ils ne peuvent plus communiquer avec Relution et doivent être réinscrits. Lors du passage du certificat par défaut de Relution à un certificat personnalisé, les appareils existants continuent d'utiliser le certificat par défaut jusqu'à leur réinscription.

Informations affichées sur la page

Dans la zone APNS, la page sous `Paramètres` → `Certificats d'organisation` affiche pour le certificat enregistré le topic push (Certificat existant), la date d'expiration (valable jusqu'au) et le Compte Apple associé. Si aucun certificat n'est enregistré, l'avis Aucun certificat configuré s'affiche. Le bouton Démarrer ouvre l'assistant Modifier le certificat APNS.

Dans les organisations standard, la zone Certificat Push pour l'App Store affiche en outre le certificat push pour l'App Store avec sa date d'expiration ; cette zone sert uniquement à l'affichage.

Un certificat APNS enregistré dans l'organisation globale ou une méta-organisation s'applique à toutes les sous-organisations qui n'ont pas leur propre certificat APNS. Si un certificat personnalisé est enregistré dans une sous-organisation, il remplace le certificat hérité pour cette organisation. Un avis sur la page indique si le certificat est hérité ou géré par l'organisation mère.

Pour la version 26.4.0

Certificat par défaut (installations existantes)

Les installations Relution existantes peuvent utiliser le certificat par défaut de Relution (`com.apple.mgmt.mway.mwaysolutions`). Ce certificat est mis à jour automatiquement à chaque mise à jour de Relution — aucune action manuelle n'est requise. Voir Mise à jour →.

À partir de Relution 26.3.0, les nouvelles installations n'utilisent plus le certificat par défaut de Relution. Les nouvelles installations doivent fournir leur propre certificat via l'assistant en libre-service.

Pour les installations existantes utilisant encore le certificat par défaut, il est recommandé de passer à l'assistant en libre-service — en particulier lors de la création de nouvelles organisations —, car le certificat par défaut de Relution est prévu d'être abandonné dans une future version.

Configuration d’un certificat personnalisé

L’assistant en libre-service dans `Paramètres` → `Certificats d'organisation` guide tout au long du processus : Relution génère automatiquement une CSR signée qu’il suffit de téléverser chez Apple, puis de reporter le certificat résultant dans Relution — aucun ticket de support requis.

Configurer ou renouveler les certificats APNS Push →

Migration depuis l’ancien processus

Si l’installation utilisait précédemment un certificat fourni via le Helpdesk Relution, un avis de migration apparaît sur cette page, suivi de l’option Migrer votre ancien certificat APNS avec le bouton Migrer. La migration est une opération en un clic et n’affecte pas les appareils inscrits. Tant que la migration n’a pas été effectuée, l’assistant (Démarrer) n’est pas disponible.

Après la migration, l’assistant en libre-service est disponible pour tous les futurs renouvellements.

Guide complet de migration et de configuration →

Pour la version 26.4.0

Secure Mail Gateway

Avec la Secure Mail Gateway (SMG, dans le portail : Passerelle Secure Mail), Relution offre la possibilité de se connecter à un serveur Exchange sans le rendre disponible sur Internet. Relution fonctionne comme un proxy pour la communication via Exchange Active Sync (EAS). L'utilisation de SMG nécessite la disponibilité d'une authentification de base sur le serveur Exchange. L'authentification moderne n'est pas prise en charge.

> Le service SMG doit être accessible aux appareils sur le port 443. Pour cela, le reverse proxy redirige le chemin `/Microsoft-Server-ActiveSync` vers le service SMG (port 8093). Le service SMG doit pouvoir accéder au serveur Exchange (URL Exchange) et au serveur Relution. Une connexion du serveur Exchange vers le serveur Relution n'est pas nécessaire.

Il est recommandé de configurer les options de restriction seulement après que la connexion a été testée avec succès afin d'exclure les erreurs possibles. Une fois que la connexion a été testée avec succès et que l'on peut travailler avec les points finaux, les autorisations peuvent être configurées en conséquence.

> Breaking change avec Relution 26.4.0 : À partir de la version 26.4.0, la fonctionnalité SMG nécessite un service autonome dédié. Instructions d'installation : Secure Mail Gateway →.

Pour la version 26.4.0

Configuration de Secure Mail Gateway

Nouveau dans 26.4

Les paramètres se trouvent sous `Paramètres` → `Gestion des appareils` → `Passerelle Secure Mail`. Ils s'appliquent par organisation ; la vignette n'est pas disponible dans l'organisation globale.

Pour la version 26.4.0

Configuration du proxy

- Activé Active SMG pour l'organisation. Si l'interrupteur est désactivé, les autres champs sont verrouillés et l'option Utiliser Secure Mail Gateway ne peut pas être activée dans les configurations Exchange des politiques.
- URL d'échange (URL du serveur Exchange) L'adresse à laquelle le serveur Exchange peut être atteint. Champ obligatoire.
- URL du service SMG L'URL publiquement accessible du service SMG. Il peut s'agir d'un sous-domaine dédié (ex. `https://smg.votreserveur.example.com`) ou de la même URL que le serveur Relution — à condition que le proxy inverse transfère correctement `/Microsoft-Server-ActiveSync` au service SMG.

  Ce champ est disponible à partir de Relution 26.4.1 et est obligatoire. Si une URL différente de l'URL du serveur Relution est saisie, les configurations Exchange existantes ne reprennent pas automatiquement le nouvel hôte. Une nouvelle version doit être créée dans chaque politique contenant une configuration Exchange. Dans la configuration Exchange, l'option Utiliser Secure Mail Gateway doit être activée afin que l'hôte soit défini sur la nouvelle URL du service SMG. La politique doit ensuite être publiée.
- Domaine Exchange Le domaine correspondant au serveur Exchange auquel il faut accéder. Facultatif ; s'il est renseigné, SMG utilise ce domaine lors de la transmission des requêtes au serveur Exchange (voir Aperçu technique →).
- En-tête d'hôte Exchange personnalisé Valeur facultative de l'en-tête Host utilisé pour la communication avec le serveur Exchange. Si une valeur est saisie, elle remplace l'en-tête Host dérivé sinon de l'URL du serveur Exchange.

Pour la version 26.4.0

Règles d’autorisation pour les appareils enrôlés

Les règles d’autorisation (dans le portail : Règles relatives aux allocations) définissent quels appareils enrôlés dans Relution peuvent se synchroniser avec le serveur Exchange via SMG. Une requête n’est transmise que si l’appareil respecte toutes les règles.

- Propriété Types de propriété autorisés : Appareil appartenant à l’entreprise (COD), appareil personnel (BYOD) et Inconnu. Par défaut, tous sont sélectionnés.
- États de l’appareil États autorisés : Conforme, Inactif et Non conforme. Par défaut, seul Conforme est sélectionné ; les appareils inactifs et non conformes sont refusés.
- Plateformes Plateformes autorisées : Android, iOS et Windows. Par défaut, toutes sont sélectionnées.
- Mettre certaines versions de ⋯ sur la liste de blocage Un champ distinct apparaît pour chaque plateforme sélectionnée, par ex. Mettre certaines versions de iOS sur la liste de blocage. Les appareils exécutant l’une des versions de système d’exploitation saisies sont refusés.

Une connexion doit d’abord être établie et la fonction testée avant de configurer toute restriction.

Pour la version 26.4.0

Tolérance pour les appareils inconnus

L’interrupteur autorise la synchronisation via SMG des appareils inconnus ou non enrôlés, par ex. des ordinateurs portables ou des PC qui ne peuvent pas être enrôlés dans Relution. Est considéré comme inconnu tout appareil que Relution ne peut associer à aucun appareil enrôlé à partir de la requête. L’option est activée par défaut. Si elle est désactivée, des appareils enrôlés peuvent, le cas échéant, être également refusés lors de la configuration initiale du compte, tant que Relution ne peut pas encore les identifier.

Utilisation dans les politiques

Pour que les appareils utilisent SMG, l’option Utiliser Secure Mail Gateway est activée dans la configuration Exchange d’une politique, par ex. pour iOS → ou Windows →. Hôte Exchange et Domaine Exchange sont alors définis automatiquement. Si la plateforme ou une version du système d’exploitation est bloquée dans les paramètres SMG, la configuration affiche un avertissement.

Aperçu technique

Pour les configurations Exchange utilisant SMG, l'URL du service SMG sans protocole (`https://`) est définie comme adresse du serveur sur l'appareil. L'appareil se connecte ainsi au point de terminaison EAS `<URL du service SMG>/Microsoft-Server-ActiveSync`. Le domaine est défini sur le nom unique de l'organisation. Relution utilise ce domaine pour identifier les paramètres SMG correspondants.

Si SMG est activé et configuré dans ces paramètres, les en-têtes de requête `DeviceId` et `DeviceType` sont évalués pour identifier l'appareil qui déclenche la requête. En fonction des paramètres SMG, si le dispositif a pu être identifié, et des propriétés et du statut du dispositif (voir la section Règles d'autorisation pour les appareils enrôlés), la requête est refusée ou transmise à l'hôte Exchange configuré dans les paramètres SMG et la réponse est renvoyée au dispositif. Le domaine est ajusté à celui configuré dans les paramètres SMG s'il est présent.

Mot de passe

Exchange et SMG utilisent BasicAuth, il est donc possible que des erreurs de compte se produisent sur l'appareil final lors de l'utilisation de caractères spéciaux tels que `$ # / * ü ö ä` et `espace`.

Pour vérifier cela, un mot de passe simple composé de lettres et de chiffres doit être utilisé pour le test.

Pour la version 26.4.0

---

macOS

MacOS utilise la connexion Exchange via EWS. Cependant, SecureMailGateway ne peut transmettre qu'ActiveSync. Par conséquent, il n'est actuellement pas possible d'utiliser des appareils macOS avec SMG.

Contrat de sous-traitance (AVV)

Pour garantir une conformité RGPD totale, il est nécessaire, en tant que responsable du traitement, de conclure un contrat de sous-traitance (AVV / DPA) avec l'exploitant de l'environnement Relution (le sous-traitant). La zone Créer un nouveau DPA (dans l'interface, l'AVV est désigné par DPA) permet de configurer et de signer ce contrat entièrement en ligne.

Relution permet ainsi une conclusion efficace, transparente et conforme à la loi des contrats de sous-traitance entre Relution GmbH et le client.

Tant que la version actuelle de l'AVV n'est pas signée dans une organisation, le message Signature DPA requise apparaît dans la zone de notifications (1). Il est affiché aux utilisateurs disposant du droit Gestion de l'APD → Actualisation. Lorsqu'une nouvelle version de l'AVV est fournie, le message apparaît à nouveau ; le formulaire est alors prérempli avec les informations de la dernière version signée.

L'AVV peut être conclu individuellement pour chaque mandant. Il peut également être conclu pour toutes les organisations subordonnées dans l'organisation globale ou dans une organisation Meta avec l'option Signer pour tous les sous-mandants (libellé du portail : Signe pour tous les sous-locataires). Dans ces organisations, le message et les paramètres de l'AVV ne sont alors plus affichés.

Pour la version 26.4.0

L'accès aux paramètres de l'AVV est possible de deux façons :

1. Directement via la notification (1 + 2) dans la zone de notifications.
2. Via le chemin de menu (3) : `Paramètres` → `Général` → `Gestion de l'APD`

1. Informations générales

Pour la version 26.4.0

Cette section permet d’identifier clairement le signataire et la personne morale qui conclut le contrat. La personne qui remplit cette section doit être habilitée à signer pour l’organisation.

