AppTec360 Enterprise Mobile Manager & ContentBox

Manuel d’administration | Version 5.0 (202110)

Table des matières

- Restrictions et réglages
  - Apps sur liste noire / liste blanche
  - Restrictions SysApp
  - App-VPN
  - Paramètres de l’application
- App Store d’entreprise
  - Applications iTunes
  - En interne
- Mode kiosque
  - Type d’application
    - Paquet
    - URL
  - Paramètres du mode kiosque

Android Enterprise – Configuration des appareils entièrement gérée

Général

- Aperçu du profil du groupe (uniquement au niveau du groupe)
- Aperçu de l’appareil (uniquement au niveau de l’appareil)
- Révision de la configuration (uniquement au niveau de l’appareil)
- Journal de l’appareil (uniquement au niveau de l’appareil)
  - Journal des commandes
  - États possibles de la commande
- Paramètres de l’appareil
  - Configuration du client
  - Papier peint

Gestion des actifs (uniquement au niveau de l’appareil)

- Informations sur l’appareil
  - Wi-Fi
- Cellulaire
- Bluetooth

Gestion de la sécurité

- Antivol (uniquement au niveau de l’appareil)
  - Informations GPS (uniquement au niveau de l’appareil)
  - Effacement et verrouillage (uniquement au niveau de l’appareil)

- Gestion du PIM
  - Exchange Active Sync
  - eMail
- Gestion des applications
  - Gestionnaire d’applications d’entreprise
    - Applications installées
    - Applications obligatoires
    - Restrictions des applications système
    - Liste noire et liste blanche

Configuration de MacOS

Général

- Aperçu du profil du groupe (uniquement au niveau du groupe)
- Aperçu de l’appareil (uniquement au niveau de l’appareil)
- Révision de la configuration (uniquement au niveau de l’appareil)
- Journal de l’appareil (uniquement au niveau de l’appareil)
  - Journal des commandes
  - États possibles de la commande

Gestion des actifs (uniquement au niveau de l’appareil)

- Informations sur l’appareil
- WiFi
- Cellulaire
- Bluetooth

Gestion des mises à jour (uniquement au niveau de l’appareil)

- Mise à jour des informations

Gestion de la sécurité

- Lutte contre le vol
  - Essuyer et verrouiller
- Configuration de la sécurité
  - Code d’accès
  - Certificat
- Paramètres de restriction
  - Fonctionnalité de l’appareil
  - iCloud
  - Gestion des médias

Vue d’ensemble

Introduction à AppTec360

La solution de gestion mobile d'entreprise d'AppTec offre la possibilité de gérer et de configurer tous les appareils mobiles à l'aide de sa console de gestion intuitive. Dans ce scénario, le serveur EMM peut fonctionner dans votre propre environnement ou vous pouvez utiliser notre solution basée sur le nuage.

Même en ce qui concerne l'installation centralisée d'applications d'entreprise sur les smartphones, vous êtes au bon endroit. Avec Enterprise Mobile Manager, vous pouvez distribuer des applications et des documents d'entreprise sur les appareils en quelques secondes ou bloquer les applications indésirables à l'aide d'une liste blanche ou noire.

L'utilisation d'appareils privés dans les entreprises pose un nouveau défi pour la sécurisation des smartphones et des tablettes. Étant donné que les employés souhaitent utiliser de plus en plus leurs smartphones, les administrateurs informatiques doivent protéger un grand nombre de types d'appareils différents. Nous vous aiderons à sécuriser tous les appareils et les données sensibles qui y sont stockées et à les gérer à partir d'une console intuitive.

Systèmes d’exploitation des appareils pris en charge

AppTec360 offre un support pour les appareils iOS, Android et Windows. Veuillez noter que la capacité des fonctions des plateformes mentionnées peut varier d'un système d'exploitation à l'autre.

- Apple iOS 11.0 ou supérieur*
- Apple macOS 10.11 ou supérieur
- Google Android 4.4 ou supérieur** sur la version Cloud
- Google Android 4.1 ou supérieur** sur la version OnPrem
- MS Windows 10 ou supérieur*** (ordinateur de bureau, ordinateur portable et tablette)

**Veuillez noter que les appareils équipés d'iOS 10 ou d'une version antérieure ne peuvent pas être enregistrés en raison des changements radicaux apportés par Apple au processus d'enregistrement.*

***Les appareils peuvent être connectés et configurés même s'ils utilisent une version qui n'est plus prise en charge par le fabricant. Veuillez noter que certaines fonctionnalités peuvent nécessiter une certaine version d'Android. Dans les cas d'assistance, nous suivons l'assistance officielle du fabricant. En cas de problèmes ou de bogues causés par une version obsolète qui n'est plus prise en charge par le fabricant, nous nous réservons le droit de n'offrir qu'une assistance limitée.*

****Les versions domestiques de Windows ne sont pas prises en charge en raison des limitations du système d'exploitation. Nous vous recommandons vivement d'utiliser une version du système d'exploitation qui est encore prise en charge par le fabricant. Non seulement pour des raisons de compatibilité, mais aussi pour des raisons de sécurité. C'est pourquoi nous recommandons iOS 12 ou une version plus récente et Android 9 ou une version plus récente.*

Annuaires LDAP pris en charge

- Microsoft Active Directory
- Ouvrir LDAP

Des informations actualisées sur les "systèmes d'exploitation supportés" et les "annuaires LDAP supportés" sont disponibles ici :

https://www.apptec360.com/products/systemrequirements/

Explication du « mode supervisé » sur les appareils Apple

Le mode supervisé représente une interface élargie pour les appareils iOS.

Sur l'appareil configuré, des limitations supplémentaires peuvent être appliquées, dans la mesure où elles se rapportent à la fonctionnalité de l'appareil de l'utilisateur final. Elles figurent également dans le manuel d'administration et sont signalées par un bandeau.

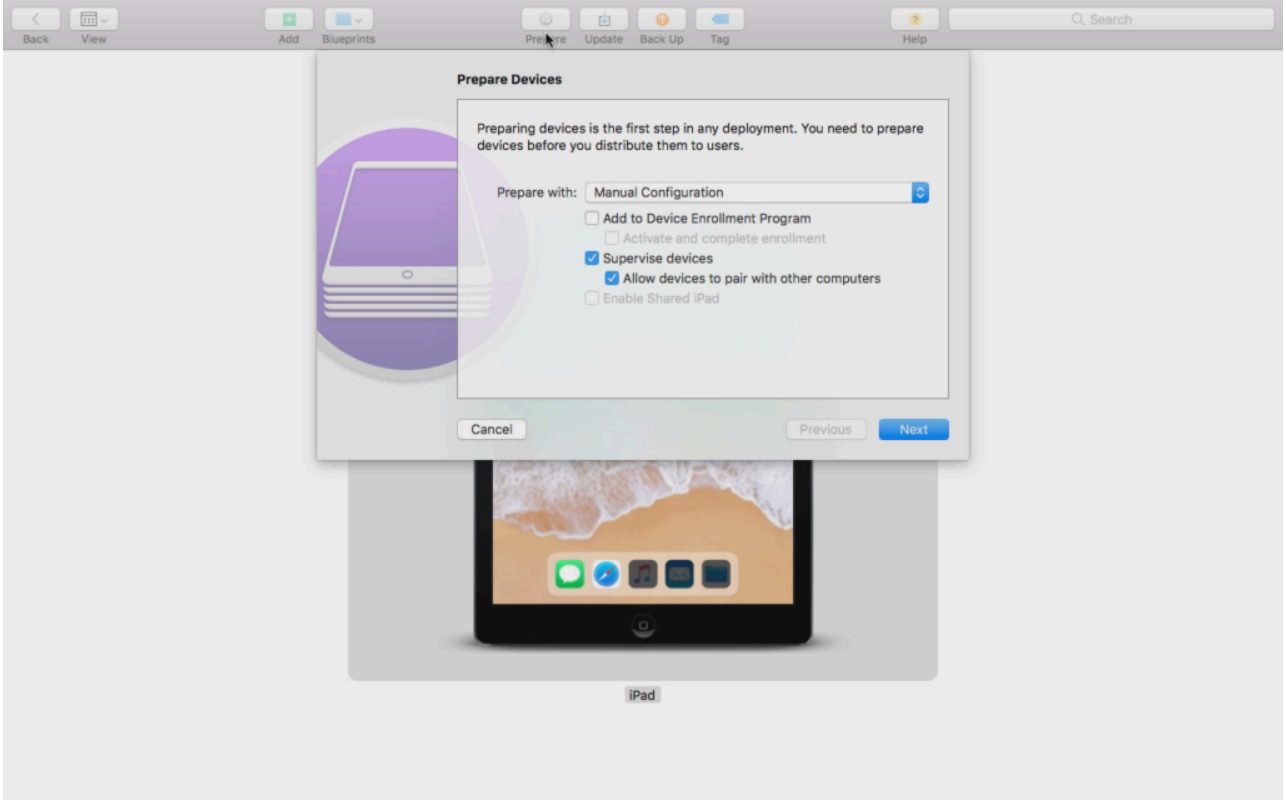
Disponible en mode supervisé

Le "mode supervisé" peut être activé à l'aide du programme "Apple Configurator". L'Apple Configurator peut définir les paramètres par défaut des nouveaux appareils iOS en tant qu'outil de configuration (via l'interface USB).

L'outil peut non seulement installer des profils de configuration, mais aussi des applications. Il est gratuit, mais nécessite un ordinateur Mac.

Activer le mode supervisé

1. Ouvrir le configurateur Apple



2. Cliquez sur l'appareil et choisissez "Préparer"
3. Choisissez "Configuration manuelle" et "Supervision des appareils"
4. Cliquez sur "Suivant"
5. (optionnel) Vous pouvez maintenant ajouter un serveur MDM où l'appareil sera enrôlé. Le lien se trouve dans "Réglages généraux - Configuration iOS - Configurateur et URL" Choisissez votre organisation ou créez-en une nouvelle.
6. Choisissez votre organisation ou créez-en une nouvelle
7. Choisissez les étapes à ignorer lors de la configuration initiale et cliquez sur "Suivant" (ATTENTION : La poursuite de la procédure effacera votre appareil !)

Votre appareil est alors placé en mode supervisé. Cette opération peut prendre quelques minutes. Une fois l'opération terminée, l'appareil redémarre.

Votre appareil est maintenant surveillé !

Ajout d’un dispositif au DEP

Vous pouvez également ajouter des appareils au DEP (Device Enrollment Programm) à l'aide de l'Apple Configurator, si vos appareils sont sous iOS 11 ou supérieur.

Plus d'informations sur le DEP : https://www.apple.com/business/dep/

Suivez les mêmes étapes que pour la supervision d'un appareil et cochez en plus la case "Ajouter au programme d'inscription des appareils". Si vous ne vous êtes jamais connecté à DEP à l'aide de l'Apple Configurator, il vous sera demandé vos données de connexion à DEP.

Une fois le processus terminé, l'appareil peut être trouvé dans le serveur DEP "Devices Added by Apple Configurator 2" (Appareils ajoutés par le configurateur Apple 2). Vous pouvez maintenant utiliser ce serveur et le connecter à la console de gestion ou transférer le dispositif vers un serveur déjà existant.

Vous avez ajouté avec succès un appareil au DEP !

Explication d’Android Enterprise

Qu’est-ce qu’Android Enterprise ?

Android Enterprise offre un meilleur contrôle des appareils professionnels qui sont gérés avec un MDM. Cela permet aux administrateurs d'avoir un contrôle total sur leurs appareils Android ou de séparer les données de l'entreprise des données privées sur les appareils conteneurs. En outre, Android Enterprise facilite l'enrôlement des appareils et la distribution des applications.

Quelles sont les conditions requises pour utiliser Android Enterprise ?

Android Enterprise peut être utilisé gratuitement par tout le monde. Il suffit de connecter un compte Google au MDM pour activer toutes les fonctionnalités d'Android Enterprise. Pour en savoir plus, consultez la section Android Enterprise.

Android Enterprise peut être utilisé sur des appareils équipés d'Android 5.1 ou supérieur, à l'exception de Enhanced Work Profile (voir ci-dessous). Nous recommandons au moins Android 7 ou une version plus récente pour une inscription plus facile ou Android 11 pour utiliser toutes les fonctionnalités disponibles.

Quels sont les modes disponibles avec Android Enterprise ?

Il existe trois modes différents pour l'utilisation d'Android Enterprise.

AE Dispositif entièrement géré (géré par le travail): Un appareil entièrement géré qui n'est utilisé que pour le travail. Cela permet à l'administrateur d'exercer un contrôle total sur l'appareil. Cela ne permet pas une utilisation privée de l'appareil. Pour inscrire des dispositifs dans ce mode, les dispositifs doivent être réinitialisés et inscrits à l'aide d'un code QR (voir l'inscription AE) ou inscrits via l'inscription Knox ou Zero Touch.

AE BYOD Container: Le conteneur BYOD (bring your own device) permet aux utilisateurs d'accéder aux données de l'entreprise sur leur téléphone personnel dans un conteneur séparé. Dans ce mode, les applications privées ne peuvent pas voir les données et les applications de l'entreprise et vice versa. Pour enregistrer les appareils dans ce mode, l'application AppTec doit être téléchargée et un code QR peut être scanné. Créez un appareil dans la console et sélectionnez "AE Container (BYOD & Enahnced Work Profile)" comme type d'appareil. Cliquez sur le code QR de l'appareil nouvellement généré pour obtenir le code QR et réglez le premier commutateur sur "Legacy & BYOD".

Profil de travail amélioré AE: (nécessite Android 11 ou une version plus récente) Alors que le conteneur BYOD mentionné ci-dessus apporte les données de l'entreprise sur un appareil privé, le profil de travail amélioré fait la même chose, mais pour un appareil appartenant à l'entreprise. Il crée le même conteneur, mais donne à l'administrateur un peu plus de contrôle sur l'appareil, de sorte que

l'utilisateur ne peut pas simplement supprimer le MDM de l'appareil. Créez un appareil dans la console et sélectionnez "AE Container (BYOD & Enahnced Work Profile)" comme type d'appareil. Cliquez sur le code QR de l'appareil nouvellement généré pour obtenir le code QR et réglez le premier commutateur sur "Profil de travail amélioré". Ce code QR peut être scanné après avoir réinitialisé l'appareil et tapé 6 fois sur l'écran comme expliqué dans la méthode 1 de l'inscription à l'AE.

Comment affecter des applications aux appareils Android Enterprise ?

Vous devez d'abord approuver les applications que vous souhaitez utiliser dans Paramètres généraux → Gestion des applications → AE Play Store → Play Store Apps. Après avoir approuvé une application, vous pouvez l'ajouter à la liste des applications obligatoires → de votre profil en cliquant sur le "+" et en sélectionnant l'application dans l'onglet "AE Play Store". Le téléchargement et l'installation de l'application se feront automatiquement. Aucun compte Google n'est requis sur l'appareil et l'utilisateur n'a pas à le confirmer ou à l'autoriser.

Téléchargez vos propres applications sur le Google Play Store

Il est possible de télécharger vos applications maison sur le Google Play Store. Vous pouvez ainsi bénéficier de différents avantages tels que le mécanisme de mise à jour du Play Store.

Pour ce faire, vous devez disposer d'un compte développeur Google. Connectez-vous à l'aide de Google Play Console(https://play.google.com/apps/publish)

Cliquez sur "Créer une application". Choisissez votre langue par défaut et le titre de l'application.

Create application

Default language *

English (United Kingdom) – en-GB ▾

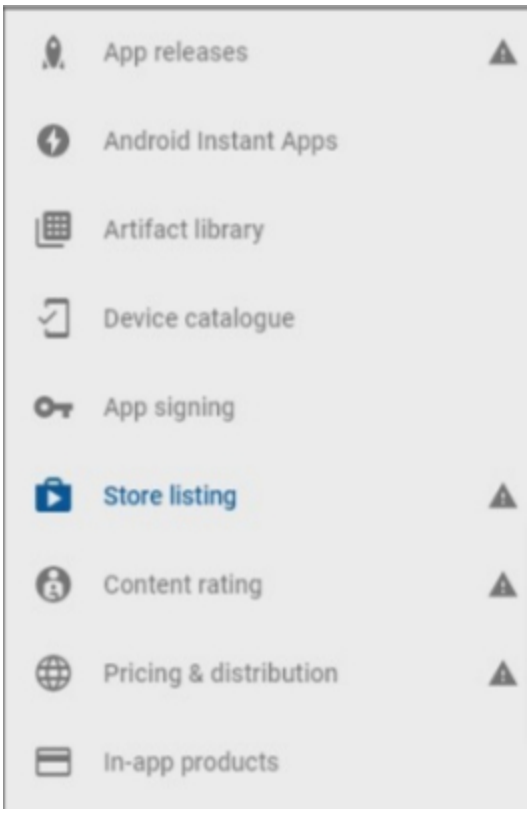
Title *

AppTec Demo App

15/50

CANCEL CREATE

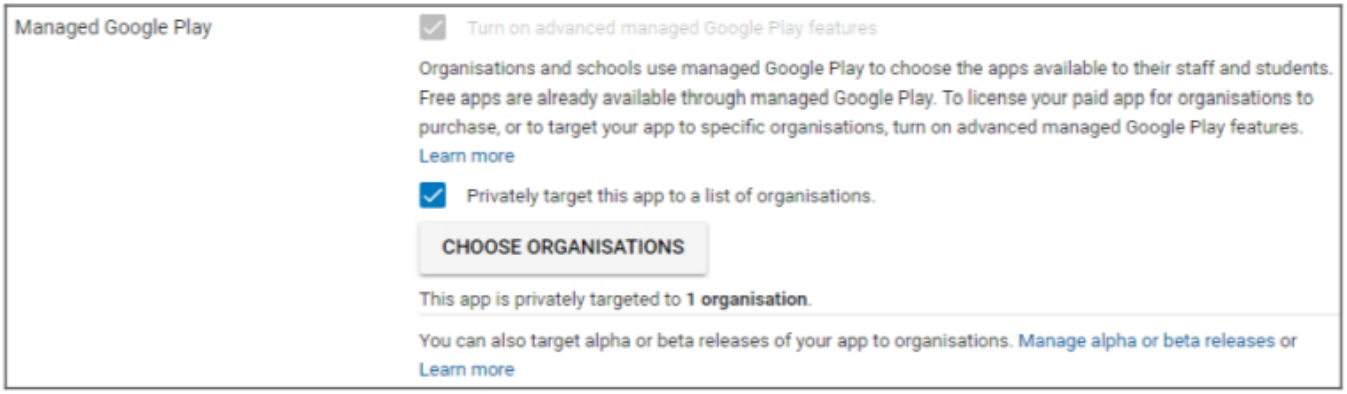
Sur la page suivante, il vous sera demandé d'entrer différents détails concernant votre application.



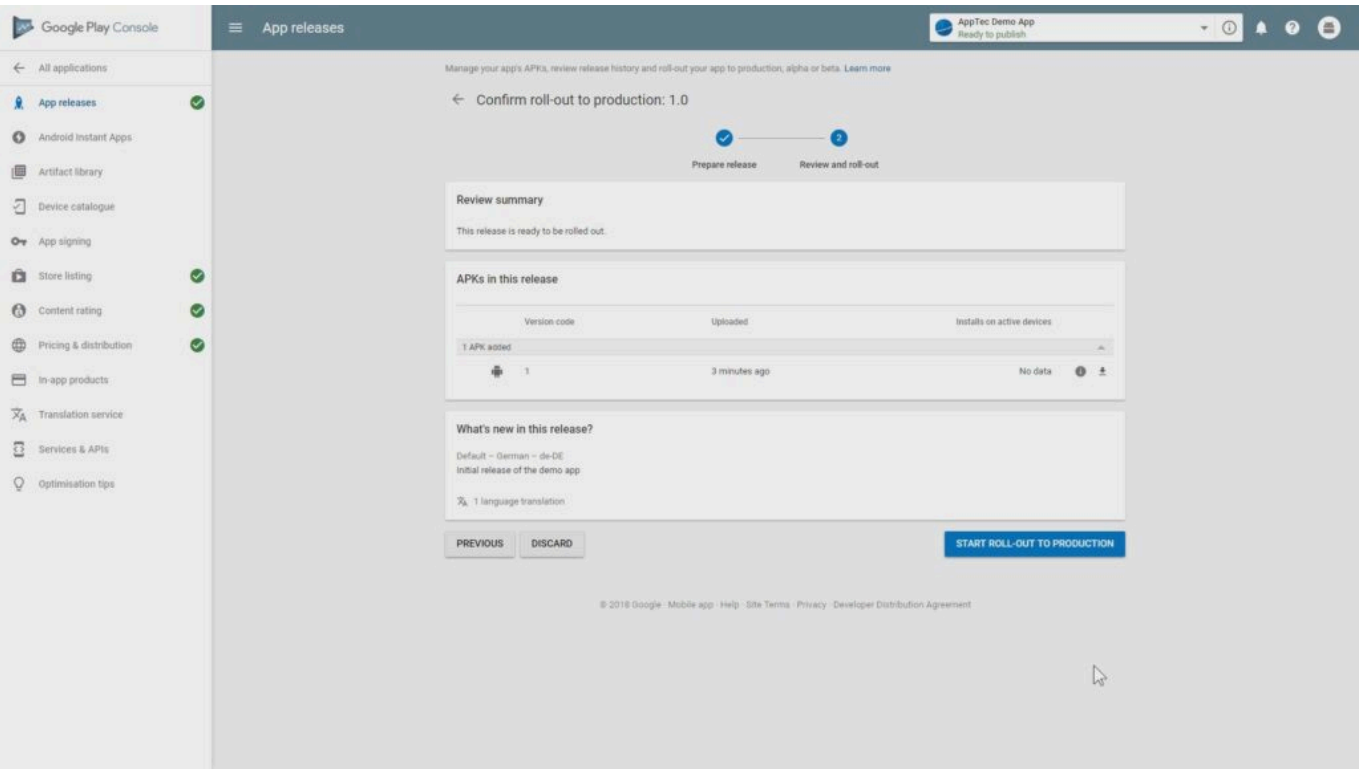
Une fois que vous avez saisi tous les détails, vous verrez différents symboles d'indices sur le côté gauche.

Survolez-les pour voir quelles sont les étapes restantes et suivez-les dans l'ordre que vous souhaitez.

Remarque : Veillez à cocher les deux cases de la rubrique "Gestion de Google Play" sous "Tarification et distribution". Dans le cas contraire, l'application sera publique et accessible à tous. Veillez également à choisir le pays de distribution.



Une fois que vous avez terminé toutes les étapes, vous pouvez aller à "App releases". Cliquez sur "Review" et "Start Roll-Out to Production" pour finaliser votre projet et publier l'application.



Il faudra peut-être attendre un certain temps avant que l'application ne soit disponible dans le Play Store. Une fois le processus terminé, vous pouvez rechercher votre application dans le magasin Play for Work et l'approuver. Ensuite, il suffit d'affecter l'application aux appareils à l'aide de la console EMM, comme vous le faites avec d'autres applications.

Exigences et installation

Exigences

Exigences du système

L'appliance virtuelle est disponible au format Open Virtualization (VMWare, VirtualBox, Citrix Xen Server) et sous forme de fichier compressé .vhdx (Hyper-V)*.

*Note : La machine doit être créée avec la génération 1 lorsque l'on utilise Hyper-V.

Le disque virtuel a une taille cible de 20 Go et la machine nécessite 4 Go de RAM.

L'appliance est basée sur Debian 9 64bit

Mettez à jour la machine importée avec la compatibilité la plus récente (par exemple dans VMWare) et assurez-vous que le type de système d'exploitation de la machine est correctement défini dans votre hyperviseur.

Clé de licence

Afin d'activer et d'installer le serveur avec succès, vous aurez besoin d'un fichier de licence valide. Vous pouvez l'obtenir directement auprès d'AppTec360 et/ou de votre revendeur respectif.

Résolution des adresses IP et DNS

L'appliance AppTec360 doit être accessible par le dispositif utilisant le nom d'hôte pour lequel la licence a été émise.

Pour inscrire les appareils Windows 10, vous devez également configurer un sous-domaine supplémentaire sous la forme de "enterpriseenrollment.", pointant vers l'appliance.

Certificat SSL

Comme toutes les connexions vers et depuis les appareils doivent être sécurisées à l'aide de SSL, vous devez disposer d'un certificat valide pour le nom d'hôte, délivré par une autorité de certification à laquelle l'appareil fait confiance. La clé privée du certificat doit être téléchargée sans protection par mot de passe. Dans la plupart des cas, un certificat intermédiaire pour l'autorité de certification est nécessaire pour que les appareils reconnaissent le certificat du serveur.

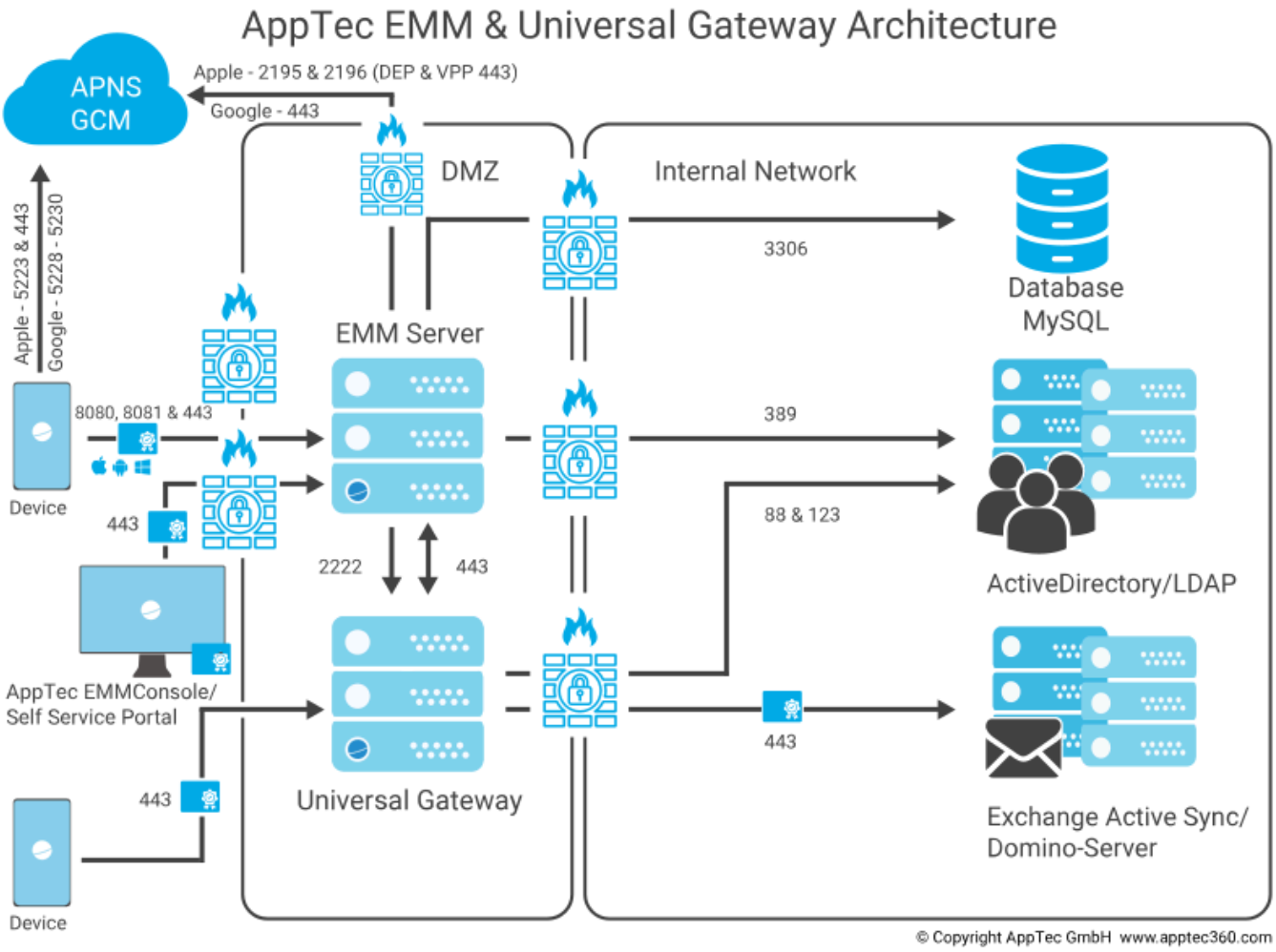
Les appareils Windows 10 nécessiteront un certificat spécifique pour votre sous-domaine d'inscription d'entreprise.

À partir de la version 202104 de l'appliance, vous pouvez également utiliser des certificats Let's Encrypt, qui sont générés automatiquement (voir l'étape 2 - Certificat SSL).

Serveur SMTP

Un serveur de courrier électronique et/ou un relais de courrier électronique est nécessaire pour permettre à l'AppTec360 EMM d'envoyer des courriers électroniques (par exemple pour l'enregistrement d'un appareil et la validation d'un compte).

Règles de pare-feu



Ce diagramme montre quelle connexion est nécessaire en fonction des services que vous souhaitez utiliser.

Pour une description plus détaillée, voir le tableau de la page suivante.

Tous (externes/appareils)	→	**AppTec360 Appliance / emmconsole.com**
Ports	443	Gestion, AppStore d'entreprise et Windows Phone Communication
	8080	Communication Android et iOS
	80	Première installation de Let's Encrypt. Utilise 443 par la suite.
Tous (dispositifs)	→	**Tous (externe)**
Ports	5223, 443	Apple Push Service, doit être accessible sans proxy, 443 comme Fallback, voir https://support.apple.com/en-us/HT203609
	5228-5230	Android Push Service (FCM), doit être accessible sans proxy
AppTec360 Appliance	→	**Contrôleur de domaine**
Ports	389, (LDAPS 636)	Synchronisation des utilisateurs avec LDAP
AppTec360 Appliance	→	**Tous**
Port	443	Utilisé pour le service Android Push (GCM) Recherche dans l'AppStore / Play Store
AppTec360 Appliance	→	**emmconsole.com**
Ports	443	Mises à jour de l'Appliance AppTec360, génération de certificats APNS
AppTec360 Appliance	→	**Réseau Apple (17.0.0.0/8)**
Ports	2195, 2196	Apple Push Service & Feedback Service
	443	DEP & VPP

Mises à jour de la sécurité

Le système d'exploitation Debian doit être mis à jour régulièrement pour bénéficier des derniers correctifs de sécurité. Cependant, assurez-vous de ne pas mettre à jour manuellement vers une version majeure plus récente de Debian. Lorsque l'EMM AppTec360 sera compatible avec une version majeure plus récente, nous ajouterons un moyen de mise à niveau dans une mise à jour de l'appliance.

Mots de passe par défaut de l’applicatif virtuel

Login User (le login root est désactivé, utilisez "sudo" pour les tâches d'administration)

apptec

Mot de passe de connexion

apptec

Utilisateur racine de MySQL

racine

Mot de passe racine MySQL

apptec

Utilisateur par défaut de MySQL

AppTec

Mot de passe par défaut de l'utilisateur MySQL

AppTec

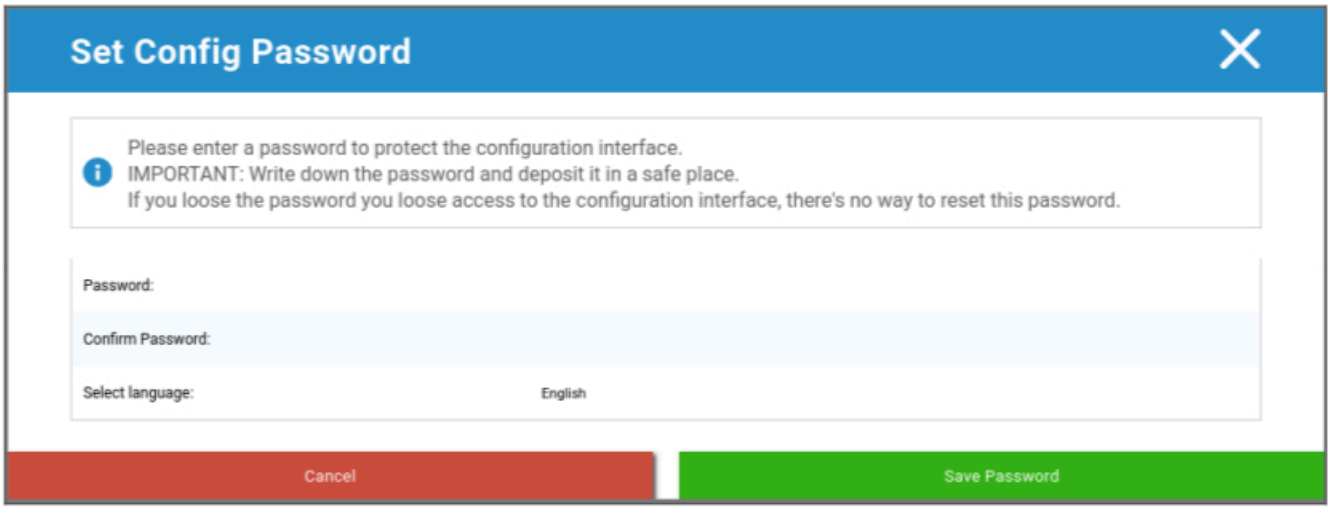
Configuration de l’Appliance Virtuelle

Important : avant de commencer la configuration de l'applicatif virtuel, la résolution de l'écran doit être d'au moins 1280 x 800 pixels.

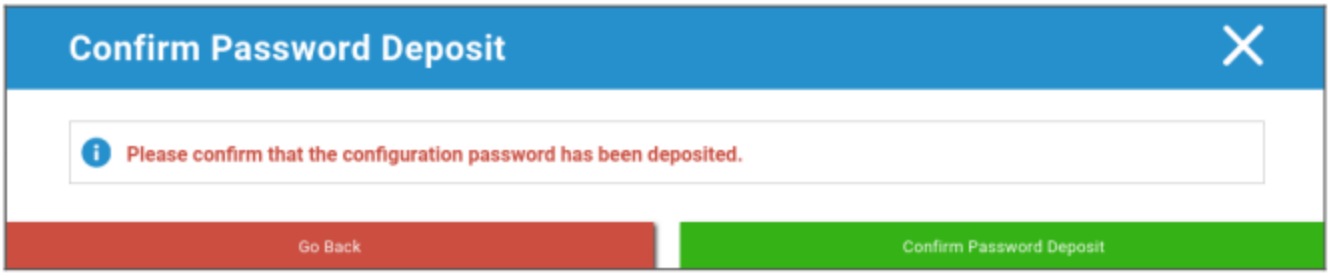
Après s'être connecté à l'Appliance, Firefox devrait démarrer automatiquement et afficher l'interface de configuration.

Préparation

Vous devez d'abord fournir un mot de passe pour l'interface de configuration. Ce mot de passe est utilisé pour crypter toutes les informations et tous les fichiers saisis dans l'interface de configuration. Vous pouvez également définir ici la langue dans laquelle l'interface doit être affichée (vous pourrez la modifier ultérieurement).

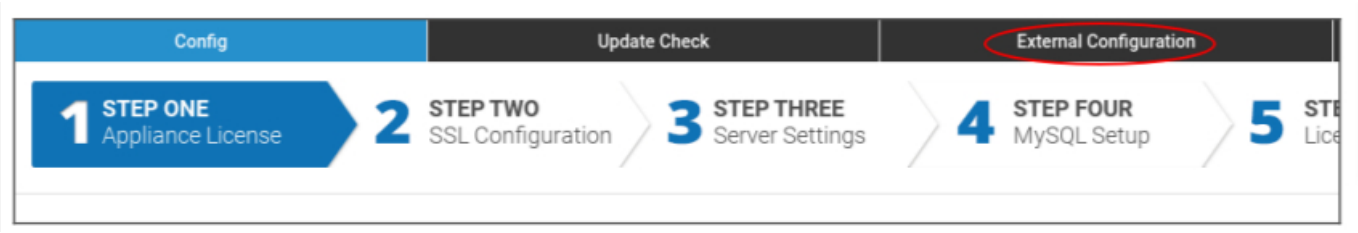


Le mot de passe ne peut être réinitialisé que par le support AppTec360, alors assurez-vous de le déposer dans un endroit sûr et de confirmer le popup à venir.