Champ	Description
Nom complet du signataire	Le nom de la personne qui signe le contrat de manière juridiquement contraignante.
E-mail	L’adresse e-mail de la personne signataire.
Nom de l’entreprise	Le nom officiel de l’organisation (le responsable du traitement).
Adresse, code postal, ville, pays	L’adresse officielle de l’organisation.

Le nom et l’e-mail sont préremplis avec les données de l’utilisateur connecté, le nom de l’entreprise et l’adresse avec les informations des paramètres généraux de l’organisation. Les valeurs peuvent être modifiées avant la signature.

2. Remarque importante concernant l’art. 9 du RGPD

L’avertissement suivant, mis en évidence en bleu, doit être pris en compte :

> Le traitement des données conformément à l’article 9 du RGPD n’est pas autorisé et doit être empêché par le responsable du traitement.

Contexte : L’article 9 du RGPD régit les catégories particulières de données à caractère personnel (par exemple, les données de santé, l’origine ethnique, les opinions politiques). Relution étant un système MDM qui traite principalement des données techniques et administratives, le traitement de ces catégories de données hautement sensibles n’est pas autorisé en fonctionnement standard et doit être empêché par le responsable du traitement.

3. Type de données

Cette section permet de définir quelles catégories de données à caractère personnel sont traitées dans le cadre de l’utilisation de Relution. Cocher toutes les catégories concernées dont les données figurent dans l’instance Relution :

- Données de base (par ex. nom, prénom, sexe, adresse e-mail, adresse, numéro de téléphone)
- Données contractuelles de base (produits, contrat d’achat, prix d’achat, garanties)
- Données de journalisation (adresse IP, horodatage, événements avec contexte utilisateur)
- Contenus générés par les utilisateurs (par ex. messages de forum, demandes de fonctionnalités, demandes de support)
- Données d’appareils (type d’appareil, numéro d’appareil, adresse IP, informations sur le système d’exploitation, applications installées)
- Données de localisation (iBeacons, position GPS, réseau mobile, réseaux WiFi)

Si nécessaire, des catégories de données supplémentaires non listées ici peuvent être ajoutées via Ajouter d’autres.

Au moins une catégorie de données doit être sélectionnée ou ajoutée via Ajouter d’autres, sinon Prévisualisation et Signer le DPA restent désactivés.

Pour la version 26.4.0

4. Groupe des personnes concernées

Sélectionner quels groupes de personnes sont concernés par le traitement des données dans l'instance Relution :

- Parents et représentants des parents
- Clients finaux et fournisseurs
- Collaborateurs (par ex. salariés, enseignants, apprentis, personnel administratif)
- Élèves

La fonction Ajouter d'autres peut également être utilisée ici si d'autres groupes, non listés, sont concernés. Ici aussi, au moins un groupe doit être sélectionné ou ajouté.

---

5. Contact d'urgence

Indiquer ici les coordonnées de la personne de l'organisation qui peut être contactée immédiatement en cas de violation de données ou d'autres urgences liées à la sécurité. Le nom et l'e-mail sont obligatoires, le numéro de téléphone est facultatif.

Pour la version 26.4.0

- Nom
- E-mail
- Téléphone

---

6. Conclusion et signature

Avant de conclure le contrat, l'habilitation à signer doit être confirmée :

- Confirmation de l'habilitation à signer : atteste que le signataire est habilité à conclure le contrat au nom de l'organisation.

Dans l'organisation globale et dans les organisations Meta, la sélection facultative Signer pour tous les sous-mandants (libellé du portail : Signe pour tous les sous-locataires) est également disponible. Elle est pertinente si, en tant qu'instance supérieure (par ex. un organisme scolaire), le contrat est également conclu pour des unités subordonnées gérées (par ex. des écoles individuelles). Si elle est cochée, l'AVV s'applique également à toutes les organisations subordonnées ; aucun AVV distinct n'y est alors proposé.

Deux actions sont disponibles pour conclure le contrat :

- Prévisualisation : affiche au préalable le texte intégral du contrat. Disponible dès que les informations générales ainsi que le type de données et le groupe de personnes concernées sont renseignés.
- Signer le DPA : conclut le contrat de manière numérique. L'AVV devient alors juridiquement valide. Le bouton n'est actif que lorsque le contact d'urgence (nom et e-mail) est également renseigné et l'habilitation à signer confirmée.

> Conserver soigneusement le document signé dans le cadre des obligations de documentation (obligation de rendre compte au titre du RGPD).

Lors de la signature, les informations du contrat sont automatiquement transmises au serveur de licences Relution. Sont transmis :

- les informations du formulaire : personne signataire et e-mail, nom de l'entreprise et adresse, type de données, groupe des personnes concernées, contact d'urgence ainsi que la sélection Signer pour tous les sous-mandants
- la date et l'heure de la signature, l'adresse IP et le nom d'utilisateur Relution avec lequel la signature a été effectuée

Les documents PDF de l'AVV ne sont pas transmis au serveur de licences. Sans cette transmission, l'AVV ne peut pas être signé.

Après la signature, l'AVV est envoyé au format PDF en version allemande et anglaise par e-mail à l'adresse e-mail saisie pour la personne signataire. Si l'envoi échoue, la signature reste valide.

Pour la version 26.4.0

AVV signé

Après la signature, la Gestion de l'APD affiche la zone Accord signé sur le traitement des données avec Version DPA, Date de signature, Signé par et le Contact en cas d'urgence. Dans l'organisation globale et dans les organisations Meta, l'indication de la signature pour les sous-mandants (libellé du portail : Signé pour les sous-locataires) est également affichée.

Pour la version 26.4.0

- Télécharger : télécharge l’AVV signé au format PDF, en allemand si la langue du portail est l’allemand, sinon en anglais.
- Révoquer : révoque l’AVV signé. La date et l’utilisateur de la révocation sont transmis au serveur de licences Relution. L’AVV est ensuite de nouveau proposé à la signature.

Autorisations

Les droits relatifs à l’AVV se trouvent dans les rôles, dans le groupe d’autorisations Gestion de l’APD :

- Lire : affiche l’aperçu de l’AVV signé.

- Actualisation : affiche le message et le formulaire de signature.
- Supprimer : permet de révoquer un AVV signé.

Le rôle Administrateur contient les trois droits. Tant qu'aucun AVV n'est signé, les utilisateurs sans le droit Actualisation ne voient que la mention Aucun DPA n'a encore été signé à la place du formulaire.

Remarques concernant la signature de l'AVV

Si la personne concernée n'est pas habilitée à signer le contrat de sous-traitance (AVV), procéder comme suit :

- Création de compte : créer un compte dédié pour le collègue habilité à signer, dans l'organisation pour laquelle l'AVV est conclu. Le compte nécessite un rôle disposant du droit Gestion de l'APD → Actualisation (par ex. le rôle Administrateur) ; sans ce droit, ni la notification AVV ni le formulaire de signature ne sont affichés.
- Signature : Le collègue peut ensuite se connecter au portail et signer l'AVV de manière autonome.

Relution 26.0.0

Pour la version 26.4.0

Paramètres de langue

Dans Relution, la langue de l'interface peut être définie pour chaque utilisateur, et les langues dans lesquelles les contenus tels que les descriptions d'applications et les notifications sont gérés peuvent être configurées.

Langues de l'organisation et langue par défaut

Sous `Paramètres` → `Général` → `Langues`, les langues dans lesquelles les contenus sont gérés dans Relution sont définies. Chaque langue ajoutée fournit des champs localisés supplémentaires, par exemple le nom et la description des applications, les textes des notifications d'inscription et d'applications ainsi que les informations de support. Ces langues sont indépendantes de la langue de l'interface de Relution, que chaque utilisateur définit lui-même (voir Langue de l'utilisateur).

L'allemand et l'anglais sont disponibles par défaut dans chaque organisation. Une nouvelle organisation reprend comme langue par défaut celle de l'organisation globale ; à la livraison, il s'agit de l'anglais.

Pour la version 26.4.0

- D'autres langues peuvent être ajoutées via Ajouter. De nombreuses langues et variantes régionales (locales) sont disponibles, par exemple le néerlandais, le polonais ou l'allemand (Autriche), indépendamment des langues de l'interface. Les contenus manquants d'une nouvelle langue sont copiés à partir de la langue par défaut.
- Le menu à 3 points → Définir par défaut permet de définir une langue comme langue par défaut. Avant le changement, une boîte de dialogue de confirmation s'affiche : les traductions des applications existantes, des notifications d'inscription et des notifications d'applications doivent être disponibles au préalable dans la nouvelle langue, car des traductions manquantes peuvent entraîner des erreurs lors de l'inscription.
- Supprimer retire une langue. La langue par défaut ne peut pas être supprimée.

La langue par défaut est utilisée pour les notifications push, par exemple les notifications d'applications envoyées par push ou les messages push d'une action de groupe d'appareils de type Action de notification, ainsi que pour les e-mails envoyés à des adresses e-mail saisies en plus, sans compte utilisateur Relution. En outre, les nouveaux utilisateurs sans langue définie reçoivent la langue par défaut comme langue de l'utilisateur si elle fait partie des langues prises en charge par l'interface, sinon l'anglais.

Les e-mails adressés aux utilisateurs Relution, par exemple pour la réinitialisation du mot de passe ou concernant des applications, sont envoyés dans la langue de l'utilisateur destinataire.

Si aucune traduction n’existe dans cette langue, ils sont envoyés en anglais.

Langue de l’utilisateur

La langue de l’utilisateur peut être définie individuellement par chaque utilisateur et affecte l’ensemble de l’interface dans Relution. Ainsi, par exemple, le tableau de bord, les politiques et les tableaux seront affichés dans la langue choisie. Les e-mails que Relution envoie à l’utilisateur suivent également cette langue.

Le réglage se trouve dans le menu utilisateur en haut à droite sous `Profil`. Dans l’onglet Informations sur l’utilisateur, la carte Préférences contient l’entrée Langue. La langue se modifie via l’icône crayon (Éditer Langue).

Langues prises en charge

Relution prend actuellement en charge les langues suivantes dans son interface graphique :

- Allemand
- Anglais
- Français
- Italien
- Espagnol
- Turc

Pour la version 26.4.0

REST API

L’ensemble des fonctionnalités de Relution est disponible via une API REST complète. Cette API permet de contrôler Relution depuis toute autre application ou à l’aide de scripts.

Documentation de l’API

Chaque serveur Relution embarque la spécification complète de l’API, correspondant exactement à la version installée du serveur. Elle documente tous les points de terminaison avec leurs paramètres, les corps de requête et de réponse ainsi que les codes de statut retournés.

La spécification s’ouvre depuis le portail Relution : l’entrée API Web du menu de support (en haut à droite) ouvre la documentation interactive. Elle est également accessible directement à l’adresse `https://<serveur>/web-api/index.html`.

Les requêtes adressées à l’API REST sont soumises aux mêmes contrôles de permissions que les actions effectuées dans le portail ; les actions liées à la sécurité sont consignées dans le Journal d’audit →.

Pour la version 26.4.0

Créer des jetons d’accès à l’API

Pour accéder à Relution depuis des systèmes tiers ou des scripts, un jeton d’accès API est nécessaire.

Pour la version 26.4.0

1. Cliquer sur le nom d’utilisateur en haut à droite du portail Relution.
2. Naviguer vers : `Profil` → `Jetons d’accès` → `Ajouter`.
3. Donner un nom au jeton et le copier.

Les options suivantes sont également disponibles lors de la création :

- Durée d’utilisation limitée : activée par défaut. La Date d’expiration est préremplie avec la date du jour plus 180 jours et peut être modifiée ultérieurement via Modifier le jeton d’accès. Si l’option est désactivée, le jeton n’expire pas.
- Portées d’API : le jeton ne peut être utilisé que pour des requêtes vers les points de terminaison des portées sélectionnées (sélection multiple, valeur par défaut : Portail de gestion). Les exemples de cet article utilisent des points de terminaison sous `/api/management/` et nécessitent cette portée.

Le jeton est utilisé dans l’en-tête HTTP `X-User-Access-Token` pour authentifier les requêtes.

Les administrateurs disposant de l’autorisation de créer des jetons d’accès API peuvent également créer un jeton pour un autre utilisateur, par exemple pour un compte de service. Pour cela, un seul utilisateur est sélectionné sous `Utilisateurs` → `Utilisateurs`, puis l’action Ajouter un jeton d’accès est appelée depuis le menu contextuel.

> Le jeton n'est affiché qu'une seule fois lors de sa création.

---

1. Utilisateurs au format CSV

- La première ligne du fichier `.csv` doit contenir une ligne d'en-tête avec les noms des propriétés souhaitées.
- L'ordre des colonnes n'a pas d'importance.
- Les propriétés non nécessaires peuvent être omises.
- Champs obligatoires : la ligne d'en-tête doit contenir la colonne `email`, et chaque ligne nécessite un nom d'utilisateur dans la colonne `name`. Le modèle du portail commence par les colonnes suivantes :

```
name,email,givenName,surname,password
```

La casse des noms de colonnes n'a pas d'importance. Les mots de passe doivent respecter la politique définie sous `Paramètres` → `Gestion des connexions`. Les numéros de téléphone doivent être au format international, par ex. `+4912345`.

Il est possible d'ajouter jusqu'à 15 propriétés personnalisées : **`custom1`** – **`custom15`**

Le modèle du portail contient d'autres colonnes, comme `disablePasswordAuthentication`, `locale`, `permissions`, `memberOfGroups`, `teacherOfClasses` et `studentOfClasses`. Leur signification est décrite dans l'article Import CSV →.

👉 Un modèle peut être téléchargé dans le portail Relution : `Utilisateurs` → `Utilisateurs` → `Menu trois points` → `Importer des utilisateurs via CSV`. Dans la boîte de dialogue, il est disponible via le lien modèle du texte de description.

Exemple CSV :

```
name,email,givenName,surname,password,phone,position,country,managedAppleId,cu
user1,user1@company.com,Heinz,Ketchup,p4ssw0rd,+49234346345,user1 position,use
user2,user2@company.com,Heinz,Ketchup,p4ssw0rd,+49234346345,user2 position,use
user3,user3@company.com,Heinz,Ketchup,p4ssw0rd,+49234346345,user3 position,use
user4,user4@company.com,Heinz,Ketchup,p4ssw0rd,+49234346345,user4 position,use
```

Pour la version 26.4.0

```
user5,user5@company.com,Heinz,Ketchup,p4ssw0rd,+49234346345,user5 position,use
user6,user6@company.com,Heinz,Ketchup,p4ssw0rd,+49234346345,user6 position,use
```

---

2. Importer des utilisateurs via le portail Relution

1. Aller dans : `Utilisateurs` → `Utilisateurs` → `Menu trois points` → `Importer des utilisateurs via CSV`
2. Sélectionner le fichier CSV et le séparateur. L'option Créer automatiquement des groupes et des classes crée les groupes et classes mentionnés dans le fichier qui n'existent pas encore.
3. Assigner les utilisateurs importés à un ou plusieurs groupes.
4. Les utilisateurs apparaîtront ensuite dans l'aperçu.

---

3. Créer des utilisateurs via l'API Relution

Pour la version 26.4.0

Changement dans Relution 5.34 :

- L'import d'utilisateurs est désormais un job en arrière-plan avec les états CREATED, RUNNING, FINISHED et FAILED.
- Chaque job enregistre un rapport par ligne.
- L'ancien import a été supprimé.
- Certains noms de colonnes ont changé :
  - `first name` → `givenName`
  - `last name` → `surname`
  - `managed apple id` → `managedAppleId`
  - `phone number` → `phone`
  - `userId` → `name`

Étapes

1. Créer un fichier `users.csv`.
2. Copier le script bash suivant dans un fichier, par ex. `uploadUserCSV.sh`.
3. Rendre le fichier exécutable :

```
chmod +x ./uploadUserCSV.sh
```

4. L’exécuter :

```
./uploadUserCSV.sh -f 'FILEPATH' -h 'HOST' -a 'YOUR-ACCESS-TOKEN'
```

Arguments

Argument	Signification	Exemple	Défaut	Obligatoire
`-f`	Chemin vers le fichier `users.csv`	user.csv		✅
`-h`	Hôte Relution	https://relution.io		
`-a`	Jeton d’accès API	xxxxxxxx		
`-r`	Groupe (nom ou UUID) auquel les utilisateurs importés sont attribués ; espaces codés en `%20`	Ecole%20Enseignants	`Organame%20Device%20User`	❌
`-s`	Séparateur utilisé pour le parsing	SEMICOLON	COMMA	

Argument	Signification	Exemple	Défaut	Obligatoire
`-w`	Écraser les utilisateurs existants	true	false	❌

- Les utilisateurs sont importés dans l'organisation du compte auquel appartient le jeton d'accès API. Ce compte nécessite les autorisations de création et de modification d'utilisateurs.
- Sans `-r`, le script utilise le groupe `Organame Device User`. « Organame » doit être remplacé dans le script par le nom de sa propre organisation ; sinon, aucun groupe n'est attribué.
- Avec `-w true`, les utilisateurs existants sont écrasés ; la correspondance se fait via la colonne `name`. Les utilisateurs provenant d'un annuaire externe tel que LDAP sont ignorés.
- L'API prend en charge en plus le paramètre `createMissingGroupsAndClasses=true`. Il correspond à l'option Créer automatiquement des groupes et des classes du portail et n'est pas défini par le script.

Pour la version 26.4.0

Exemple de sortie

```
============
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. Importer des utilisateurs via script Bash CSV

Afficher l'exemple de configuration complet

5. Créer une nouvelle organisation

Le script suivant crée une nouvelle organisation ainsi qu'un administrateur d'organisation. Le jeton utilisé appartient à un utilisateur disposant de l'autorisation de créer des organisations ou des sous-organisations, par exemple l'administrateur système. Le nom court `orgaName` est obligatoire ; les informations sur l'administrateur (`orgaAdminUser`, `orgaAdminGivenName`, `orgaAdminSurName`, `orgaAdminPwd`) sont requises tant que `skipAdminCreation` n'est pas défini sur `true`. Le mot de passe de l'administrateur doit respecter la politique de mot de passe par défaut. En cas de succès, le serveur répond avec le code HTTP 202 et renvoie l'UUID de l'organisation, son nom et l'UUID de l'administrateur.

> Afficher l'exemple de configuration complet

---

6. Interroger les appareils d'une organisation

> Afficher l'exemple de configuration complet

Pour la version 26.4.0

Bonnes pratiques pour les jetons API

- Toujours définir une date d'expiration pour les jetons d'accès API. Les jetons sans date d'expiration restent valides indéfiniment.
- Révoquer immédiatement les jetons lorsque le rôle du compte associé change, que le compte est désactivé ou que son titulaire quitte l'organisation.
- Les secrets des jetons sont stockés uniquement sous forme de hachage (SHA-256, ou HMAC-SHA-256 si une clé HMAC est configurée) et ne peuvent pas être récupérés après la création. Si nécessaire, créer un nouveau jeton au lieu d'essayer de récupérer un jeton existant.

Voir aussi

- Créer des jetons d'accès à l'API dans Relution → — instructions pour générer un jeton.
- Connexion LDAP / Active Directory → — synchroniser les utilisateurs et les groupes.

Journal d'audit

Avec la version `5.25.0`, un journal d’audit a été introduit dans Relution. Il permet de suivre les activités sans avoir à chercher dans les journaux.

Journal d’audit

Le journal d’audit est disponible sous `Paramètres` → `Journal d'audit`. L’accès est contrôlé par deux autorisations :

- Journal d’audit : toutes les entrées.
- Journal d’audit de gestion des appareils : uniquement les entrées de la catégorie gestion des appareils.

Les administrateurs d’organisation disposent des deux autorisations par défaut. Les entrées de l’organisation actuelle sont affichées ; dans une méta-organisation, celles de ses sous-organisations s’y ajoutent. Dans l’organisation Global, le journal d’audit comprend les entrées de toutes les organisations.

Les données sont conservées par défaut pendant 180 jours et peuvent être recherchées et filtrées dans le portail Relution.

Pour la version 26.4.0

Les colonnes suivantes sont disponibles pour information :

- Date
- Nom d’utilisateur
- Dispositif authentifié
- Client
- Usurpateur (utilisateur à l’origine de l’usurpation d’identité)
- Méthode (POST, GET, PUT, DELETE)
- Description
- Point de terminaison (dans le portail : Point final ; masqué par défaut, peut être affiché via le sélecteur de colonnes)
- Statut HTTP
- Organisation (uniquement dans l’organisation Global et dans les méta-organisations)
- IP
- Catégorie (uniquement avec l’autorisation Journal d’audit)
- Résultat
- Type d’événement

Des filtres sont disponibles pour la méthode, le statut HTTP (2xx, 4xx, 5xx), le nom d'utilisateur, le dispositif authentifié, le client, l'organisation, la catégorie, le résultat et le type d'événement ; les mêmes restrictions que pour les colonnes s'appliquent à l'organisation et à la catégorie.

Cela permet de suivre les modifications apportées au serveur ; les événements enregistrés dépendent de la configuration du serveur (voir Étendue de la journalisation →).

Export

Dans le menu trois points, Exporter le journal d'audit complet ouvre la boîte de dialogue Export du journal d'audit. Démarrer un nouvel export crée un fichier CSV en arrière-plan, qui peut ensuite être téléchargé dans la même boîte de dialogue. Un seul export est conservé à la fois ; un nouvel export remplace le précédent. Un export en cours peut être interrompu via Annuler.

Comportement en cas de limite de stockage

Les entrées d'audit sont supprimées automatiquement lorsqu'elles dépassent la durée de conservation. La valeur par défaut est de 180 jours ; dans la configuration du serveur (`application.yml`), la durée peut être modifiée en jours via `relution.cleanup.audit-log.remove-after` (par ex. `365d`, au moins 1 jour). Le nettoyage s'exécute environ toutes les 17 minutes entre 18 h 00 et 7 h 00 et supprime au maximum 10 000 entrées par exécution, par lots de 1 000, afin d'éviter les verrous de base de données. Chaque exécution qui supprime des entrées ou qui échoue est elle-même consignée dans le journal d'audit sous l'événement Journaux d'audit nettoyés.

Pour la version 26.4.0

Si l'espace disque est épuisé avant le nettoyage, les nouvelles entrées d'audit risquent de ne pas pouvoir être écrites. L'administrateur système doit surveiller l'utilisation du disque et s'assurer que l'espace disponible est suffisant pour la durée de conservation configurée. Il n'existe aucune notification automatique en cas d'espace disque faible — cela relève de la responsabilité de l'administrateur système.

Étendue de la journalisation

L'activation et l'étendue du journal d'audit sont contrôlées via le bloc `relution.audit-log` du fichier `application.yml` ; le journal d'audit est activé par défaut. Dans la configuration par défaut, certains événements d'appareil très fréquents ne sont pas enregistrés : l'identification des appareils, les modifications des paramètres des appareils ainsi que les modifications des apps et certificats installés. Certains points de terminaison générant beaucoup de requêtes sont également exclus, par exemple les actions sur les appareils et les requêtes de l'appareil actuel. Dans la configuration pour une exploitation selon les Critères communs (CC-EAL4), la journalisation complète est active ; ces valeurs ne doivent pas y être modifiées.

Le démarrage et l'arrêt du serveur sont également consignés sous les événements Démarrage du serveur Relution et Arrêt du serveur Relution, avec la version du serveur et le nœud du cluster.

Journaux d'accès nginx

Le proxy inverse nginx consigne les requêtes HTTP/HTTPS entrantes. Ces journaux complètent le journal d'audit de l'application Relution au niveau du canal réseau. Dans le modèle de configuration pour une exploitation selon les Critères communs (CC-EAL4), le protocole TLS et la suite de chiffrement négociés pour les requêtes HTTPS sont également enregistrés. Le modèle standard de l'installation Docker → ne consigne pas ces deux champs.

Accès aux journaux :