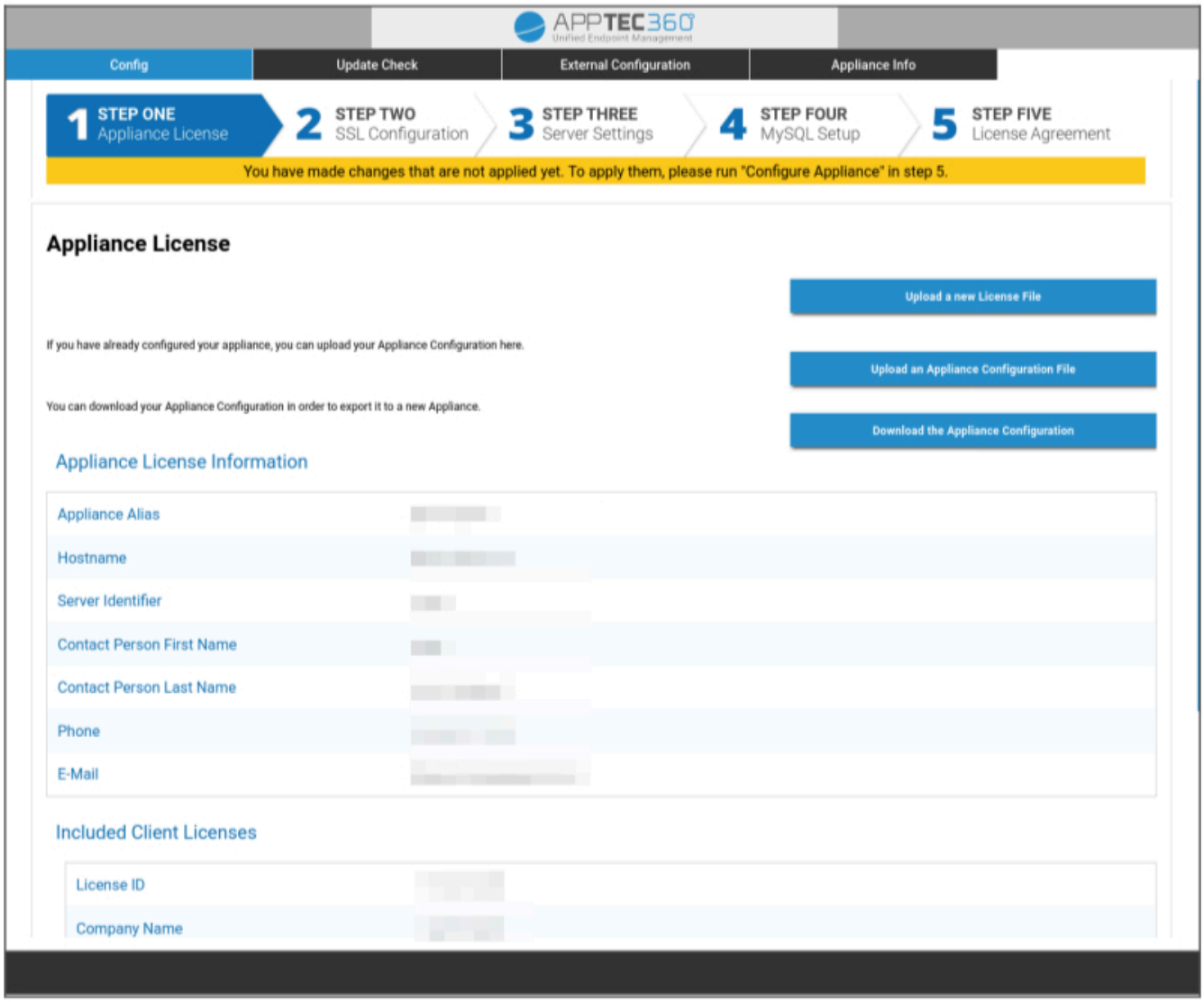
Configuration à partir d’un hôte externe

Pour faciliter le processus d'installation, vous pouvez rendre la page de configuration accessible à distance. Pour ce faire, suivez les étapes décrites dans la section "Configuration à partir d'un hôte externe".



Première étape – Licence de l'appareil

1. Veuillez télécharger le fichier de licence que vous avez reçu d'AppTec.
2. Si le fichier de licence a été téléchargé avec succès, vous pouvez voir les informations de licence de l'appliance comme dans la capture d'écran ci-dessous.



Deuxième étape – Certificat SSL

Vous pouvez soit utiliser la configuration automatique des certificats à l'aide de Let's Encrypt, soit fournir les certificats vous-même (voir SSL-Certificate pour plus d'informations).

Automatique

Le certificat sera automatiquement généré à l'aide du service Let's Encrypt.

L'AppTec360 EMM utilise le défi HTTP-01 pour la validation du domaine, ce qui signifie que le port HTTP doit être ouvert depuis l'internet pour la première demande de certificat. Les demandes de renouvellement ultérieures peuvent être validées via HTTPS.

Sélectionnez "Automatique (Let's Encrypt)" dans les cases d'option et appuyez sur "SAUVEGARDER LES VALEURS". Le certificat sera automatiquement demandé lors de l'application de la configuration à l'étape 5 - Accord de licence. Le certificat sera automatiquement renouvelé si nécessaire et vous recevrez un e-mail si le certificat est sur le point d'expirer (ce qui implique que le renouvellement a peut-être échoué).

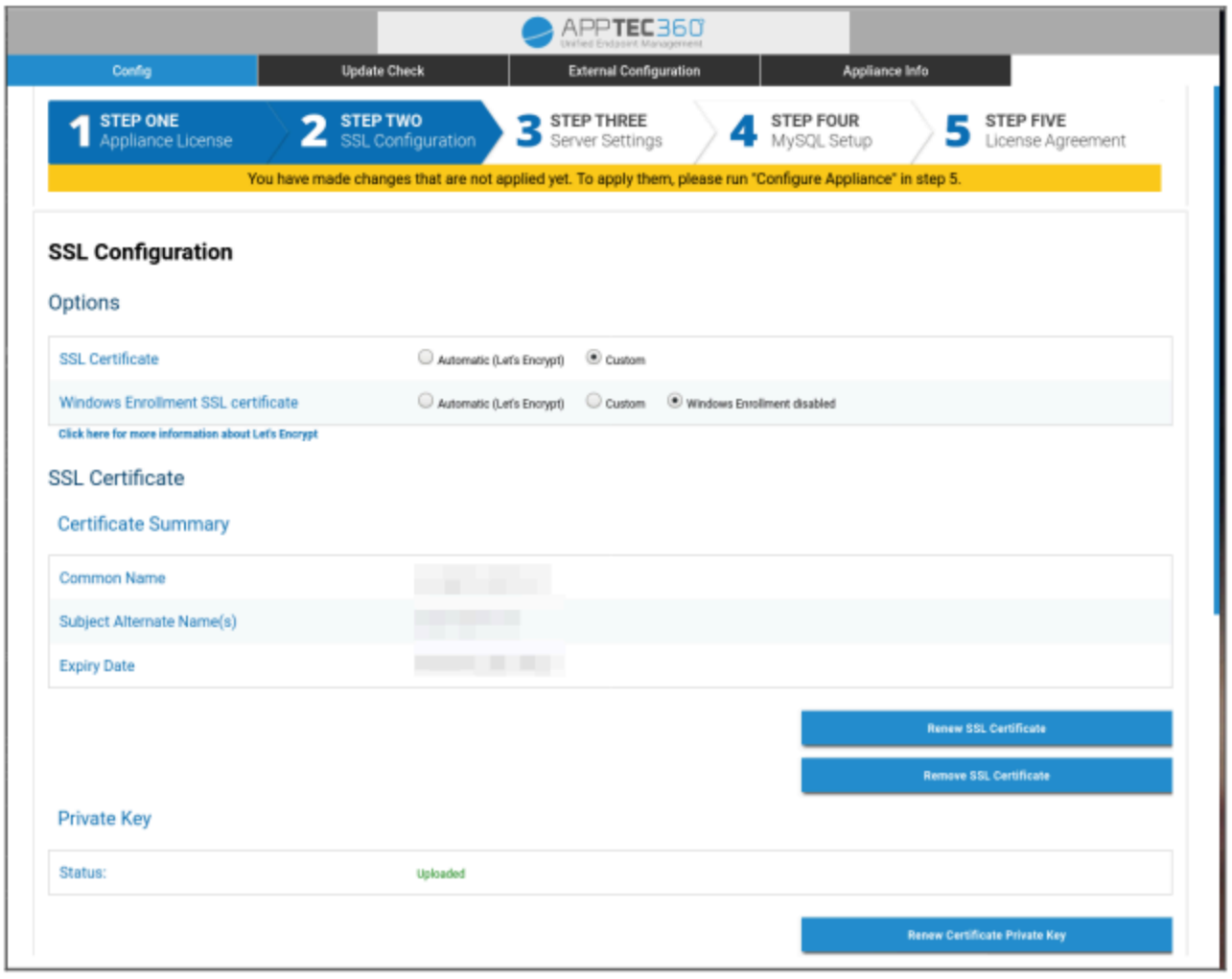
Sur mesure

1. Téléchargez le certificat SSL pour votre nom d'hôte sous licence. Vous pouvez voir le nom d'hôte à l'étape 1 - Licence de l'appliance.

2. Veuillez également télécharger la clé privée du certificat et, le cas échéant, le certificat intermédiaire.

Important : la clé ne doit pas être protégée par un mot de passe. Si c'est le cas, veuillez supprimer le mot de passe avant de télécharger.

Conseil : Si vous souhaitez également utiliser des appareils Windows 10, vous devez activer le "certificat SSL d'inscription Windows" et télécharger le certificat, la clé privée et le certificat intermédiaire pour votre sous-domaine (décrit dans le téléchargement de l'adresse IP et de la résolution DNS) au bas de la page.



Troisième étape – Paramètres du serveur

1. Veuillez saisir une adresse électronique d'assistance globale. Cette adresse sera utilisée dans les courriels adressés à vos utilisateurs afin qu'ils sachent qui contacter en cas de problème concernant leur appareil.
2. Fournir les paramètres de courrier électronique à utiliser par le système pour envoyer des courriers électroniques. Les paramètres seront utilisés pour envoyer des courriels à l'utilisateur et pour envoyer des rapports de bogues et des demandes de fonctionnalités à"support@apptec360.com". Après avoir enregistré vos paramètres de courrier électronique, vous devez les vérifier en cliquant sur "Test E-Mail Configuration" et en suivant les instructions.

Étape 4 – Configuration de MySQL

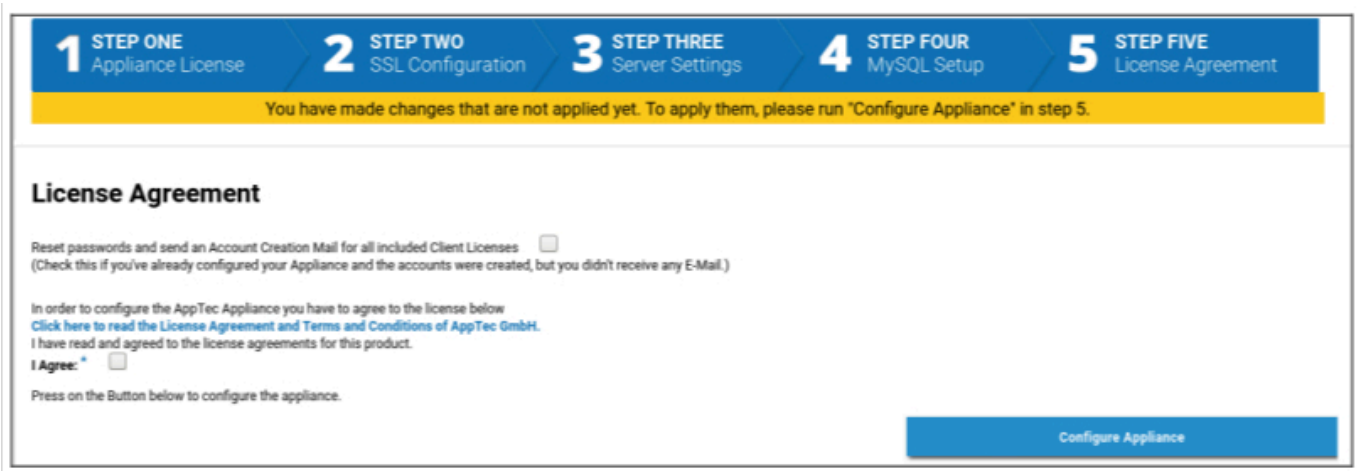
1. Si vous souhaitez utiliser la base de données interne, vous pouvez sauter cette étape. Sinon, vous pouvez saisir les informations de connexion pour votre serveur de base de données externe.


1 STEP ONE
Appliance License
2 STEP TWO
SSL Configuration
3 STEP THREE
Server Settings
4 STEP FOUR
MySQL Setup
5 STEP FIVE
License Agreement
You have made changes that are not applied yet. To apply them, please run "Configure Appliance" in step 5.
MySQL Setup
The MySQL connection has been successfully tested at April 7, 2021, 8:45 am.
If you change the settings after the initial configuration, you have to reconfigure your appliance by clicking on "Configure now" in step 5.
IP Address or Hostname
127.0.0.1
(Default: 127.0.0.1)
Username
AppTec
(Default: AppTec)
Password
(Default: AppTec)
Port
3306
(Default: 3306)

Cinquième étape – Accord de licence

1. Veuillez lire l'accord de licence.
2. Cochez "J'accepte" et appuyez sur le bouton "Configurer l'appareil" pour appliquer les paramètres.

Conseil : Vous devrez exécuter "Configure Appliance" chaque fois que vous modifiez les paramètres dans les 5 étapes pour appliquer les paramètres.



Félicitations !

Vous avez terminé la configuration de l'appliance virtuelle.

Un e-mail contenant votre mot de passe a été envoyé à l'adresse que vous avez fournie pour la licence (visible dans "Licences client incluses" à l'étape 1 - Licence de l'appareil).

Vous pouvez maintenant vous connecter à la console en utilisant ce mot de passe et l'adresse e-mail sur laquelle vous l'avez reçu.

Pour vous connecter à la console, veuillez saisir le nom d'hôte de la console dans la barre d'adresse de votre navigateur.

Vous trouverez le nom d'hôte de votre appareil à l'étape 1 - Licence de l'appareil.

Dépannage

1. Vous n'avez pas reçu d'e-mail lors de la configuration de l'appliance à l'étape 5 - Accord de licence :

Assurez-vous que vos paramètres de courrier électronique sont corrects, comme indiqué à l'étape 3 - Paramètres du serveur. Pour renvoyer le mot de passe, cochez la case "Réinitialiser les mots de passe et envoyer un courrier de création de compte pour toutes les licences client incluses" à l'étape 5 - Contrat de licence, avant d'exécuter à nouveau la commande "Configurer l'appareil".

2. Vous avez reçu une erreur concernant Let's Encrypt lors de la configuration à l'étape cinq - Accord de licence :

Assurez-vous que l'appareil est accessible par son nom de domaine sur le port 80. Let's encrypt écrit également un journal dans "/var/log/letsencrypt" qui peut aider à la résolution des problèmes.

Recommandations en matière de sécurité

Il est recommandé d'effectuer les étapes suivantes pour sécuriser votre appliance AppTec360.

Il ne s'agit pas d'un ensemble complet d'instructions, mais simplement d'une recommandation pour une configuration de base.

- Modifier le mot de passe de l'utilisateur AppTec360
- Modifiez le mot de passe des utilisateurs MySQL "root" et "AppTec" et mettez à jour l'étape 4 - Configuration de MySQL en conséquence.
- Modifier le port par défaut du serveur SSH
- Bloquez le port 80 dans votre console et interdisez le trafic HTTP entrant, utilisez uniquement HTTPS. Une fois configuré, une configuration externe via HTTPS est également possible.
- Restreindre l'accès à l'interface de gestion à certains Ips seulement au bas de l'étape 3 - Paramètres du serveur.
- Configurer le pare-feu

Paramètres généraux

Aperçu du compte

Informations sur le compte

Vue d’ensemble

Vous y trouverez un aperçu de votre compte AppTec360.

Nom de l'entreprise	Le nom de votre entreprise
Date de création	Date de création de votre compte
Type de licence	Payé = licence payée Gratuit = licence non payée Note : Pour des raisons techniques, les comptes d'un appareil sur site seront toujours affichés comme étant payés.
Identifiant du client	Identifiant de votre compte (il ne s'agit PAS de votre numéro de client)
Date d'expiration de la licence	Date d'expiration de votre licence AppTec360
Licence ContentBox	Gratuit = licence gratuite pour 25 appareils Payé = licence payée pour x appareils
Lanceur	Indique si vous pouvez ou non utiliser le lanceur personnalisé pour Android
Dispositifs	Nombre de licences actuellement utilisées / total des licences
Personne de contact	Personne de contact fournie
Téléphone	Numéro de téléphone fourni
eMail*	Adresse électronique fournie
Utilisateur racine	Utilisateurs racine pouvant se connecter
Version du logiciel	Version actuelle du logiciel

**Remarque : L'adresse électronique indiquée ici est celle que vous avez saisie lors de l'enregistrement du compte. Sur cette base, un utilisateur sera créé dans l'arborescence des utilisateurs/appareils et pourra être modifié. La modification de cet utilisateur changera l'adresse électronique que vous devez utiliser pour vous connecter, mais pas les informations figurant dans la vue d'ensemble du compte..*

Rapport de bug

Un rapport de bogue peut être envoyé directement à l'assistance pour signaler des problèmes ou des bogues. Il comprend des informations et des journaux concernant votre compte et votre configuration.

Sujet	Le sujet du rapport de bogue. Incluez un numéro de ticket si vous souhaitez ajouter ce rapport à un ticket d'assistance existant.
Comportement attendu	Décrivez en détail ce que vous avez fait et ce que vous attendiez.
Comportement réel	Décrivez en détail ce qui s'est passé. Veuillez citer les messages d'erreur EXACTEMENT. Il est également utile d'ajouter des captures d'écran à la pièce jointe.
À quel moment avez-vous rencontré le problème ?	Veuillez indiquer l'heure précise à laquelle vous avez reçu un message d'erreur/problème spécifique. Dans le meilleur des cas, indiquez également les secondes, par exemple 18:55:27
Le problème peut-il être reproduit ? Si oui, comment (en détail) ?	Décrivez en détail comment vous pouvez reproduire le problème.
Cette fonction a-t-elle déjà fonctionné comme vous le souhaitiez ? Si oui, jusqu'à quand ?	Laissez vide si vous ne savez pas.
Des modifications spécifiques ont-elles été apportées au système avant l'apparition de ce problème ? Si oui, quelles sont ces modifications (en détail) ?	Mentionnez toujours le dernier changement ou la dernière action avant l'apparition du problème, même si vous pensez qu'il n'est pas pertinent.
Le cas échéant : Quels sont les modèles d'appareils et les versions du système d'exploitation concernés ?	Veuillez toujours indiquer la version exacte du système d'exploitation (par exemple iOS 14.7.1 ou Android 11).
Le cas échéant : Quelle est l'adresse IP publique et/ou le numéro de série de l'appareil ?	Nommez-en au moins un, même si tous les dispositifs sont concernés.
Inclure les fichiers journaux	Cochez cette case pour envoyer le fichier journal avec le rapport de bogue. Il est recommandé de le faire.

Récupérer l'état actuel du VPP auprès d'Apple et l'inclure dans le rapport de bogue	Comprend des informations sur l'attribution des licences VPP. N'activez cette option que si l'assistance vous le demande ou si votre problème concerne les VPP.
Pièce jointe	Joignez tout fichier qui pourrait être utile (par exemple, des captures d'écran d'un message d'erreur).

Demande de fonctionnalité

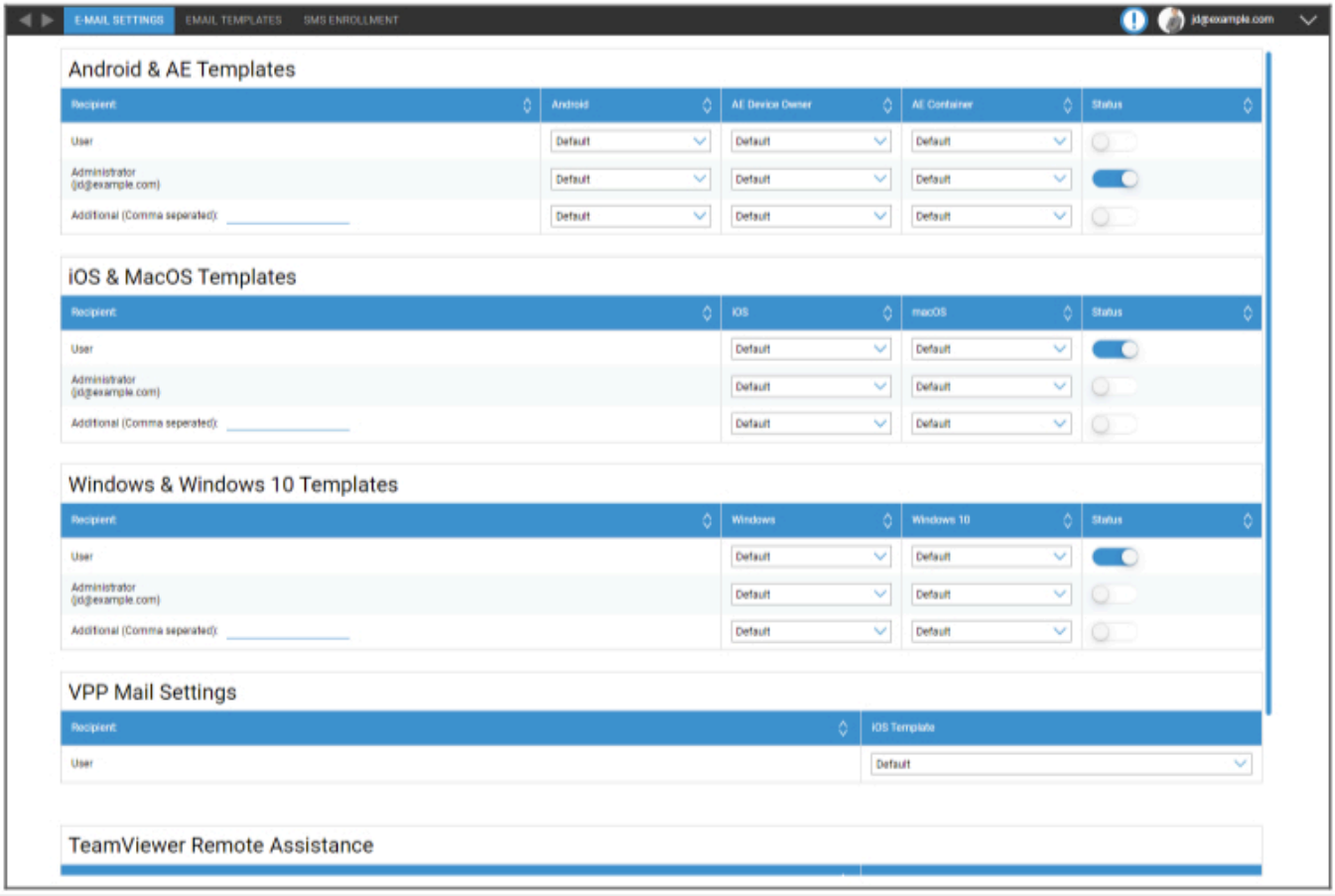
Une demande de fonctionnalité peut être envoyée directement à l'assistance. Il peut s'agir d'une demande d'une fonctionnalité spécifique ou d'une amélioration pour

Résumé	Un bref résumé de votre problème
Description	Une description détaillée de votre problème, aussi précise que possible.
Pièce jointe	Joindre des fichiers au rapport de bogue

Configuration globale

Paramètres de l'eMail

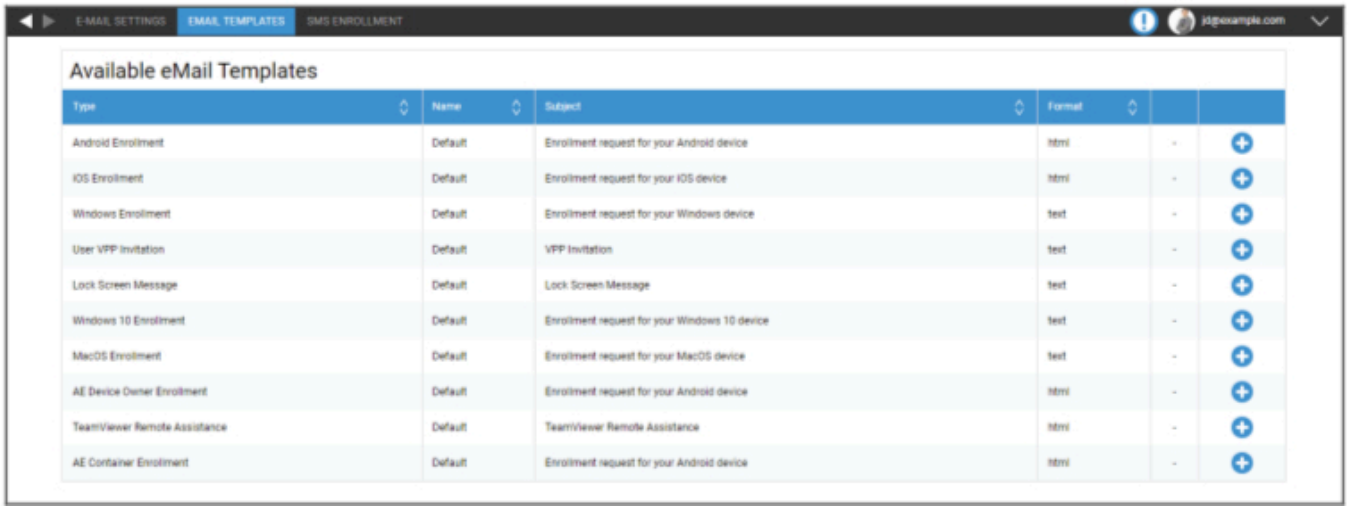
Vous pouvez définir ici qui reçoit un courrier lorsqu'une demande d'inscription est générée et quel modèle de texte est utilisé pour ce courrier.



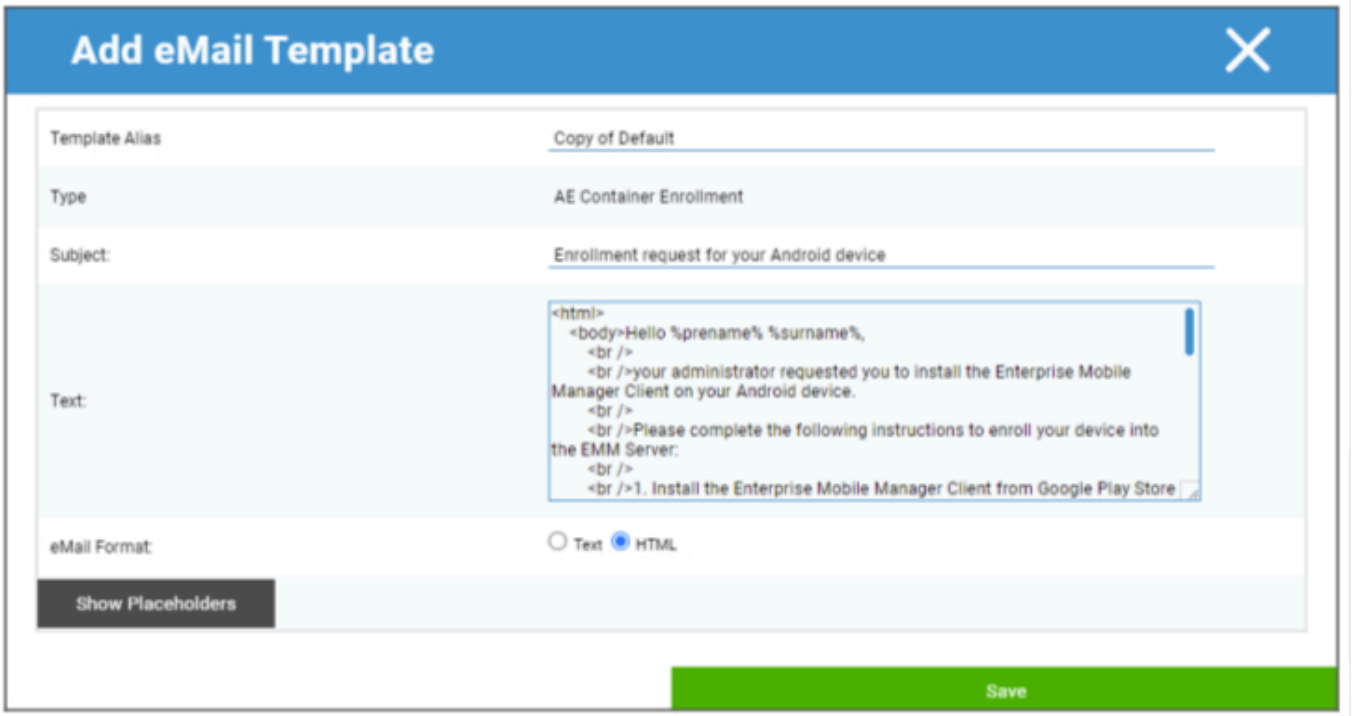
Modèles de courrier électronique

Ici, vous pouvez générer et modifier vos modèles pour différents scénarios. Ils peuvent être sous forme de texte normal ou en HTML. Avec HTML, vous pouvez mieux contrôler la mise en forme de votre texte.

Les modèles par défaut ne peuvent être ni modifiés ni effacés.



Vous pouvez également utiliser des Placeholders comme variables qui seront automatiquement remplacées. Cliquez sur "Afficher les espaces réservés" lors de la modification pour voir les espaces réservés disponibles. Les différentes catégories ont des espaces réservés différents.



Inscription par SMS

Vous pouvez ici désactiver le processus d'inscription par SMS.

(Par défaut : désactivé)

Vous verrez également un écran indiquant le nombre de crédits SMS encore disponibles.

Les crédits SMS doivent être achetés séparément.

Vie privée

Accès au GPS

Ici, vous pouvez protéger la vue GPS pour chaque appareil avec 1 ou 2 mots de passe (principe des quatre yeux). Vous serez invité à saisir votre (vos) mot(s) de passe chaque fois que vous tenterez d'accéder à la localisation d'un appareil.

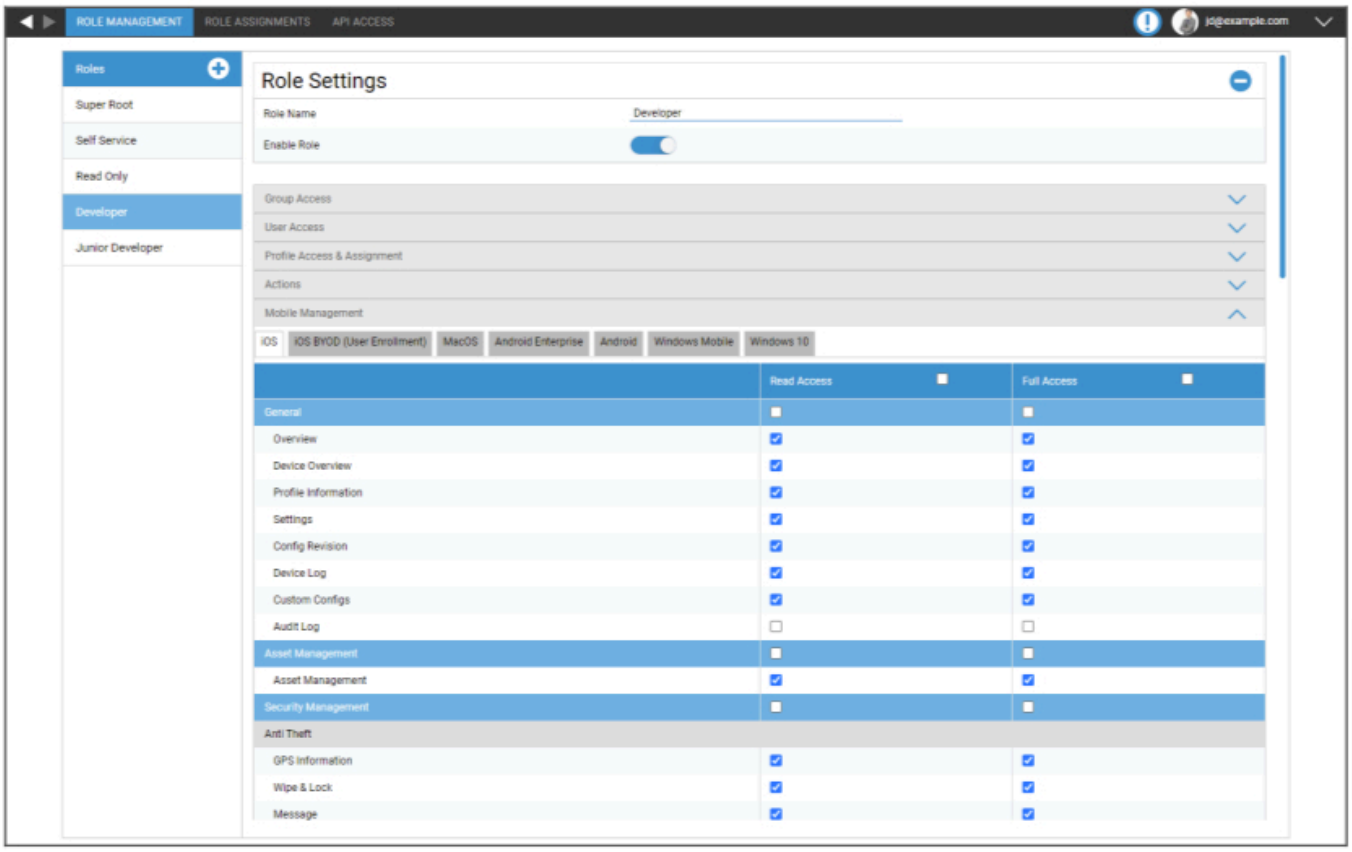
Restreindre l'accès aux paramètres du GPS	Désactivé = la fonction est désactivée et aucun mot de passe n'est requis pour la localisation.
	Activé = la fonction est activée et un mot de passe est requis pour la localisation.
Méthode de protection	Utiliser un seul mot de passe = utiliser un seul mot de passe pour la localisation
	Utiliser deux mots de passe = utiliser deux mots de passe pour la localisation
Entrez le mot de passe (1)	Entrez le mot de passe choisi
Répéter le mot de passe (1)	Saisissez à nouveau le mot de passe choisi
facultatif : Entrez le mot de passe 2	Entrez le deuxième mot de passe choisi
optionnel : Répétez le mot de passe 2	Saisissez à nouveau le deuxième mot de passe choisi

Remarque : Après avoir défini votre (vos) code(s) d'accès, vous devez le(s) saisir une nouvelle fois avant qu'il(s) ne soit(nt) complètement activé(s).

Accès basé sur les rôles

Gestion des rôles

Les rôles définissent ce qu'un utilisateur peut voir et faire lorsqu'il se connecte à la console de gestion. Cela vous permet de créer des utilisateurs qui peuvent se connecter mais dont les fonctionnalités sont limitées.



Le rôle de super-racine est un rôle par défaut qui permet de tout voir et de tout modifier. Il ne peut être ni modifié ni supprimé. Le rôle de libre-service ne peut voir que son propre utilisateur et ses propres appareils. Vous pouvez combiner le self-service et un rôle personnalisé pour, par exemple, permettre aux utilisateurs de se connecter et d'enrôler des appareils de leur propre chef et uniquement pour leur utilisateur.

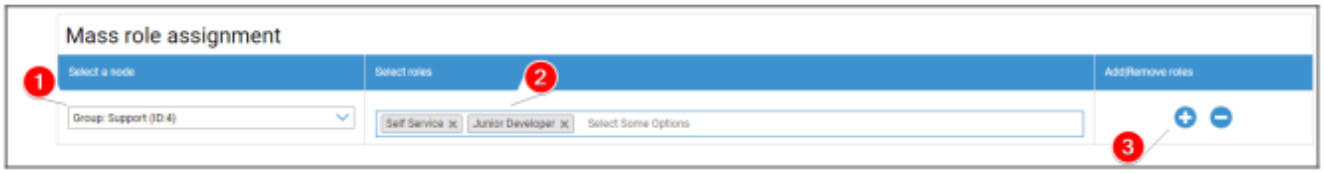
Les rôles personnalisés peuvent être activés ou désactivés manuellement. Les nouveaux rôles sont désactivés par défaut. Les utilisateurs ayant un rôle handicapé travaillent comme s'ils n'avaient pas ce rôle. Cela vous permet, par exemple, de limiter temporairement les actions d'un rôle donné.

Toutes les autorisations sont réparties entre "Accès en lecture" et "Accès complet". L'attribution d'un accès en lecture à un rôle lui permet de voir la partie spécifique de la console. Le fait de leur donner

un accès complet leur permet de voir et de modifier la partie spécifique de la console.

Attribution des rôles

Vous obtenez ici une vue d'ensemble de tous les utilisateurs qui ont un rôle et voyez lequel. Vous pouvez également attribuer un rôle à des utilisateurs ou à des groupes entiers :

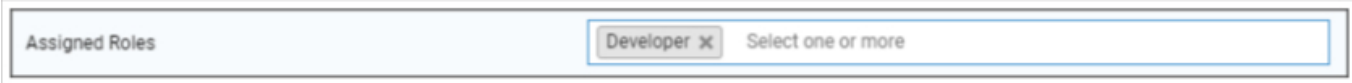


1. Sélectionnez le groupe ou l'utilisateur pour lequel vous souhaitez ajouter ou supprimer des rôles. Vous pouvez sélectionner un seul utilisateur ou un groupe. Lorsque vous sélectionnez un groupe, vos modifications affecteront tous les utilisateurs de ce groupe et tous les utilisateurs des sous-groupes du groupe sélectionné.
2. Sélectionnez le rôle que vous souhaitez ajouter ou supprimer. Vous pouvez sélectionner un ou plusieurs rôles.
3. . Sélectionnez l'opération que vous souhaitez effectuer. En cliquant sur le "+", les rôles sélectionnés sont ajoutés si l'utilisateur ne les avait pas déjà. En cliquant sur le "-", les rôles sélectionnés sont supprimés pour le(s) utilisateur(s). Si vous ajoutez des rôles à un utilisateur qui n'en avait pas encore, l'option "Peut se connecter" sera automatiquement activée pour l'utilisateur.
4. Sauvegarder pour terminer le processus. Les utilisateurs qui n'avaient pas de rôle et dont l'option "Connexion possible" était désactivée recevront automatiquement un courrier électronique contenant un lien leur permettant de définir un mot de passe.

Sous l'affectation des rôles de masse, vous trouverez une vue d'ensemble des rôles affectés. Vous pouvez également y modifier manuellement les rôles de certains utilisateurs.

Attribution d’un rôle

Pour attribuer un rôle à un utilisateur, vous devez vous rendre dans la Gestion mobile, où vous trouverez l'arborescence de vos groupes, utilisateurs et appareils. Modifiez l'utilisateur pour lui attribuer un rôle. Vous pouvez également utiliser la méthode susmentionnée pour les utilisateurs uniques.



Accès à l'API

Accéder à l'API REST d'AppTec360

L'API REST d'AppTec360 nécessite un jeton d'authentification (clé API) et une clé privée qui doivent être générés dans la console de gestion.

Pour ce faire, connectez-vous à l'AppTec360 EMM et allez à

Paramètres généraux → Accès basé sur le rôle → Accès API et ajoutez une nouvelle clé.

Vous devez sélectionner un utilisateur dont les autorisations s'appliqueront à la clé API.

La clé privée ne peut être téléchargée qu'une seule fois. Une fois que le téléchargement a commencé, la clé est supprimée et le bouton "Télécharger" disparaît.

Si vous perdez votre clé privée, vous devez générer une nouvelle clé API.

Règles générales

- L'API REST est disponible sous l'URL de base :

/public/external/api

- Toutes les demandes doivent être envoyées via POST.
- L'API REST ne prend en charge que les requêtes via HTTPS.
- Les demandes doivent contenir les en-têtes suivants :

Nom de l'en-tête	Valeur de l'en-tête	Description
Type de contenu	application/json	fixe
authentification	123...xyz	Clé API à partir de l'onglet "Accès API
signature	Signature encodée en base64	Signature de la charge utile générée avec la fonction clé privée dans l'onglet "Accès à l'API

- Le corps de la demande doit être un objet encodé en json qui doit contenir les valeurs suivantes :

Champ d'application	Champ Exemple Valeur	Description
api	v2/device/listdevices	Nom de l'API
temps	1529662725	Horodatage Unix (UTC) de la machine cliente. Le décalage horaire maximum autorisé entre le client et le serveur est de 30 minutes.

- En cas de succès, l'API renvoie les données demandées (voir les requêtes ci-dessous) et un code d'état HTTP 200.
- En cas d'erreur, le code d'état HTTP sera compris entre 4xx et 5xx en fonction de l'erreur et l'objet de réponse contiendra un tableau avec la clé "errors", qui contient une liste de messages d'erreur lisibles par l'homme.
- S'il n'y a pas de données correspondantes pour un appareil, un tableau vide sera renvoyé.
- Si l'identifiant d'un appareil n'existe pas, les données renvoyées seront nulles.

Exemple de demande

POST /public/external/api HTTP/1.1
Host: myapptecemm.com
Accept: /
Content-Type: application/jsonauth: 1234567890abcdefghijklmnopqrstuvwxyz
signature: a/bnOV466a0SiyVfsbpspZ+NxiTpmeF18NkfnOIq+OrEZDu9+VW7ESKziPXvw
kTM5B9j/t1WGN1mRcIKe80m8fDKPj+lr3BqoMJe7wGXift+uy6iS7Chpdz2iZA4KPxxU9Z
GU2cdQ/SQceX57pi+ch7ApxBeVX2+lJapTwA6CfB0mJFaf4MPcg/
7LZWkzKxKF7LNzNJHiy/vSpZcqjbXjpC4HWrX6j2uZG5eSP8kYcTR
9VQfGtkX9pcyaNAwguR7zOOwMu/8L0oKq21/19rkabE4ZgUjtKS2+
+q+rh6mrP1g4BCZ7Xq/wvgZkaP
b0CStBdMRvj46i3enxCXcLQQ==
Content-Length: 74
{"api":"v2/device/listposition","time":1529665112,"params":{"ids": [10]}}

Requêtes

Liste de tous les appareils

Fonctionnalité : Renvoie une liste de tous les appareils contenant l'ID de l'appareil, l'IMEI et le numéro de série.
URI de l'API : v2/device/listdevices
Paramètres obligatoires : aucun
Paramètres facultatifs : aucun

Exemple de corps de requête

{
"api": "v2/device/listdevices",
"time": 1529662725
}

Exemple de corps de réponse

{
"errors": [],
"list":[
{ "id":"10","serial":"987612345","imei":"899938455454"},
{ "id":"11","serial":"619723118","imei":"713032378599"}
]
}

Obtenir la liste des positions (GPS)

Fonctionnalité : Renvoie une liste de toutes les entrées du journal des positions stockées pour les numéros d'identification des appareils.
URI de l'API : v2/device/listposition
Paramètres obligatoires : "ids" - tableau d'identifiants de dispositifs
Paramètres facultatifs : aucun

Exemple de corps de requête


```
{
"api": "device/listposition",
"params": {
"ids": [10, 11]
},
"time": 1529662725
}
```


Exemple de corps de réponse


```
{
"errors": [],
"list":[
"10":[
{"time":"1529632725","pos":"47.5572,7.5967"},
{"time":"1529642725","pos":"47.5572,7.5968"},
{"time":"1529652725","pos":"47.5573,7.5969"},
],
"88":[],
]
}
```

Obtenir la carte des actifs

Fonctionnalité :
Renvoie une liste de tous les biens stockés pouvant être demandés à l'aide de la fonction Get any asset data.
Vous pouvez utiliser le formulaire lisible par l'homme ou l'étiquette d'immobilisation pour demander les données.
URI de l'API : v2/device/getassetmap
Paramètres obligatoires : aucun
Paramètres facultatifs : aucun

Exemple de corps de requête

{
"api": "v2/device/getassetmap",
"time": 1529662725
}

Exemple de corps de réponse

Cette réponse a été raccourcie pour des raisons de lisibilité.

{
"AssetKeys": {
"UDID": "AT001",
"Device Alias": "AT002",
"OS Version WinMobile iOS MacOS": "AT003",
"Model Name": "AT004",
"Serial Number": "AT005",
"Total Storage": "AT006",
"Free Storage": "AT007",
"IMEI": "AT008",
…
"apptecID": "APPTECID"
},
"errors": []
}

Obtenir n'importe quelle donnée sur les actifs

Fonctionnalité : Renvoie une liste des données de biens demandées pour les identifiants de dispositifs.
URI de l'API : v2/device/getassetdata
Paramètres obligatoires : "ids" - tableau d'identifiants de dispositifs
Paramètres facultatifs :
"assetkeys" - Clés de données sur les actifs à renvoyer. Si elle n'est pas spécifiée, toutes les données disponibles sur les actifs seront prises en compte.
a été renvoyée. Vous pouvez obtenir une liste des clés d'actifs à l'aide de l'option Obtenir la carte des actifs.

Exemple de corps de requête


```
{
"api": "v2/device/getassetdata",
"time": 1529662725,
"params": {
"ids": [
26
],
"assetkeys": [
"imei"
]
}
}
```


Exemple de corps de réponse


```
{
"result": {
"26": {
"imei": "349157642516427”
}
},
"errors": []
}
```

Exemple de code en Python3

```
! /usr/bin/python
import base64
from Crypto.Hash import SHA512
from Crypto.Signature import PKCS1_v1_5
from Crypto.PublicKey import RSA
import os
import time
import json
import urllib.request
import urllib.parse
import urllib.error
import http.client
applianceDomain = "YOURAPPLIANCE.COM"
apiURL = "https://"+applianceDomain+"/public/external/api"
privateKeyPath = "/path/to/PrivateKey-XXXXXXXXXXX.pem"
apptecAPIAuthToken = "7eXXXXXXXXXXXXXXXXXXXXXXXXXXX20"
currentTimestamp = int(time.time())
# Get Devices
#requestData = {"api": "v2/device/listdevices", "time": currentTimestamp}
# Get Positions
#requestData = {"api": "v2/device/listposition", "time": currentTimestamp,
"params":{"ids":[26]}}
# Get AssetData
requestData = {"api": "v2/device/getassetdata", "time": currentTimestamp,
"params":{"ids":[26], "assetkeys": ["imei"]}}
# encode the request data to json
print(json.dumps(requestData, indent=1))
jsonEncodedRequestData = json.dumps(requestData)
# Sign the request data json with the API private key
message = jsonEncodedRequestData.encode('utf-8')
print("Body:", message)
digest = SHA512.new()
digest.update(message)
```

```
# Read private key from file
with open(privateKeyPath, "r") as myKeyFile:
private_key = RSA.importKey(myKeyFile.read())
```

```
# Load private key and sign message
signer = PKCS1_v1_5.new(private_key)
signatureOfRequestData = signer.sign(digest)
Base64EncodedSignature = base64.b64encode(
signatureOfRequestData).decode("utf-8")

headers = {"Content-type": "application/json",
"auth": apptecAPIAuthToken, "signature": Base64EncodedSignature}
print("Headers:", headers, "\n")

# Send request to Server
httpsClient = http.client.HTTPSConnection(applianceDomain, 443, timeout=10)
httpsClient.request("POST", apiURL, jsonEncodedRequestData, headers)

# Get answer
response = httpsClient.getresponse()
status = response.status
data = response.read()

if data == False:
print("Invalid answer from the server")
else:
print("Answer:")
print(json.dumps(json.loads(data), indent=1))
if status != 200:
print("http error: lastReceivedHttpCode")
print(status)
```

Configuration de la pomme

Certificat APNS

Ici, vous pouvez télécharger un certificat APNS. Il est nécessaire pour gérer les appareils iOS et MacOS.

Remarque: le certificat APNS n'est valable qu'un an. Il doit être renouvelé avant son expiration. La procédure de renouvellement est identique à celle de la création (voir ci-dessous) et ne prend que quelques minutes.

Si vous oubliez de renouveler l'inscription à temps, vous ne pourrez pas modifier les appareils déjà inscrits. **et vous devez réenregistrer tous les appareils.** .

Étape 1

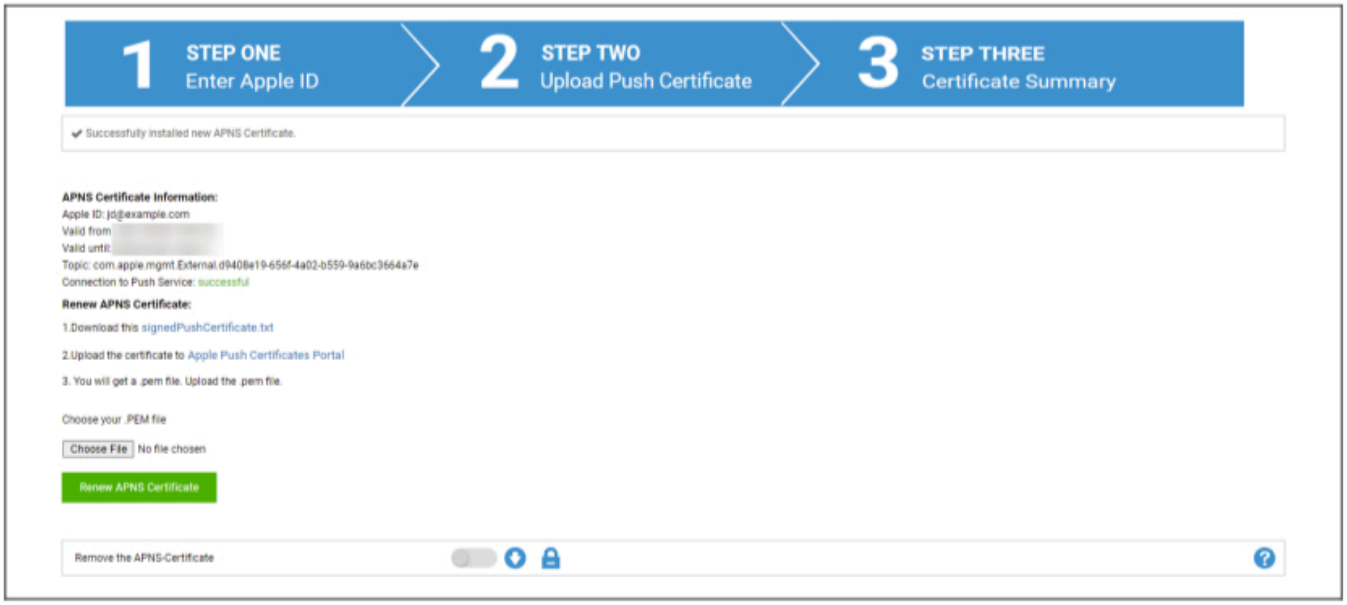
- Tout d'abord, saisissez l'identifiant Apple que vous souhaitez utiliser pour créer le certificat APNS.

Remarque : cet identifiant Apple n'est utilisé que pour la création du certificat APNS. Cet identifiant Apple n'a rien à voir avec les appareils et ces derniers n'en ont pas connaissance. En outre, vous devez également avoir accès à cet identifiant Apple pour renouveler le certificat APNS. Il est donc recommandé d'utiliser un identifiant Apple générique et de documenter les données de connexion. Un rappel est envoyé à l'adresse électronique utilisée pour l'Apple ID avant l'expiration du certificat APNS.

- Cliquez sur "Étape suivante" pour continuer.
- (facultatif) Vous pouvez également récupérer le certificat APNS précédemment supprimé si vous l'avez supprimé par accident.

Étape 2

- Télécharger le fichier signedPushCertificate.txt
- Allez sur https://identity.apple.com/pushcert/ et connectez-vous avec l'Apple ID de l'étape 1.
- Cliquez sur "Créer un certificat"
- (facultatif) saisir une note. Cela peut être utile si vous gérez plusieurs locataires afin de les identifier facilement.
- Cliquez sur "Choose File" pour sélectionner le fichier signedPushCertificate.txt précédemment téléchargé.
- Cliquez sur "Upload".
- Vous verrez maintenant la confirmation que vous avez créé un certificat APNS.
- Cliquez sur "Télécharger" et sauvegardez-le.
- Retournez à la console de gestion.
- Cliquez sur "Choose File" et sélectionnez le certificat APNS que vous souhaitez télécharger.
- Cliquez sur "Télécharger"



Étape 3

Vous avez maintenant configuré avec succès le certificat APNS et vous pouvez maintenant gérer les appareils iOS et MacOS.

À l'étape 3, vous verrez une vue d'ensemble de votre certificat APNS actuellement utilisé.

Vous avez également la possibilité de renouveler le certificat APNS en suivant les étapes indiquées à l'écran. N'oubliez pas de la renouveler avant qu'elle n'expire.

Lors du renouvellement du certificat APNS, n'oubliez pas de vous connecter avec l'identifiant Apple indiqué à l'étape 3 et de renouveler le certificat précédemment utilisé et de NE PAS en créer un nouveau. Vous verrez le "sujet" du certificat APNS à l'étape 3 et lorsque vous cliquerez sur le "i" dans le portail du certificat Apple Push. Il s'agit de l'identifiant unique qui permet d'identifier le certificat. Cela vous aidera à identifier et à renouveler le bon.

Lorsque vous obtenez le message "Error : Le certificat Push a un sujet différent" lors du renouvellement, cela signifie que vous avez renouvelé un autre certificat ou que vous en avez créé un nouveau.

Si vous souhaitez télécharger un nouveau certificat, par exemple si vous ne pouvez plus accéder à l'identifiant Apple utilisé précédemment, vous devez d'abord supprimer le certificat actuellement téléchargé.

Quoi qu'il en soit, la suppression du certificat APNS signifie que vous ne pouvez plus effectuer de modifications pour les appareils actuellement inscrits jusqu'à ce que vous les inscriviez à nouveau.

Veillez donc à vous préparer à cette éventualité et ne retirez le certificat que s'il n'y a pas d'autre solution.

Accès géré

Ici, vous pouvez activer l'inscription des utilisateurs pour les appareils iOS et l'iPad partagé pour les appareils iOS.

Inscription des utilisateurs

L'inscription des utilisateurs permet d'activer un mode spécial pour les appareils BYOD.

Pour chaque utilisateur, un Apple-ID géré doit être créé dans l'Apple Business Portal.

Au cours de la procédure d'inscription, les utilisateurs devront fournir leurs identifiants Apple-ID.

L'enrôlement de l'utilisateur garantit une sécurité maximale pour l'utilisateur car il ne permet qu'un ensemble limité de paramètres et de restrictions à configurer par le MDM.

Domaine géré :

Le domaine utilisé pour associer l'adresse électronique de l'utilisateur à son Apple-ID géré (doit être au format : "@appleid.company.com") ; par exemple, john.doe@example.com sera associé à john.doe@appleid.company.com.

Consultez l'Apple Business Manager pour connaître votre domaine géré.

iPad partagé

Un iPad partagé est un appareil DEP configuré avec un profil DEP spécial.

Cela permet à plusieurs utilisateurs de se connecter à l'appareil à l'aide de leur Apple-ID géré.

L'Apple-ID géré doit être créé dans l'Apple Business Portal ou l'Apple School Manager.

Les utilisateurs qui se connectent à un iPad partagé se voient demander leurs identifiants Apple-ID gérés.

Domaine géré :

Le domaine utilisé pour associer l'adresse électronique de l'utilisateur à son Apple-ID géré (doit être au format : "@appleid.company.com") ; par exemple, john.doe@example.com sera associé à john.doe@appleid.company.com.

Consultez l'Apple Business Manager pour connaître votre domaine géré.

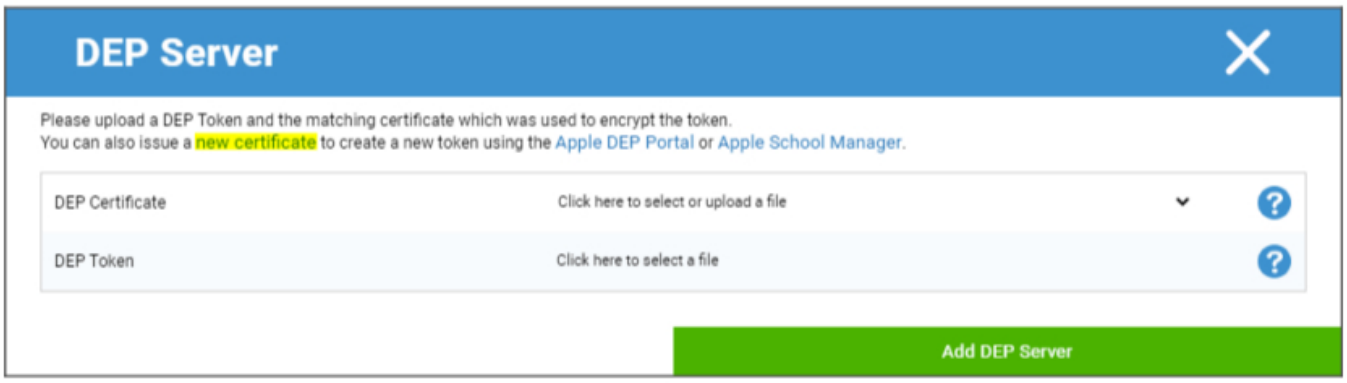
DEP

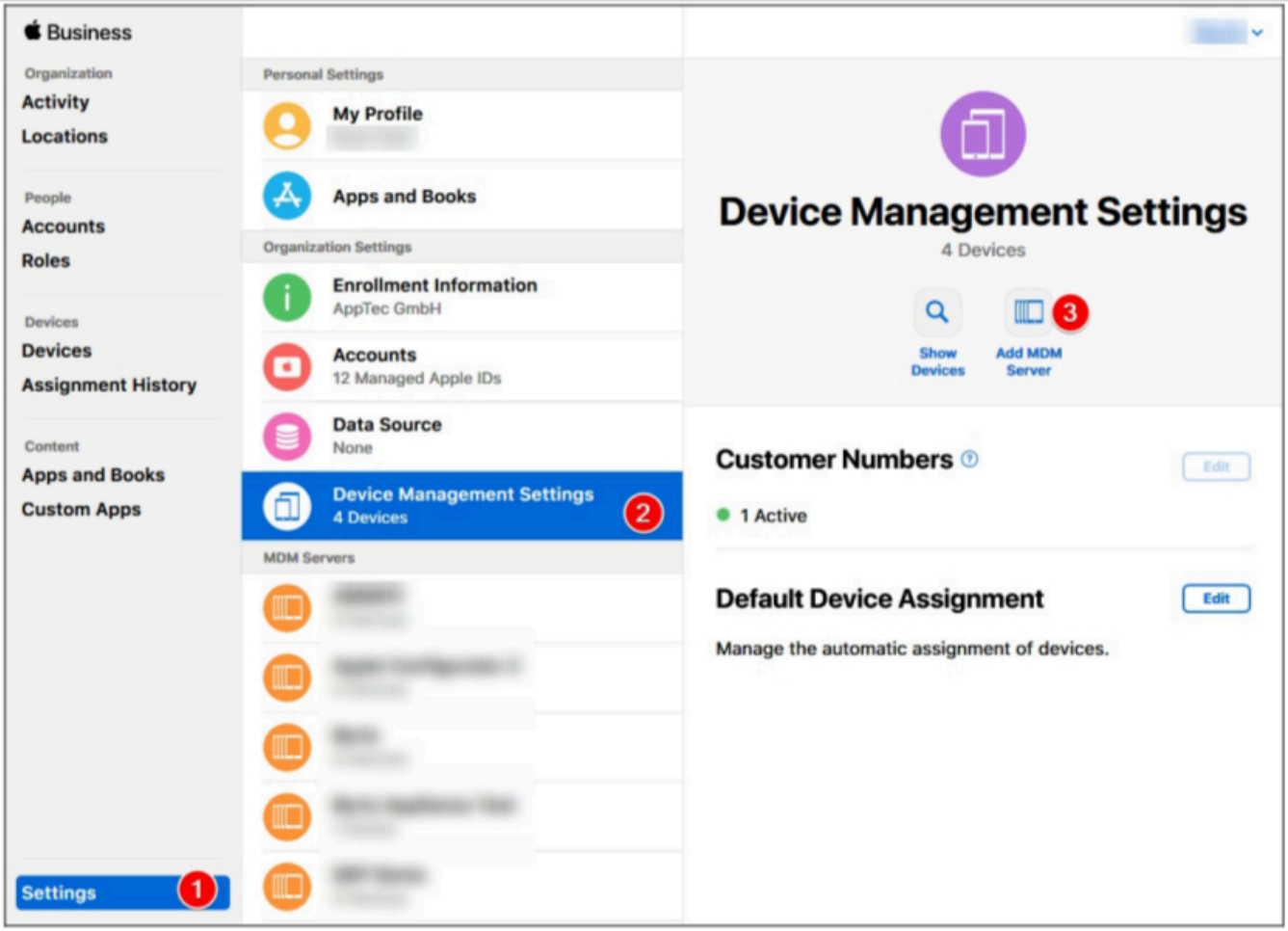
DEP (Device Enrollment Program) vous permet d'enregistrer facilement des appareils dans le MDM. Lorsque vous utilisez DEP, les appareils sont automatiquement connectés au MDM lors de la configuration de l'appareil. Vous pouvez également sauter presque toutes les étapes de configuration qui sont généralement obligatoires sur iOS.

N'oubliez pas que vous devez acheter les appareils auprès d'un revendeur qui prend en charge le DEP. Pour plus d'informations, contactez votre revendeur ou Apple.

Plus d'informations sur le DEP : https://www.apple.com/business/dep/

Cliquez sur le "+" pour ajouter un jeton DEP. Dans la fenêtre contextuelle, cliquez sur "nouveau certificat" dans le texte (marqué en jaune dans l'image ci-dessous). Cette opération permet de générer et de télécharger un certificat DEP. Allez ensuite dans Apple Business Manager(https://business.apple.com/) ou Apple School Manager(https://school.apple.com/).

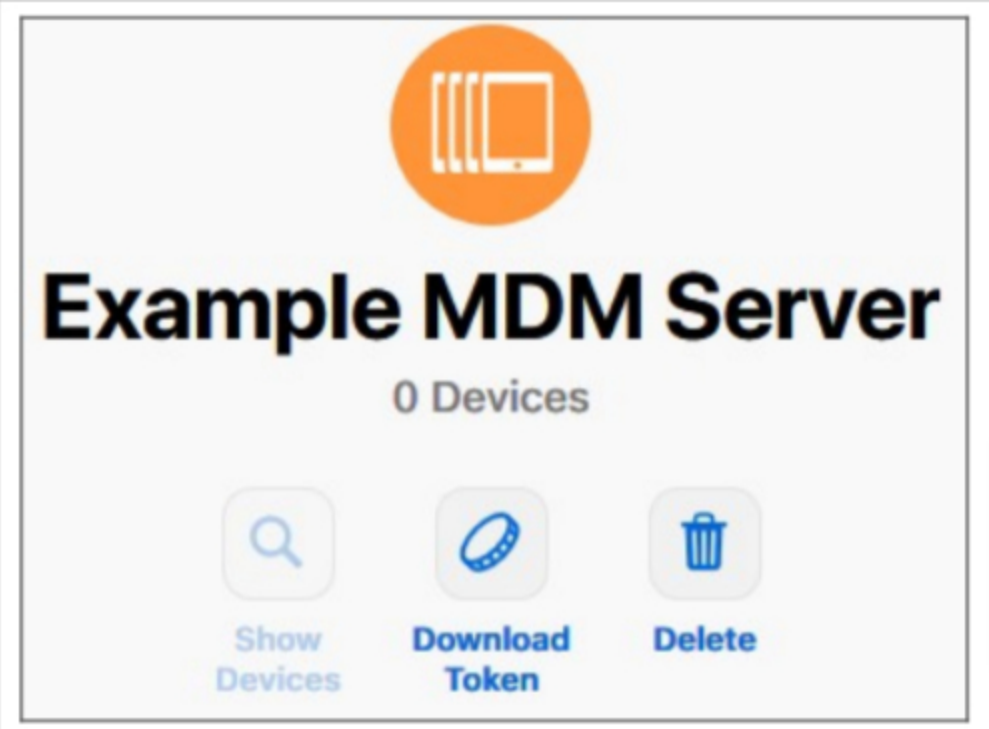




Dans l'Apple Business Manager, suivez les étapes indiquées dans l'image ci-dessus. Paramètres → Gestion des appareils Paramètres → Ajouter un serveur MDM.

Donnez au serveur le nom que vous souhaitez et téléchargez le certificat DEP précédemment téléchargé sous MDM Server Settings → Upload Public Key et cliquez sur "Save".

L'option "Download Token" (télécharger le jeton) s'affiche. Cliquez sur ce lien et sauvegardez-le. Le jeton n'est valable qu'un an. Mais il suffit de cliquer à nouveau sur "Télécharger le jeton" pour en obtenir un nouveau, ce qui rend le renouvellement du jeton très facile.



Vous pouvez maintenant retourner dans le MDM, où vous avez précédemment téléchargé le certificat DEP. Si vous n'avez pas fermé l'onglet, la fenêtre contextuelle permettant d'ajouter un serveur DEP devrait toujours être ouverte et le certificat DEP devrait déjà être sélectionné. Vous pouvez maintenant télécharger votre Token dans le champ "DEP Token" et cliquer sur DEP Server.

La colonne "**Dispositifs**" indique le nombre de dispositifs affectés à ce serveur DEP. Les appareils ajoutés à ce serveur DEP seront automatiquement créés dans le pool DEP de la gestion mobile.

En cliquant sur ce numéro, vous obtiendrez une vue d'ensemble de tous vos appareils DEP et de leur état.

Remarque: en fonction de votre flux de travail ou de votre configuration dans le Business Manager, il est possible que vous deviez affecter manuellement ces dispositifs au serveur DEP. Vous pouvez également définir un serveur DEP par défaut dans l'Apple Business Manager pour les nouveaux appareils.

La colonne "**Profils**" indique le nombre de profils DEP dont vous disposez. Vous pouvez également cliquer sur ce numéro pour voir les détails de vos profils DEP et vous pouvez supprimer d'anciens profils ou des profils inutilisés. Il n'est actuellement pas possible de les modifier. Si vous voulez changer quelque chose, vous devez en créer un nouveau.

Dans la colonne "**Dernière synchronisation**", vous pouvez synchroniser manuellement le serveur DEP (par exemple, si vous venez d'ajouter un nouvel appareil à DEP) et voir la date de la dernière synchronisation réussie.

Dans la colonne "**Profil auto**", vous pouvez définir un profil DEP comme valeur automatique par défaut. Ce profil sera attribué automatiquement aux nouveaux appareils. Si vous ne définissez pas de profil automatique, vous devez à chaque fois attribuer manuellement un profil aux nouveaux appareils.

Dans la colonne "**Ajouter un profil**", vous pouvez ajouter un nouveau profil DEP. L'appareil recevra cette information au début de la configuration de l'appareil. Le profil DEP définit la manière dont l'appareil est configuré et les étapes de la configuration qui seront ignorées.

Remarque: après l'enregistrement d'un appareil, ces paramètres ne peuvent être modifiés qu'en procédant à une réinitialisation d'usine et en enregistrant l'appareil avec un nouveau profil. Ceci est particulièrement important pour les options "**Amovible**" et "**Autoriser l'appariement**". Dans le cas de "**Allow pairing**", il est recommandé de l'activer, car il peut être désactivé via les restrictions MDM, mais il ne peut pas être réactivé s'il a été désactivé dans le profil DEP.

Dans la colonne "**Modifier**", vous pouvez télécharger un nouveau jeton, par exemple lors du renouvellement du jeton.

Configurateur et URL

URL de l'inscription à la piscine

Vous pouvez y créer une URL d'inscription et un code QR d'inscription qui sont valables pour un nombre déterminé d'inscriptions et jusqu'à une date donnée. Cela vous permet d'inscrire plusieurs appareils à l'aide d'un seul lien ou code QR.

Les appareils enregistrés avec cette URL ou ce code QR seront dans le pool de la gestion mobile et vous devrez les affecter manuellement à un groupe ou à un utilisateur par la suite.

Note: ceci ne concerne que l'inscription manuelle. N'utilisez pas cette URL si vous enregistrez les appareils via Apple Configurator.

Profil MDM – Apple Configurator

Vous pouvez obtenir ici l'URL dont vous avez besoin pour enregistrer des appareils via Apple Configurator. Lorsque vous préparez des appareils avec l'Apple Configurator, vous pouvez les ajouter au MDM au cours de la même procédure. Le configurateur Apple a besoin de cette URL pour cela.

Les appareils ajoutés via Apple Configurator se trouvent dans le pool de la gestion mobile et vous devez ensuite les affecter manuellement à un groupe ou à un utilisateur.

Vous y trouverez également un fichier .mobileconfig qui peut être utilisé pour enregistrer les appareils via Apple Configurator. Quoi qu'il en soit, il est recommandé d'utiliser l'URL.

Configuration Android

Configuration Android

Désinstaller la protection	Si cette fonction est activée, l'utilisateur ne peut pas désactiver l'administrateur du dispositif sans saisir le mot de passe défini par l'administrateur MDM. Le mot de passe est défini lors de l'inscription, les appareils doivent donc être réinscrits pour mettre à jour le mot de passe. Il existe deux options pour supprimer les administrateurs de périphériques : 1. Manuellement sur l'appareil ◦ Ouvrez l'application EMM sur l'appareil ◦ Passez à l'onglet Statut ◦ Tapez sur "Désinstaller la protection" ◦ Saisissez le mot de passe Vous pouvez utiliser la révision pour obtenir le mot de passe correct à partir de l'"Historique des mots de passe" dans la console. ◦ Faites défiler vers le bas et appuyez sur le point nouvellement ajouté, "Tap to uninstall AppTec360 MDM App" (vous avez 20 secondes pour effectuer cette tâche). ◦ Confirmez le dialogue "Uninstall AppTec360 MDM App" avec "ok". L'appareil sera alors désinscrit de la console. ◦ Pour supprimer l'application de l'appareil, confirmez le dialogue "AppTec360 MDM va être désinstallé" en cliquant sur "UNINSTALL". 2. l'automatique (Console) ◦ Sélectionnez l'appareil dans la console ◦ Cliquez sur l'icône bleue en forme d'engrenage et sélectionnez "Enterprise Wipe" (nettoyage d'entreprise) Remarque : disponible uniquement avec Android 4.x et les versions inférieures ou sur les appareils dotés de l'API KNOX (appareils Samsung).

Mot de passe de désinstallation (révision x)	Le mot de passe établi, avec lequel l'utilisateur peut supprimer l'administrateur de l'appareil. Révision x = compteur, combien de fois le mot de passe a déjà été modifié Il est important de savoir de quel mot de passe l'utilisateur a besoin, car il est possible que l'appareil n'ait pas communiqué avec le serveur AppTec360 et que le mot de passe le plus récent n'ait donc pas encore été transmis.
Historique des mots de passe	Lorsque vous cliquez sur le bouton bleu ("Afficher l'historique"), vous pouvez consulter les mots de passe établis précédemment.
Protection étendue contre la désinstallation	Cette option offre une protection contre les dispositifs non-SAFE. Tant que ce paramètre est activé, il n'est pas possible de désactiver facilement l'administrateur du dispositif.
Inviter l'utilisateur à désinstaller les applications bloquées ?	Si possible, les applications bloquées seront non seulement bloquées mais aussi désinstallées automatiquement. L'utilisateur sera invité à désinstaller les applications bloquées si la désinstallation automatique n'est pas possible.
Système intelligent Blocage des applications	Si la liste blanche est activée, le client MDM Android bloque toutes les applications installées par l'utilisateur. Activez ce paramètre pour bloquer toutes les applications système lançables en mode liste blanche.

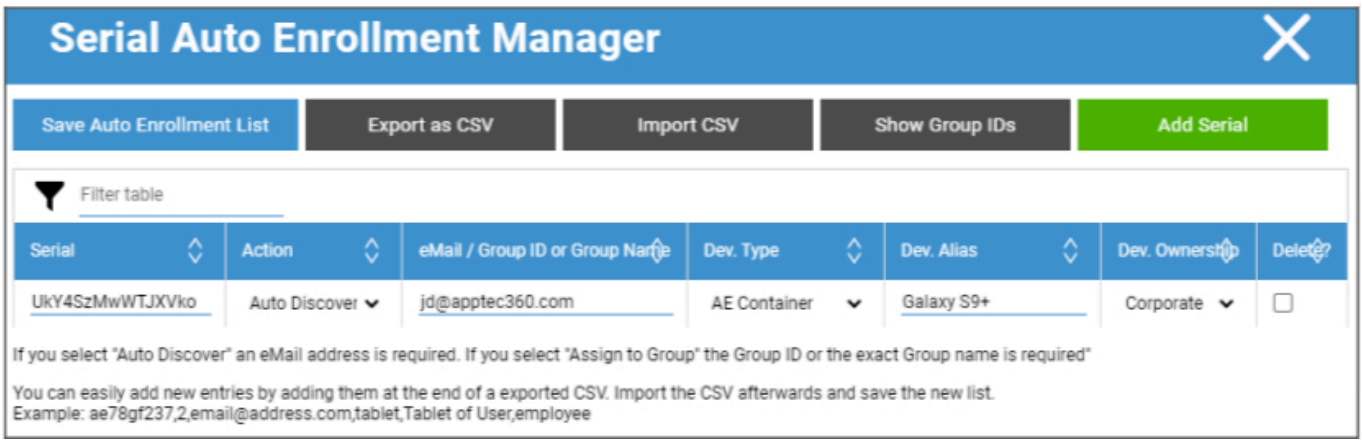
Enrôlement automatique

Ici, vous pouvez activer la fonction d'enrôlement automatique pour enrôler vos appareils automatiquement lorsque le client MDM AppTec360 est ouvert sur l'appareil.

Important : cette méthode d'inscription est obsolète et ne fonctionne plus sous Android 10 ou supérieur. Quoi qu'il en soit, lorsque vous utilisez Android 7 ou une version plus récente, vous devriez inscrire les appareils comme étant entièrement gérés par Android Enterprise. Si vous souhaitez utiliser le conteneur Android Enterprise BYOD et que vous utilisez Android 10 ou une version plus récente, vous devez enregistrer manuellement l'appareil via des informations d'identification, un code QR ou un SMS. Quoi qu'il en soit, la liste d'inscription automatique est toujours utilisée pour automatiser le processus d'inscription, par exemple pour l'inscription AE, l'inscription Knox, etc.

Quoi qu'il en soit, la liste d'inscription automatique est toujours utilisée pour automatiser le processus d'inscription, par exemple pour l'inscription AE, l'inscription Knox, etc.

En cliquant sur "Serial Manager" ou "IMEI Manager", vous pouvez ajouter le numéro de série ou l'IMEI de vos appareils respectivement. Il n'est pas nécessaire de faire les deux pour vos appareils, un seul suffit.



L'**action** définit si les appareils seront inscrits dans le pool, un utilisateur ou un groupe.

Vous pouvez également exporter et importer un fichier .csv et filtrer vos entrées par mots-clés.

Android Enterprise

Ici, vous pouvez configurer Android Enterprise. Cela est nécessaire pour utiliser toutes les fonctionnalités d'Android Enterprise.