```
docker logs nginx
```

Ou pour un suivi en temps réel :

```
docker logs -f nginx
```

Dans le modèle CC-EAL4 `relution-nginx.conf`, chaque ligne du journal d'accès des ports HTTPS (443 et 8443) a le format suivant :

```
<remote_addr> - <user> [<time>] "<request>" <status> <bytes> "<referer>" "<use
```

Les champs `$ssl_protocol` et `$ssl_cipher` en fin de ligne enregistrent la version TLS et la suite de chiffrement de la connexion (par ex. `TLSv1.3 TLS_AES_256_GCM_SHA384`). Les requêtes sur le port 80, redirigées vers HTTPS, sont consignées au format par défaut de l'image nginx, sans ces champs.

Le journal des erreurs est écrit sur `stderr` et est également accessible via `docker logs nginx`.

Référence des événements d’audit

- Événements de gestion des appareils
- Événements généraux

Références des journaux serveur

Échecs d’intégrité lors du chiffrement/déchiffrement :

```
INTEGRITY_FAILURE operation=ENCRYPT entity={} attribute={} outcome=FAILURE sub
INTEGRITY_FAILURE operation=DECRYPT entity={} attribute={} outcome=FAILURE sub
INTEGRITY_FAILURE operation=DEK_UNWRAP entity=DataEncryptionKeyset attribute=w
TLS_INTEGRITY_FAILURE host={} outcome=FAILURE reason="{}" error="{}"
```

Dérivation de clés cryptographiques (la ligne `TLS_KEY_DERIVATION` est écrite une seule fois au démarrage du serveur) :

Pour la version 26.

```
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 d
```

Canaux TLS :

```
TLS_CHANNEL_ATTEMPT host={} port={} tls={} cipher={} cert_subject="{}" cert_fi
TLS_CHANNEL_SUCCESS host={} outcome=SUCCESS
TLS_CHANNEL_FAILURE host={} outcome=FAILURE reason="{}"
```

Les messages relatifs aux tentatives de connexion TLS et aux connexions réussies peuvent être supprimés via `logging.level.io.relution.security.audit.tls.channel: WARN` ; les messages d’erreur (`TLS_CHANNEL_FAILURE`) restent consignés.

Gestion des licences

Des licences d'appareils sont nécessaires pour configurer les appareils dans Relution. Ces licences peuvent être obtenues soit directement auprès de l'équipe de vente, soit auprès d'un partenaire.
Une fois achetées, les licences sont attribuées soit au serveur, soit aux organisations. En cas de serveur propre (OnPrem / serveur cloud dédié), il est également possible de limiter le nombre de licences pour chaque organisation (p. ex. des sites ou des écoles).

Cette limitation permet de restreindre le nombre d'appareils enregistrés dans une organisation en fonction du nombre de licences. La limitation est définie par type de licence limité dans la licence du serveur, p. ex. Appareils, Utilisateurs ou Apps natives. Chacun de ces types de licence dispose de son propre onglet dans les informations sur la licence.
Cette fonction permet de s'assurer que les organisations n'utilisent pas plus de licences qu'elles n'en ont besoin. Par défaut, les organisations n'ont pas de limite, sauf si les licences sont explicitement attribuées par l'équipe de vente.

Pour la version 26.4.0

Conditions préalables

- Un modèle de licence payant ; avec la licence gratuite, la section Limites d'organisation n'est pas affichée.
- Connexion en tant qu'administrateur système dans l'organisation Global. Les droits relatifs aux attributions de licences n'existent que dans l'organisation Global ; la modification et la suppression des limites nécessitent le droit de modification.

Ajuster la limitation

1. La connexion au portail Relution s'effectue en tant qu'administrateur système dans l'organisation Global.
2. Le menu de support (icône point d'interrogation) en haut à droite est ouvert et Informations sur la licence est sélectionné. Les limites figurent dans la section Limites d'organisation.
3. Dans l'onglet du type de licence concerné (p. ex. Appareils), l'organisation est repérée dans la liste et le bouton avec les trois points est ouvert.
4. Éditer ouvre la boîte de dialogue Modifier la limite de l'organisation. Le nombre souhaité est saisi dans le champ limite et validé avec Confirmer.

La valeur ne peut pas être inférieure au nombre de licences déjà utilisées par l'organisation (colonne des licences utilisées, intitulée « D'occasion » dans le portail). La colonne Assigné indique la limite définie. La ligne Global en bas du tableau totalise les licences utilisées par toutes les organisations et compare la somme des limites attribuées à la limite globale de la licence du serveur.

> La somme des limites d'organisation peut dépasser la limite globale de la licence du serveur ; la boîte de dialogue le signale. Une fois la limite globale atteinte, aucune organisation ne peut plus consommer de licences, quelle que soit sa propre limite.

Pour la version 26.4.0

Supprimer la limitation

Via le bouton avec les trois points et l'entrée de suppression (intitulée « Clair » dans le portail), la limite d'une organisation est levée après confirmation dans la boîte de dialogue qui s'affiche. L'organisation peut ensuite utiliser toutes les licences disponibles.

Exporter les limitations

Le bouton Exporter au format CSV (Télécharger les limites de l’organisation) de la section Limites d’organisation télécharge les limites des organisations sous forme de fichier CSV.

Limitation lors de la création d’une organisation

La limite peut être définie directement lors de la création d’une organisation : une fois l’organisation créée, le bouton Allouer des licences de l’étape Résumé mène à l’étape facultative Limites. Cette étape n’apparaît qu’avec un modèle de licence payant comportant des types de licence limités et avec le droit de modifier les attributions de licences. Plus d’informations sous Créer des organisations →.

Pour la version 26.4.0

Licences Lifetime

Les licences Lifetime (licences à vie) sont valables de manière permanente pour un seul appareil. Cela supprime les coûts de licence annuels récurrents.

Une licence Lifetime est définitivement attribuée au numéro de série (SN) de l'appareil et ne peut pas être transférée vers un autre appareil.

Attribution au numéro de série

Les licences Lifetime doivent être attribuées à un numéro de série pour s'appliquer à un appareil. Les appareils dont le numéro de série est attribué à une licence Lifetime sont inscrits même si le contingent d'appareils des autres licences est épuisé.

Les appareils et les inscriptions automatiques sans numéro de série ne peuvent pas être attribués. Le nombre d'attributions est limité par la limite d'appareils de la licence Lifetime ; une fois celle-ci atteinte, les attributions supplémentaires sont refusées.

> Important : Si les licences Lifetime ne sont pas attribuées à des numéros de série, l'inscription peut être limitée dans les environnements mixtes utilisant des licences Lifetime et des licences perpétuelles / par abonnement.

Pour la version 26.4.0

Condition préalable à l'utilisation

Pour que la fonctionnalité des licences Lifetime soit disponible, au moins une licence Lifetime doit être attribuée soit à l'organisation globale, soit à un tenant.

> L'attribution peut uniquement être effectuée au niveau Global ou sur un tenant — pas sur les deux niveaux en même temps.

Le niveau applicable est indiqué par le champ Type d'affectation des informations sur la licence : avec une affectation basée sur l'organisation Global (« à l'échelle mondiale » dans le portail), les licences Lifetime et leurs attributions se trouvent dans l'organisation Global ; avec une affectation basée sur l'organisation (« basé sur la location » dans le portail), elles se trouvent dans le tenant concerné.

Toutes les méthodes d’attribution nécessitent le droit de modifier les Informations sur la licence. Sans licence Lifetime, les boutons sont verrouillés (indication L’organisation n’a pas de licence Lifetime).

Plateformes prises en charge

Actuellement, les licences Lifetime sont uniquement disponibles pour les plateformes suivantes :

- iOS / iPadOS
- Android Enterprise

Les plateformes non prises en charge restent couvertes par d’autres types de licence, p. ex. :

- Perpetual – reste valable jusqu’à résiliation
- Subscription – reste valable jusqu’à la fin de vie (EoL) définie

---

Aucun retrait possible

Il n’est pas possible de retirer des licences Lifetime déjà attribuées.

Pour la version 26.4.0

Méthodes d’attribution des licences Lifetime

Il existe actuellement 4 façons d’attribuer des licences Lifetime :

1. Via les inscriptions automatiques

Les licences Lifetime peuvent être attribuées au niveau Global / Tenant via les inscriptions automatiques. Pour cela, les entrées souhaitées sont sélectionnées sous `Appareils` → `Inscriptions automatiques`. L’action Attribuer le numéro de série à la licence Lifetime est ensuite choisie et la boîte de dialogue est confirmée avec Attribuer les numéros de série à la licence Lifetime. L’attribution ne peut pas être annulée.

L’action n’est disponible que si une licence Lifetime existe et que toutes les entrées sélectionnées possèdent un numéro de série et appartiennent à la même organisation.

2. Directement dans l’inventaire de l’appareil

L’attribution peut être effectuée directement dans l’inventaire sur l’appareil. Pour cela, les appareils souhaités sont sélectionnés sous `Appareils` → `Inventaire`, l’action Attribuer le numéro de série à la licence Lifetime est choisie et la boîte de dialogue est confirmée avec Attribuer les numéros de série à la licence Lifetime.

Conditions requises :

- l’attribution est effectuée sur le tenant
- l’appareil possède un numéro de série
- tous les appareils sélectionnés appartiennent à la même organisation

Pour la version 26.4.0

3. Lors d’une inscription manuelle sur un tenant

Les licences Lifetime peuvent être attribuées dans le cadre d’une inscription manuelle sur un tenant. Lors de la création d’une inscription pour iOS / iPadOS ou Android Enterprise sous `Appareils` → `Inscriptions`, la section Configuration contient un commutateur qui attribue le numéro de série de l’appareil à la licence Lifetime une fois l’inscription réussie (libellé dans le portail : « Attribuez le numéro de série de l’appareil à votre licence Lifetime une fois l’inscription réussie »).

Le commutateur n’est affiché que si une licence Lifetime est disponible pour l’organisation. Il ne peut être activé que lors de la création de l’inscription, et non lors d’une modification ultérieure. Relution n’attribue le numéro de série à la licence Lifetime qu’après une inscription réussie. Cette attribution ne peut pas être annulée.

> Pour iOS / iPadOS, Relution vérifie la licence d’appareil dès avant l’inscription. Si, dans un environnement mixte, aucune licence Perpetual ou Subscription n’est plus disponible, l’inscription échoue. Dans ce cas, le numéro de série est attribué au préalable via les inscriptions automatiques ou un import CSV (méthodes 1 ou 4).

Pour la version 26.4.0

4. Via l’import CSV

L’attribution est également possible via un import CSV. Pour cela, le menu de support (icône point d’interrogation) est ouvert en haut à droite et Informations sur la licence est sélectionné. Dans la liste des attributions de licences (intitulée « Demande de licence » dans le portail), le bouton Téléchargement via CSV ouvre l’import. Le fichier CSV contient une colonne `serialNumber` avec un numéro de série par ligne.

La liste des attributions de licences n’existe que si une licence Lifetime est disponible. L’endroit où elle apparaît dépend du Type d’affectation : avec une affectation basée sur l’organisation Global, uniquement dans l’organisation Global ; avec une affectation basée sur l’organisation, uniquement sur le tenant sur lequel les licences Lifetime sont stockées.

Les numéros de série déjà attribués sont ignorés lors de l’import. Une fois la limite d’appareils de la licence Lifetime atteinte, les lignes restantes sont signalées comme ayant échoué.

Pour la version 26.4.0

Pour la version 26.4.0

Vue d’ensemble des attributions

La liste des attributions de licences des informations sur la licence répertorie tous les numéros de série attribués à la licence Lifetime, quelle que soit la méthode d’attribution. Pour chaque entrée sont notamment affichés la date d’attribution, l’utilisateur ayant effectué l’attribution, le Nom de l’appareil et l’Organisation.

Résumé

- Les licences Lifetime sont valables pendant toute la durée de vie d’un seul appareil
- elles sont définitivement attribuées au numéro de série
- le transfert vers un autre appareil n’est pas possible
- les licences Lifetime déjà attribuées ne peuvent pas être retirées
- actuellement, seuls iOS / iPadOS et Android Enterprise sont pris en charge
- les plateformes non prises en charge nécessitent toujours d’autres types de licence (p. ex. Perpetual ou Subscription)

Gestion des licences par les partenaires

La gestion des licences peut être confiée à un partenaire ou prestataire de services. Pour cela, la clé de connexion affichée dans Relution est transmise au partenaire. Relution reçoit cette clé du serveur de licences lors de la vérification de licence. À l'aide de cette clé, le partenaire se connecte à l'organisation via le serveur de licences et peut ensuite gérer les licences.

Cette connexion peut être établie non seulement pour l'organisation Global, mais aussi pour des tenants individuels gérés par le partenaire.

> La clé de connexion donne accès à la gestion des licences de l'organisation. Elle ne doit être transmise que par un canal de confiance et sécurisé.

Copier la clé de connexion (client)

1. Se connecter à Relution et basculer vers l'organisation Global ou vers le tenant dont les licences doivent être gérées.
2. Ouvrir le menu de support (icône point d'interrogation) en haut à droite et sélectionner Informations sur la licence. L'entrée n'apparaît qu'avec le droit de lecture sur les Informations sur la licence.
3. Dans la section Général, copier la valeur du champ Clé de connexion, p. ex. à l'aide du bouton de copie situé à côté de la valeur.

La clé de connexion n'est affichée qu'après une vérification de licence réussie. Si le champ est vide, par exemple faute de connexion au serveur de licences, la vérification de licence peut être relancée dans la même section à l'aide du bouton situé à côté de Dernière vérification de licence.

Pour la version 26.4.0

Pour la version 26.4.0

Transmettre la clé de connexion

La clé de connexion copiée est transmise au partenaire ou prestataire de services qui doit prendre en charge la gestion des licences.

Connecter l’organisation (partenaire)

1. Le partenaire se connecte au serveur de licences : https://license.relution.io →
2. Ouvrir Tenants dans la navigation latérale et cliquer sur Connect.
3. Coller la clé de connexion (Connection Key) dans le champ de saisie et confirmer avec Connect.

Pour la version 26.4.0

Résultat

L’organisation est désormais connectée au partenaire et apparaît dans sa liste Tenants. À partir de maintenant, le partenaire peut gérer les licences de l’organisation connectée.

Résumé

- La gestion des licences peut être déléguée à un partenaire ou prestataire de services.
- Le point de départ est la clé de connexion, disponible sous Informations sur la licence.
- La connexion est possible aussi bien pour l’organisation Global que pour des tenants individuels.