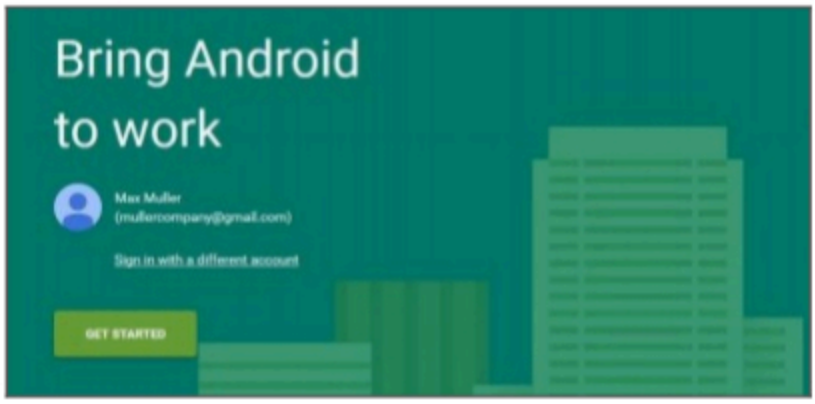
Première méthode : Compte d’entreprise Android (compte Google)

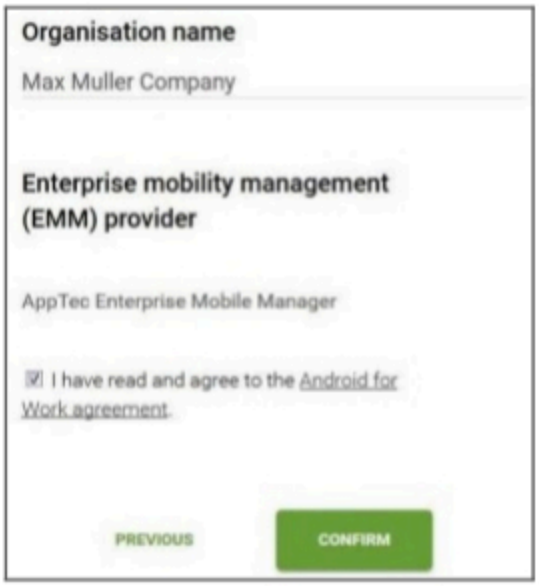
Appuyez d'abord sur "Prepare Setup", puis, après un court instant, sur le bouton "Start Setup".

Vous accéderez ainsi à la page de configuration d'Android Enterprise de Google.

Connectez-vous avec le compte Google que vous souhaitez utiliser, si vous n'êtes pas déjà connecté, et cliquez sur "Commencer".

Vous pouvez maintenant saisir le nom de votre entreprise. Ensuite, cochez la case et appuyez sur "Confirmer"





La dernière étape consiste à terminer l'enregistrement et à revenir à la console. Si tout a fonctionné, cela devrait ressembler à ceci :

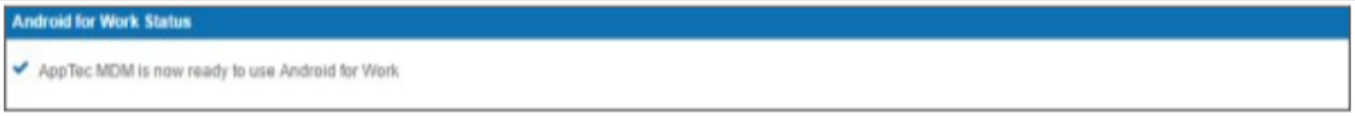
Vous pouvez maintenant commencer à configurer votre Android Enterprise Container.

Deuxième méthode : Compte G-Suite

Cliquez sur "Utiliser G-Suite" et connectez-vous à votre compte Google Admin. Là, vous allez à "Security" -> "Show more" -> "Manage EMM provider for Android" et générez un Token. Remarque : si vous ne voyez pas les paramètres d'entreprise Android dans votre compte G-Suite, vous devez aller dans "Obtenir plus d'applications et de services" et ajouter la gestion des appareils Android. Entrez maintenant le Token et votre domaine primaire dans notre console et cliquez sur "Enregistrer les changements". Lorsque vous avez terminé, cliquez sur "Utiliser le compte d'entreprise Android".

Vous devriez maintenant voir le bouton "Créer un compte de service". Cliquez dessus. Ce processus peut prendre quelques instants.

Si tout a fonctionné, il devrait ressembler à ceci :



Vous pouvez maintenant commencer à configurer votre Android Enterprise Container.

Protection contre la réinitialisation d'usine

Avec la protection contre la réinitialisation d'usine, vous pouvez lier votre appareil à un compte Google de votre choix, ce qui annule également toute liaison existante à un compte Google. Pour utiliser la protection contre la réinitialisation d'usine, vous devez d'abord la configurer ici et l'activer ensuite dans vos profils.

Pour configurer la protection contre la réinitialisation d'usine, cliquez sur "FRP Setup" et suivez les instructions à l'écran.

REMARQUE : Lisez attentivement et suivez les étapes. Nous vous recommandons d'effectuer cette opération dans une nouvelle fenêtre de navigateur incognito afin d'éviter de vous connecter automatiquement au mauvais compte Google. Vous pouvez vous bloquer complètement hors de l'appareil si vous entrez un identifiant erroné ou si vous perdez l'accès au compte Google utilisé !

Inscription à l'AE

Ici, vous pouvez activer le logiciel Android Enterprise Ernollment. L'utilisation de cette méthode inscrira vos appareils dans le mode propriétaire d'appareil d'entreprise Android. Dans ce mode, vous aurez le contrôle total de l'appareil.

Activer l'inscription à l'EA	Active l'inscription AE Attention : Si vous désactivez l'inscription AE, les codes QR existants et les programmateurs NFC déjà configurés cesseront de fonctionner. Si vous réactivez l'inscription AE, vous devrez renvoyer les configurations NFC push / générer de nouveaux codes QR.
Activer la découverte automatique	Lorsqu'un appareil s'inscrit lui-même via "AE Enrollment", le système tente de l'attribuer à un utilisateur sur la base des informations définies dans la liste blanche série / IMEI ("General Settings" > "Android Configuration" > "Auto Enrollment").
Bloquer les dispositifs inconnus	Seuls les appareils qui ont été inscrits sur la liste blanche des numéros de série et des numéros IMEI ("Paramètres généraux" > "Configuration Android" > "Inscription automatique") sont autorisés à s'inscrire.

Note sur les méthodes 1 et 2 : L'écran de bienvenue est le premier écran qui s'affiche après la réinitialisation d'usine. L'apparence peut varier en fonction de la version d'Android et/ou du modèle d'appareil que vous utilisez.

Méthode 1 : Inscription par code QR

(nécessite Android 7.0 ou plus) Nous vous recommandons de toujours utiliser cette méthode si vous utilisez Android 7 ou une version plus récente.

1. Réinitialisation de l'appareil
2. Générer le code QR pour l'inscription en utilisant l'une des deux méthodes suivantes :
   - Cliquez dans "General Settings -> Android Configuration -> AE Enrollment" sur "Generate QR Code". Choisissez si vous souhaitez ignorer le cryptage du stockage et/ou si toutes les applications système doivent être supprimées.
   - (alternativement) Choisissez un appareil existant. Dans la "Vue d'ensemble de l'appareil", cliquez sur le code QR affiché. Choisissez si vous souhaitez ignorer le cryptage du stockage et/ou si toutes les applications système doivent être supprimées.
3. Tapez 6 fois sur l'écran d'accueil de votre appareil. Cela devrait lancer le mode d'inscription QR.
4. Connectez-vous maintenant à un réseau sans fil et attendez un peu que le lecteur de code QR soit installé.
5. Scannez maintenant le code QR
6. C'est tout. Votre appareil est maintenant inscrit dans le mode appareil d'entreprise Android.

- a. Si vous avez utilisé le code QR dans les "Paramètres généraux", vous pouvez trouver votre appareil dans "Pool -> AE Device Owner Devices". (Conseil : il est possible que vous deviez recharger le site pour voir les appareils). Si vous avez coché la case "Activer la découverte automatique", vous le trouverez dans votre utilisateur de découverte automatique.
- Si vous avez utilisé le code QR d'un profil d'appareil existant, l'appareil sera enregistré dans ce profil.

Méthode 2 : Enrôlement NFC

(nécessite NFC et Android 6.0 ou supérieur)

Préparation : Entrez vos informations WiFi dans "General Settings -> Android Configuration -> AE Enrollment -> Data for NFC provisioning" (Paramètres généraux -> Configuration Android -> Enrôlement AE -> Données pour le provisionnement NFC). Utilisez ensuite "Appareil NFC" pour rechercher l'appareil qui deviendra le programmateur. Cet appareil sera utilisé pour envoyer les informations d'inscription aux autres appareils via NFC.

1. Réinitialisation d'usine de votre appareil
2. Ouvrez l'application d'appairage NFC d'AppTec360 sur votre programmateur.
3. Choisissez si vous souhaitez ignorer le cryptage du stockage et/ou si toutes les applications système doivent être supprimées.
4. Tenir les deux appareils dos à dos
5. L'inscription d'Android Enterprise devrait maintenant être plus claire.
6. Vous trouvez maintenant votre appareil dans la console
    - a. Dans le pool, si vous n'avez pas configuré Auto Discover
    - b. Au sein de l'utilisateur, vous avez configuré la fonction Auto Discover
    - c. Conseil : il est possible que vous deviez recharger le site pour voir les appareils.

Méthode 3 : Compte Google

(nécessite Android 5.1 ou plus)

(Remarque : si vous utilisez cette méthode, l'appareil ne sera pas automatiquement inscrit. Vous devez l'inscrire manuellement ou automatiser le processus en utilisant l'inscription automatique).

1. Réinitialisation d'usine de votre appareil
2. Suivez les étapes de configuration jusqu'à ce que vous puissiez vous connecter avec un compte Google.
3. Entrez "afw#apptec" comme nom d'utilisateur/mail
4. Tapez sur "Suivant"

5. Votre appareil est maintenant un appareil Android Enterprise

KNOX Inscription

Ici, vous pouvez activer l'inscription KNOX et trouver les informations nécessaires pour créer un profil d'inscription KNOX dans le portail de déploiement KNOX. Vous avez besoin d'un compte sur le portail de déploiement KNOX pour le configurer et l'utiliser.

(https://www.samsungknox.com/en/knox-deployment-program)

Activer l'inscription KNOX	Active l'inscription KNOX. Attention : Si vous désactivez l'inscription KNOX, les profils MDM existants cesseront de fonctionner. Si vous réactivez KNOX Enrollment, vous devrez mettre à jour le champ "Custom JSON Data" de votre profil MDM.
Activer la découverte automatique	Lorsqu'un appareil s'enregistre via "KNOX Enrollment", le système tente de l'attribuer à un utilisateur sur la base des informations définies dans la liste blanche série / IMEI ("General Settings" > "Android Configuration" > "Auto Enrollment").

1. Connectez-vous au portail d'inscription mobile Samsung KNOX https://eukme.samsungknox.com/itadmin
2. Aller à "Profils MDM"
3. Cliquez sur "Ajouter"
4. Choisissez "Server URI not required for my MDM" et cliquez sur "Next".
5. Créez maintenant un profil avec les informations affichées dans la console de gestion

Ce profil d'inscription KNOX peut être installé directement sur l'appareil par Samsung si vous achetez l'appareil directement auprès de Samsung.

Vous pouvez également télécharger l'application KNOX Deployment, vous connecter avec votre compte KNOX Deployment et envoyer le profil d'enrôlement KNOX via NFC à d'autres appareils.

Si l'appareil a un profil d'inscription KNOX installé, il téléchargera notre application et inscrira l'appareil, s'il dispose d'une connexion Internet fonctionnelle.

L'enrôlement des dispositifs via KNOX Enrollment peut être trouvé dans "Pool -> KNOX Enrollment", ou dans l'utilisateur que vous avez spécifié dans l'Auto Discover.

Zero-Touch

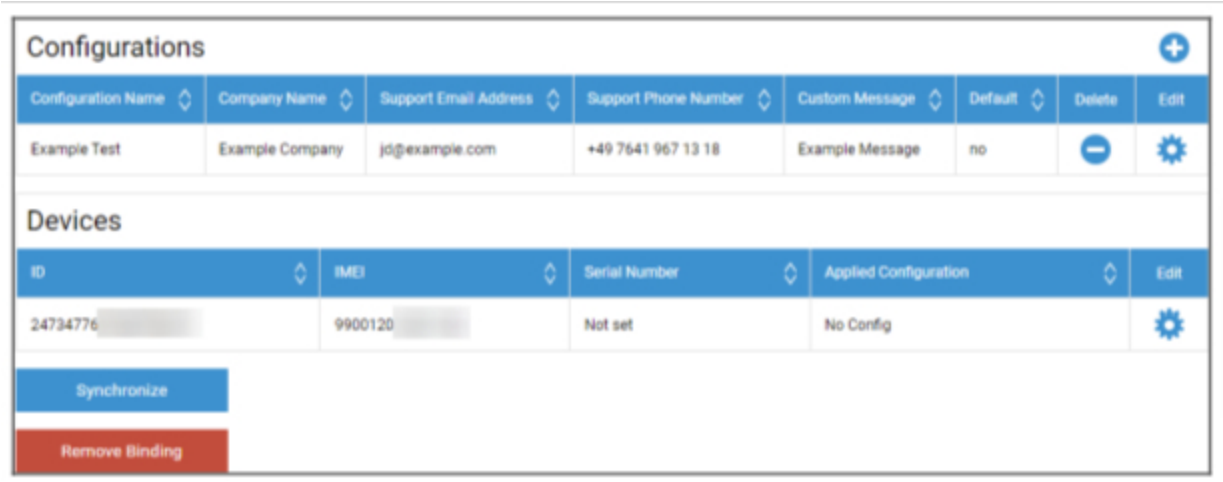
Avec Zero-Touch, vous pouvez facilement enregistrer vos appareils sans avoir à les toucher ou à configurer quoi que ce soit sur l'appareil lui-même. Il suffit de l'allumer, de procéder à la configuration comme d'habitude et l'appareil recevra automatiquement toutes les informations relatives à la configuration et à la connexion au MDM.

Pour utiliser Zero-Touch, vous devez acheter vos appareils auprès d'un revendeur qui supporte Zero-Touch. Le même revendeur crée également un compte pour vous dans le portail Zero-Touch. Contactez votre revendeur pour obtenir plus d'informations sur la procédure ou si vous avez des problèmes pour accéder au portail Zero-Touch.

Cliquez sur "Start Setup" pour démarrer l'installation. Vous serez redirigé vers une page de connexion où vous devrez sélectionner votre compte Google qui a accès au portail Zero-Touch.

NOTE : Il est possible de sélectionner N'IMPORTE QUEL compte. Veillez donc à sélectionner le bon compte dans cette étape. Si vous ne voyez pas vos appareils/configurations, vous avez probablement utilisé le mauvais compte.

Une fois la connexion effectuée, la fenêtre se présente comme suit :



Cliquez sur le "+" pour ajouter une configuration et remplissez les champs tels qu'ils apparaissent à l'écran. Si vous activez la configuration par défaut, elle sera automatiquement attribuée aux nouveaux appareils. La création ou la définition d'une configuration par défaut ne l'affecte pas aux appareils déjà existants.

Si aucune configuration n'est attribuée à un appareil, celui-ci sera configuré comme un appareil normal et ne se connectera pas au MDM. Veillez donc à ce qu'une configuration soit attribuée à vos appareils.

Une fois que vous avez connecté votre compte, que vos appareils sont visibles et qu'une configuration leur a été attribuée, vous pouvez commencer à configurer les appareils.

Vous pouvez ajouter les appareils à la liste d'inscription automatique afin qu'ils soient inscrits automatiquement dans un groupe ou un utilisateur spécifique. Si vous n'avez rien configuré dans la liste d'enrôlement automatique, les appareils seront enrôlés dans le pool.

Configuration de Windows

Configuration de Windows

Ici, vous avez la possibilité d'activer les configurations suivantes sur votre PC Windows 10 :

Connexion instantanée au DM	
Délai de réessai initial	Etablit la première tentative de connexion à l'appareil, cette valeur augmente de manière exponentielle.
Tentatives de connexion	Indique le nombre de tentatives de connexion que le client DM doit effectuer en cas d'erreur de connexion.
Durée maximale de sommeil	Indique le temps de sommeil maximum après une erreur de connexion
Premiers essais de synchronisation	Intervalles au cours desquels l'appareil doit communiquer avec le serveur, après la première connexion
Premier intervalle de réessai	En rapport avec "First Sync Retries" (premiers essais de synchronisation) Ici, les durées sont indiquées en minutes Par exemple, sous "First Sync Retries", la valeur "2" est indiquée et sous "First Retry Interval", la valeur "4 Minutes" est indiquée, de manière à ce que l'appareil communique 2 fois toutes les 4 minutes, après la première connexion.
Secondes tentatives de synchronisation	Intervalles au bout desquels l'appareil doit communiquer avec le serveur, après avoir effectué les "First Sync Retries" (premiers essais de synchronisation)
Intervalle de réessai de deux secondes	Même principe que pour "First Retry Interval" - juste qu'ici, il s'applique à "Second Sync Retries"
Tentatives de synchronisation régulières	Intervalles, fréquence à laquelle l'appareil doit communiquer avec le serveur à l'avenir Valeur par défaut : "Infini" Nous vous recommandons de ne pas modifier cette valeur, car si vous entrez "10", l'appareil communiquera avec le serveur 10x puis s'arrêtera. La communication avec le serveur AppTec360 est donc coupée !
Intervalle de réessai régulier	Même principe que pour "First/Second Retry Interval" - mais ici, les paramètres sont appliqués pour l'avenir.

Intervalle de réessai régulier	Même principe que pour "First/Second Retry Interval" - mais ici, les paramètres sont appliqués pour l'avenir.

ContentBox

Configuration

Vous pouvez ici configurer la boîte de contenu. Vous pouvez placer des fichiers pour des groupes dans la boîte de contenu qui peuvent être accédés avec l'application ContentBox sur l'appareil.

Activer la boîte de contenu	Activer ContentBox. Désactiver cette option si vous n'utilisez pas ContentBox permet d'économiser des ressources sur les machines OnPremise.
Utiliser l'installation externe de ContentBox	La ContentBox peut également fonctionner avec votre propre Nextcloud.
URL	URL complète de l'entité Nextcloud
Utilisateur racine	Utilisateur racine du compte Nextcloud
Mot de passe racine	Mot de passe racine du compte Nextcloud
Autorisations par défaut pour les dossiers de groupe	Autorisations par défaut pour les dossiers de groupe, modifiables individuellement par groupe (dans Mobile Management)
Partager un dossier de groupe avec des sous-groupes	S'il est actif, chaque sous-groupe peut lire tous les dossiers du groupe principal ; il peut également être configuré individuellement pour chaque groupe (gestion mobile).
Autorisations pour les sous-groupes	Autorisations pour les sous-groupes peut être configuré individuellement pour chaque groupe (Mobile Management)
Permettre le partage	Permet à l'utilisateur de partager le contenu via des liens ; peut être configuré individuellement pour chaque groupe.
Taille maximale du fichier téléchargé en Mo	Taille maximale d'un fichier Standard : 512 Mo Configuration maximale : 2048
Références WebDAV	
URL WebDAV	Vous pouvez également ouvrir la ContentBox avec WebDAV. Ne supprimez en aucun cas les dossiers suivants : /apptecgroups /apptecgroups/AppTecGroup-X
Utilisateur racine	Nom de l'utilisateur racine
Mot de passe	Mot de passe de l'utilisateur racine

La synchronisation avec la ContentBox se fait automatiquement. Vous pouvez cependant effectuer une synchronisation manuelle avec "Synchroniser ContentBox".

En outre, vous pouvez ici activer/désactiver la ContentBox sur chaque appareil individuel.

Ceci n'est pertinent que si vous n'avez pas acquis de licence supplémentaire pour le ContentBox. Vous avez alors accès à 25 appareils avec lesquels vous pouvez tester le ContentBox - ici, vous pouvez activer ceci pour les appareils respectifs.

Configuration LDAP

Vue d’ensemble de LDAP

Vous pouvez ici établir une connexion avec votre Active Directory via LDAP pour importer en masse des utilisateurs et des groupes. La synchronisation doit être effectuée manuellement. Vous pouvez configurer plusieurs connexions LDAP vers différents systèmes ou avec différentes configurations/filtres.

Nom du serveur	Nom d'affichage du serveur
Type	Actuellement, seuls les Active Directories qui supportent LDAP sont pris en charge.
Domaine LDAP	Le domaine LDAP primaire (par exemple, example.com)
Hôte LDAP	Nécessaire uniquement si l'hôte LDAP n'est pas accessible dans le domaine LDAP donné.
Port	Laissez vide pour utiliser le port standard (389 ou 636 pour SSL)
Nom d'utilisateur	Par exemple : CN=John,OU=Users,DC=EXAMPLE,DC=COM Remarque : la plupart des systèmes exigent que le nom d'utilisateur soit dans ce format et n'acceptent pas "John" comme nom d'utilisateur.
Mot de passe	
Confirmer le mot de passe	
Sécurité des connexions	Remarque : lors de l'utilisation de SSL ou TLS, le certificat de l'Active Directory sera vérifié. S'il est auto-signé, vous devez ajouter l'autorité de certification racine au stockage de confiance de la machine sur site. Si vous êtes dans le nuage, l'Active Directory doit fournir un certificat de confiance, sinon la connexion ne fonctionnera que sans cryptage.
Synchronisation automatique.	Active la synchronisation automatique du répertoire LDAP dans l'intervalle de temps spécifié dans les paramètres généraux LDAP.
Base DN	Si vous ne souhaitez pas synchroniser l'ensemble du répertoire, vous pouvez spécifier une OU ici, par exemple OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM.
Membre de	Tous les utilisateurs importés seront ajoutés au groupe sélectionné.
Uniquement les utilisateurs activés ?	Lorsque cette option est activée, l'attribut userAccountControl sera pris en compte, les utilisateurs ne possédant pas cet attribut ne seront pas importés.

Filtre LDAP	Vous pouvez utiliser le filtre LDAP pour filtrer les utilisateurs qui seront importés.
Filtre Regex	Vous pouvez utiliser le filtre Regex pour filtrer les utilisateurs qui seront importés.
Test de connexion	Teste la connexion lors de l'enregistrement de la configuration
Réinitialiser la structure des répertoires lors de la synchronisation ?	Si cette option est activée, toutes les entrées LDAP seront replacées à leur emplacement d'origine dans l'arborescence LDAP. Il est recommandé de l'activer.
Réimporter des utilisateurs et des groupes supprimés ?	Lorsque cette option est activée, les utilisateurs et les groupes qui ont été supprimés sont recréés. Il est recommandé de l'activer.
Synchroniser les suppressions ?	Lorsque cette option est activée, les groupes et les utilisateurs sont supprimés lorsqu'ils sont supprimés sur le serveur LDAP. Les appareils des utilisateurs supprimés seront également supprimés.

Sous la liste de vos configurations LDAP, vous pouvez définir la période pendant laquelle le système se synchronise automatiquement. N'utilise pour la synchronisation automatique que les configurations LDAP pour lesquelles l'option correspondante est activée.

Gestion des applications

App DB interne

Android

Ici, vous pouvez télécharger les applications Android que votre entreprise a développées et les distribuer ultérieurement dans la gestion mobile dans des profils d'appareils ou de groupes.

Veuillez noter que nous conseillons de ne distribuer de cette manière que les applications qui ne sont pas disponibles dans le Google Play Store.

Cliquez sur le "+" pour télécharger l'APK d'une application que vous souhaitez télécharger. Seul le format APK est actuellement pris en charge.

La limite de téléchargement sur les appliances OnPremise peut être augmentée à l'étape 3 de la configuration de l'appliance. Si vous souhaitez augmenter la limite de téléchargement dans le nuage, veuillez contacter le service d'assistance pour plus d'informations.

Sachez que les APK sont généralement un peu plus petits que leur contenu. Il est possible qu'un téléchargement échoue pour cette raison, car l'APK est décompressé au cours du processus. Par exemple, il est possible qu'un APK de 95MB échoue avec une limite de téléchargement de 100MB. Dans ce cas, augmentez la limite de téléchargement comme indiqué ci-dessus.

Nous vous conseillons également de déplacer manuellement l'APK vers un appareil de test (par exemple via USB) et d'essayer de l'installer manuellement avec l'application Fichiers de l'appareil. Si cela ne fonctionne pas pour une raison quelconque, cela échouera également via MDM.

Mise à jour de l'objectif

La fonction "Cible de mise à jour" vous permet de choisir la version d'une application à installer ou la version d'une application à mettre à jour si vous avez activé l'option "Tenir à jour" pour une application.

Si vous n'avez pas sélectionné de cible de mise à jour, la version la plus récente sera utilisée.

Gardez à l'esprit qu'Android ne peut pas rétrograder les applications. Sachez également que le "code de version" détermine si une version est supérieure, inférieure ou identique. Veillez donc à augmenter correctement cette version dans votre application lorsque vous créez une mise à jour.

iOS

Ici, vous pouvez télécharger les applications iOS que vous avez développées et les distribuer plus tard dans la gestion mobile dans votre profil d'appareil ou de groupe.

Cliquez sur le "+" pour télécharger l'API d'une application que vous souhaitez télécharger. Pour l'instant, seul le format IPA est pris en charge.

La limite de téléchargement sur les appliances OnPremise peut être augmentée à l'étape 3 de la configuration de l'appliance. Si vous souhaitez augmenter la limite de téléchargement dans le nuage, veuillez contacter le service d'assistance pour plus d'informations.

Mise à jour de l'objectif

La fonction "Cible de mise à jour" vous permet de choisir la version d'une application à installer ou la version d'une application à mettre à jour si vous avez activé l'option "Tenir à jour" pour une application.

Si vous n'avez pas sélectionné de cible de mise à jour, la version la plus récente sera utilisée.

MacOS

Ici, vous pouvez télécharger les applications MacOS que vous avez développées et les distribuer plus tard dans la gestion mobile dans votre profil d'appareil ou de groupe.

Cliquez sur le "+" pour télécharger le PKG d'une application que vous souhaitez télécharger. Pour l'instant, seul le format PKG est pris en charge.

La limite de téléchargement sur les appliances OnPremise peut être augmentée à l'étape 3 de la configuration de l'appliance. Si vous souhaitez augmenter la limite de téléchargement dans le nuage, veuillez contacter le service d'assistance pour plus d'informations.

Mise à jour de l'objectif

La fonction "Cible de mise à jour" vous permet de choisir la version d'une application qui doit être installée ou la version d'une application qui doit être mise à jour si vous avez activé l'option "Tenir à jour" pour une application.

Si vous n'avez pas sélectionné de cible de mise à jour, la version la plus récente sera utilisée.

Windows 10

Ici, vous pouvez télécharger les applications Windows 10 et les distribuer plus tard dans la gestion mobile dans votre profil d'appareil ou de groupe.

Cliquez sur le "+" pour télécharger l'APPX, l'APPXBUNDLE ou le MSI d'une application que vous souhaitez télécharger. Seuls les formats APPX, APPXBUNDLE ou MSI sont pris en charge pour l'instant.

Vous pouvez également télécharger et définir des dépendances pour une application, qui seront automatiquement distribuées et installées avant l'installation de l'application souhaitée.

La limite de téléchargement sur les appliances OnPremise peut être augmentée à l'étape 3 de la configuration de l'appliance. Si vous souhaitez augmenter la limite de téléchargement dans le nuage, veuillez contacter le service d'assistance pour plus d'informations.

Mise à jour de l'objectif

La fonction "Cible de mise à jour" vous permet de choisir la version d'une application qui doit être installée ou la version d'une application qui doit être mise à jour si vous avez activé l'option "Tenir à jour" pour une application.

Si vous n'avez pas sélectionné de cible de mise à jour, la version la plus récente sera utilisée.

Paquet Win32 (.exe)

Vous pouvez également distribuer des fichiers .exe/installateurs sur vos appareils.

Nom du paquet	Le nom qui sera affiché dans le MDM
Description	Description affichée dans le MDM
Fichier de paquets	Seuls les fichiers .zip sont autorisés. Placez les fichiers que vous souhaitez déployer dans ce fichier zip.
Contexte de déploiement	**Système**: La commande d'installation s'exécute avec les privilèges du système, qui sont plus élevés que ceux de l'utilisateur. De plus, lorsque vous utilisez "System", le processus n'a pas d'interface utilisateur, il est donc silencieux et le profil de l'utilisateur, par exemple les variables d'environnement telles que %AppDat%, n'est pas accessible. **Utilisateur**: La commande d'installation a accès au profil de l'utilisateur et peut afficher l'interface utilisateur si nécessaire. Remarque : certains processus peuvent ne fonctionner que dans un seul contexte. Par exemple, si un logiciel s'installe dans AppData, il ne fonctionnera que si vous sélectionnez "Utilisateur"
Commande d'installation	La commande utilisée pour installer le programme. Par exemple, la commande d'installation d'un fichier zip contenant "setup.exe" dans sa racine, qui prend en charge le paramètre "/s" pour une installation silencieuse, serait "setup.exe /s". N'oubliez pas que les paramètres peuvent varier d'un logiciel à l'autre.
Commande de désinstallation	La commande à exécuter pour désinstaller le logiciel via MDM. En général, elle pointe vers le programme de désinstallation. Par exemple, "C:\NProgram Files\NExampleSoftware\Nuninstall.exe".
Exigences	
Remarque : toutes les conditions requises doivent être remplies pour que le logiciel puisse être installé. Dans le cas contraire, il ne sera pas installé. Certains champs peuvent être obligatoires. Si aucune valeur n'est définie pour une exigence, celle-ci sera ignorée.	
Architecture du système d'exploitation	Architecture du système d'exploitation
Version minimale du système d'exploitation	Version minimale du système d'exploitation
Espace disque libre minimum (MB)	Espace disque libre minimum (MB)

Mémoire physique minimale (Mo)	Mémoire physique minimale (Mo)
Nombre minimal de processeurs logiques	Nombre minimal de processeurs logiques
Vitesse minimale du CPU (MHz)	Vitesse minimale du CPU (MHz)
Exigences supplémentaires	Vous pouvez également définir manuellement des règles ou télécharger un script pour effectuer des contrôles supplémentaires si vous le souhaitez.
Règles de détection	
Méthode de détection	Vous pouvez définir ici comment détecter si l'application est installée sur l'appareil. Les commandes d'installation ne seront exécutées que si ces règles détectent que l'application n'est PAS installée. Les commandes de désinstallation ne sont exécutées que lorsque ces règles détectent que l'application n'est pas installée. **Définir manuellement des règles**: Vous permet de définir manuellement une ou plusieurs règles pour vérifier, par exemple, la présence d'un certain fichier, dossier, MSI ou clé de registre. Si toutes les règles de détection données sont vraies, l'application sera considérée comme présente. **Utiliser un script**: Téléchargez votre propre script avec vos propres vérifications. Si le script renvoie "$TRUE", l'application sera considérée comme présente.
Règles de détection	

Paramètres de l’application

Réglages de l’application iOS

Vous pouvez définir ici les paramètres par défaut pour l'ajout d'une application à la liste des applications obligatoires ou à la liste des applications d'entreprise.

Remarque : cette option permet uniquement de définir ce qui est sélectionné par défaut lors de l'ajout d'applications. Cela ne modifie PAS les paramètres existants pour les applications qui sont déjà ajoutées dans le magasin d'applications obligatoires ou d'entreprise.

Restez informé	Maintient automatiquement l'application à jour. Veuillez noter qu'il peut s'écouler jusqu'à 7 jours après la publication d'une mise à jour avant que l'application ne soit mise à jour.
Dépassement en l'absence de gestion	Si une application est déjà installée comme non gérée (par l'utilisateur), l'application sera remplacée et gérée par le MDM.
Supprimer l'application lorsque le profil MDM est supprimé	Désinstalle l'application lorsque le MDM est supprimé.
Empêcher la sauvegarde des données de l'application	Empêche la sauvegarde des données de l'application.

Paramètres de l’application Android

Vous pouvez définir ici les paramètres par défaut pour l'ajout d'une application à la liste des applications obligatoires ou à la liste des applications d'entreprise.

Note : Ceci ne fait que définir ce qui est sélectionné par défaut lors de l'ajout. Cela ne modifie PAS les paramètres des applications déjà ajoutées dans le magasin d'applications obligatoires ou d'entreprise.

Restez informé	Maintient automatiquement l'application à jour. Uniquement disponible pour les applications InHouse.
Mise à jour du client EMM AppTec360 contrôlé	Si cette option est activée, les administrateurs peuvent spécifier la cible de mise à jour pour le client AppTec360 EMM. Une liste de toutes les versions disponibles du client AppTec360 EMM sera affichée dans "General Settings" → "App Management" → "In-House App DB" → "Android".

Applications tierces

Android

Ici, vous pouvez définir votre code d'activation pour Ikarus.

Réglez cette option sur "Utiliser le code d'activation" et entrez votre code d'activation ici.

Remarque: Après avoir saisi le code et sauvegardé, le code n'est pas encore ajouté au profil envoyé à l'appareil. Vous devez modifier votre profil pour que le code soit ajouté au profil. Par exemple, changer n'importe quel commutateur du profil de désactivé → activé → désactivé - Enregistrer → Attribuer maintenant.

iOS

Vous pouvez ici saisir votre licence SecurePIM. Après avoir saisi la licence, cliquez sur "Enregistrer les modifications" et vous pourrez utiliser les options de SecurePIM.

VPP / KNOX Premium

Le programme d'achat en volume (VPP) d'Apple vous permet de distribuer facilement des applications payantes et gratuites sur vos appareils. Ceci est fortement recommandé car vous n'avez pas besoin d'un identifiant Apple sur les appareils, les utilisateurs n'ont pas à confirmer l'installation (supervisée), les utilisateurs n'auront pas à entrer le mot de passe de l'identifiant Apple et vous pouvez facilement distribuer des applications payantes sans les acheter à nouveau sur chaque appareil.

Pour utiliser le VPP, vous devez vous enregistrer dans l'Apple Business Manager.

Licences VPP

Vous pouvez ici avoir une vue d'ensemble de vos applications VPP, du nombre de licences utilisées et du nombre de licences disponibles.

En cliquant sur la roue, vous verrez quels sont les appareils auxquels une licence a été attribuée et quel est le statut de cette attribution.

En cliquant sur le bouton, le cache VPP est actualisé et les licences attribuées dans le MDM sont comparées aux licences attribuées du côté d'Apple. Cela peut résoudre les problèmes de licence dans certains cas.

Jeton VPP

Vous pouvez y télécharger votre jeton VPP, qui se trouve dans l'Apple Business Manager sous Réglages → Apps & Livres. Vous pouvez télécharger plusieurs jetons VPP.

Vous pouvez renouveler un token en téléchargeant simplement un nouveau token dans l'Apple Business Manager, en cliquant sur la roue "Modifier" et en téléchargeant le nouveau token.

Le "Mode VPP" détermine la manière dont l'attribution de la licence est gérée. En fonction de votre scénario, vous devez utiliser différents modes :

L'option "Device based" doit être utilisée lors de l'enregistrement des appareils via un code QR, un lien, Apple Configurator ou DEP.

La mention "basé sur l'utilisateur" est requise si les dispositifs sont inscrits avec l'inscription de l'utilisateur ou en tant qu'iPad partagé.

Si vous activez la "Gestion automatisée des licences", les utilisateurs qui sont déplacés d'un groupe à un autre se verront automatiquement attribuer des licences Apple VPP en fonction du profil du groupe vers lequel ils sont déplacés.

Les licences Apple VPP existantes du groupe qu'ils ont quitté ne seront pas révoquées.

Les nouveaux utilisateurs ajoutés à un groupe se verront automatiquement attribuer des licences Apple VPP en fonction du profil du groupe concerné.

Clé KNOX Premium

Vous pouvez y saisir votre clé KNOX Premium pour utiliser le conteneur KNOX de Samsung.

Sachez que cette fonction n'est plus prise en charge depuis Android 10. Utilisez plutôt l'Android Enterprise Container.

Paramètres de l’App Store

Région et langue

Vous pouvez ici définir la langue et la région par défaut pour la recherche d'applications dans la gestion des applications.

Sachez que les paramètres d'iTunes définissent également la manière dont le système recueille des informations sur certaines applications. Si vous rencontrez des applications dans vos listes qui sont affichées d'une manière étrange (par exemple, une icône manquante), vous avez peut-être défini une région où l'application en question n'est pas disponible.

AE Play Store

Vous trouverez ici toutes les options du Play Store pour les appareils d'entreprise Android afin d'approuver les applications, de télécharger vos propres applications sur le Play Store ou de créer vos propres applications Web.

Applications approuvées

Vous pouvez ici avoir un aperçu de toutes les applications que vous avez approuvées.

Apps Play Store

Cela chargera une iFrame affichant le Play Store. Recherchez l'application de votre choix, cliquez dessus et approuvez-la. Lors de l'approbation de l'application, vous pouvez également définir que l'approbation sera révoquée si les autorisations requises changent. Nous recommandons de laisser ces paramètres par défaut lors de l'approbation des applications.

Une fois qu'une application a été approuvée, vous pouvez l'ajouter à vos profils.

Le bouton "Approuver" se transformera en "Révoquer l'approbation" après l'approbation, afin que vous puissiez toujours supprimer les applications si vous n'en avez plus besoin.

Applications privées

Ici, vous pouvez télécharger votre propre application en tant qu'application privée sur le Google Play Store. Cela vous permet de distribuer l'application par l'intermédiaire des services Google et de la mettre à jour par leur intermédiaire. Cela présente également l'avantage de permettre l'installation de vos propres applications sans la confirmation de l'utilisateur qui est normalement nécessaire.