- La clé de connexion ne doit être transmise que par un canal sécurisé.

Pour la version 26.4.0

Configurer TeamViewer

Avec le module complémentaire de licence Relution pour l'assistance à distance TeamViewer, la licence TeamViewer est incluse dans la licence Relution. Dans ce cas, un compte TeamViewer existant peut également être associé directement à Relution sans licence TeamViewer propre.

Avec Relution, il est possible de distribuer l'application TeamViewer directement sur les appareils gérés et de démarrer des sessions d'assistance à distance via le portail Relution.

Conditions requises

> L'intégration TeamViewer dans le mode de licence Licence incluse nécessite une licence supplémentaire pour ce module complémentaire. Son acquisition se fait auprès de l'équipe commerciale de Relution.

Pour la version 26.4.0

Plateformes prises en charge

Une fois la connexion établie, les sessions d'assistance à distance peuvent être lancées via Relution sur les plateformes suivantes :

- Android Enterprise
- macOS
- Windows

Pour plus d'informations sur la manière d'enregistrer l'appareil, consulter Sessions d'assistance à distance →.

Configuration du compte

L'association s'effectue dans le portail Relution sous `Paramètres` → `Assistance à distance` : un clic sur Connecter à côté de Connecter le compte Teamviewer lance la procédure. La configuration se termine par la connexion avec les identifiants du compte TeamViewer. Les boutons de cette page ne sont disponibles qu'avec l'autorisation de modifier les paramètres d'assistance à distance.

Une fois connecté, le compte TeamViewer est lié à l'organisation Relution en tant que compte locataire sous le fournisseur Relution. La page affiche ensuite, sous Informations sur le compte, les champs Compte (adresse e-mail), Nom et Description du compte TeamViewer. La connexion peut être testée à tout moment via Vérifier la connexion. En cas de problème, le compte peut être associé de nouveau via le bouton Connecter à côté de Reconnecter le compte Teamviewer afin de rétablir l'intégration.

La configuration nécessite le module complémentaire pour la licence TeamViewer incluse (dans les informations de licence : Support à distance Teamviewer). Le champ Mode de licence doit afficher Licence incluse. Relution définit le mode automatiquement en fonction de la licence ; il ne peut pas être sélectionné. Si un mode incorrect s'affiche, une vérification de licence met à jour les fonctions disponibles. Elle se déclenche dans les Informations sur la licence (via le centre d'aide et d'information en haut à droite) à l'aide du bouton à côté de Dernière vérification de licence. Si le module complémentaire est absent alors que Licence incluse est actif (par ex. après l'expiration de la licence), la page affiche un avertissement.

Un compte TeamViewer ne peut être associé qu'à une seule organisation. S'il est déjà associé à une autre organisation, l'association est refusée avec un message d'erreur correspondant.

Pour la version 26.4.0

Plusieurs organisations

La connexion est configurée soit dans une organisation supérieure (organisation globale ou méta-organisation), soit dans des sous-organisations individuelles, mais pas dans les deux. Si elle est déjà configurée dans une organisation supérieure, elle s'applique également à ses sous-organisations ; un message l'indique et les boutons ne sont pas affichés. Si elle est configurée dans une sous-organisation, elle ne peut être configurée dans l'organisation supérieure qu'après avoir été supprimée de toutes les sous-organisations.

Supprimer le compte

Dans la section Supprimer le compte, le bouton de déconnexion (Déconnecter) à côté de Déconnexion du compte Teamviewer supprime la connexion. Le locataire TeamViewer est alors désactivé et les identifiants TeamViewer des appareils de l’organisation sont supprimés de Relution. Le retour au mode de licence propre (BYOL) n’est possible qu’après la déconnexion.

Pour la version 26.4.0

Sessions d'assistance à distance

L’intégration de TeamViewer à Relution permet de fournir une assistance à distance efficace aux appareils gérés via le portail Relution. Une fois qu’un compte TeamViewer est configuré dans les paramètres *Assistance à distance* et que l’application TeamViewer Host est installée sur l’appareil, il est possible de lancer des sessions d’assistance à distance avec ou sans assistance.

Ce guide explique comment configurer et distribuer l’application TeamViewer Host sur les appareils Android Enterprise, macOS et Windows, enregistrer l’appareil pour l’assistance à distance et démarrer des sessions d’assistance à distance via Relution.

Enregistrement de l’appareil

Pour enregistrer un appareil, il est nécessaire d’installer l’application TeamViewer Host. L’action S’inscrire à l’assistance à distance récupère ensuite les données de connexion TeamViewer nécessaires pour les sessions d’assistance à distance. Elle est exécutée par l’application compagnon Relution de la plateforme concernée (Android Enterprise : application Relution, macOS : compagnon macOS, Windows : Windows Companion). Si l’application compagnon n’est pas active, l’appareil n’est pas enregistré.

Pour la version 26.4.0

- Android Enterprise : l’action est déclenchée automatiquement dès que l’appareil signale l’application TeamViewer Host comme installée.
- macOS : l’action est déclenchée automatiquement après l’installation, à condition que le compagnon macOS soit activé (`Paramètres` → `Applications client Relution`, interrupteur Activer le compagnon macOS). Les Mac inscrits par l’utilisateur (User Enrollment) ne sont pas pris en charge.
- Windows ainsi que tous les cas sans enregistrement automatique : l’action peut être envoyée manuellement via la boîte de dialogue d’assistance à distance (voir Lancer des sessions d’assistance à distance →).

Si l’application TeamViewer Host est désinstallée de l’appareil, Relution supprime automatiquement l’enregistrement de l’appareil.

Les explications ci-dessous décrivent comment distribuer les applications TeamViewer via Relution et les installer sur les appareils en fonction de la plateforme.

Android Enterprise

Créer une configuration Gérer les applications → dans le portail Relution et ajouter l'application TeamViewer Host → ainsi que le module complémentaire TeamViewer spécifique au fabricant ou le module complémentaire TeamViewer Universal Add-On depuis le Google Play Store géré. Aucune configuration supplémentaire n'est nécessaire ici.

> Après l'installation de l'application TeamViewer Host, celle-ci doit être lancée afin de suivre les étapes affichées et d'accorder toutes les autorisations requises.
>
> Si l'action S'inscrire à l'assistance à distance échoue avec l'erreur verify failed, il est probable que toutes les autorisations requises n'ont pas été accordées dans l'application TeamViewer Host.

macOS

Télécharger l'application TeamViewer Host depuis le site Web TeamViewer et ajouter le fichier .dmg en tant qu'application native dans l'App Store Relution. Définir une règle de détection en spécifiant l'identifiant du bundle de TeamViewer Host (`com.teamviewer.TeamViewerHost`).

Distribuer l'application sur les appareils à l'aide d'une configuration de conformité d'application ou d'une action Déployer l'application Relution Store.

Ouvrir l'application installée sur l'appareil macOS et suivre les étapes affichées pour terminer l'installation.

Windows

Déployer l'application TeamViewer Host depuis le magasin WinGet → sur les appareils. L'identifiant du paquet WinGet est `TeamViewer.TeamViewer.Host` .

Lancer des sessions d'assistance à distance

Une session d'assistance à distance se lance depuis la vue détaillée de l'appareil dans le portail Relution, via l'icône Démarrer la session d'assistance à distance dans l'en-tête. La liste des appareils propose également le bouton Démarrer la session d'assistance à distance dès qu'un seul appareil est sélectionné. Les deux nécessitent l'autorisation de demander des sessions d'assistance à distance.

Pour la version 26.4.0

Une boîte de dialogue s’ouvre et permet de choisir entre une session assistée (dans le portail : Présents) et une session non assistée (Sans surveillance) ; la session non assistée est présélectionnée. La principale différence entre les deux types de session réside dans la nécessité d’une interaction de l’utilisateur :

- Session assistée : nécessite qu’un utilisateur présent sur l’appareil approuve la connexion.
- Session non assistée : aucune interaction de l’utilisateur n’est nécessaire pour démarrer la connexion.

Pour la version 26.4.0

Des liens sont générés pour l’application Web TeamViewer et l’application de bureau TeamViewer. Les administrateurs peuvent utiliser l’un des deux liens pour démarrer une session d’assistance à distance.

Pour ouvrir le lien du bureau, une application de bureau TeamViewer, telle que TeamViewer Full Client, est nécessaire.

En mode assisté, le lien est valable 24 heures ; en mode non assisté, 5 minutes. Une nouvelle demande est ensuite nécessaire. Si l’appareil est hors ligne ou n’est pas joignable via TeamViewer, la boîte de dialogue affiche un message d’erreur correspondant.

Si les identifiants TeamViewer de l’appareil n’ont pas encore été transmis à Relution, la boîte de dialogue affiche un message correspondant. Sous Enregistrer le dispositif, le bouton Envoyer une action envoie l’action S’inscrire à l’assistance à distance à l’appareil ; la boîte de dialogue se ferme ensuite. Une fois l’action terminée avec succès, la session d’assistance à distance peut être lancée à nouveau.

Pour la version 26.4.0

Une fois toutes les étapes de la session d’assistance à distance effectuées avec succès, une autorisation peut être nécessaire sur le terminal souhaité.

Configurer TeamViewer

Avec Relution, il est possible de connecter son propre compte TeamViewer disposant de sa propre licence afin de permettre une intégration fluide dans Relution. De plus, TeamViewer Host peut être efficacement distribué et configuré sur les appareils gérés, ce qui permet un support à distance simplifié directement via le portail Relution.

Exigences

Pour utiliser cette intégration, une licence TeamViewer (Classic) Corporate ou Tensor est requise. De plus, le compte utilisateur doit avoir accès au portail TeamViewer afin d'effectuer les configurations nécessaires.

Plates-formes prises en charge

L'application TeamViewer peut être distribuée et configurée via Relution sur les plates-formes suivantes :

- Android Enterprise →
- iOS →
- macOS →
- Windows →

Pour la version 26.4.0

Création de la configuration de déploiement

Pour configurer les appareils, un *ID d'assignation* est requis. Suivre les étapes décrites dans le Guide de configuration de déploiement → dans le TeamViewer Portal →.

Pour permettre des sessions de support à distance avec un accès non surveillé aux appareils, attribuer aux utilisateurs la permission Accès facile dans la section Gestion des droits d’accès.

Pour la version 26.4.0

Connecter un compte TeamViewer dans Relution

L’association s’effectue dans le portail Relution sous `Paramètres` → `Assistance à distance`. Dans la section Informations sur le compte, le bouton Connecter à côté de Connecter le compte Teamviewer mène à la page de connexion de TeamViewer. La connexion avec le compte TeamViewer termine l’intégration ; Relution affiche ensuite les informations du compte associé.

Le Mode de licence est déterminé automatiquement à partir de la licence Relution : sans le module complémentaire pour la licence TeamViewer incluse, il correspond à la licence propre de l’organisation (BYOL).

Une fois l’authentification réussie, la connexion peut être vérifiée sous Tester la connexion au support à distance avec Vérifier la connexion. En cas de problème de connexion, le compte est réautorisé via Connecter à côté de Reconnecter le compte Teamviewer afin de rétablir

l’intégration avec TeamViewer. Dans la section Supprimer le compte, le bouton Déconnecter supprime l’association.

Restrictions

Les restrictions suivantes s’appliquent à l’association :

- Un compte TeamViewer ne peut être associé qu’à une seule organisation. Si le compte est déjà associé à une autre organisation, Relution refuse l’association.
- Si la connexion est configurée dans une organisation supérieure (globale ou méta-organisation), elle s’applique également aux organisations subordonnées et ne peut pas y être modifiée. Si elle est déjà configurée dans une sous-organisation, elle ne peut être configurée globalement qu’après la suppression de la configuration dans toutes les sous-organisations.

Pour la version 26.4.0

Android Enterprise

Cet article explique comment configurer l'application TeamViewer Host dans Relution pour permettre l'assignation automatique des appareils dans le portail TeamViewer.

Configuration de l'application TeamViewer Host

Créer une configuration Gérer les applications → dans le portail Relution et ajouter les deux applications suivantes depuis le Managed Google Play Store :

1. TeamViewer Host
2. TeamViewer Universal

Ajuster ensuite la configuration de l'application et définir les paramètres pertinents suivants :

26.4.0

Nom	Description
ID d'assignation	Pour l'assignation automatique en tant qu'appareil géré dans TeamViewer.
Alias de l'appareil	Nom affiché dans l'interface web de TeamViewer.

Pour la version 26.4.0

Détails des paramètres

- ID d’assignation Saisir l’ID d’assignation issu du portail TeamViewer, reçu lors de l’étape de configuration →.
- Alias de l’appareil Configurer le nom composé du nom de l’appareil et du numéro de série à l’aide des espaces réservés listés sous Espaces réservés disponibles dans la boîte de dialogue de configuration :