Applications Web

Ici, vous pouvez créer des applications Web, qui sont des liens vers certaines pages Web qui peuvent être assignées comme des applications.

Vous pouvez également lui attribuer une icône personnalisée et définir plus précisément son mode d'affichage.

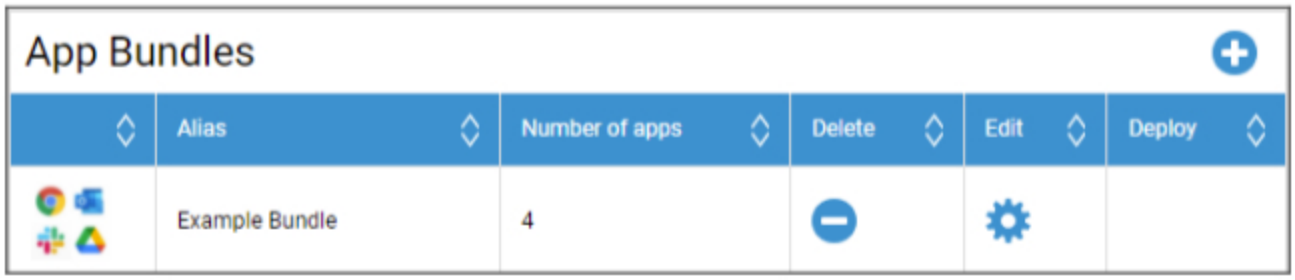
Disposition du magasin

La présentation de la boutique définit la manière dont les applications sont affichées dans la boutique Play Store, ou si elles sont affichées du tout.

Gardez à l'esprit que si vous souhaitez afficher les applications du Play Store que l'utilisateur doit installer manuellement, celles-ci doivent être ajoutées ici dans la mise en page. **ET** dans le profil vers l'Enterprise Play Store. Si vous n'ajoutez une application qu'à l'une d'entre elles, elle ne sera pas affichée.

Offre groupée d'applications

Avec les App Bundles, vous pouvez définir des groupes d'applications qui peuvent être assignés à des profils d'appareils ou de groupes en un seul clic.



Cliquez sur le "+" pour créer un nouvel ensemble d'applications. Après avoir créé un App Bundle, vous pouvez cliquer sur "Edit" pour ajouter des applications de différentes sources à l'App Bundle.

Une offre groupée peut être ajoutée aux profils comme n'importe quelle autre application. Lorsque vous ajoutez des applications, vous disposez d'un onglet supplémentaire appelé "App Bundles" dans lequel vous avez vos Bundles.

Si vous apportez une modification à un App Bundle, un bouton dans la colonne "Deploy" apparaîtra. Cela vous permettra d'appliquer ces modifications à tous les profils contenant cet ensemble. Gardez donc à l'esprit que vous devez effectuer cette opération manuellement après avoir ajouté ou supprimé des applications dans un ensemble.

Télécommande

TeamViewer

Connecteur TeamViewer

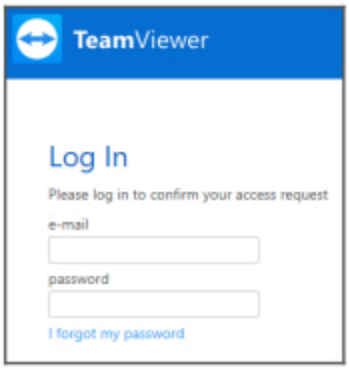
Note : Dans l'essai gratuit de notre version cloud, vous ne pouvez pas connecter votre compte TeamViewer. Un compte de démonstration gratuit vous sera automatiquement attribué.

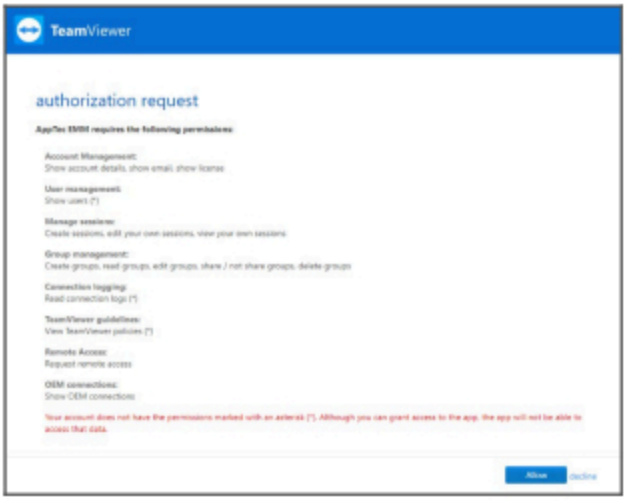
Allez dans Paramètres généraux -> Contrôle à distance -> TeamViewer. Ici, vous pouvez lier votre compte TeamViewer à la console ou voir des informations sur votre compte actuellement connecté. Vous pouvez également consulter toutes les sessions actives en vous rendant dans la rubrique "Sessions actives".

Pour lier votre compte, cliquez sur "Start Setup".

Cela vous amènera à une nouvelle page où vous devrez vous connecter avec votre compte TeamViewer.

Après vous être connecté, vous devez autoriser le MDM AppTec360 à utiliser ce compte. Après confirmation, vous devez attendre quelques secondes et le compte est connecté.


TeamViewer
Log In
Please log in to confirm your access request
e-mail
password
I forgot my password


TeamViewer
authorization request

Installer TeamViewer QuickSupport

Ajoutez l'application "TeamViewer QuickSupport" aux applications obligatoires de votre profil d'appareil ou de groupe et cliquez sur "Attribuer maintenant". Attendez que l'application soit installée sur l'appareil.

Si vous essayez d'accéder à un appareil sur lequel l'application n'est pas installée, elle sera installée ou il vous sera demandé de l'installer, en fonction de la configuration de l'appareil.

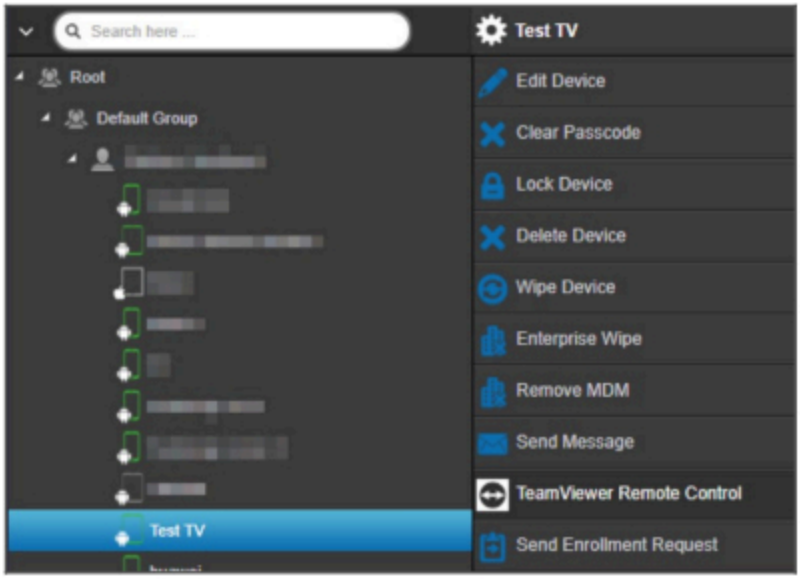
Télécommandez votre appareil

Pour contrôler votre appareil à distance, sélectionnez l'appareil, cliquez sur la roue et choisissez "TeamViewer Remote Control"

S'il existe déjà une session active, vous pouvez soit utiliser l'ancienne session, soit en créer une nouvelle.

Confirmez que vous souhaitez créer une nouvelle session TeamViewer.

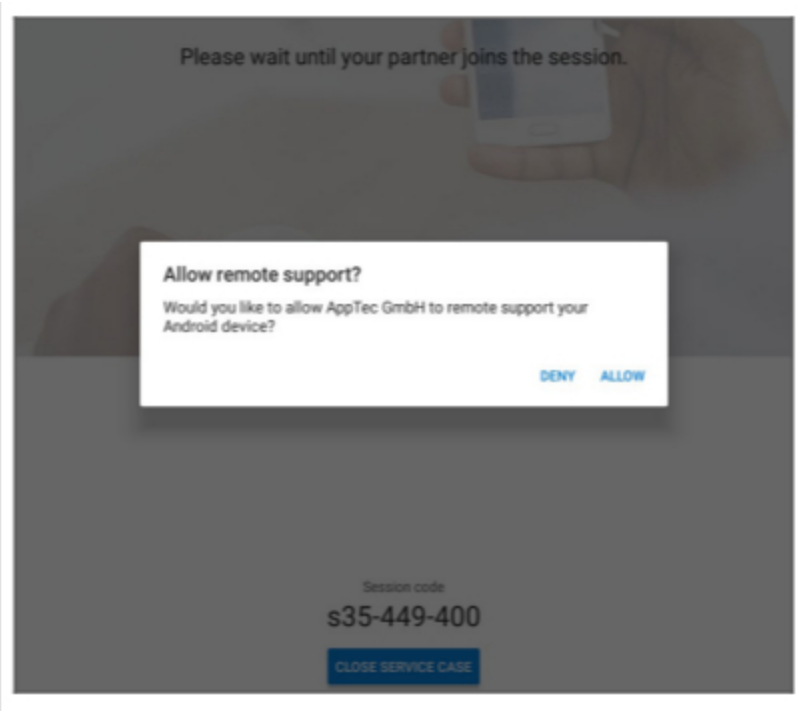
Après quelques secondes, vous obtiendrez un lien pour votre session TeamViewer. Vous pouvez cliquer sur "Démarrer" pour ouvrir ce lien dans une nouvelle fenêtre.


Search here ...
Root
Default Group
Test TV
Test TV
Edit Device
Clear Passcode
Lock Device
Delete Device
Wipe Device
Enterprise Wipe
Remove MDM
Send Message
TeamViewer Remote Control
Send Enrollment Request


Remote Control
Supporter URL: https://get.teamviewer.com/v13/
Click on "Start" to open the TeamViewer Remote Control in a new window.
Cancel
Start

Ce lien ouvrira votre TeamViewer installé et vous connectera à votre appareil.

Vous devez maintenant confirmer la connexion sur l'appareil lui-même pour le contrôler à distance.

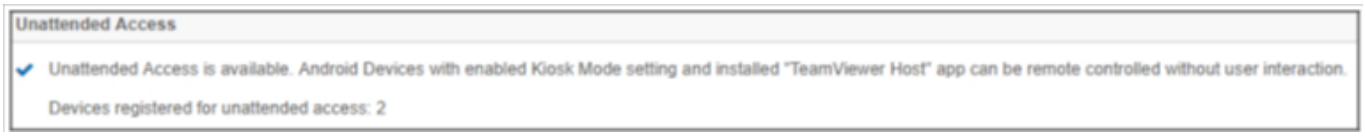


Si vous utilisez iOS, vous obtiendrez un message dans le Client MDM AppTec360. Grâce à ce lien, l'appareil rejoindra la session à distance. Selon les paramètres de notification de l'appareil, il est possible que vous ne receviez pas de notification et que vous deviez ouvrir le client MDM AppTec360 manuellement.

Sur certains appareils Android (par exemple Samsung), il est nécessaire d'installer une application supplémentaire en tant qu'addon. L'application TeamViewer sur l'appareil vous en informera, si cela est nécessaire sur votre appareil.

Accès sans surveillance

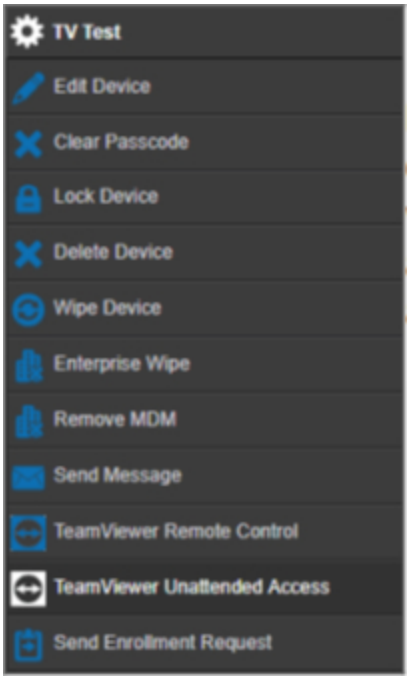
Remarque : l'accès sans surveillance n'est possible que sur les appareils Android.



Vous ne pouvez vous connecter à vos appareils, sans accepter la connexion sur l'appareil, que si votre compte TeamViewer utilise une licence "Tensor" ou "Corporate".

Vous pouvez le vérifier, après avoir connecté votre compte, dans les "Paramètres généraux"

Pour utiliser l'accès sans surveillance, vous devez installer l'application "TeamViewer Host" et activer "Enable Unattended Access" sous "Kiosk Mode & Launcher" dans votre profil. Veuillez noter que cela n'est possible que si vous utilisez le mode kiosque.



Vous pouvez maintenant sélectionner l'accès sans surveillance en sélectionnant votre appareil et en cliquant sur la roue. Cela vous connectera à votre appareil sans qu'il soit nécessaire de le confirmer sur l'appareil lui-même. Sachez qu'il peut s'écouler quelques instants avant que vous n'obteniez le lien d'accès à votre appareil.

Splashtop

Si vous activez l'option Splashtop, les options de configuration de Splashtop s'affichent dans vos profils.

Pour utiliser Splashtop, vous devez définir Splashtop Streamer (com.splashtop.streamer.csrs) comme application obligatoire dans votre profil. Ensuite, vous pouvez activer la configuration de Splashtop dans votre profil dans "Contrôle à distance". L'activation de cette option permet de configurer l'application Splashtop Streamer. Si vous utilisez Splashtop Streamer mais pas en combinaison avec le MDM, vous devez laisser cette option désactivée.

Dans votre profil, sous "Télécommande", vous devez également définir un code de déploiement. Allez sur https://my.splashtop.com et connectez-vous à votre compte Splashtop. Cliquez sur "Ajouter un ordinateur" et copiez le code de déploiement à 12 chiffres de la page qui s'affiche.

Sans le code de déploiement, le contrôle à distance n'est PAS possible.

Ensuite, vous pouvez faire un clic droit sur votre appareil et démarrer une session à distance en cliquant sur "Splashtop Remote Control".

Gestion des cartes SIM

Importation en masse de CSV

Cette fonction permet d'avoir une vue d'ensemble des cartes Sim attribuées et de toutes les informations les concernant. Cela vous permet d'avoir toutes les informations, non seulement sur vos appareils mais aussi sur vos cartes Sim dans un seul système.

NOTE : IL S'AGIT D'UN MANUEL DE GESTION/DOCUMENTATION : Il s'agit d'une gestion/documentation manuelle. Il n'est pas possible d'obtenir ces données automatiquement à partir des appareils en raison des mécanismes de confidentialité/sécurité des systèmes d'exploitation.

Vous pouvez également importer cette liste au format CSV.

Transporteur et tarif

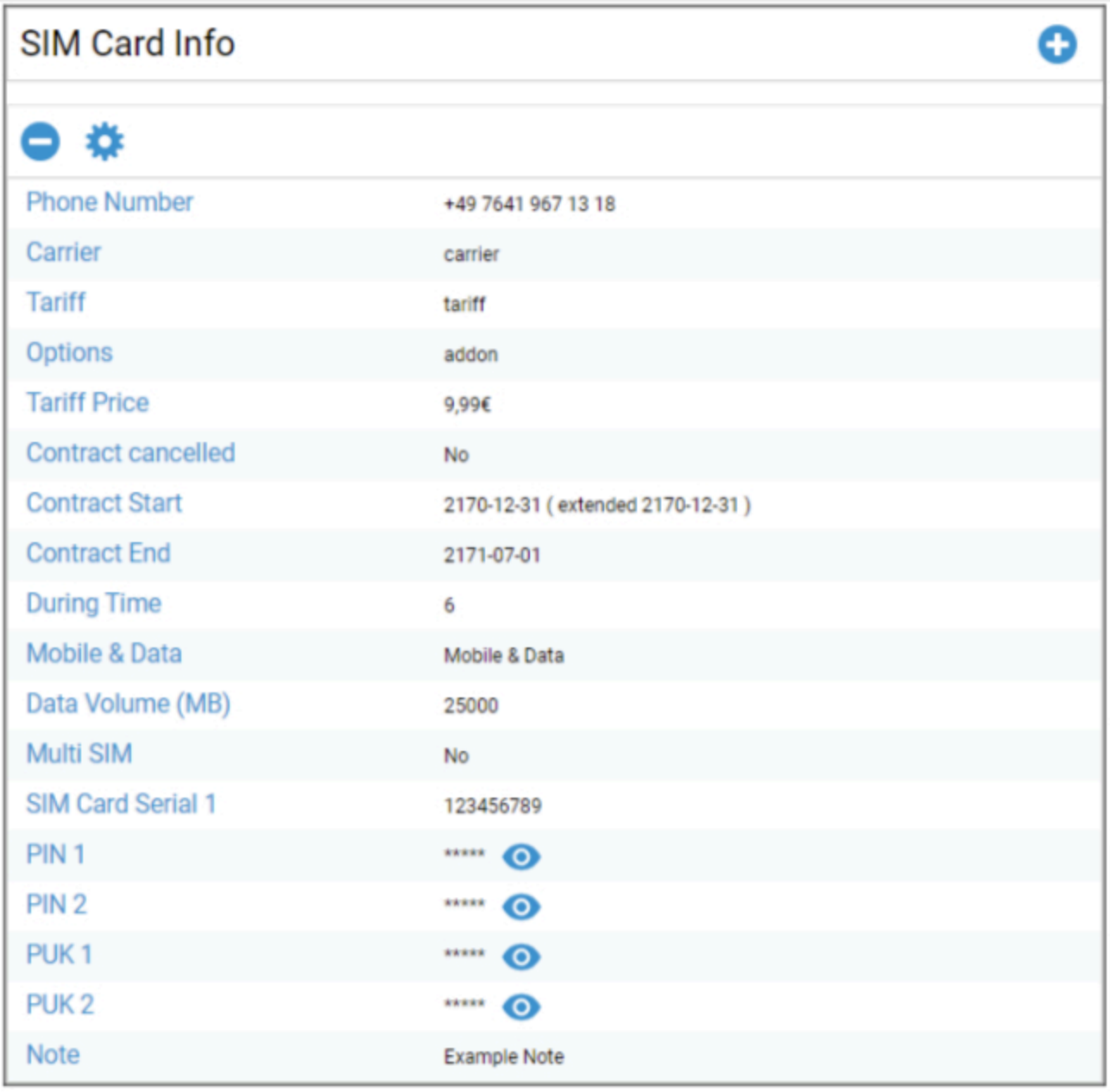
Pour ajouter une carte Sim, cliquez d'abord sur le bouton permettant d'ajouter un ou plusieurs opérateurs.

Cliquez ensuite sur le "+" dans "Informations tarifaires" pour ajouter un tarif à un transporteur.

En option, vous pouvez ajouter des compléments optionnels ci-dessous si vous avez quelque chose comme ça.

Il prépare tout ce dont vous avez besoin pour ajouter une carte Sim. Les cartes Sim sont actuellement attribuées à un utilisateur. Allez donc dans la Gestion mobile, sélectionnez un utilisateur et allez à "Aperçu de la carte Sim".

Vous voyez ici les cartes Sim de cet utilisateur. S'il y en a un, vous pouvez le modifier ou le supprimer. Les utilisateurs peuvent avoir plusieurs cartes Sim.

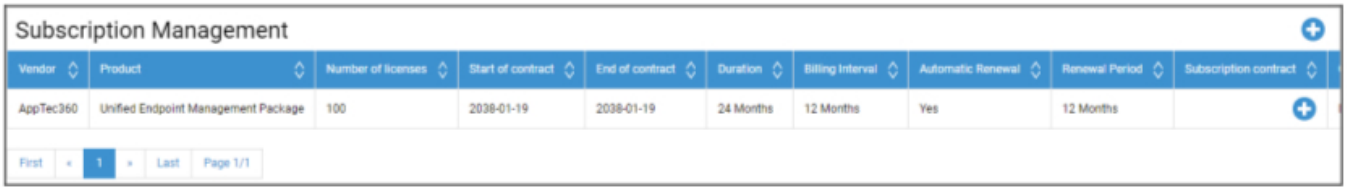


Cliquez sur le "+" pour ajouter une carte Sim et ajoutez toutes les informations dont vous avez besoin. Ces cartes Sim seront également répertoriées dans la liste de toutes vos cartes Sim dans Paramètres généraux → Gestion des cartes Sim.

Gestion des abonnements

Gestion des abonnements

Vous pouvez y documenter les abonnements en cours, leurs détails et également stocker différents fichiers, par exemple un contrat signé, une lettre de résiliation, etc. Vous pouvez également mettre en place des rappels qui vous rappellent par courrier avant la fin de l'abonnement et qui le prolongent éventuellement automatiquement.



Cliquez sur le "+" en haut pour ajouter un abonnement. Vous pouvez ajouter autant d'abonnements que vous le souhaitez.

Cliquez sur le "+" dans les différents champs pour télécharger des fichiers concernant cet abonnement. Vous pouvez techniquement télécharger n'importe quel type de fichier, mais sachez que tous les types de fichiers ne peuvent pas être visualisés dans le navigateur.

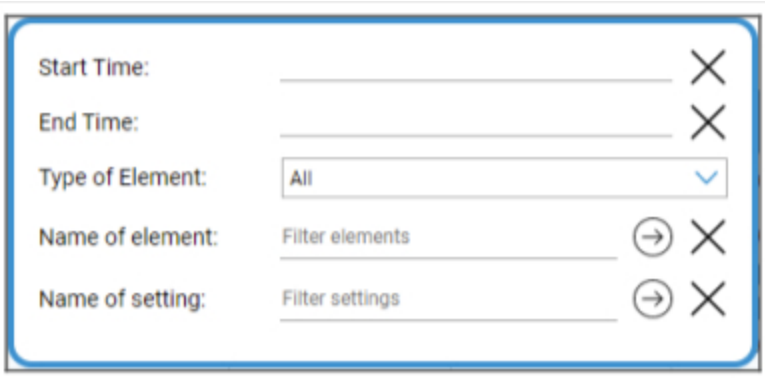
Journal d’audit général

Journal d’audit

Vous disposez ici d'un journal d'audit général qui indique toutes les modifications apportées. Alors que le journal d'audit d'un utilisateur ou d'un groupe n'affiche que les modifications relatives à cet utilisateur ou à ce groupe, ce journal affiche TOUT changement effectué n'importe où dans la console.

Vous pouvez voir ce qui a été modifié, par qui, quand et où. Dans certains cas, vous pouvez également étendre l'entrée pour voir plus de détails.

Il est possible de cliquer sur l'utilisateur ou sur l'entrée dans "Chemin / Type" pour accéder à l'endroit où la modification a été effectuée.



En haut à droite, vous pouvez également définir un filtre qui peut aider à repérer certains changements dans un environnement où de nombreux changements se produisent.

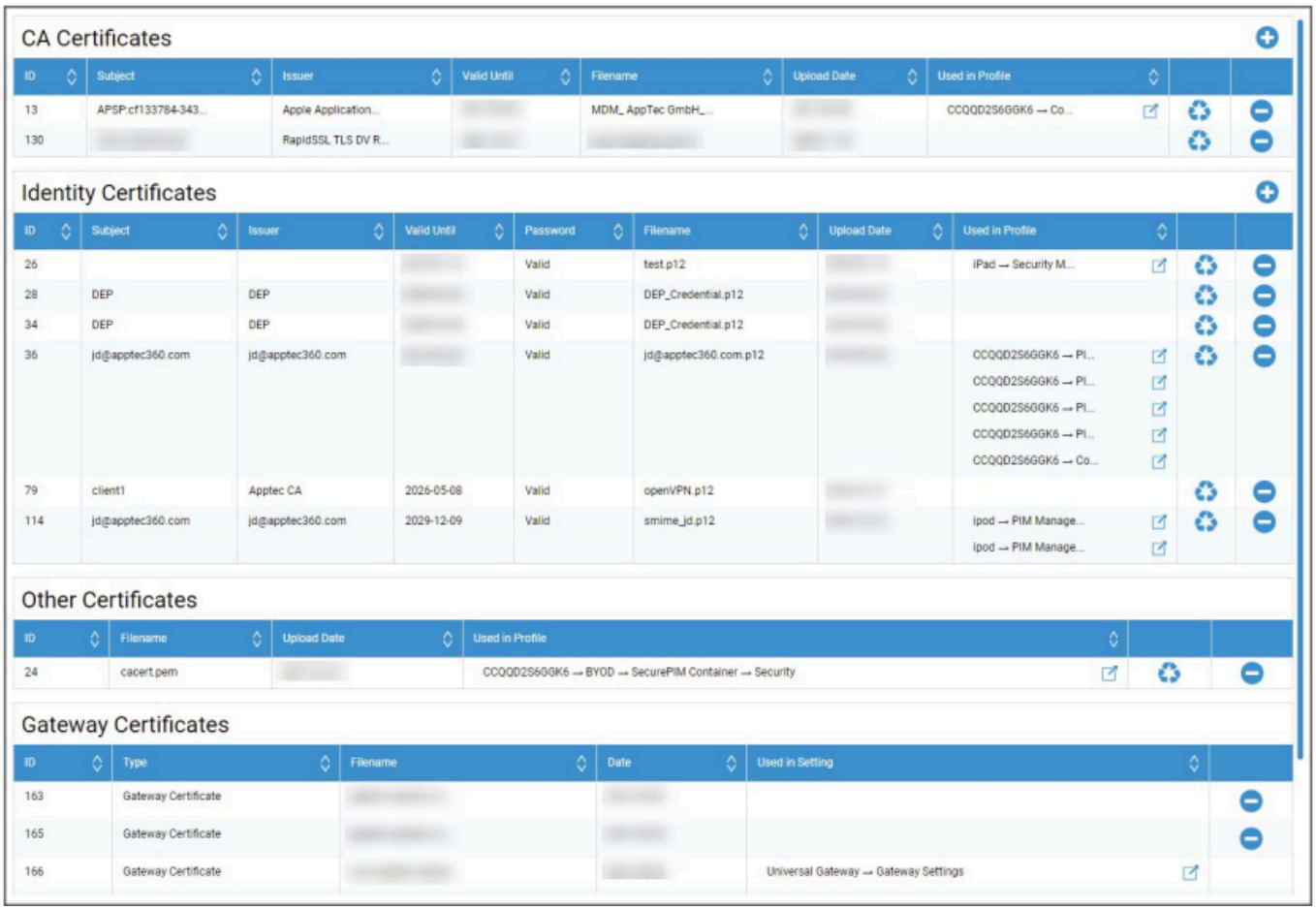
Paramètres du journal d’audit

La "période de conservation des journaux d'audit" définit la durée pendant laquelle les journaux d'audit doivent être conservés avant d'être supprimés.

Gestion des certificats

Vous obtiendrez ici un aperçu de tous les certificats téléchargés et utilisés dans la console. Il ne s'agit que d'un aperçu. La configuration réelle des certificats Wi-Fi, par exemple, est toujours effectuée dans le profil à l'emplacement correspondant.

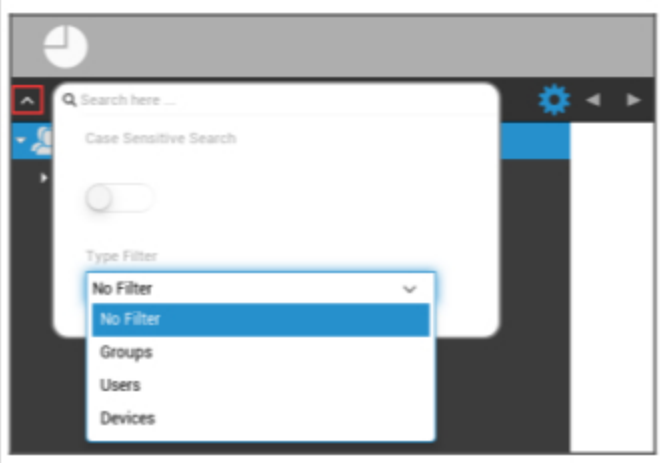
Vous pouvez également supprimer ou mettre à jour des certificats, ce qui se répercutera automatiquement sur les profils concernés. Cliquez sur l'information dans "Utilisé dans le profil" pour voir où exactement un certificat est encore attribué.



Gestion mobile

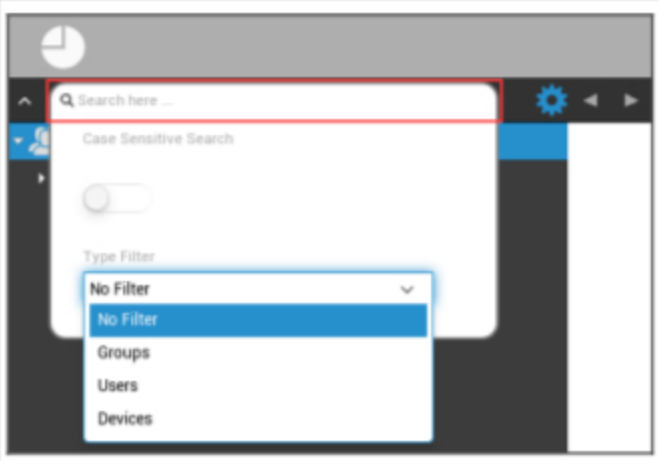
Écran de gestion mobile

Filtre de l’appareil



En cliquant dans le coin supérieur gauche de l'écran, vous trouverez une variété de filtres pour l'affichage des appareils.

Fenêtre de recherche



La fenêtre de recherche vous permet de rechercher tous les appareils et/ou utilisateurs à l'aide d'un mot-clé spécifique.

Engrenage d’options

Après avoir cliqué sur le symbole correspondant, une liste des options disponibles s'affiche.

Ceux-ci changent avec chaque fenêtre courante et sont expliqués dans les chapitres correspondants.

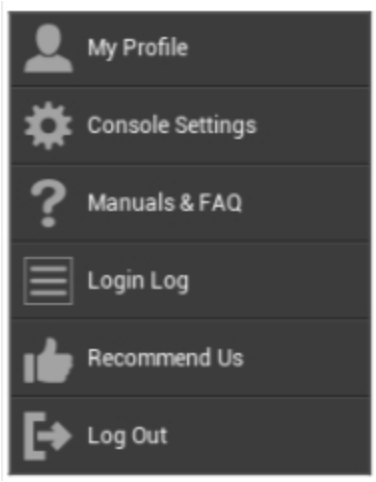
Flèches de navigation

En cliquant sur la flèche de gauche, vous accéderez à la page précédente.

Ensuite, en cliquant sur la flèche de droite, vous serez ramené à la page que vous venez de quitter.

Administration paramètres du compte

En cliquant sur l'adresse électronique comme indiqué ci-dessus, le menu suivant s'affiche :



Mon profil	Modifier les détails du compte des administrateurs
Paramètres de la console	Configurer les paramètres de la console pour le compte Admins
Manuels et FAQ	Consultez la page "Manuels et FAQ" dans "Paramètres généraux".
Journal de connexion	Accéder au "Journal de connexion"
Recommandez-nous	Affichez la page "Recommandez-nous" dans les "Paramètres généraux".
Déconnexion	Déconnectez-vous de la console MDM

Informations sur l’utilisateur

Vous pouvez ici modifier les détails du compte de l'administrateur actuellement connecté.

Nom d'utilisateur	Nom d'utilisateur et/ou adresse électronique du compte
Nom	Prénom de l'administrateur
Nom de famille	Nom de famille des administrateurs
Nom de connexion	Nom de connexion des administrateurs
Adresse électronique	Adresse électronique des administrateurs
Autre adresse électronique	Autre adresse électronique de l'administrateur
Photo	Photo de profil
Numéro de téléphone	Numéro de téléphone des administrateurs
Numéro de téléphone mobile	Numéro de portable de l'administrateur
Extension du téléphone	Poste téléphonique
Localisation	Localisation
Position	Position dans l'entreprise
Groupe d'utilisateurs	Sélectionnez le groupe d'utilisateurs auquel vous souhaitez attribuer le compte administrateur.
Commentaire	Saisissez un commentaire
Entrez le nouveau mot de passe	Saisissez le mot de passe pour un changement de mot de passe
Répéter le nouveau mot de passe	Répétez le nouveau mot de passe pour confirmer

Veuillez noter que l'accès à l'administration peut également être classé comme un compte d'utilisateur local dans la structure hiérarchique. Sans la mise en place d'un administrateur supplémentaire, celui-ci ne doit pas être supprimé !

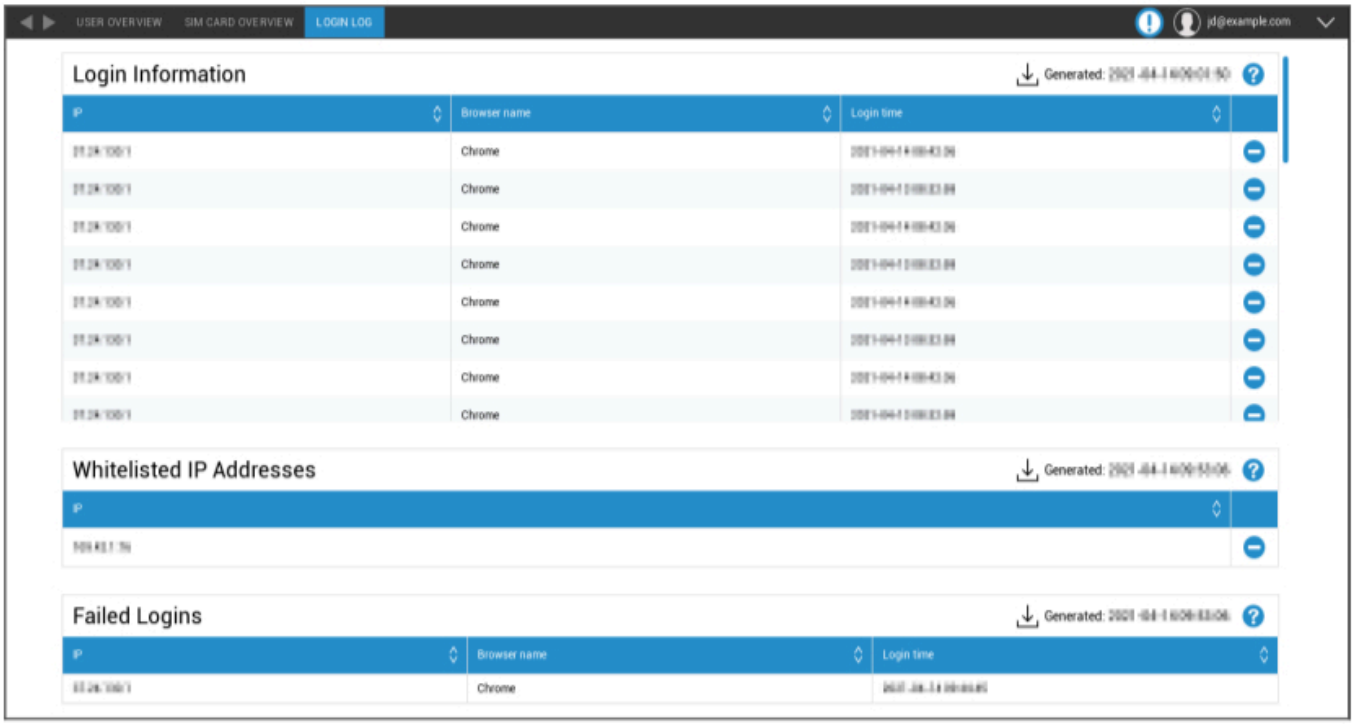
Paramètres de la console

Vous pouvez ici configurer les paramètres suivants de la console pour le compte Admins :

Options d'affichage de l'utilisateur de l'annuaire	Définir comment les utilisateurs doivent être étiquetés dans l'arbre
Options d'affichage de l'appareil de répertoire	Définir comment les appareils doivent être étiquetés dans l'arborescence
Délai d'attente de la session	Si l'utilisateur ne fait rien dans le délai spécifié, il sera déconnecté. La valeur par défaut est de 60 minutes. Veuillez vous déconnecter et vous reconnecter après avoir modifié ce paramètre.
Fuseau horaire	Choisissez le fuseau horaire utilisé
Format de l'heure	Choisissez le mode d'affichage des horodatages
Langue de la console	Choisissez la langue dans laquelle la console doit être affichée. L'anglais et l'allemand sont disponibles.
Couleur principale	Vous pouvez définir une couleur qui servira de base à la palette de couleurs de la console. Vous pouvez utiliser le sélecteur de couleurs ou saisir une couleur en notation HTML HEX. Les formateurs RVB tels que "rose", "jaune" fonctionnent également.
Sauvegarder la commande	Combinaison de touches permettant de déclencher une sauvegarde sans appuyer sur le bouton "Sauvegarder".
Utilisez l'authentification à deux facteurs	Activez l'utilisation de l'authentification à deux facteurs lors de la connexion. Vous recevrez un courriel avec un code que vous devrez entrer pour vous connecter.
Délai d'authentification à deux facteurs	Définissez un délai pendant lequel il ne vous sera pas demandé de vous authentifier à deux facteurs après une authentification déjà réussie.
Envoyez le code de vérification via	Le code de vérification sera envoyé aux options sélectionnées. Le message de l'appareil sera affiché dans l'AppTec360 MDM App sur tous les appareils Android et iOS qui vous appartiennent.
Envoyer un message de connexion après la connexion	Si cette option est activée, un courriel sera envoyé pour chaque connexion à partir d'une adresse IP qui n'est pas sur la liste blanche. L'e-mail contient des informations sur la connexion (par exemple, l'adresse IP, le navigateur).