```
${device.name}_${device.serialnumber}
```

Pour établir un lien univoque entre les appareils dans Relution et TeamViewer, le numéro de série doit faire partie du nom de l'appareil. Cela est garanti par l'utilisation de l'espace réservé `${device.serialnumber}`.

Finalisation

Les applications nouvellement ajoutées reçoivent par défaut le Type d'installation Installé de force et sont donc installées automatiquement. Appliquer la configuration aux appareils Android Enterprise. Une fois l'installation terminée, l'assignation est effectuée automatiquement et les appareils apparaissent correctement dans le portail TeamViewer.

Remarques

> Connexion annulée ou authentification refusée

Informations importantes sur l'interaction utilisateur

Le comportement lors de l'accès à distance varie selon la version d'Android :

- Android 13 et versions antérieures : Sur de nombreux appareils (notamment avec des modules complémentaires TeamViewer propres au fabricant), l'accès fonctionne souvent entièrement en arrière-plan, sans interaction de l'utilisateur.
- Android 14 et versions ultérieures : En raison des règles de sécurité renforcées de Google (Media Projection API), une fenêtre contextuelle système apparaît obligatoirement au démarrage d'un accès à distance. L'utilisateur doit confirmer manuellement le partage de l'écran. Cela ne peut actuellement pas être contourné sur les appareils Android Enterprise standard.

Pour la version 26.4.0

iOS

Cet article décrit comment déployer et configurer l'application TeamViewer QuickSupport sur des appareils iOS en utilisant Relution.

Déployer l'application TeamViewer QuickSupport

Créer une politique avec une configuration Conformité App →. Ajouter l'application TeamViewer QuickSupport (identifiant du bundle: `com.teamviewer.teamviewerQS`) depuis l'App Store à la liste des applications requises.

Configurer l'application pour l'enregistrement des appareils

Ajouter une configuration App gérée → et sélectionner l'application TeamViewer QuickSupport depuis l'App Store. Dans le champ Charge utile, ajouter les clés suivantes à l'intérieur de l'élément `<dict>` prédéfini (entre `<dict>` et `</dict>`) ; en dehors de celui-ci, le XML est considéré comme invalide et la configuration ne peut pas être enregistrée :

```
<key>mdv2AssignmentID</key>
<string>YOUR_ASSIGNMENT_ID</string>
<key>partnerListDeviceName</key>
<string>${device.name}_${device.serialnumber}</string>
```

Pour la version 26.4.0

- mdv2AssignmentID: Utilisé pour l'attribution automatique des appareils en tant qu'appareil géré dans TeamViewer. Saisir l'identifiant d'attribution depuis le portail TeamViewer, reçu lors de l'étape de configuration →.

- partnerListDeviceName: Nom d’affichage de l’appareil dans l’interface web de TeamViewer. Configurer le nom de l’appareil en utilisant le nom de l’appareil et le numéro de série comme suit, en utilisant les espaces réservés disponibles : `${device.name}_${device.serialnumber}`

Pour établir un lien entre les appareils dans Relution et TeamViewer, le numéro de série doit faire partie du nom de l’appareil. Cela est garanti en utilisant l’espace réservé `${device.serialnumber}`. Le nom peut être composé différemment tant qu’il contient toujours le numéro de série ; au démarrage d’une session, Relution recherche dans TeamViewer un appareil dont le nom contient le numéro de série.

Appliquer les configurations aux appareils iOS concernés. Une fois l’installation terminée, l’affectation sera effectuée automatiquement et les appareils apparaîtront dans le portail TeamViewer.

Sessions d’assistance à distance sur les appareils iOS

Dans Relution, les sessions d’assistance à distance pour les appareils iOS, y compris avec l’Inscription des utilisateurs iOS, ne sont disponibles qu’avec une licence fournie par l’organisation. Elles sont démarrées comme décrit sous Sessions d’assistance à distance →. Sur l’appareil iOS, la session doit être confirmée par l’utilisateur dans l’application TeamViewer QuickSupport.

Pour la version 26.4.0

macOS

Cet article explique comment déployer et configurer le TeamViewer Host sur des appareils macOS à l'aide de Relution.

Téléchargement du client TeamViewer

Se connecter au portail TeamViewer et accéder à `Paramètres administrateur` → `Configuration de déploiement` pour télécharger l'installateur macOS. Le package contient à la fois le *TeamViewer Full Client* et le *TeamViewer Host*. Pour l'intégration avec Relution, seul le *TeamViewer Host* est nécessaire.

Distribution du client TeamViewer

Se connecter au portail Relution et accéder à `Apps` → `App Store`. Créer une nouvelle application native en utilisant le fichier PKG précédemment téléchargé. Ajouter une règle de détection du type Nom du paquet (seul type de règle disponible pour les applications macOS) et y saisir l'identifiant de bundle du TeamViewer Host (`com.teamviewer.TeamViewerHost`).

L'application peut être distribuée sur les appareils macOS soit via une configuration Conformité App, soit en utilisant l'action Déployer l'application Relution Store.

Pour la version 26.4.0

Affectation via script

Créer un script dans le portail Relution pour la plateforme macOS et insérer la commande suivante:

Script pour TeamViewer Host:

```
sudo /Applications/TeamViewerHost.app/Contents/Helpers/TeamViewer_Assignment -
```

Remplacer `YOUR_ASSIGNMENT_ID` par l'ID d'assignation depuis le portail TeamViewer, reçu lors de l'étape de configuration →.

Pour établir un lien entre les appareils dans Relution et TeamViewer, le numéro de série doit être inclus dans le nom de l'appareil. Cela est assuré grâce à l'utilisation du placeholder `${device.serialnumber}` dans le script. Le nom combiné sera affiché dans le portail TeamViewer après une inscription réussie.

L'exécution nécessite que le compagnon macOS soit activé (`Paramètres` → `Applications client Relution`, interrupteur Activer le compagnon macOS). Le compagnon macOS n'est déployé que sur les Mac à partir de macOS 12 et pas sur les Mac inscrits par l'utilisateur ; aucun script ne peut y être exécuté. Contrairement à Windows, le script ne peut pas être associé à l'application. Il est donc exécuté après l'installation de TeamViewer Host, de l'une des manières suivantes :

- une seule fois via l'action Exécuter un script shell (voir Actions macOS →) ou sur la page `Scripts` → `Scripts` via Exécuter sur l'appareil,
- de manière planifiée via une configuration de type Script dans une politique macOS ; celle-ci couvre également les Mac ajoutés ultérieurement.

Une fois l’assignation terminée, les appareils devraient apparaître dans le portail TeamViewer.

Pour la version 26.4.0

Windows

Le guide suivant décrit les étapes à suivre pour configurer TeamViewer Host pour Windows via Relution, y compris la distribution de TeamViewer Host en tant qu'application Relution Store et la création d'un script pour configurer l'application.

Téléchargement du package MSI

Commencer par télécharger le package MSI adapté à l'architecture concernée depuis TeamViewer. Se connecter au portail TeamViewer, accéder à `Paramètres administrateur` → `Configuration de déploiement`, et télécharger le package MSI. L'installateur téléchargé inclut le *TeamViewer Full Client* et le *TeamViewer Host*. Pour l'intégration avec Relution, seul le *TeamViewer Host* est requis. Des informations détaillées sur le téléchargement du package MSI sont disponibles dans la Documentation de TeamViewer →.

Pour la version 26.4.0

Création de l'application Relution Store

Après avoir téléchargé le package MSI de TeamViewer, se connecter au portail Relution. Sous `Apps` → `App Store`, créer une nouvelle application native à l'aide du fichier MSI précédemment téléchargé. Au moins une règle de détection est requise pour l'application ; sinon, elle ne peut pas être enregistrée. L'installation et l'exécution des scripts sur les appareils sont prises en charge par le Relution Companion, qui doit donc être installé sur les appareils cibles : Compagnon Windows →. Plus de détails sont disponibles sous Installation des applications Windows →.

Création du script d'assignation

Pour configurer TeamViewer Host sur les appareils, créer un nouveau script pour la plate-forme Windows dans le portail Relution sous `Scripts` → `Scripts`. Selon l'architecture de l'appareil cible, utiliser l'un des scripts suivants:

Script pour les appareils avec un système d'exploitation 64 bits:

```
& "C:\Program Files\TeamViewer\TeamViewer.exe" assignment --id $assignmentId -
```

Script pour les appareils avec un système d'exploitation 32 bits:

```
& "C:\Program Files (x86)\TeamViewer\TeamViewer.exe" assignment --id $assignme
```

Dans la section Exécution, saisir dans le champ Arguments l'ID d'assignation provenant du portail TeamViewer, reçu lors de l'étape de configuration → : `$assignmentId='YOUR_ASSIGNMENT_ID'`. Le contenu de ce champ est inséré au début du script lors de son exécution.

Pour établir un lien entre les appareils dans Relution et TeamViewer, le numéro de série doit être inclus dans le nom de l'appareil. Cela est assuré grâce à l'utilisation du placeholder `${device.serialnumber}` dans le script. Le nom combiné apparaîtra dans le portail TeamViewer après inscription réussie.

Pour la version 26.4.0

Pour la version 26.4.0

Exécution du script après l’installation

Pour exécuter le script, ouvrir l’application TeamViewer Host MSI créée précédemment dans Relution. Dans l’onglet Scripts, ajouter le script de configuration sous Scripts de post-installation.

Plusieurs scripts peuvent y être ordonnés par glisser-déposer selon leur ordre d’exécution. L’onglet n’apparaît que pour les applications Windows classiques de sa propre organisation et uniquement avec le droit de lecture des scripts.

Installer l’application sur les appareils Windows souhaités en utilisant soit une configuration Conformité App, soit l’action Déployer l’application Relution Store.

Une fois TeamViewer Host installé, le script s’exécutera automatiquement. Après la fin de la configuration, les appareils devraient apparaître dans le portail TeamViewer.

Pour la version 26.4.0

Sessions d'assistance à distance

Une fois qu'un compte TeamViewer avec une licence valide est configuré dans les paramètres Relution et que l'appareil est correctement enregistré dans le portail TeamViewer, il est possible de lancer des sessions d'assistance à distance sans surveillance. Cela s'applique à Android Enterprise (appareils entièrement gérés et profils professionnels), macOS et Windows. Avec une licence fournie par l'organisation, les appareils iOS sont également pris en charge, y compris avec l'Inscription des utilisateurs iOS. Pour iOS, l'application TeamViewer QuickSupport ne permet que les sessions supervisées qui nécessitent une interaction active de l'utilisateur.

Le client TeamViewer approprié doit être installé sur l'appareil géré et enregistré dans le portail TeamViewer (voir Android Enterprise →, iOS →, macOS → et Windows →). Pour ouvrir la session via le lien pour les administrateurs, une application de bureau TeamViewer, par exemple le TeamViewer Full Client, est nécessaire sur l'ordinateur de l'administrateur.

Relution identifie l'appareil par son numéro de série : il recherche dans TeamViewer un appareil dont le nom contient le numéro de série enregistré dans Relution. Le nom d'appareil configuré dans les articles de déploiement doit donc contenir l'espace réservé `${device.serialnumber}`.

Pour la version 26.4.0

Démarrer une session d'assistance à distance

Une session d'assistance à distance est lancée depuis la vue détaillée de l'appareil dans Relution, via l'icône Démarrer la session d'assistance à distance dans l'en-tête. L'icône n'apparaît que si un compte TeamViewer est associé, que le type d'inscription de l'appareil est pris en charge et que l'utilisateur connecté est autorisé à demander une assistance à distance.

Avec une licence fournie par l'organisation, le choix du type de session est supprimé ; Relution génère immédiatement un lien pour une session à distance sans surveillance. La boîte de dialogue Ouverture d'une session à distance l'affiche sous Lien pour les administrateurs : sous forme de lien Bureau ; l'icône à côté permet de le copier dans le presse-papiers. Le lien généré ne peut être ouvert qu'avec une application de bureau TeamViewer installée.

Une fois toutes les étapes de la session d'assistance à distance effectuées avec succès, une autorisation peut être nécessaire sur le terminal souhaité.

Pour la version 26.4.0

Messages dans la boîte de dialogue

Si aucune session ne peut être créée, la boîte de dialogue affiche l'un des messages suivants à la place du lien :

- « L'appareil n'a pas pu être trouvé sur TeamViewer. » TeamViewer ne contient aucun appareil dont le nom inclut le numéro de série de l'appareil. L'assignation et le nom de l'appareil sont à vérifier selon l'article de déploiement correspondant.
- « L'appareil est actuellement hors ligne ou n'est pas disponible via TeamViewer » L'appareil n'est pas joignable ou la demande adressée à TeamViewer a échoué. La tentative peut être renouvelée plus tard.

Accès conditionnel Microsoft

L'accès conditionnel Microsoft (Conditional Access) → ou accès conditionnel est le moteur de règles Zero Trust de Microsoft. Dans cette documentation, l'abréviation `MSCA` est utilisée pour une meilleure lisibilité. Si les utilisateurs Relution sont synchronisés via `Entra ID`, il est également possible d'activer l'`accès conditionnel`. Dès qu'un appareil géré par Relution change son statut en conforme ou non conforme, ces informations sont automatiquement transmises à Microsoft. Sur la base des règles d'accès conditionnel →, il est alors possible, par exemple, de refuser aux utilisateurs l'accès à certaines applications si leur appareil est considéré comme non conforme.

Plateformes prises en charge

- Android Enterprise
- iOS
- macOS
- Windows
  - L'appareil doit avoir été enregistré via `Microsoft Entra Join` ou `Windows Autopilot`.

Pour la version 26.4.0

Prérequis

Pour pouvoir utiliser l'accès conditionnel avec Relution, les conditions suivantes doivent être remplies :

- Relution en version 5.33.1 ou supérieure requis.
- Une licence Microsoft Entra ID P1 active. Plus d'informations ici →.
- Une synchronisation des utilisateurs configurée avec `Entra ID`, voir Lier Entra ID et Relution →
- Pour que les utilisateurs Entra puissent se connecter à Relution, OIDC → doit également être configuré.

Pour Android Enterprise, iOS et macOS, les conditions suivantes s'appliquent en plus :

- Relution a été ajouté dans Intune comme partenaire de conformité pour la plateforme concernée, voir Configurer les plateformes →.

- Les utilisateurs concernés disposent d'une licence Intune. Si elle manque, l'appareil est listé sur la page de paramètres Accès conditionnel avec le statut La licence intune est manquante.
- La configuration `Accès conditionnel` doit être appliquée aux appareils concernés via une règle correspondante (sous iOS et macOS uniquement pour l'inscription de l'appareil). En option, la configuration marque un appareil comme non conforme tant que l'utilisateur ne l'a pas encore enregistré et invite l'utilisateur à l'enregistrer par notification push, voir Accès conditionnel (règle) →.
- L'appareil est lié à `Entra ID` via l'Agent Relution →.
- Une `application Broker` pour l'authentification :
  - Android Enterprise & iOS : `Microsoft Authenticator` (installée automatiquement dès que Relution a été ajouté dans Intune comme partenaire de conformité pour la plateforme et que la configuration `Accès conditionnel` a été attribuée à l'appareil via une règle)
  - macOS : `Company Portal App` - doit être installée sur l'appareil. Peut être téléchargée ici →.

Pour Windows, il n'existe ni configuration `Accès conditionnel`, ni application Broker, ni partenaire de conformité dans Intune. L'accès conditionnel pour Windows est activé sur la page de paramètres Accès conditionnel via Activer à côté de Activer l'accès conditionnel pour Windows, voir Configurer les plateformes →.

Pour la version 26.4.0

Restrictions

- L'`accès conditionnel` ne peut actuellement pas être configuré au sein de l'organisation globale.
- Les utilisateurs doivent avoir été importés via la synchronisation Entra ; les utilisateurs synchronisés au préalable, par exemple via LDAP, ne peuvent pas être utilisés.
- Les utilisateurs importés via la synchronisation Entra doivent exister dans la même organisation que les appareils associés.
- Sous iOS et macOS, l'inscription utilisateur (User Enrollment/BYOD) n'est pas prise en charge ; la configuration `Accès conditionnel` n'est disponible que pour l'inscription de l'appareil.
- L'`iPad partagé` présente diverses restrictions pour les configurations CA, par exemple l'exigence selon laquelle l'appareil doit être marqué comme conforme n'est pas prise en charge. Cela fait apparaître dans Relution, sur la carte Microsoft Entra ID de l'appareil, le message Microsoft Conditional Access n'est pas connecté. Plus d'informations à ce sujet dans la documentation Microsoft ici →.

Configurer les plateformes

Ce guide de configuration montre étape par étape comment connecter avec succès `Relution` à `Microsoft Entra/Intune` afin de configurer l'accès conditionnel pour les appareils gérés. S'assurer que les prérequis → sont remplis avant de commencer.

Configuration de l'accès conditionnel avec Relution et Entra ID

Les étapes de configuration suivantes permettent de connecter Relution à Microsoft Entra ID et Microsoft Intune pour activer l'accès conditionnel :

1. D'abord `créer une application Entra ID` qui valide l'accès du serveur via le microservice Relution.
2. `Accorder le consentement à l'application multi-tenant Relution`, dont Relution a besoin pour signaler le statut de conformité des appareils à Entra ID.
3. Ajouter `Relution` comme partenaire de conformité dans `Intune`.
4. Vérifier que la configuration est correcte.

Chaque étape est déterminante pour la suivante. Effectuer toutes les étapes soigneusement l'une après l'autre et, lorsqu'une vérification est demandée, s'assurer que le message Validation réussie (lors de la synchronisation Synchronisation réussie) est affiché.

Naviguer vers Accès conditionnel

Une fois Entra ID → correctement configuré et les utilisateurs synchronisés avec succès, il est possible de naviguer vers `Accès conditionnel` dans les paramètres.

Activer les plateformes : Android Enterprise, iOS et macOS

L’assistant d’activation des plateformes souhaitées est lancé dans la section Général via Ajouter à côté de Ajouter une connexion.

Pour la version 26.4.0

Assistant (1) : créer une application Entra ID

Il est également possible d’ignorer cette étape et de réutiliser l’application utilisée lors de la configuration d’Entra ID. Relution recommande toutefois d’utiliser deux applications distinctes

afin de séparer les autorisations et les usages.

Créer une nouvelle `application Entra ID` afin que le microservice Relution puisse vérifier l'accès au locataire. Une simple inscription d'application suffit - une application MDM complète n'est pas nécessaire. L'application doit se trouver dans le même locataire que l'Entra ID configuré. Le bouton Ouvrir Entra ID de l'assistant mène aux inscriptions d'applications Entra ID →. Après la création de l'application, Suivant mène à l'étape suivante, dans laquelle l'ID de l'application (client) est saisi.

Assistant (2) : enregistrer les ID d'application et la clé secrète client

L'application a également besoin d'une clé secrète client. Créer une telle clé et insérer l'ID de l'application (client) et le Secret du client dans les champs de saisie. Après une vérification réussie via Vérifier, poursuivre avec l'étape suivante.

Assistant (3) : exposer l'API

En raison de limitations techniques de Microsoft pour la validation des jetons, une API doit être exposée et une portée personnalisée ajoutée. Le bouton Ouvrir l'API Expose de l'assistant ouvre directement la page de paramètres correspondante de l'application Entra. Effectuer les étapes suivantes sur la page de paramètres Exposer une API de l'application Entra :

1. Cliquer sur Ajouter une portée.
2. Saisir les informations requises :
   - Nom de la portée : `Relution.Auth`
   - Visibilité : activer l'option Administrateurs uniquement
   - Nom d'affichage et description : indications libres possibles, par exemple : `Utilisé par Relution pour identifier l'appartenance du locataire`.
3. Cliquer sur Ajouter une portée.
4. La portée devrait maintenant être affichée sous Portées définies par cette API.

En haut de la vue Exposer une API dans Entra, une URI d'ID d'application est affichée. La valeur correspondante est sélectionnée dans l'assistant sous Type de champ d'application : `api://<ID d'application>` pour une application nouvellement créée (étape 1), ou l'URL du serveur Relution (`https://<hôte Relution>`) si l'application réutilisée provient de la configuration Entra ID. Si l'URI d'ID d'application diffère des deux, l'option Personnalisé est sélectionnée et l'URI d'ID d'application est saisie dans le champ Portée personnalisée.

Pour la version 26.4.0

Cette étape devrait maintenant pouvoir être vérifiée avec succès dans l’assistant via Vérifier.

Assistant (4) : ajouter Relution comme partenaire de conformité dans Intune

Dans le paramètre Gestion des partenaires de conformité Intune →, `Relution` doit être ajouté comme partenaire pour chaque plateforme devant être synchronisée. Le bouton Paramètres du partenaire ouvert de l’assistant ouvre directement cette page.

Pour la version 26.4.0

Pour la version 26.4.0

1. Cliquer sur Ajouter un partenaire de conformité.
2. Sélectionner la plateforme à synchroniser (ces étapes peuvent être répétées pour chaque plateforme) : Android, iOS ou macOS. Windows n'est pas configuré ici, mais activé séparément dans Relution (voir la section Prendre en charge la plateforme Windows →).
3. Assigner un groupe d'utilisateurs devant être synchronisé. Il est également possible de sélectionner Ajouter tous les utilisateurs, mais il convient alors de veiller à ne pas s'exclure soi-même par la suite.
   - Remarque : l'option Exclure des groupes n'a actuellement aucun effet.
4. Après avoir vérifié que tout a été correctement sélectionné, cliquer sur Créer.
5. `Relution` devrait apparaître avec le statut `🔄 Activation en attente` pour cette plateforme. Le statut peut différer si ce n'est pas la première configuration.

Pour Android Enterprise et iOS, Relution distribue lui-même l'application Broker `Microsoft Authenticator`. Pour macOS, la `Company Portal App` doit être distribuée séparément sur les appareils, par exemple via le Relution Store et une règle, voir Prérequis →.

Assistant (5) : accorder le consentement de l'administrateur

> Cette étape échoue si aucune plateforme n'a été liée à l'étape précédente.

Accorder à l'`application multi-tenant Relution` le `consentement administrateur` requis. Cela permet à `Relution` de gérer le statut de conformité des `appareils Entra ID`. Un clic sur le bouton d'ouverture du consentement (libellé Consentement libre dans le portail)

Pour la version 26.4.0

enregistre les données saisies jusqu'ici dans l'assistant et ouvre la page de consentement dans un nouvel onglet (celui-ci peut éventuellement être bloqué par le navigateur en tant que fenêtre pop-up). Après un consentement réussi, une page de confirmation affiche le message `Success! You can now close this tab`. Cet onglet supplémentaire peut alors être fermé. Dans l'assistant, le consentement peut être contrôlé via Vérifier avant de continuer. Si le consentement a déjà été accordé, le bouton Consentement libre est désactivé.

Pour la version 26.4.0

Assistant (6) : synchroniser les groupes Entra ID

Comme dernière étape, il faut `synchroniser les groupes Entra ID`. Dans l'étape Synchroniser de l'assistant, la configuration est d'abord vérifiée via Vérifier. Ce n'est qu'après une vérification réussie que Synchroniser les groupes Entra ID devient cliquable ; jusque-là, le bouton est verrouillé et un message signale la vérification manquante. Lors de la synchronisation, `Relution` s'assure d'une configuration correcte et synchronise les groupes assignés dans Intune à l'étape 4. Pour terminer, l'assistant est fermé via Enregistrer.

Dans les paramètres de Gestion des partenaires de conformité Intune →, `Relution` devrait maintenant être affiché comme `✅ Actif`.

> Toute modification des paramètres du partenaire de conformité dans Intune, par exemple l'ajout ou la suppression de groupes ou de plateformes, nécessite de relancer manuellement la synchronisation.

Prendre en charge la plateforme Windows

Les appareils Windows ne nécessitent ni l'assistant ni de partenaire de conformité dans Intune. Sur la page de paramètres Accès conditionnel, dans la section Windows, un clic sur Activer à côté de Activer l'accès conditionnel pour Windows suffit. La modification est appliquée immédiatement.

Pour la version 26.4.0

Les appareils Windows devraient maintenant synchroniser leur statut avec succès.

Gérer la connexion

Après la configuration, la page de paramètres Accès conditionnel affiche les zones suivantes :

- Général : Modifier la connexion ouvre à nouveau l'assistant, Supprimer la connexion supprime la connexion. Désactiver l'accès conditionnel empêche l'envoi des mises à jour de conformité à Microsoft, Activer l'accès conditionnel les réactive. Vérifier permet de contrôler la configuration à tout moment.
- Coordonnées du partenaire : Synchroniser les groupes Entra ID lance la synchronisation manuellement, par exemple après des modifications de groupes ou de plateformes dans Intune. Sont également affichés le dernier contact (Dernier battement de cœur), la Dernière synchronisation et les plateformes (Android, iOS, macOS) dont les groupes ont été synchronisés.
- Appareils ayant rencontré des problèmes lors de la dernière synchronisation : liste des appareils concernés avec utilisateur, statut (par ex. La licence intune est manquante) et Dernier message d'erreur. Une fois la cause éliminée, par exemple après l'attribution d'une licence Intune, le transfert est relancé via Synchronisation.

Si la connexion est défectueuse, par exemple en raison d'un consentement administrateur manquant, d'informations d'identification non valides (secret du client expiré), d'une portée `Relution.Auth` manquante ou d'aucune plateforme liée dans Intune, la page affiche un avertissement. Une fois le problème résolu, les informations du partenaire doivent être à nouveau synchronisées via Synchroniser les groupes Entra ID.

Pour la version 26.4.0

Sujets connexes

- Présentation de l'accès conditionnel → — prérequis et principes de l'accès conditionnel.
- Lier Microsoft Entra ID → — liaison d'Entra ID et synchronisation des utilisateurs, prérequis de l'accès conditionnel.
- OIDC avec Entra → — connexion des utilisateurs Entra à Relution via OpenID Connect.

Configurer Intune

Ce guide rapide montre comment configurer et tester des `règles d'accès conditionnel` dans `Microsoft Intune`. Ces règles définissent les mesures à appliquer pour les appareils non conformes, comme des restrictions d'accès aux applications. Plus d'informations dans la documentation officielle →.

> Une configuration incorrecte des règles d'accès conditionnel peut entraîner l'impossibilité pour les utilisateurs de se connecter. Relution n'assume aucune responsabilité pour les dommages causés par des paramètres incorrects.
>
> Des règles strictes pour Toutes les applications cloud dans les ressources cibles empêcheront également les utilisateurs d'enregistrer leurs appareils.

Recommandations pour le déploiement

Pour la version 26.4.0

`Relution` recommande de procéder avec prudence lors de l'introduction de l'accès conditionnel :

- Commencer d'abord soit
  - par l'utilisation de règles en mode Rapport uniquement plutôt que de les appliquer directement
  - OU avec dans un premier temps seulement des utilisateurs sélectionnés, pour s'assurer que tout fonctionne comme prévu.
- Éviter de sélectionner Toutes les applications cloud dans les ressources cibles. La sélection de Toutes les applications cloud avec des règles strictes empêche les utilisateurs d'enregistrer leurs appareils. Actuellement, l'`application Broker Microsoft` ne peut pas être sélectionnée dans le filtre Exclure, qui doit toujours être activé.
  - Il est recommandé de sélectionner Office 365 →.

Exemple de configuration dans Intune

Les règles peuvent être configurées sous Intune > Sécurité des points de terminaison > Accès conditionnel > Règles →.

Voir la capture d'écran suivante à titre d'exemple :

Pour la version 26.4.0

1. Sous Utilisateurs, les utilisateurs auxquels la règle s’applique sont sélectionnés.
2. Sous Ressources cibles, la règle est définie pour s’appliquer à des ressources sélectionnées.
3. Dans cet exemple, Microsoft Teams est sélectionné comme ressource.
4. Sous Accorder, l’exigence d’accès est définie, p. ex. autoriser uniquement les appareils conformes.

-

5. La règle est réglée sur Rapport uniquement pour la tester sans impact.

Sous Android Enterprise, iOS et macOS, l'exigence selon laquelle l'appareil doit être marqué comme conforme ne s'applique qu'aux appareils auxquels la configuration `Accès conditionnel` a été attribuée dans Relution via une règle et dont les utilisateurs sont synchronisés dans Intune via le partenaire de conformité Relution. Les utilisateurs concernés ont en outre besoin d'une licence Intune ; si elle manque, l'appareil est listé sur la page de paramètres Accès conditionnel avec le statut La licence intune est manquante. Après l'attribution de la licence, le transfert y est relancé via Synchronisation. Plus d'informations : Prérequis → et Configurer les plateformes →.

Pour la version 26.4.0

Désactiver les paramètres de sécurité par défaut

Parfois, lors de la configuration des règles, un message d'erreur indique que les paramètres de sécurité par défaut doivent être désactivés avant de pouvoir activer des règles d'accès conditionnel. La documentation officielle Microsoft → permet de déterminer s'il est nécessaire de passer à l'accès conditionnel ou non.

Pour désactiver les paramètres par défaut :

1. Désactiver les paramètres de sécurité par défaut est sélectionné.
2. Désactivé est sélectionné.

3. La sélection est confirmée avec Mon organisation prévoit d’utiliser l’accès conditionnel.

Pour la version 26.4.0

Résolution de problèmes et débogage

Dans la vue Journaux de connexion de `Entra/Intune`, il est possible de vérifier si et quelle règle d’accès conditionnel a été appliquée :

De plus, `Microsoft` propose un outil utile pour l’analyse des erreurs et la simulation de règles : outil What If →. Il permet ainsi de simuler et d’analyser les effets des règles avant leur activation effective.

Résolution des problèmes

- Où puis-je voir chez Microsoft si un appareil est conforme ou non conforme ?
- L'appareil est marqué comme « N/A » chez Microsoft
- L'appareil est marqué comme non conforme chez Microsoft, mais l'utilisateur peut toujours accéder aux applications bloquées
- L'utilisateur ne peut pas enregistrer son appareil car il est bloqué par MSCA
- L'appareil est bloqué comme non conforme
- L'appareil n'est pas enregistré
- L'utilisateur/l'appareil ne peut pas être enregistré

Pour la version 26.4.0