Journal de connexion

Ici, vous pouvez voir les informations concernant les connexions du compte administrateur actuellement connecté.



Informations de connexion	Une liste contenant les connexions du compte administrateur actuellement connecté qui ont été enregistrées par la console. Cette liste affiche toutes les connexions réussies au cours des 30 derniers jours.
Adresses IP sur liste blanche	Il s'agit de la liste de toutes les adresses IP inscrites sur la liste blanche. Si vous vous connectez à partir d'une adresse IP qui figure dans cette liste, vous n'obtiendrez pas le message de connexion. Vous pouvez ajouter une adresse IP à cette liste en cliquant sur le bouton situé à côté d'une entrée dans la liste "Informations de connexion" ci-dessus. Vous pouvez supprimer une adresse IP de cette liste en cliquant sur le bouton situé à côté d'une entrée dans cette liste ou dans la liste "Informations de connexion" ci-dessus.
Échecs de connexion	Il s'agit d'une liste de toutes les tentatives de connexion qui ont échoué au cours des 30 derniers jours. Si vous n'avez pas introduit le mot de passe correct au moins 3 fois en 20 minutes, une entrée apparaîtra dans cette liste. Vous serez également informé par courrier électronique des tentatives de connexion qui ont échoué.

Administration centrale (Root-Node) dans la gestion mobile

Lorsque vous avez atteint le nœud racine (premier groupe), vous pouvez effectuer une série de réglages pour votre entreprise, en ce qui concerne la gestion mobile.

Créer un sous-groupe	Créer un sous-groupe
Renommer le nœud racine	Renommer le nœud racine (par exemple, le nom de votre entreprise)
Inscription en masse	Enrôler plusieurs appareils/utilisateurs en même temps
Affectation des masses	Attribuer un profil aux différents groupes, d'un seul coup d'œil
Administration rapide des applications	Envoyez les demandes d'installation ou de désinstallation d'une application aux groupes de dispositifs respectifs.
Importation d'un utilisateur CSV	Importer des utilisateurs à partir d'un fichier CSV dans le groupe correspondant

Créer un sous-groupe

L'option "Créer un sous-groupe" permet de créer un sous-groupe supplémentaire.

Vous pouvez déterminer le groupe auquel le sous-groupe doit être affecté.

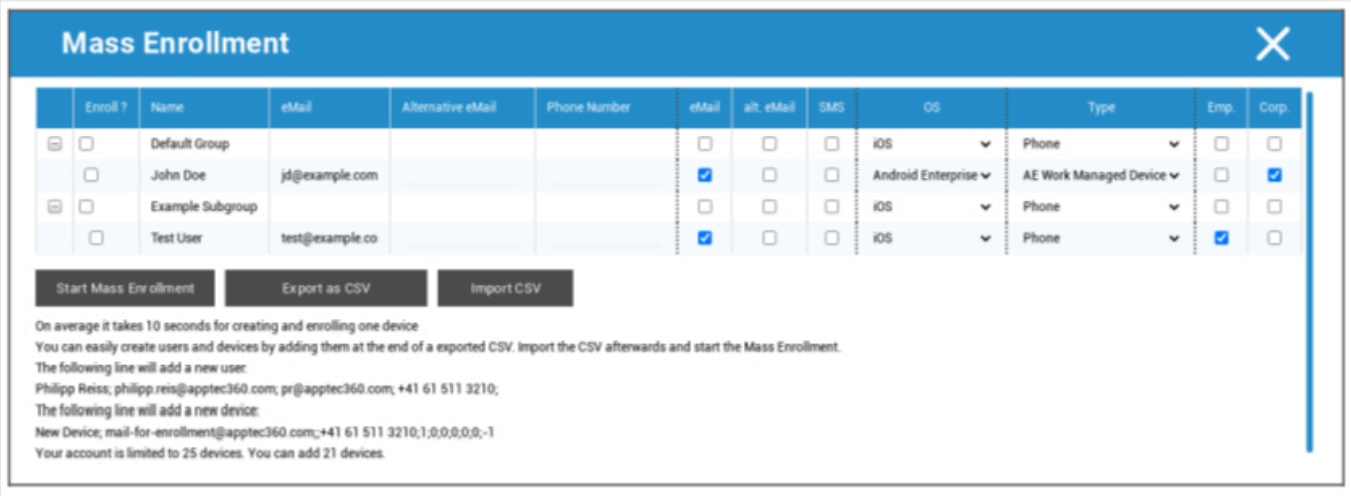
(Par défaut, un nouveau groupe est créé et assigné en tant que sous-groupe dans le nœud racine).

Renommer le nœud racine

Ici, vous pouvez renommer votre nom de racine. Il est courant que le nom de l'entreprise soit utilisé dans ce cas.

Inscription en masse

L'inscription en masse permet d'inscrire plusieurs appareils et utilisateurs.



Vous pouvez sélectionner directement la manière dont l'utilisateur doit recevoir l'inscription (e-mail, e-mail alternatif, SMS).

Selon l'appareil que l'utilisateur va recevoir (iOS, Android, Windows Phone), vous pouvez le marquer directement ici.

La distinction entre smartphone et tablette peut également être configurée ici, ce que vous devez sélectionner correctement en cochant la case correspondante.

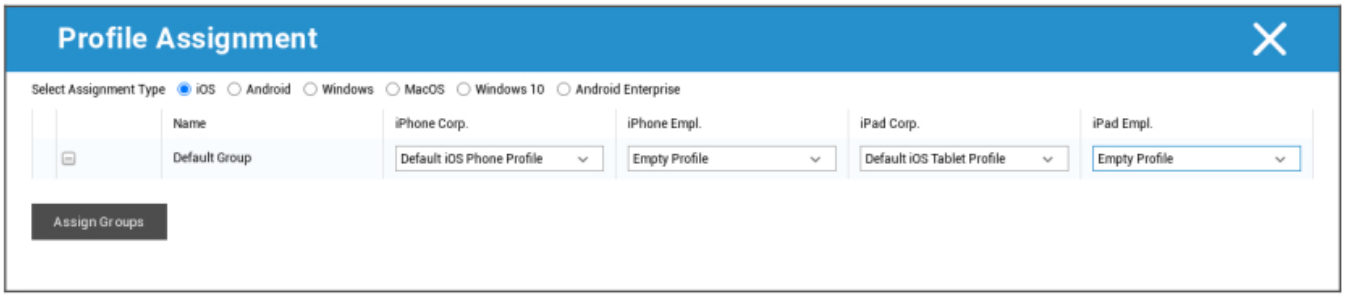
La dernière étape consiste à déterminer si l'appareil en question est un appareil d'entreprise ou un appareil privé (BYOD).

L'option "Exporter en CSV" permet d'exporter les informations dans un fichier de données CSV. En contrepartie, vous pouvez également importer le fichier de données CSV avec "Importer CSV", le fichier devrait ressembler à l'exemple ci-dessous :

Philipp Reiss ; philipp.reis@apptec360.com ; pr@apptec360.com ; +41 61 511 3210 ;

Affectation des masses

Sous Attribution en masse, vous pouvez attribuer un profil à tous les groupes, qui sont divisés en iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise.

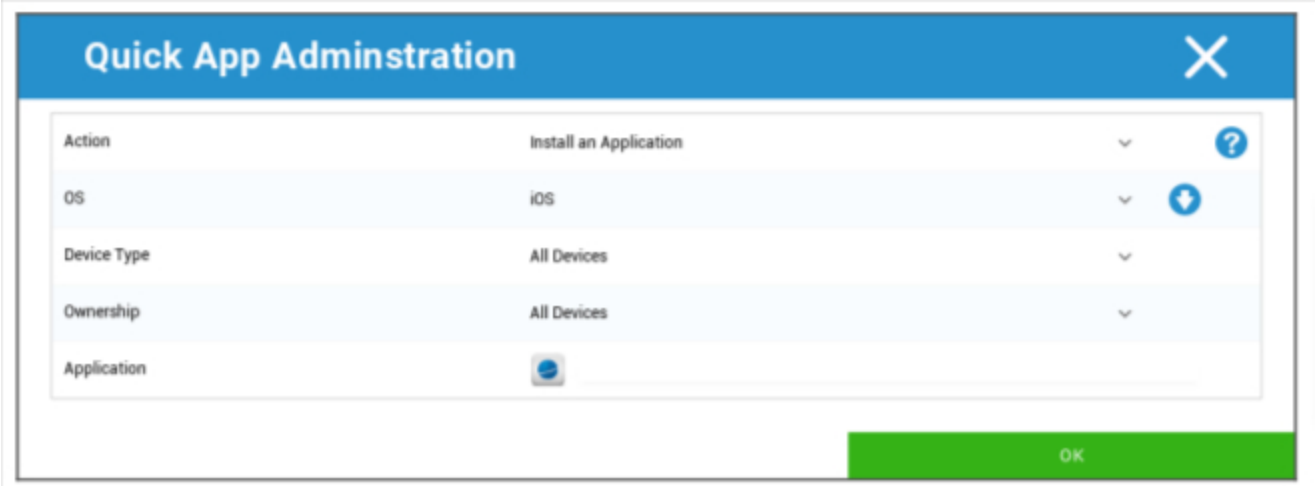


Windows - MacOS - Windows 10 - Android Enterprise

Administration rapide des applications

Sous Quick App Administration, vous pouvez envoyer des demandes d'installation ou de désinstallation d'une application spécifique à un système d'exploitation de votre choix.

Vous pouvez également définir si la demande doit être envoyée à tous les types d'appareils du système d'exploitation sélectionné ou seulement à un type d'appareil spécifique.



Importation d’un utilisateur CSV

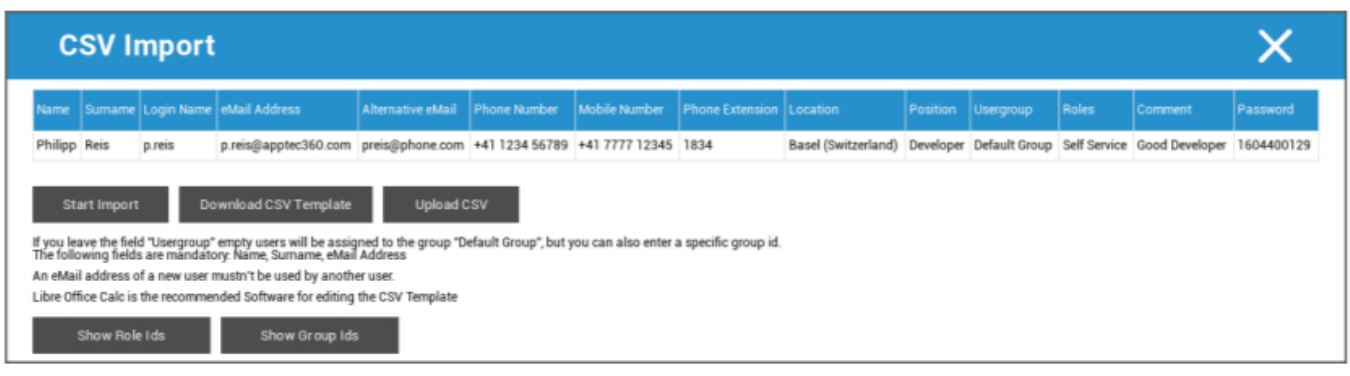
Importer les utilisateurs d'un fichier CSV dans le groupe correspondant.

Avec "Télécharger le modèle CSV", vous pouvez exporter un fichier modèle CSV, qui peut être rempli (ou utilisé comme référence).

Vous pouvez également utiliser les options "Show Role Ids" et "Show Group Ids" comme référence pour créer votre propre fichier CSV.

Le fichier CSV peut être téléchargé vers le MDM avec "Upload CSV".

Enfin, vous pouvez lancer l'importation en cliquant sur "Démarrer l'importation".



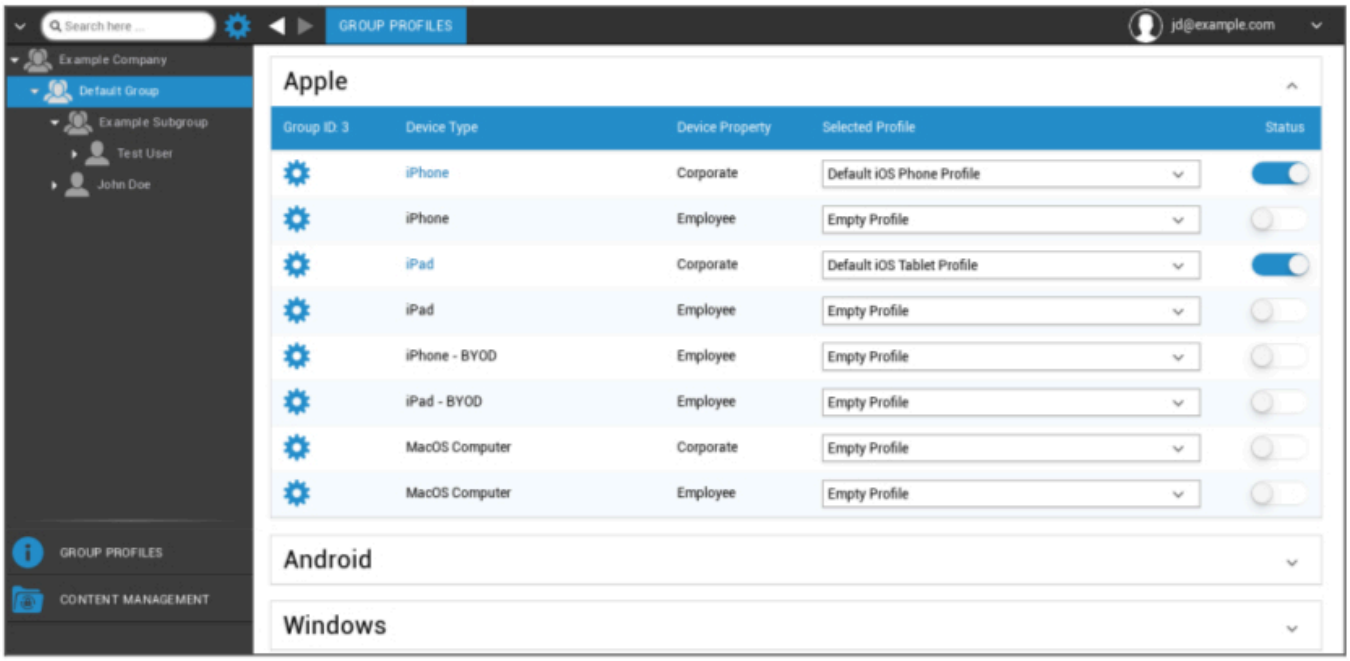
Gestion de groupe dans la gestion mobile

Un clic sur l'aperçu permet d'afficher les différents profils de configuration pour les plates-formes respectives.

Un profil contient toutes les options de réglage qui peuvent être établies avec AppTec360 à l'avance sur l'appareil de l'utilisateur final. Sur chaque plateforme, vous pouvez créer des profils pour les appareils de l'entreprise (Corporate) ou pour les appareils personnels (Bring-Your-Own-Device) (Employee).

Afin de différencier les configurations des groupes d'appareils, par exemple en fonction de l'emplacement ou de la fonction, il est conseillé de créer plusieurs sous-groupes.

Veuillez noter que la gestion des profils dans la gestion des mobiles



Le menu de l'équipement permet de définir divers paramètres pour le (sous-)groupe concerné.

Créer un sous-groupe	Créer un sous-groupe pour le (sous-)groupe concerné
Modifier le groupe sélectionné	Modifier le groupe sélectionné
Supprimer le groupe sélectionné	Supprimer le groupe sélectionné
Inscription en masse	Inscrivez plusieurs appareils/utilisateurs à la fois pour le profil sélectionné
Affectation des masses	Attribuer des profils au groupe actuellement sélectionné

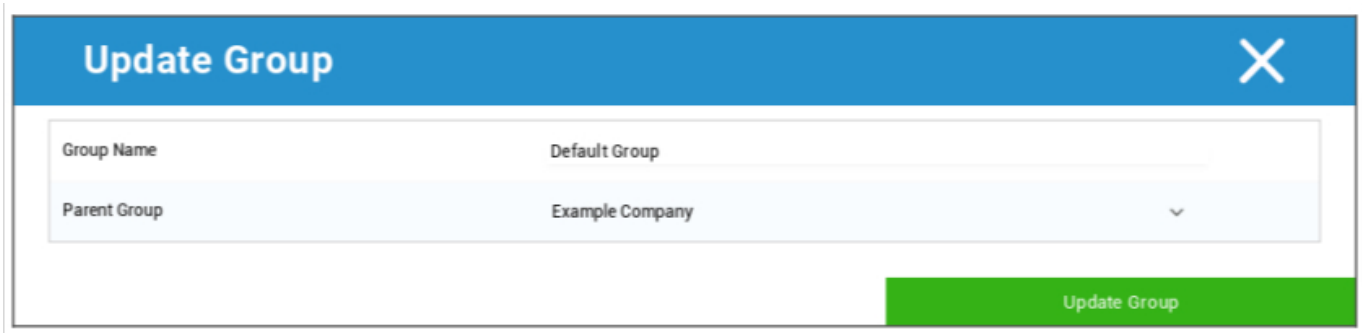
Créer un sous-groupe	Créer un sous-groupe pour le (sous-)groupe concerné
Créer un utilisateur	Créer un utilisateur pour le (sous-)groupe concerné

Créer un sous-groupe

L'option "Créer un sous-groupe" permet de créer un sous-groupe supplémentaire.

Vous pouvez déterminer le groupe auquel le sous-groupe doit être affecté (par défaut, le sous-groupe est affecté au groupe actuellement sélectionné).

Modifier le groupe sélectionné



Vous pouvez ici modifier le profil - les paramètres suivants sont possibles :

- Le nom du groupe peut être modifié
- Le groupe de parents peut être modifié

Supprimer le groupe sélectionné

Sous "Supprimer le groupe sélectionné", tous les utilisateurs et appareils appartenant au groupe en question sont répertoriés. Ici, vous avez la possibilité de les supprimer.

Pour un utilisateur, vous pouvez exécuter les commandes de suppression suivantes :

Supprimer l'utilisateur	L'utilisateur est supprimé
Déplacer l'utilisateur vers le groupe :	Vous pouvez déplacer l'utilisateur vers un autre groupe (colonne suivante, ex. "Admins").

Pour un appareil, vous pouvez exécuter les commandes de suppression suivantes :

Effacer et supprimer	Effacer et supprimer l'appareil
Supprimer du système	Retirer l'appareil uniquement d'AppTec

Référence : Inscription en masse

Référence : Affectation des masses

Créer un utilisateur

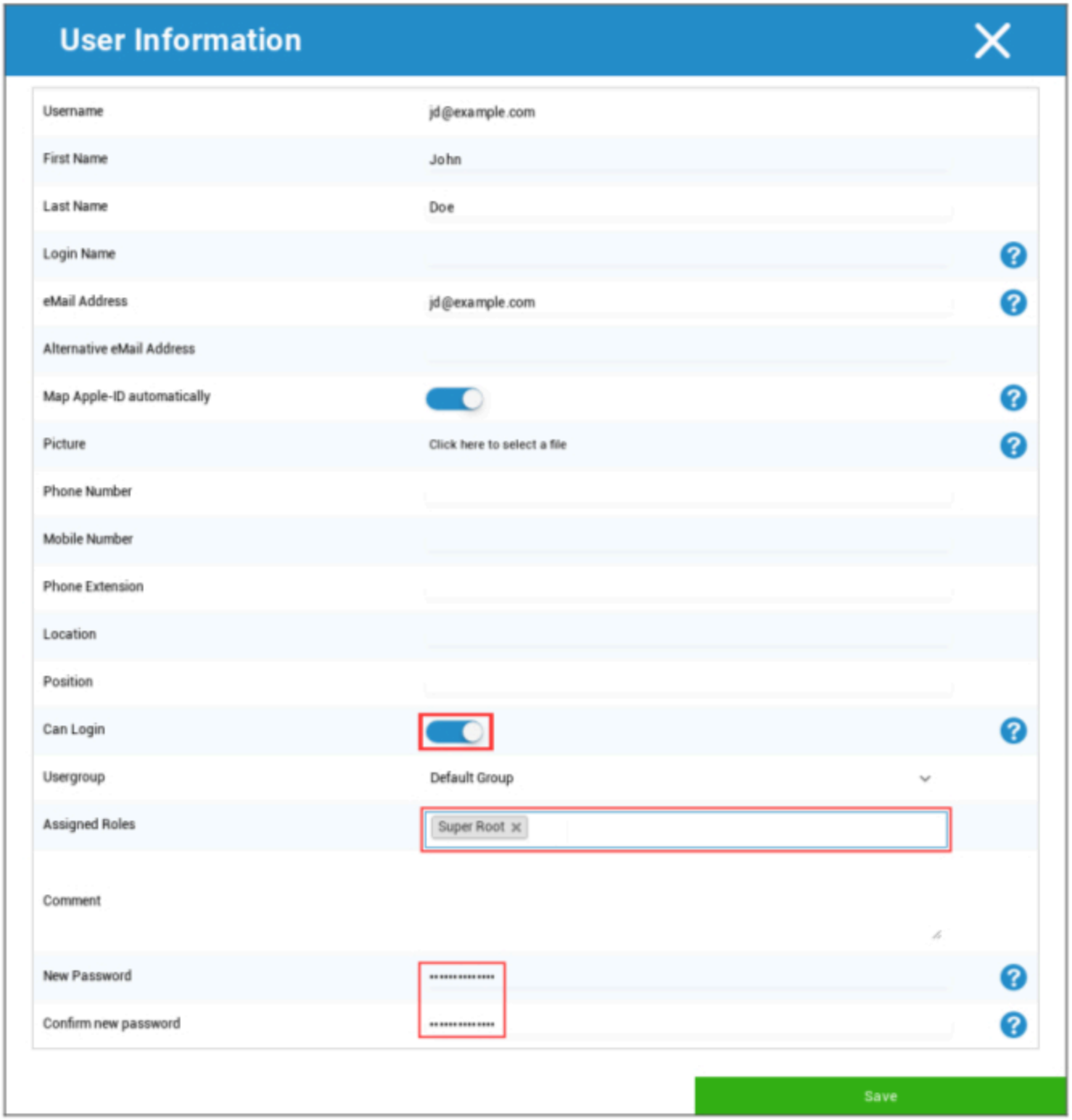
L'option "Créer un utilisateur" permet d'ajouter un nouvel utilisateur.

Créer un nouvel Admin-User

Vous pouvez définir un utilisateur comme Admin-User. Cela lui permettra de se connecter à la console et de modifier les utilisateurs/groupes/appareils.

Créez un utilisateur normal ou utilisez un utilisateur existant. Choisissez l'utilisateur auquel vous voulez donner des droits d'administrateur, cliquez sur la roue et choisissez "Modifier l'utilisateur" :

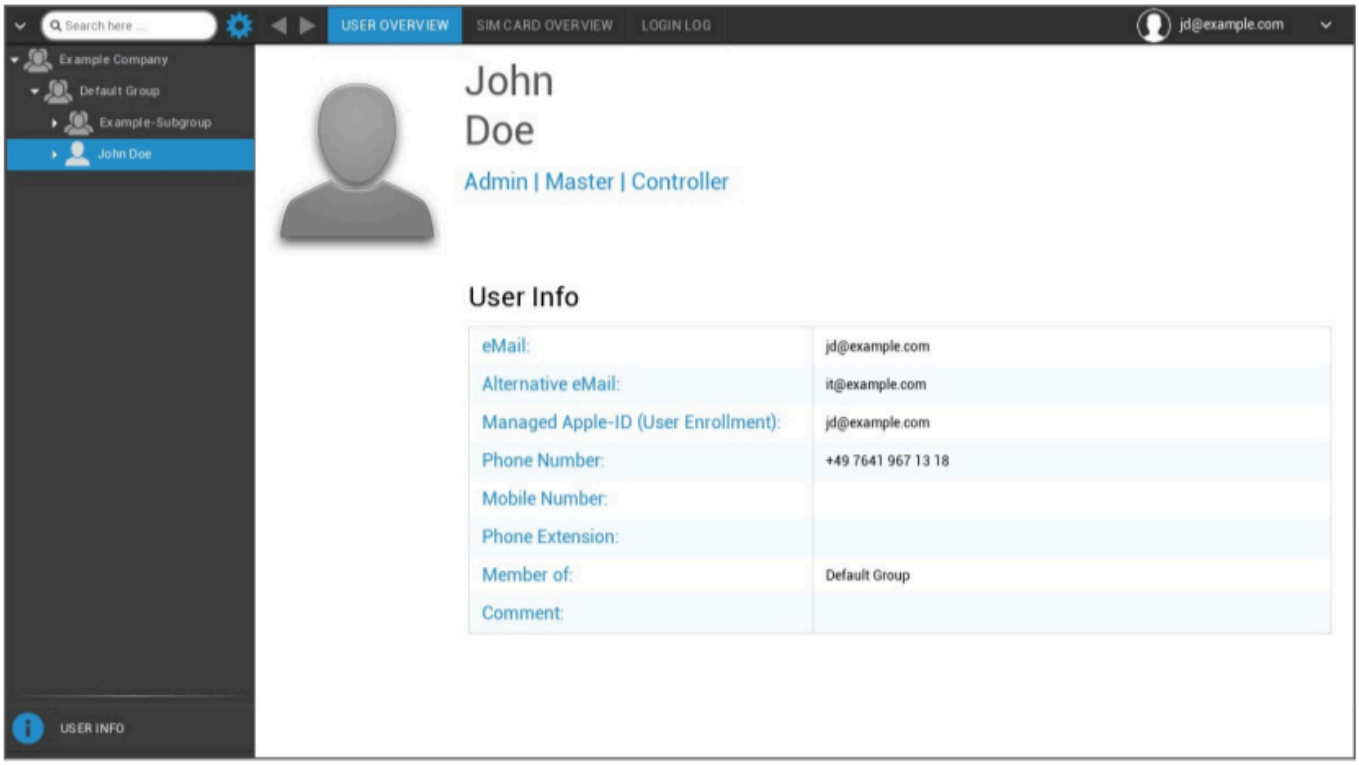
Activez le commutateur "Can Login", attribuez le rôle "Super-Root" à l'utilisateur et définissez un mot de passe.



Enregistrez ceci et l'utilisateur peut maintenant se connecter avec son nom d'utilisateur et son mot de passe.

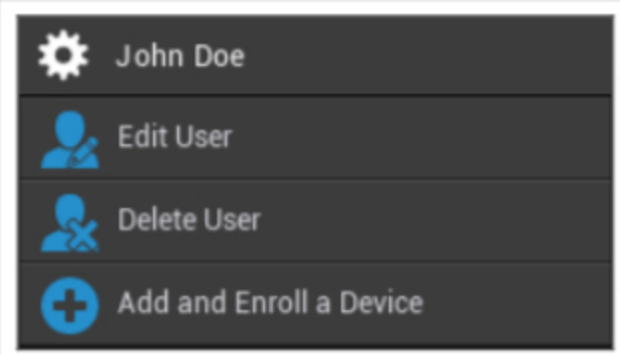
Gestion des utilisateurs dans la gestion mobile

Lorsque vous sélectionnez un utilisateur donné, l'aperçu suivant s'affiche :



Vous obtiendrez une vue d'ensemble de toutes les informations que vous avez saisies précédemment dans "Créer un utilisateur".

Avec l'équipement installé au sommet, vous pouvez effectuer les configurations suivantes :



Nom de l'utilisateur	Nom de l'utilisateur sélectionné
Modifier l'utilisateur	Modifier les informations sur l'utilisateur
Supprimer un utilisateur	Supprimer un utilisateur

	• Supprimer du système = L'appareil sera supprimé d'AppTec • Wipe & Delete = L'appareil sera restauré aux paramètres d'usine et supprimé d'AppTec.
Ajouter et enregistrer un appareil	Enrôler un appareil pour l'utilisateur sélectionné

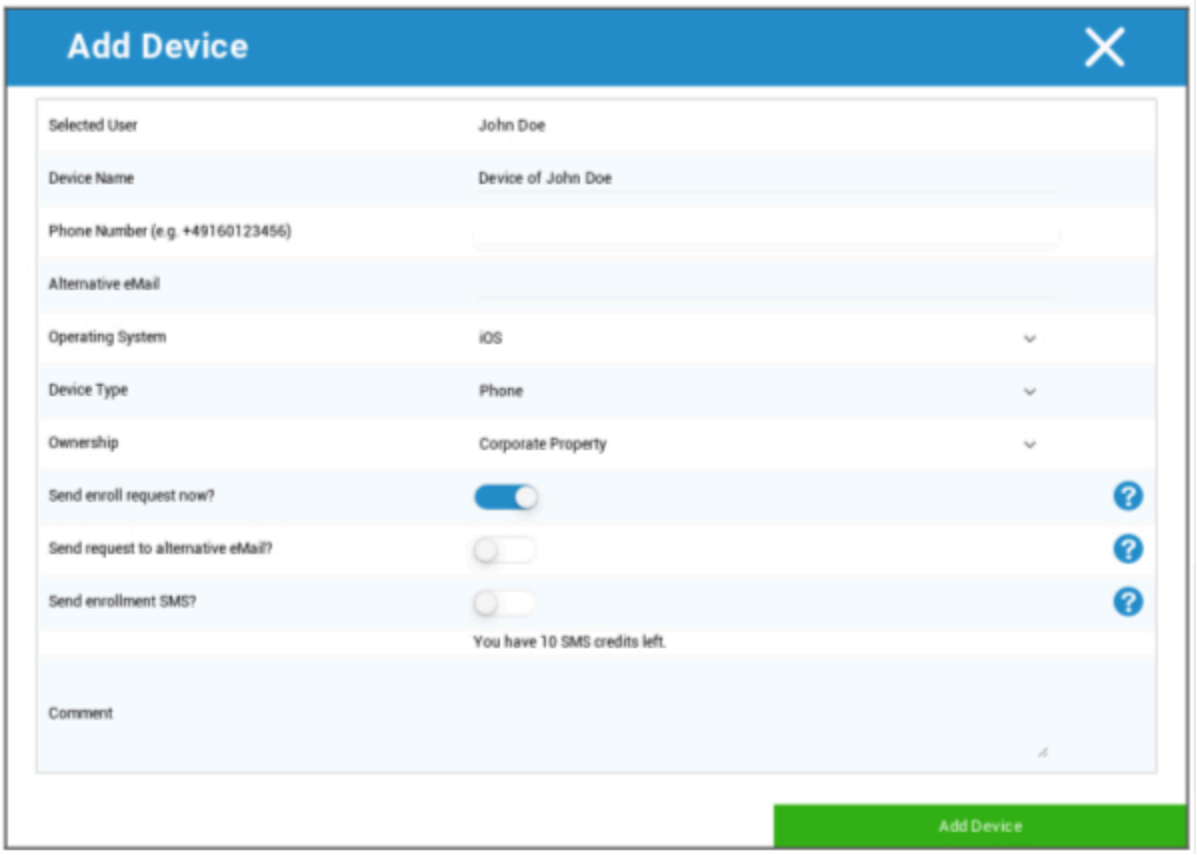
Veuillez noter que l'accès à l'administration peut également être classé comme un compte d'utilisateur local dans la structure hiérarchique. Sans la mise en place d'un administrateur supplémentaire, celui-ci ne doit pas être supprimé !

Ajouter et enregistrer un appareil

Vous pouvez ici sélectionner un appareil pour l'utilisation choisie.

Vous pouvez également inscrire directement des appareils dans un groupe. Pour ce faire, cliquez sur le groupe, cliquez sur la roue et sélectionnez "Ajouter et inscrire un appareil".

Vous devriez voir l'aperçu suivant :



Selon le type d'appareil que vous souhaitez inscrire, vous devez effectuer les configurations suivantes :

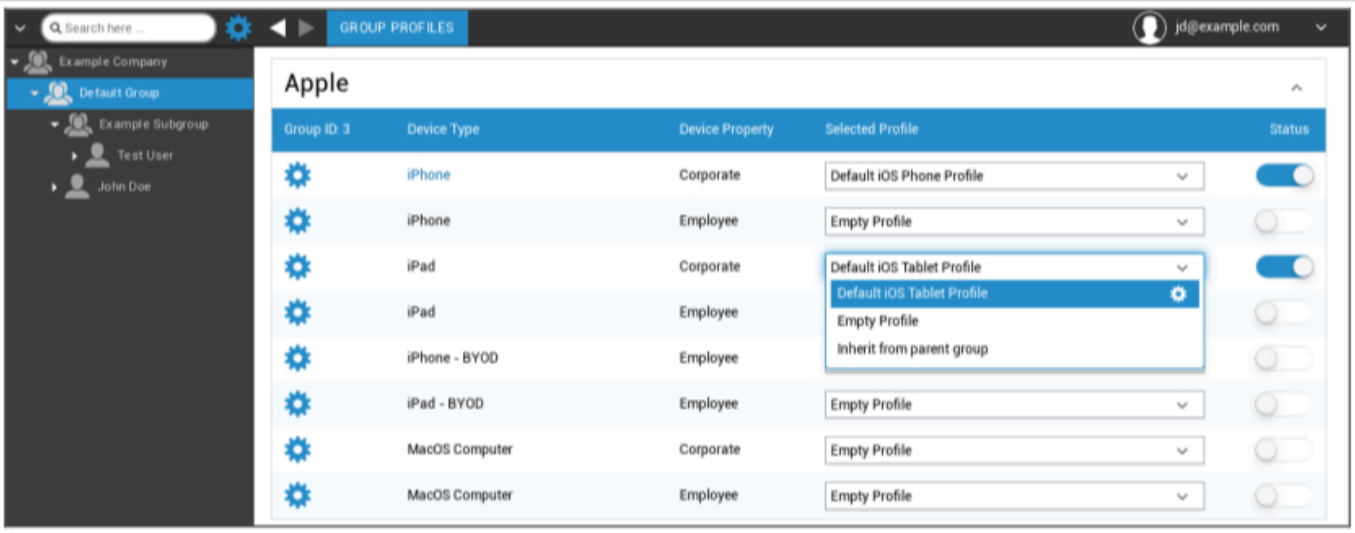
Utilisateur sélectionné	Utilisateur sélectionné (sera rempli automatiquement)
Nom de l'appareil	Sera rempli automatiquement (dispositif pour le "nom de l'utilisateur") - peut toutefois être modifié
Numéro de téléphone	Le numéro de téléphone est rempli automatiquement (pour autant qu'il ait été fourni par l'utilisateur) - vous pouvez toutefois l'ajouter ou le modifier.
Alternative eMail	L'autre adresse électronique sera remplie automatiquement (à condition qu'elle ait été fournie par l'utilisateur) - ici, cependant, elle peut être ajoutée ou modifiée.
Propriétaire de l'appareil	Propriété de l'entreprise = dispositif de l'entreprise Propriété de l'employé = appareil BYOD
Sélectionnez le système d'exploitation	Ici, vous avez le choix entre les systèmes d'exploitation suivants : • iOS • iOS BYOD (inscription des utilisateurs) • MacOS • Android Enterprise • Android • Windows Mobile • Windows 10
Envoyer une demande d'inscription ?	L'e-mail est envoyé immédiatement à l'adresse e-mail principale et l'utilisateur est invité à connecter son appareil.
Envoyer une demande à un autre courrier électronique ?	Envoyez l'e-mail en plus ou exclusivement (dans le cas où l'option "Envoyer la demande d'inscription ?" a été désactivée) à l'adresse e-mail alternative (l'e-mail est différent de l'e-mail "normal" de la demande d'inscription).
Envoyer un SMS d'inscription ?	Envoyez une demande d'inscription par SMS (le "numéro de téléphone" doit être saisi).

Après l'envoi de la demande d'inscription, l'appareil sera immédiatement affiché (marqué en rouge).

Dès que l'appareil a été connecté avec succès, il est marqué en vert et est donc prêt à recevoir des restrictions, des applications, etc.

Gestion des profils dans la gestion mobile

Après avoir cliqué sur un groupe, vous obtenez une vue d'ensemble de toutes les plates-formes d'appareils à configurer et des profils qui leur sont respectivement attribués.



	Effectuez la configuration pour le profil sélectionné
Type d'appareil	Type et/ou modèle d'appareil
Propriété de l'appareil	Propriétaire de l'appareil (Entreprise = propriété de l'entreprise, Employé = appareil d'un employé privé)
Profil sélectionné	Profil sélectionné (la roue dentée ouvre la boîte de dialogue de configuration du profil)
Statut	On/Off (le profil est activé/désactivé)

Lorsque vous sélectionnez l'engrenage, vous obtenez les options suivantes :

Créer un profil

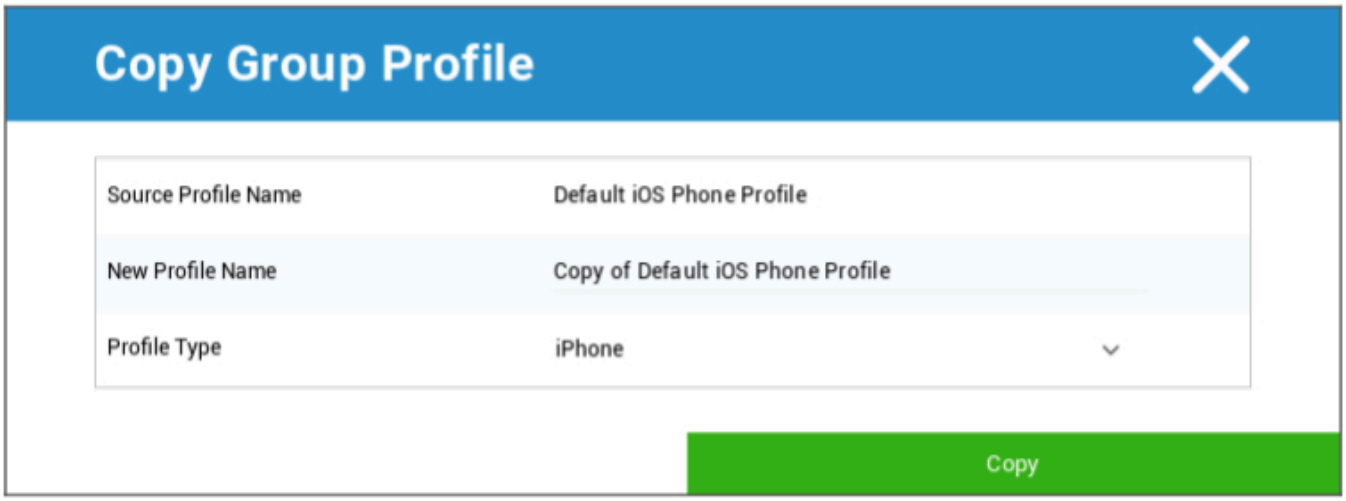
Vous pouvez créer et configurer un nouveau profil pour chaque entrée et/ou plateforme. Après avoir cliqué sur ce sous-point, le profil sera créé immédiatement et vous pourrez commencer à configurer l'iOS, l'Android et le Windows Phone tout de suite.

Modifier le profil

Après avoir cliqué sur "Modifier le profil", vous accédez à l'écran de configuration du profil concerné, où vous pouvez définir les configurations.

Profil de la copie

La fonction "Copier le profil" permet de copier les réglages/configurations d'un profil existant et de les ajouter à un nouveau profil.

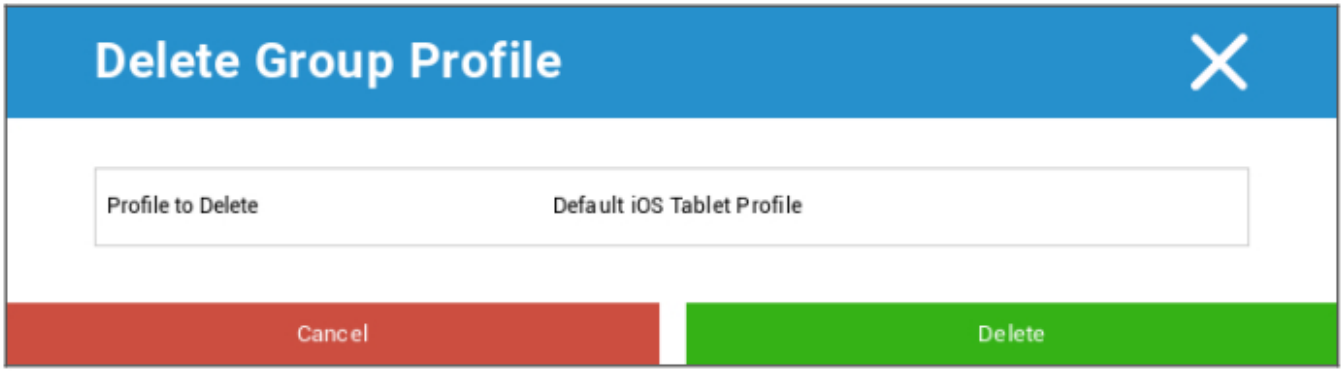


Source Nom du profil	Nom du profil à copier
Nouveau nom de profil	Nom du nouveau profil
Type de profil	Type de profil (téléphone/tablette)

Une fois que vous avez cliqué sur "Copier", le profil est créé et peut maintenant être assigné au groupe.

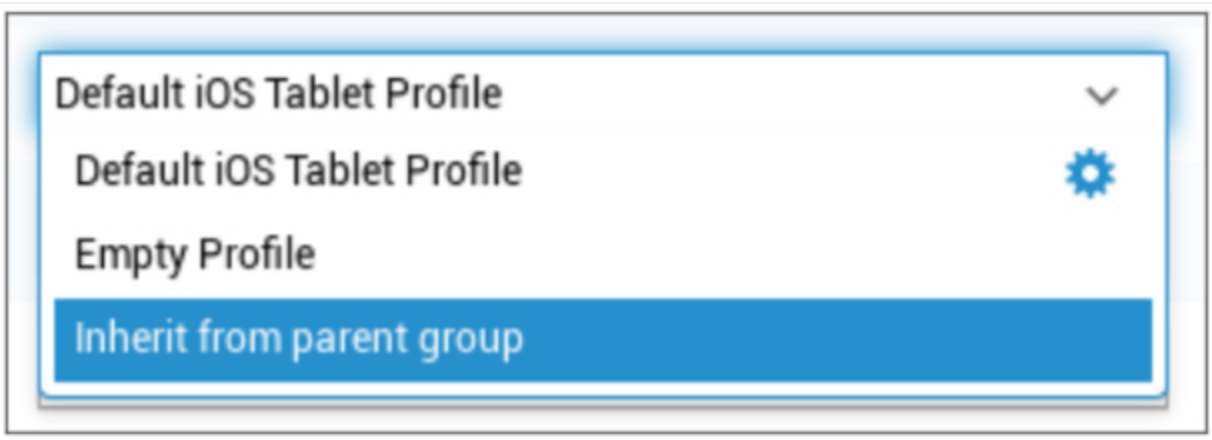
Supprimer le profil

Vous pouvez ici supprimer définitivement un profil. Veuillez noter que lors de la procédure de suppression et de la procédure suivante "Attribuer maintenant" pour le profil, la configuration disparaîtra sur les appareils respectifs d'un groupe affecté et ne pourra pas être récupérée !


Delete Group Profile
Profile to Delete
Default iOS Tablet Profile
Cancel
Delete

Héritage des profils

Lors de la sélection des profils, l'option "Hériter du groupe parent" est disponible.



Lorsque le profil est activé, le profil du groupe parent est utilisé pour l'appareil sélectionné (et le type d'appareil correspondant). Veuillez également noter que les changements apportés à ce profil pourraient affecter de nombreux groupes.

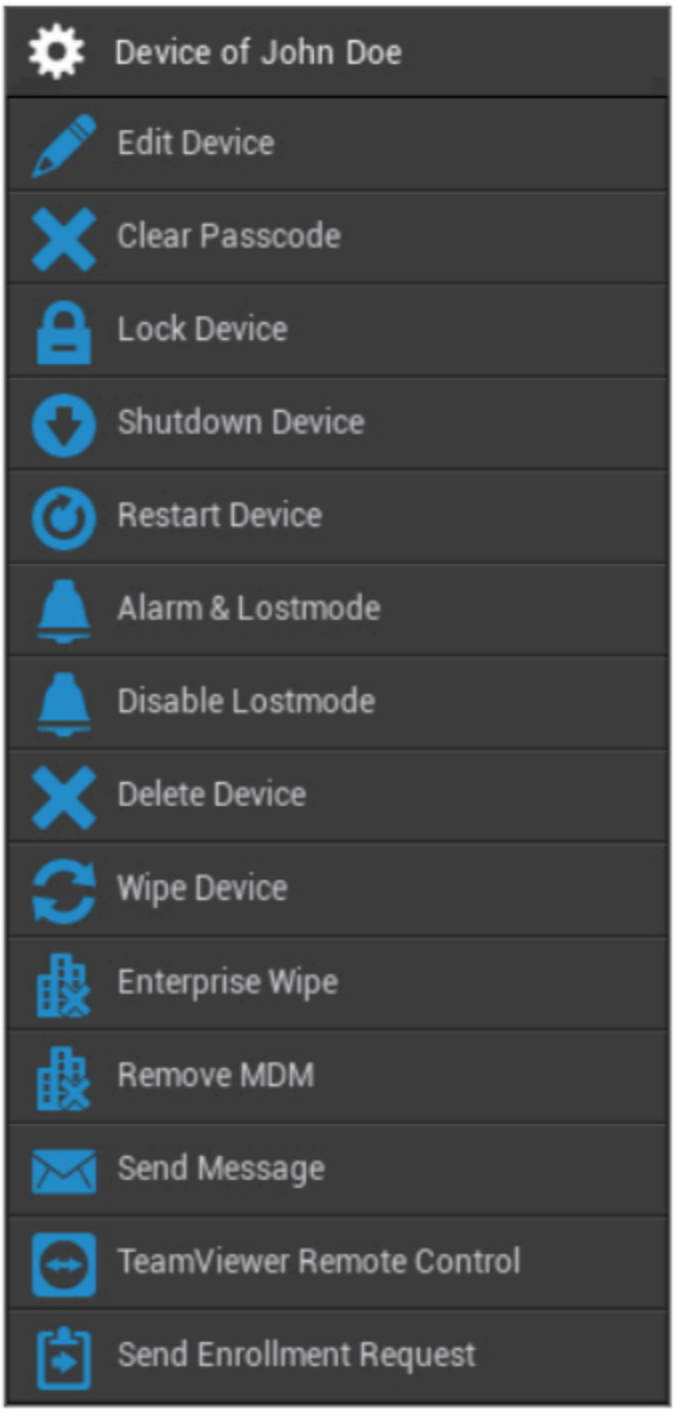
Cette configuration est définie comme valeur par défaut lors de la création d'un nouveau sous-groupe.

La configuration "Profil vide" est également disponible. Elle correspond à un profil vide, ce qui signifie qu'aucune nouvelle configuration ne sera effectuée sur l'appareil de l'utilisateur final.

Gestion des appareils dans la gestion mobile

Lorsque vous sélectionnez un appareil, vous pouvez effectuer diverses tâches à l'aide de l'"engrenage". Elles sont différentes selon les plateformes OS (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

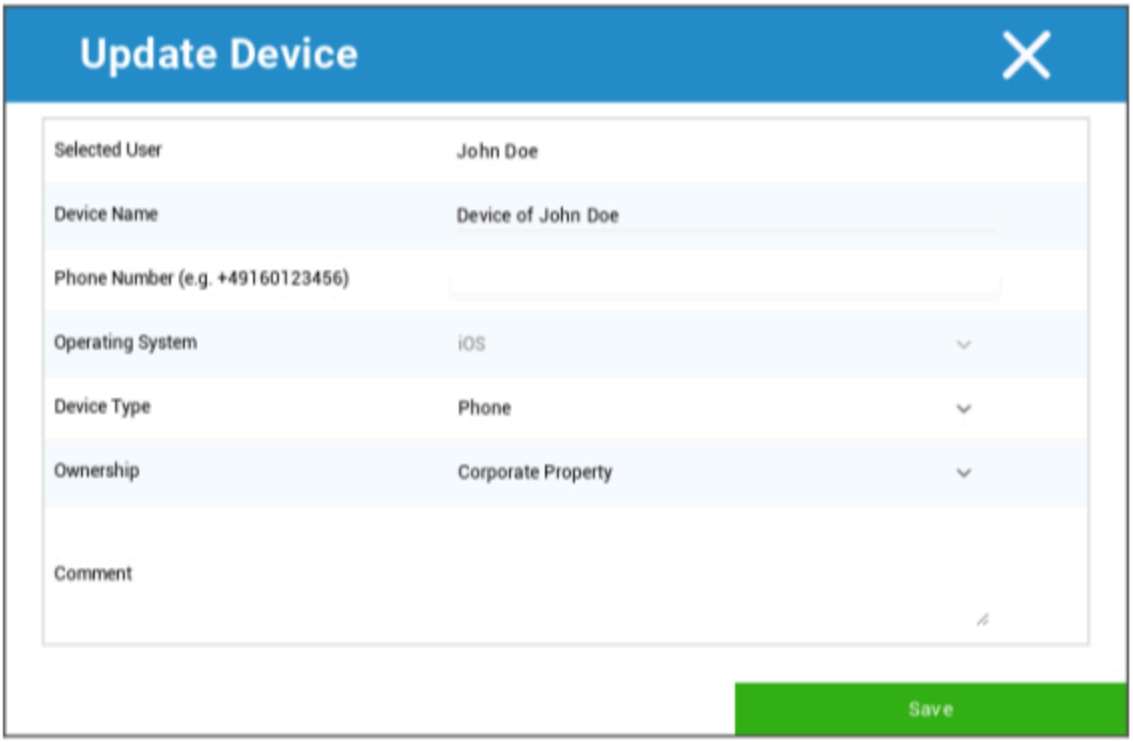
IOS



Modifier le dispositif	Modifier l'appareil
Effacer le code d'accès	Le code d'accès de l'appareil est effacé
Dispositif de verrouillage	Verrouiller le dispositif (écran de verrouillage)
Dispositif d'arrêt	Dispositif d'arrêt

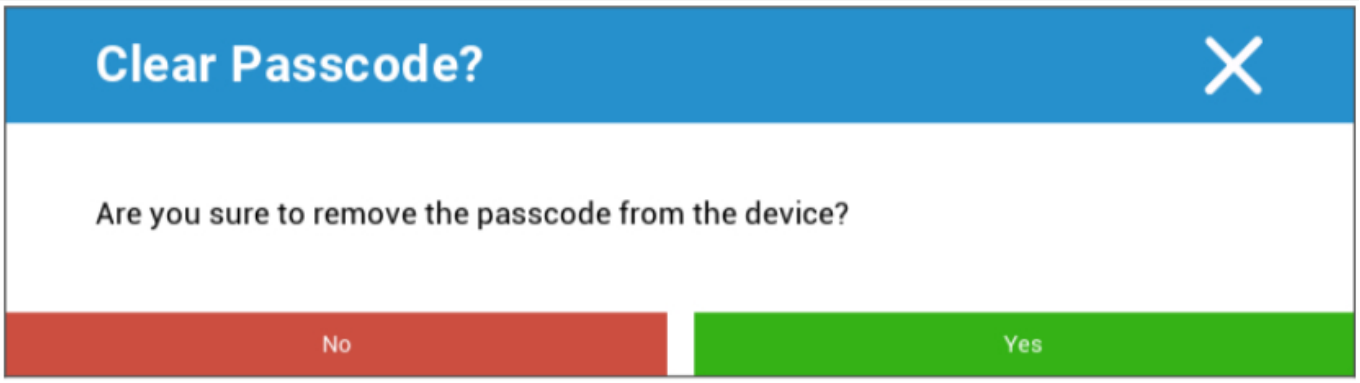
Redémarrer l'appareil	Redémarrer l'appareil
Alarme et mode perdu	Alarme de démarrage et mode perdu
Désactiver le mode Perdu	Désactiver le mode Perdu
Supprimer le dispositif	Supprimer l'appareil d'AppTec
Effacer le dispositif	Rétablir les paramètres d'usine de l'appareil
Nettoyage de l'entreprise	Les informations, applications et profils fournis par AppTec360 sont supprimés (l'appareil est séparé du MDM).
Supprimer le MDM	
Envoyer un message	Envoyer des notifications push à l'appareil Le message sera affiché dans l'application AppTec360 (onglet Message).
Contrôle à distance TeamViewer	Démarrer une session de contrôle à distance avec TeamViewer
Envoyer une demande d'inscription	Envoi (répété) de la demande d'inscription

Modifier le dispositif



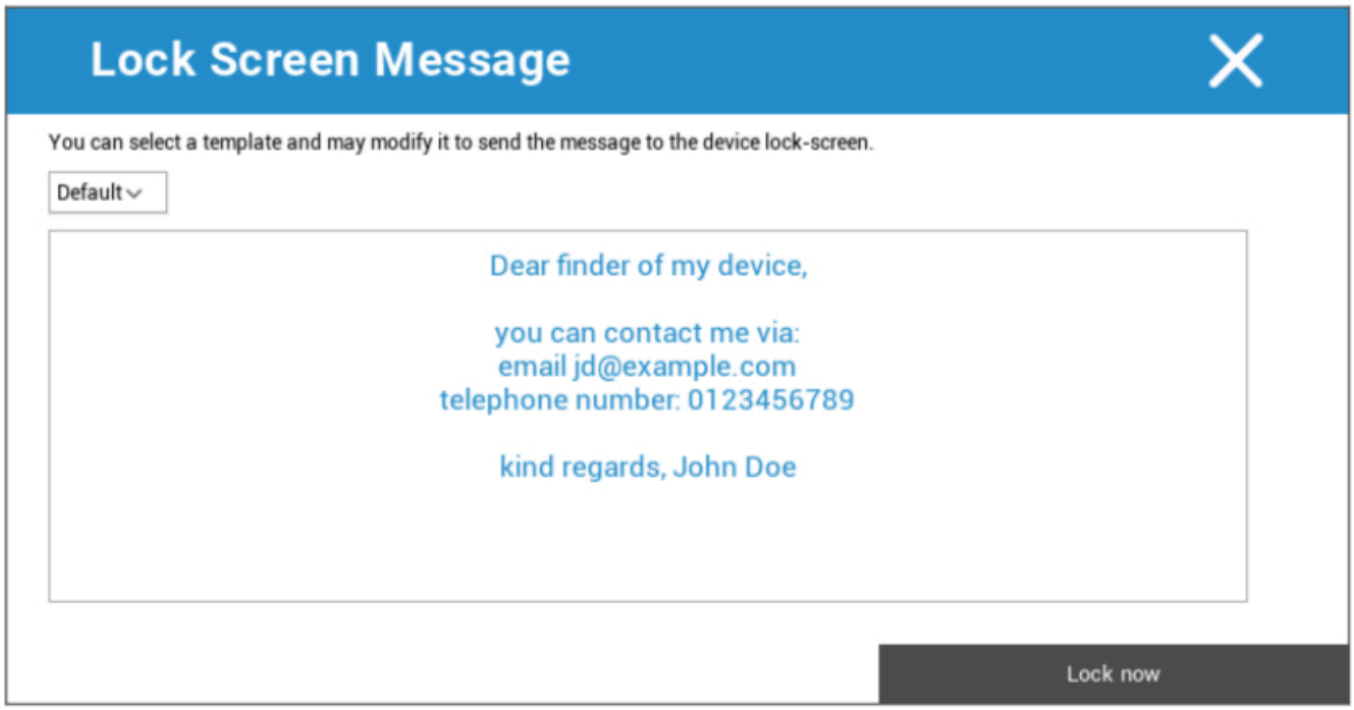
Vous pouvez y mettre à jour diverses informations sur l'appareil.

Effacer le code d’accès



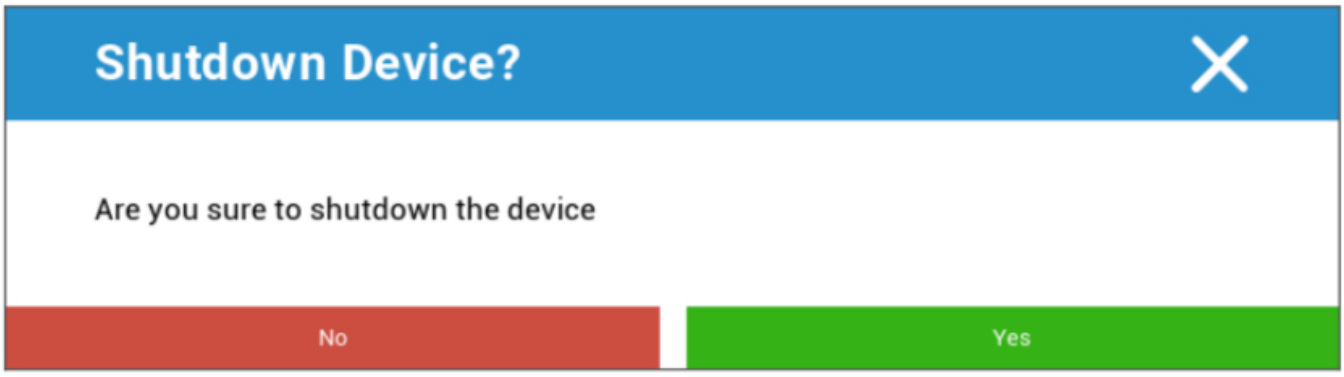
Sous "Effacer le code d'accès", vous pouvez supprimer à distance le code d'accès de l'appareil. Par la suite, l'utilisateur sera invité à créer un nouveau mot de passe (en fonction des directives relatives au code de passe).

Dispositif de verrouillage



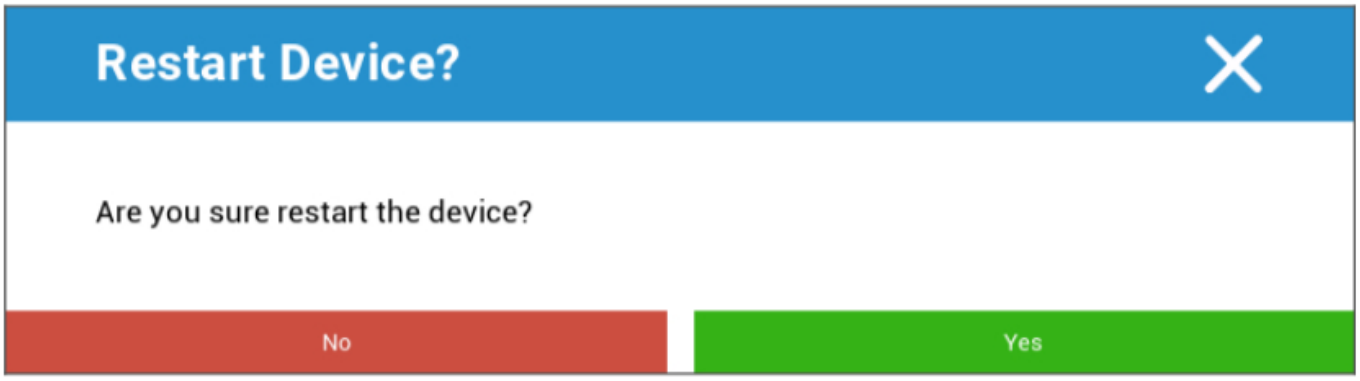
Une commande de verrouillage est envoyée à l'appareil de l'utilisateur final (écran de verrouillage).

Dispositif d’arrêt



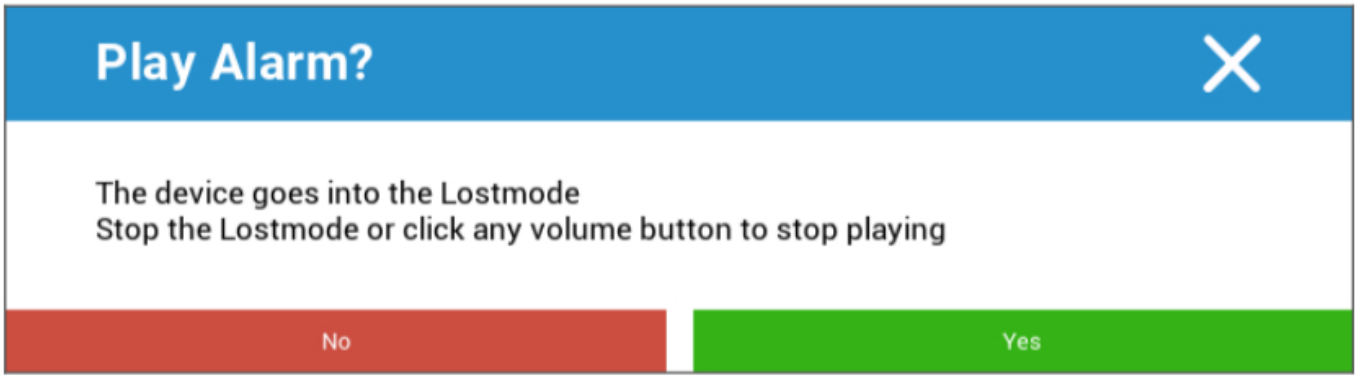
Ici, une commande d'arrêt est envoyée à l'appareil de l'utilisateur final.

Redémarrer l’appareil

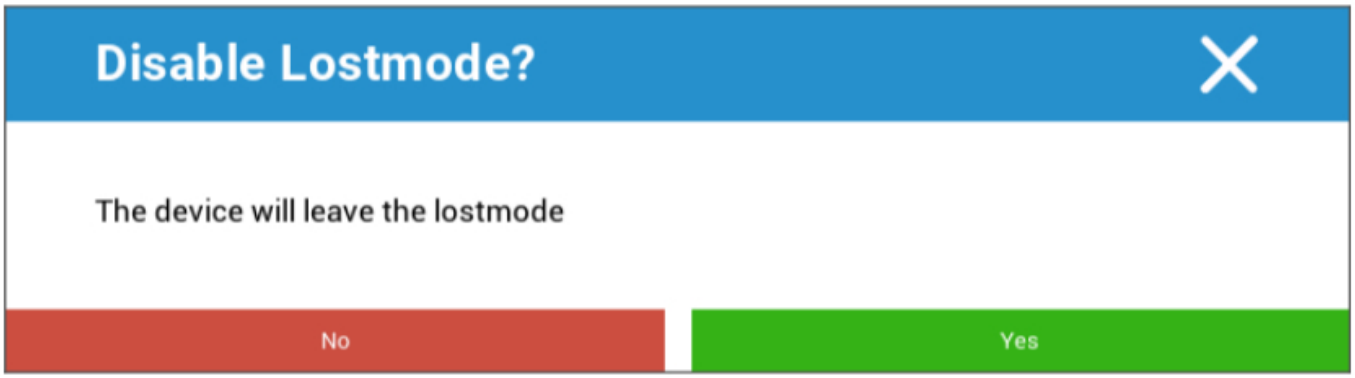


Une commande de redémarrage est envoyée à l'appareil de l'utilisateur final.

Alarm & Lostmode | Disable Lostmode



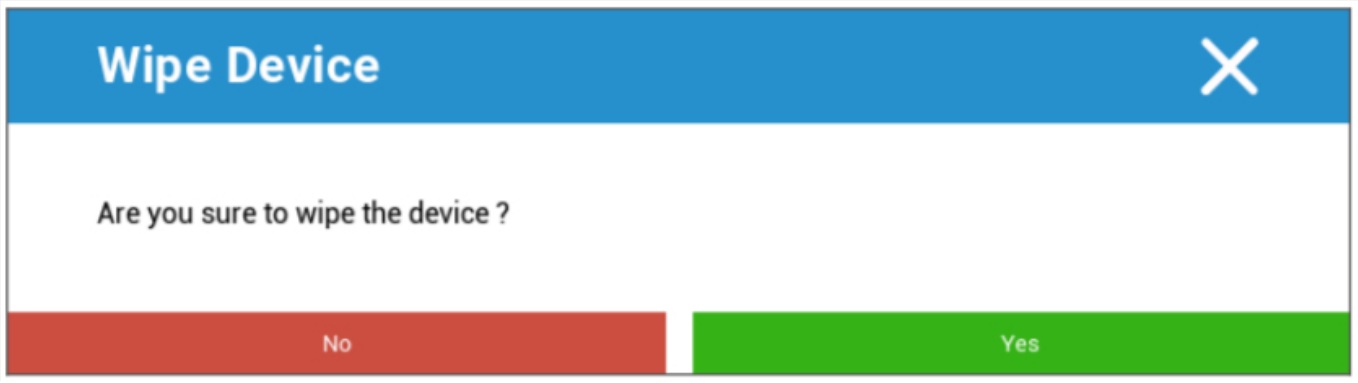
Ici, l'appareil peut être réglé en mode Perdu, ce qui permet à l'appareil de jouer en permanence un son d'alarme. Le Lostmode peut être arrêté en appuyant sur n'importe quel bouton de volume de l'appareil ou à distance en cliquant sur "Désactiver le Lostmode" :



Supprimer le dispositif

La commande de suppression peut être exécutée ici. Vous pouvez à nouveau décider si l'appareil doit uniquement être supprimé d'AppTec360 ("Supprimer du système") ou si l'appareil doit être supprimé d'AppTec360 et restauré à sa configuration d'usine ("Effacer et supprimer").

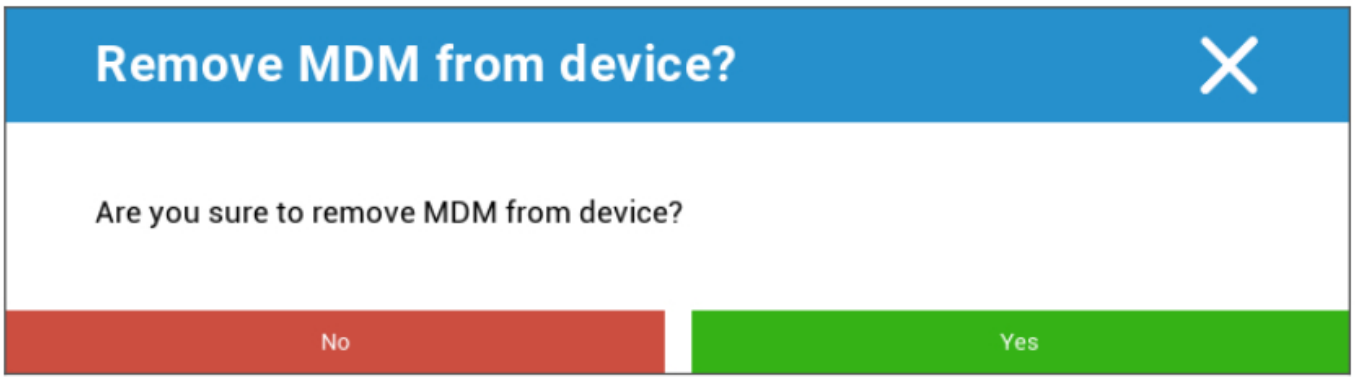
Effacer le dispositif



Sous "Effacer l'appareil", vous pouvez effectuer un effacement complet de l'appareil. Les paramètres d'usine de l'appareil sont rétablis.

Enterprise Wipe | Remove MDM

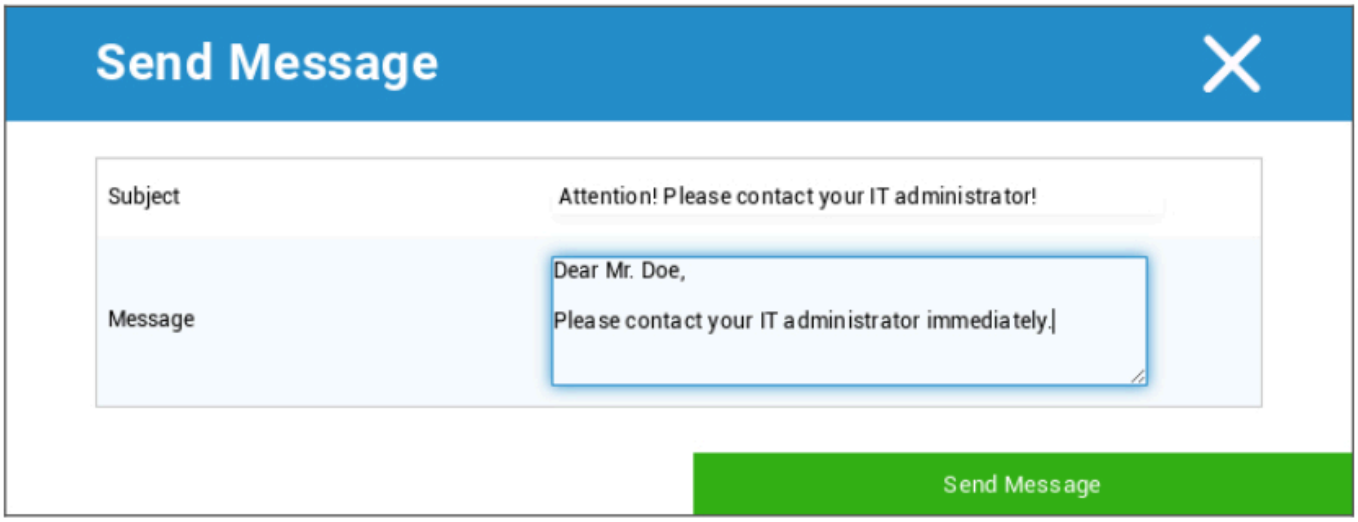
Seules les informations, applications et profils fournis par AppTec360 sont supprimés. Ainsi, les données de l'entreprise ne seront plus disponibles sur l'appareil de l'utilisateur final. La zone privée n'est pas affectée et reste sur l'appareil de l'utilisateur final.



Avec "Remove MDM" vous pouvez supprimer le profil MDM sur l'appareil de l'utilisateur final et tous les autres éléments fournis par AppTec.

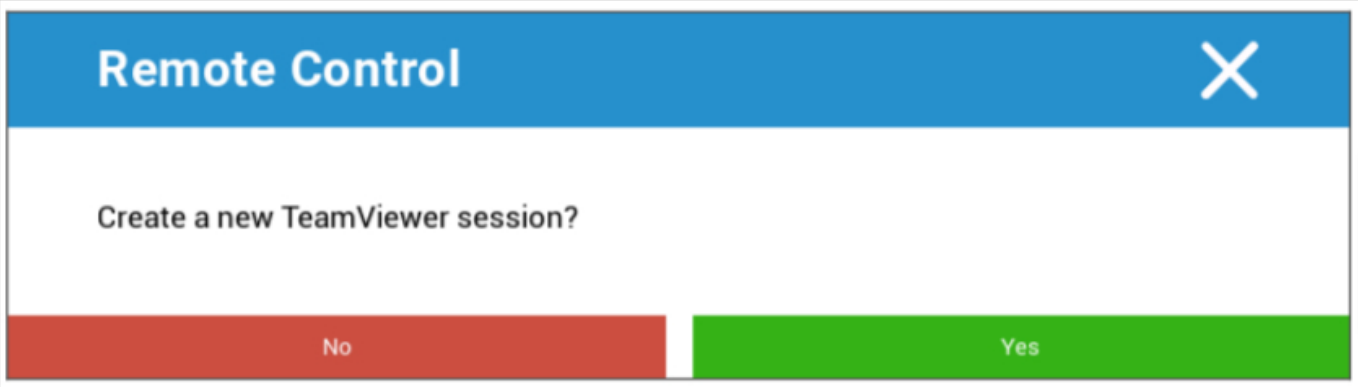
Cette commande exécute la même action que "Enterprise Wipe".

Envoyer un message



Vous pouvez ici envoyer une notification push à l'appareil concerné.

Contrôle à distance TeamViewer



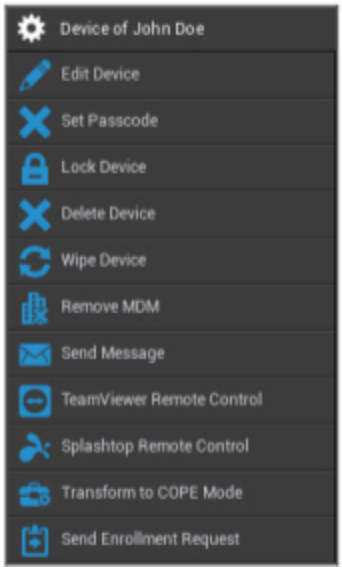
Ici, une session de contrôle à distance Teamviewer peut être lancée.

Envoyer une demande d’inscription

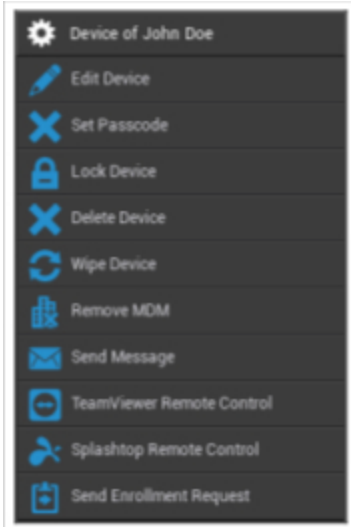
Avec "Envoyer une demande d'inscription", vous pouvez envoyer une (nouvelle) demande d'inscription à l'utilisateur concerné.

Android

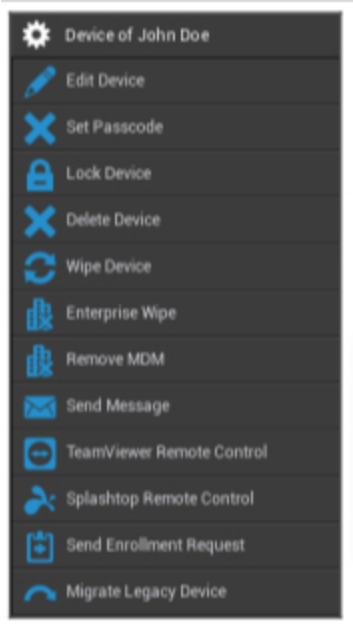
AE Dispositif entièrement géré (gestion du travail)



Profil de travail AE (conteneur)



Téléphone Android | Tablette

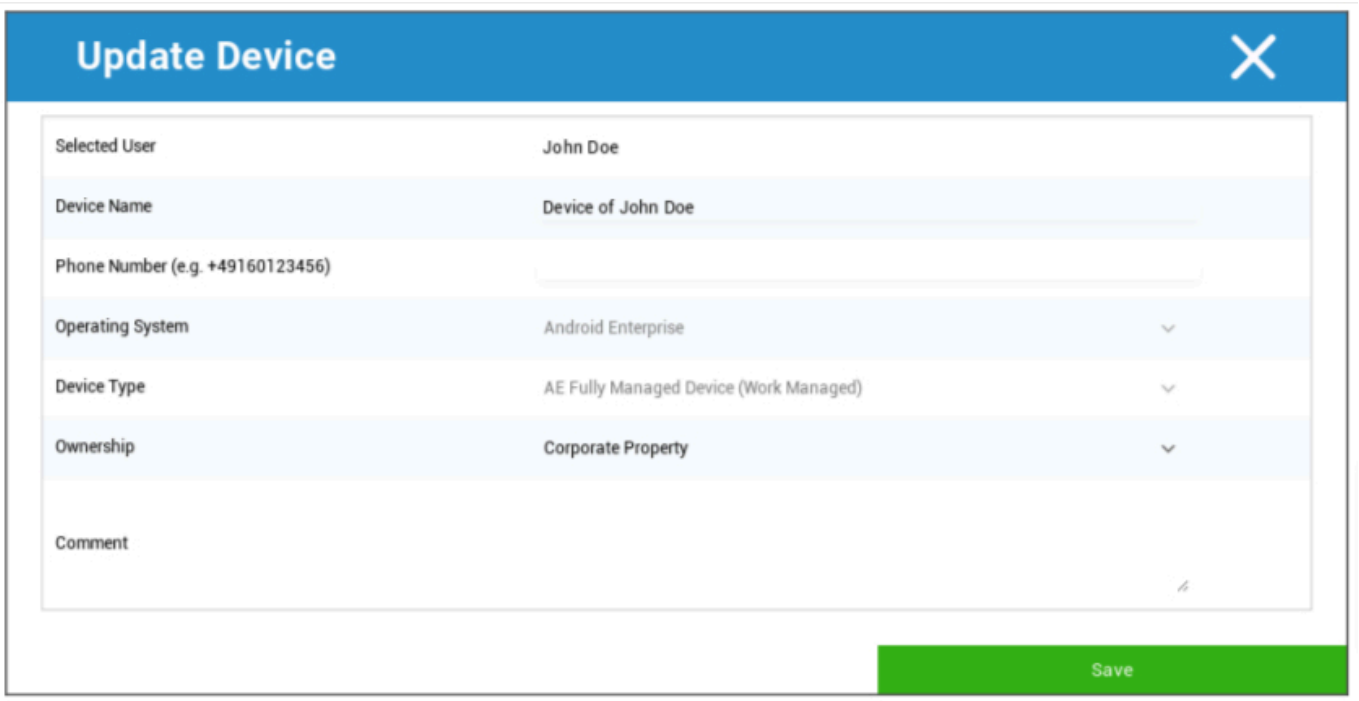


Modifier le dispositif	Modifier les informations sur l'appareil
Définir le code d'accès	Définir le code d'accès de l'appareil
Dispositif de verrouillage	Verrouiller le dispositif (écran de verrouillage)
Supprimer le dispositif	Supprimer l'appareil d'AppTec
Effacer le dispositif	Rétablir les paramètres d'usine de l'appareil
Nettoyage de l'entreprise	Les informations, les applications et les profils fournis par AppTec360 sont supprimés (l'appareil sera séparé du MDM).
Supprimer le MDM	
Envoyer un message	Envoyer des notifications push à l'appareil Le message sera affiché dans l'application AppTec360 (onglet Message).
Contrôle à distance TeamViewer	Démarrez une session de contrôle à distance pour cet appareil à l'aide de TeamViewer
Télécommande Splashtop	Démarrez une session de contrôle à distance pour cet appareil à l'aide de Splashtop
Transformation en mode COPE (uniquement sur les appareils entièrement gérés par l'AE (gestion du travail))	Créer un profil de travail sur ce dispositif AE entièrement géré (géré par le travail)
Envoyer une demande d'inscription	Envoi d'une demande d'inscription (répétée)
Migrer l'ancien appareil (uniquement sur les téléphones et tablettes Android lorsque l'inscription	Migration d'un profil de téléphone/tablette Android vers un profil d'appareil entièrement

se fait en mode propriétaire de l'appareil)	géré par AE (Work Managed)

Modifier le dispositif

Vous pouvez y mettre à jour un certain nombre d'informations sur l'appareil.



Utilisateur sélectionné	Utilisateur de l'appareil
Nom de l'appareil	Nom de l'appareil
Numéro de téléphone	Numéro de téléphone de l'appareil
Système d'exploitation	Android Enterprise Android
Type d'appareil	Android Enterprise : • AE Dispositif entièrement géré (gestion du travail) • Mode profil de travail AE (conteneur uniquement) • AE Dispositif entièrement géré avec profil de travail (COPE) Android : • Téléphone • Tablette
Propriété	Entreprise = propriété de l'entreprise

	Employé = propriété de l'employé
Commentaire	Descriptions supplémentaires pour le dispositif

Effacer le code d’accès

Vous pouvez ici supprimer le code d'accès de l'appareil sélectionné. Par défaut, sur Android, le code d'accès est fixé à "123456" - l'utilisateur peut et doit le modifier par la suite.

Dispositif de verrouillage

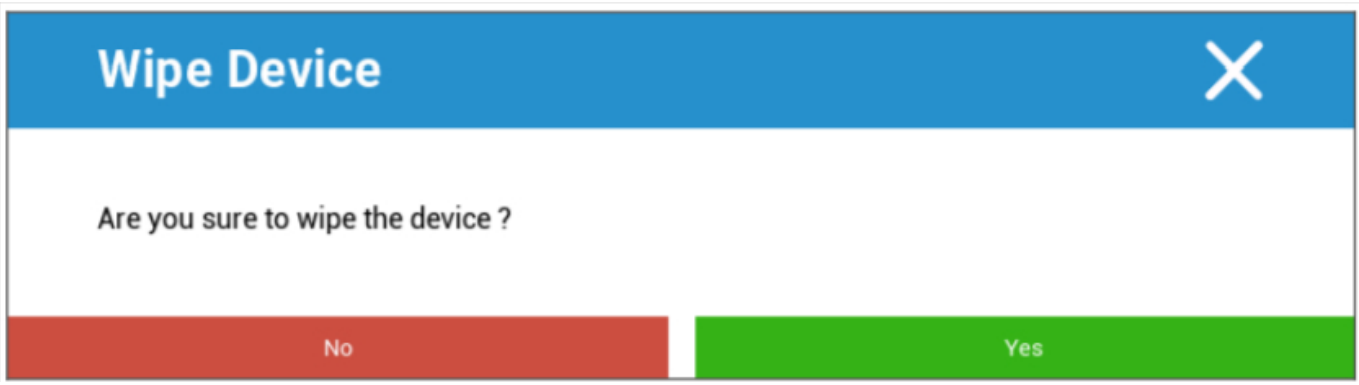
Ici, une commande de verrouillage du dispositif sera envoyée au dispositif (écran de verrouillage).

Supprimer le dispositif

Une commande de suppression peut être exécutée ici. Vous pouvez à nouveau décider si l'appareil doit seulement être supprimé d'AppTec360 ("Supprimer du système") ou si l'appareil doit être supprimé d'AppTec360 et en plus être restauré à ses paramètres d'usine ("Effacer et supprimer").

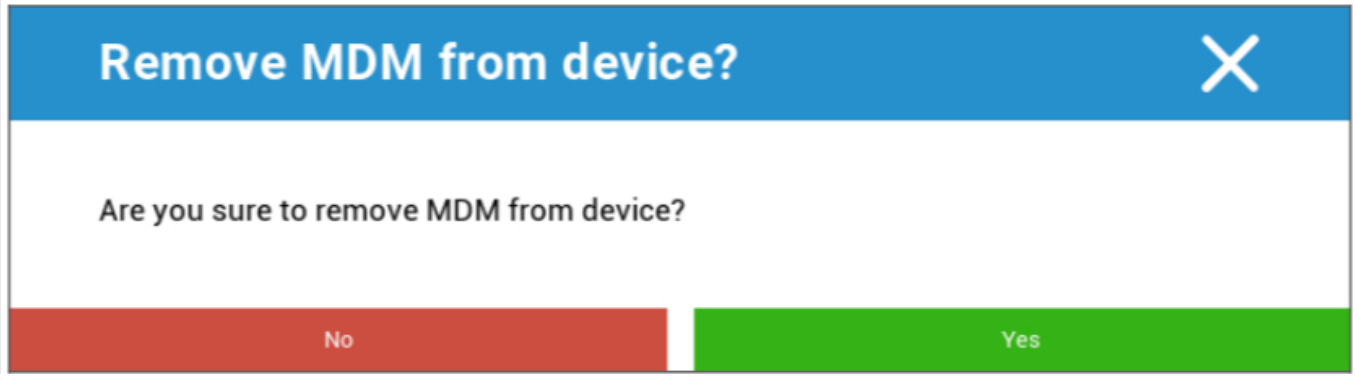
Effacer le dispositif

Sous "Effacer l'appareil", vous pouvez effectuer un effacement complet de l'appareil. L'appareil retrouvera alors ses paramètres d'usine.



En outre, si l'appareil contient une carte SD, vous pouvez l'effacer. Vous pouvez y parvenir en réglant le paramètre "Wipe SD Card too ? "sur "On".

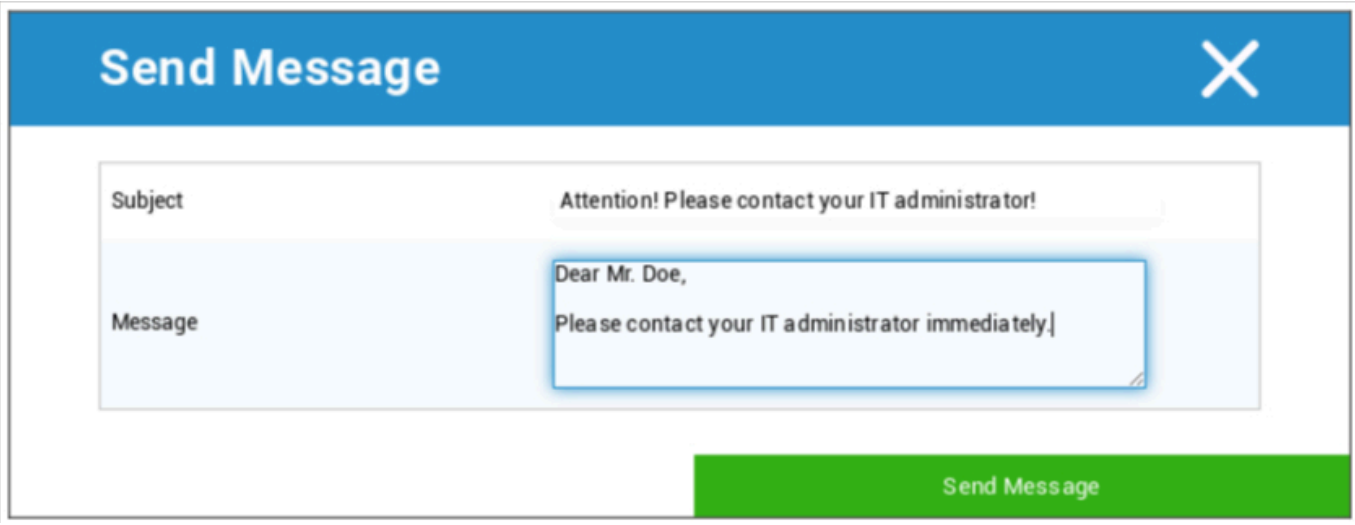
Supprimer le MDM



C'est la méthode recommandée pour créer une séparation avec le MDM.

Seules les informations, les applications et les profils fournis par AppTec360 sont supprimés, ce qui signifie que toutes les données de l'entreprise ne seront plus disponibles sur l'appareil de l'utilisateur final. La sphère privée, en revanche, n'est pas affectée et reste sur l'appareil de l'utilisateur final.

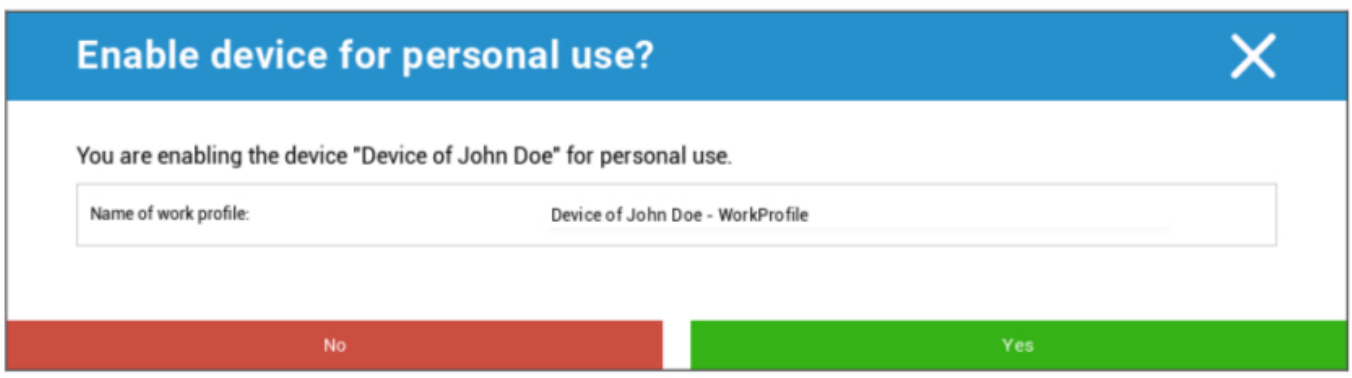
Envoyer un message



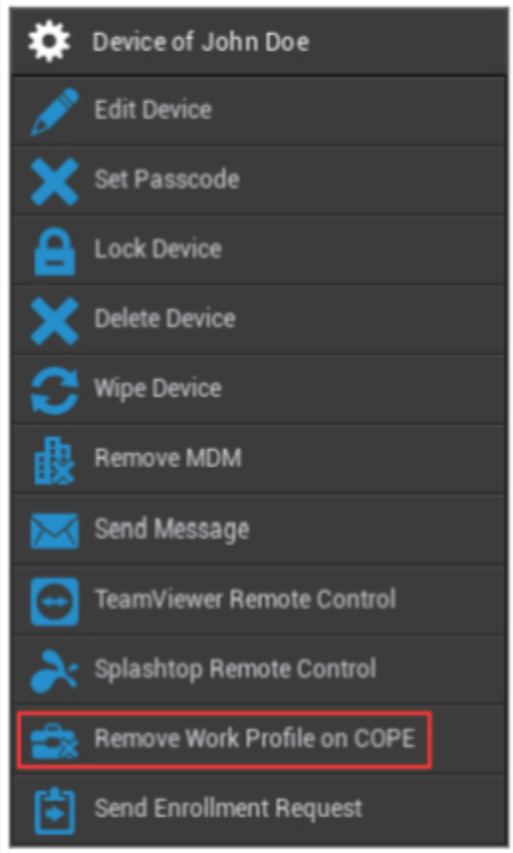
Vous pouvez ici envoyer une notification push à l'appareil de l'utilisateur final concerné.

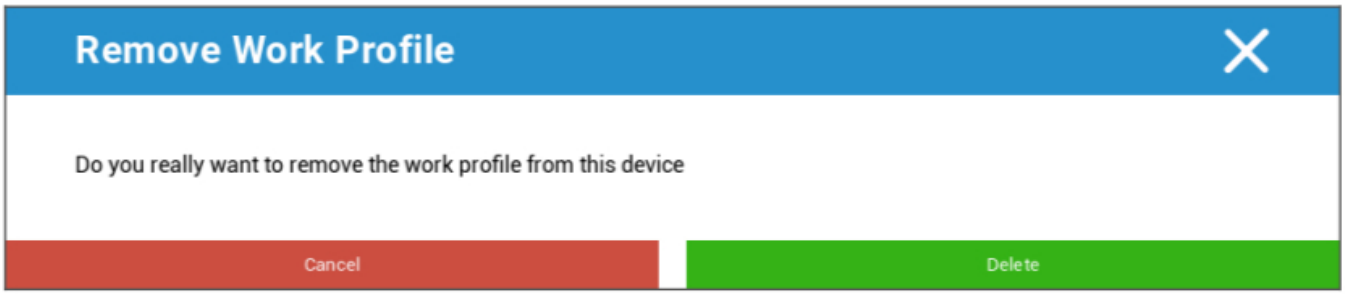
Transformer en mode COPE

Créer un profil de travail sur ce dispositif AE entièrement géré (géré par le travail)



Après avoir transformé l'appareil en mode COPE, vous pouvez supprimer le profil de travail en cliquant sur l'option de l'engrenage **Supprimer le profil de travail sur COPE**:




Remove Work Profile
Do you really want to remove the work profile from this device
Cancel
Delete

Envoyer une demande d’inscription

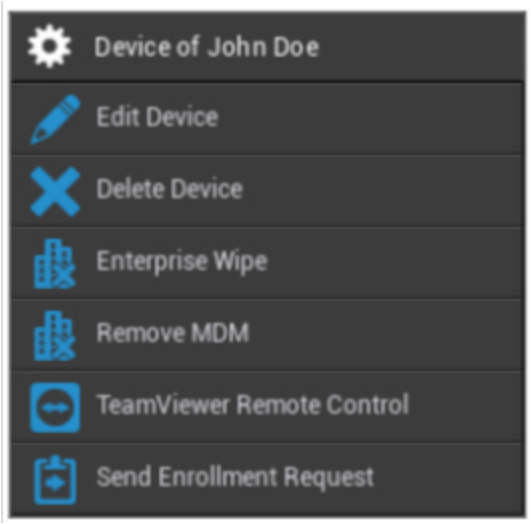
L'option "Envoyer une demande d'inscription" permet d'envoyer une nouvelle demande d'inscription à l'utilisateur concerné.

Veuillez noter que seule la demande d'inscription la plus récente est valable.

Migration d’un dispositif existant

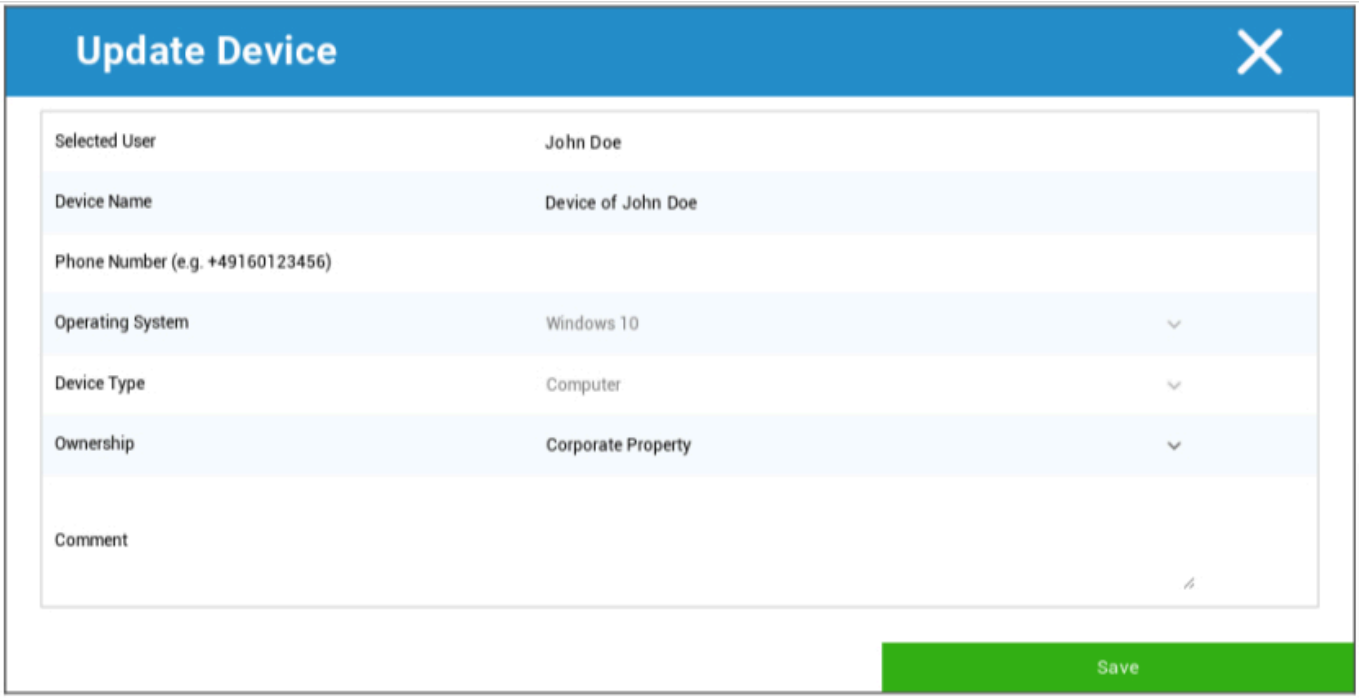
Migration d'un profil de téléphone/tablette Android vers un profil d'appareil entièrement géré par AE (Work Managed)

Fenêtres



Nom de l'appareil	Nom de l'appareil sélectionné
Modifier le dispositif	Modifier l'appareil
Supprimer le dispositif	Supprimer l'appareil d'AppTec
Nettoyage de l'entreprise	Les informations, applications et profils fournis par AppTec360 sont supprimés.
Supprimer le MDM	
Contrôle à distance TeamViewer	Contrôlez l'appareil à distance avec TeamViewer
Envoyer une demande d'inscription	Envoyer une nouvelle demande d'inscription

Modifier le dispositif

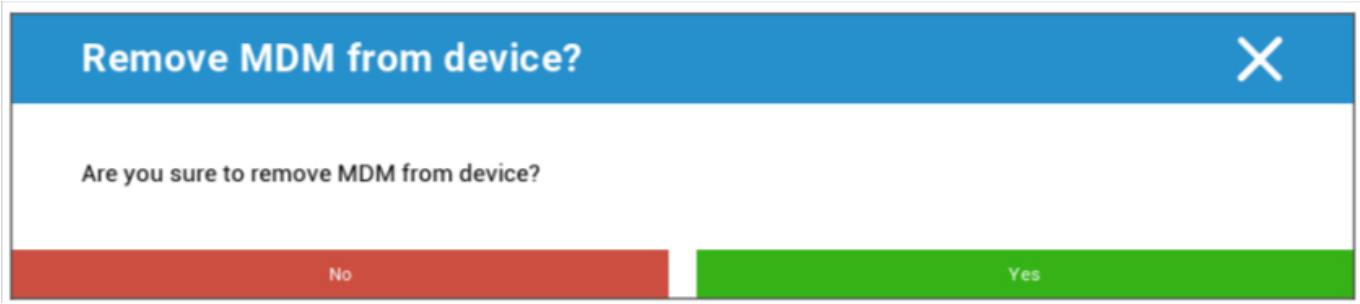


Vous pouvez y mettre à jour diverses informations sur l'appareil.

Supprimer le dispositif

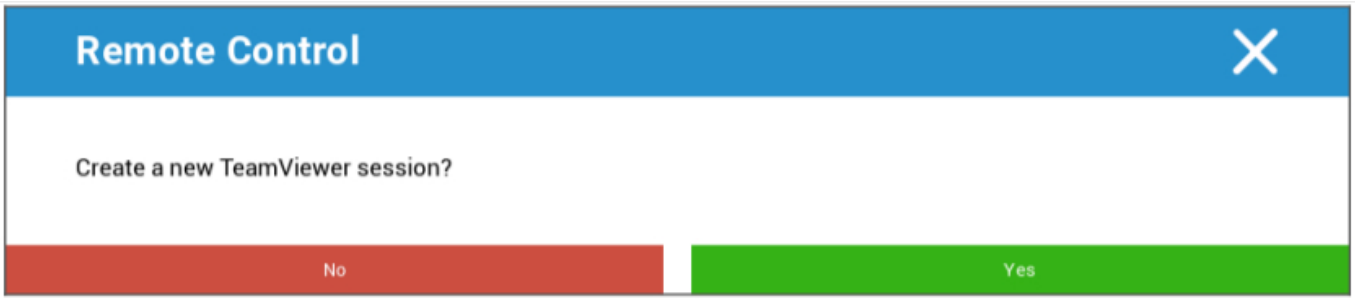
Ici, il est possible d'exécuter la commande de suppression qui supprime uniquement le dispositif d'AppTec360.

Enterprise Wipe | Remove MDM



Seules les informations, applications et profils fournis par AppTec360 sont supprimés. Ainsi, les données de l'entreprise ne seront plus disponibles sur l'appareil de l'utilisateur final. La zone privée n'est pas affectée et reste sur l'appareil de l'utilisateur final.

Contrôle à distance TeamViewer



Ici, vous pouvez démarrer une session de contrôle à distance TeamViewer pour cet appareil.

Envoyer une demande d’inscription

Avec "Envoyer une demande d'inscription", vous pouvez envoyer une (nouvelle) demande d'inscription à l'utilisateur concerné.

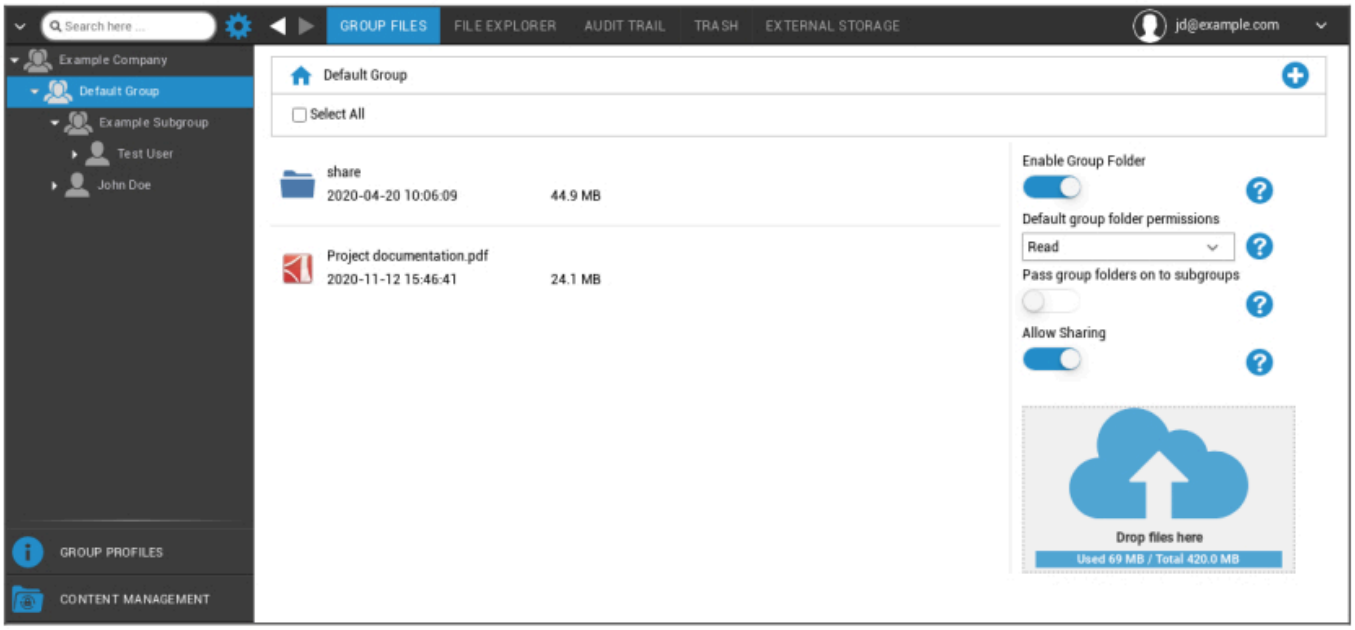
Gestion du contenu

Lorsque vous êtes dans un groupe, vous pouvez gérer la ContentBox d'AppTec avec "Content Management".

Avec la Content Box, vous pouvez distribuer en toute sécurité des documents et d'autres données d'entreprise sur les appareils des utilisateurs finaux.

Dossiers de groupe

Les "fichiers de groupe" représentent une partie fondamentale de ContentBox. Vous y définissez les paramètres, téléchargez des documents, créez de nouveaux dossiers, etc.



Le symbole situé dans le coin supérieur droit vous permet de créer de nouveaux dossiers qui seront rattachés au groupe correspondant en cliquant sur "Ajouter un dossier".

Le symbole situé dans le coin supérieur droit vous permet de créer un nouveau dossier via "Ajouter un dossier", qui doit être attribué au groupe correspondant.

Vous pouvez donner au dossier le nom que vous souhaitez.

Via "Upload Files", vous pouvez télécharger des données. Votre Standard-Explorer s'ouvre alors. Vous pouvez bien entendu effectuer ces deux actions dans chaque (sous) dossier.

Le symbole dans le coin supérieur gauche vous permet de revenir au menu principal.

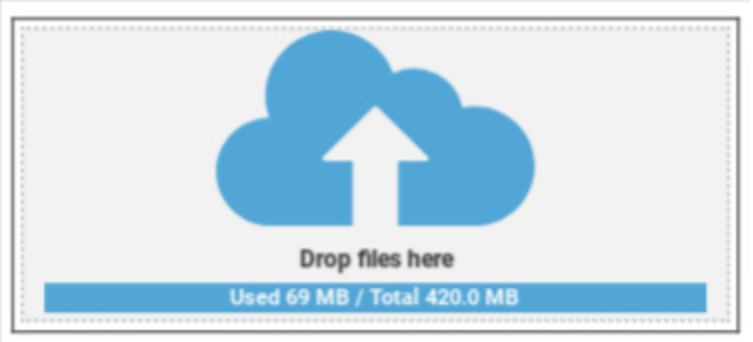
Vous pouvez sélectionner plusieurs dossiers et fichiers et les télécharger en cliquant sur "Télécharger" ou les effacer en cliquant sur "Supprimer".

Vous pouvez également sélectionner tous les fichiers et dossiers et exécuter les commandes "Télécharger" et "Supprimer".

Lorsque vous passez la souris sur un dossier ou un fichier, l'aperçu suivant s'affiche :

- Avec "Renommer", vous pouvez renommer le dossier/fichier
- Avec "Télécharger", vous pouvez télécharger le dossier/fichier.
- Avec "Supprimer", vous pouvez supprimer le dossier/fichier.

Activer le dossier de groupe	Si cette option est activée, tous les membres du groupe ont accès au dossier concerné.
Autorisations par défaut pour les dossiers de groupe	Permissions des utilisateurs du groupe sélectionné : Read = autorisation de lecture seule Mise à jour = autorisation de mise à jour Créer = autorisation de création Supprimer = supprimer l'autorisation
Transmettre des dossiers de groupe à des sous-groupes	S'ils sont activés, les sous-groupes respectifs peuvent avoir accès aux fichiers de données parents.
Autorisations pour les sous-groupes	Permissions des utilisateurs du sous-groupe sélectionné : Read = autorisation de lecture seule Mise à jour = autorisation de mise à jour Créer = autorisation de création Supprimer = supprimer l'autorisation
Autoriser le partage	Si cette option est activée, l'utilisateur peut partager des fichiers via un lien.



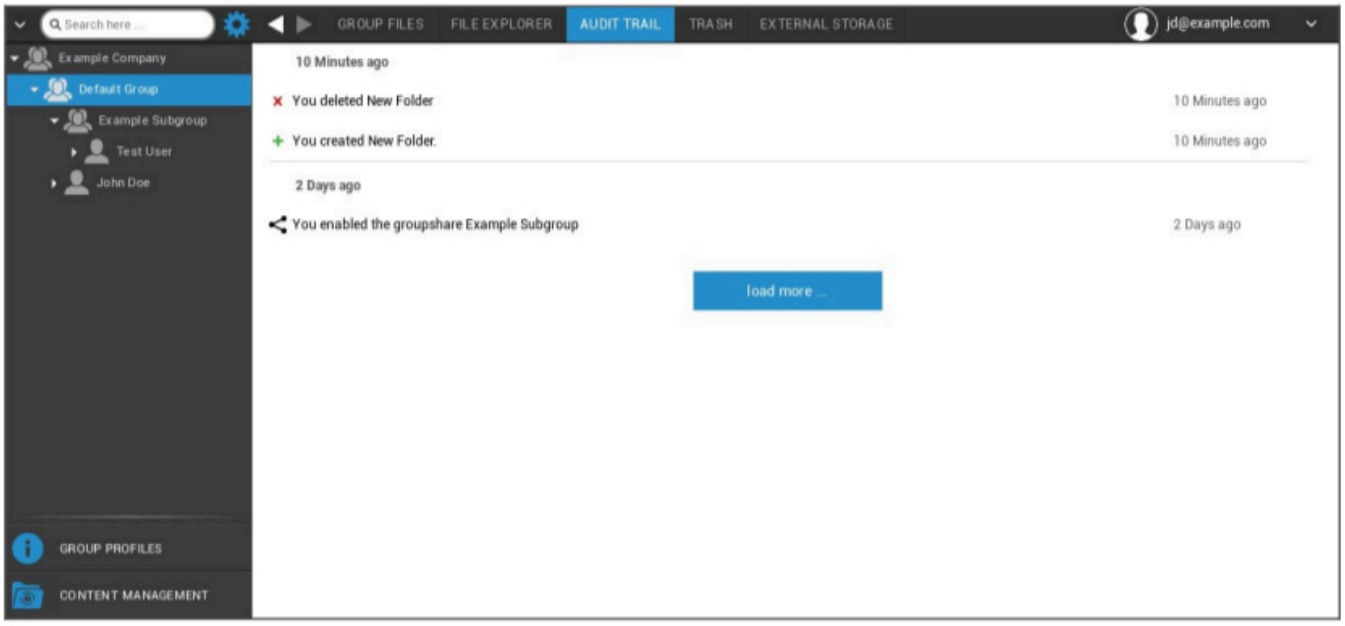
Pour télécharger des fichiers, vous pouvez utiliser ce champ, en tirant un fichier par Glisser-Déposer dans cette fenêtre. Vous pouvez également cliquer sur ce champ pour sélectionner et télécharger un fichier à l'aide d'Internet Explorer.

Explorateur de fichiers

Avec l'"Explorateur de fichiers", vous pouvez gérer tous les dossiers et fichiers, quel que soit le groupe dans lequel ils sont classés.

Vous y trouverez également les paramètres et les boutons que vous avez appris à connaître dans "Fichiers de groupe".

Piste d’audit



Dans "Audit Trail", vous pouvez voir, à partir de l'historique, quel utilisateur a créé, supprimé ou partagé quoi. Vous pouvez ainsi déterminer à tout moment ce qui a été fait des données de l'entreprise.

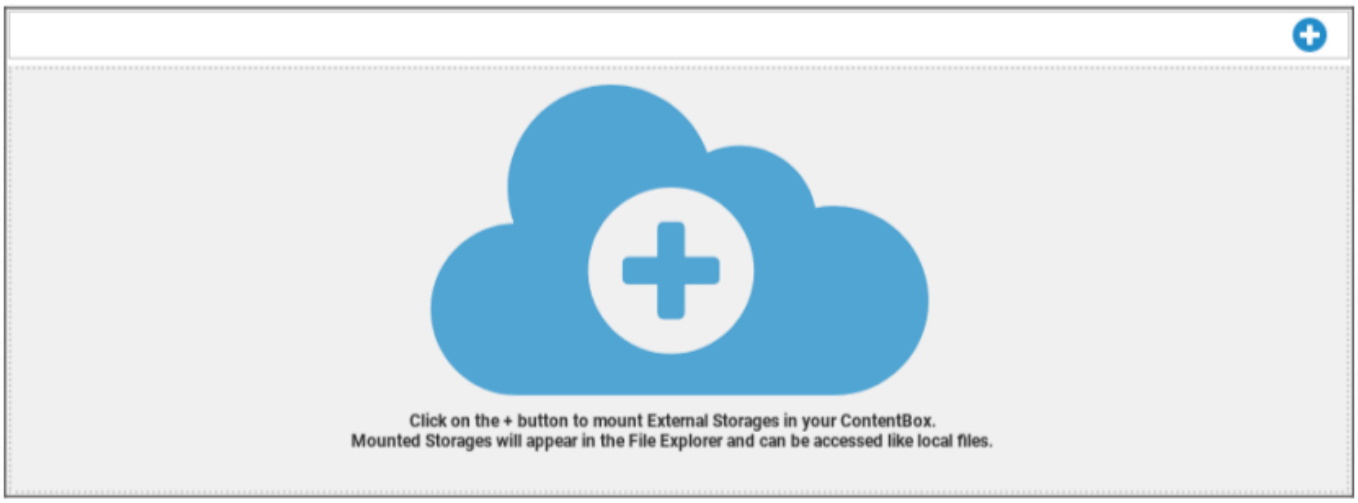
Poubelle

Si vous avez supprimé quelque chose (par accident), vous pouvez voir les dossiers et les fichiers sous "Corbeille" et les récupérer, selon vos souhaits.

- Avec "Undelete", vous pouvez récupérer les données/dossiers.
- Avec "Supprimer", vous pouvez effacer définitivement les données/dossiers - vous devez confirmer la commande de suppression une nouvelle fois.

Veuillez noter que la capacité de stockage utilisée dans la corbeille réduit l'espace total disponible - il s'agit d'une exigence d'ownCloud.

Stockage externe



Sous la rubrique "Stockage externe", vous pouvez connecter un stockage externe.

Le symbole permet d'ajouter un espace de stockage (supplémentaire).

Type	Amazon S3, FTP, SFTP, ownCloud, WebDAV, Windows Share, SharePoint

Amazon S3	
Nom d'affichage	Nom d'affichage
Clé d'accès	Clé d'accès
Clé secrète	Clé de sécurité
Seau	Identité précise du sous-dossier qui vous a été attribué
Nom d'hôte (facultatif)	Nom d'hôte (facultatif)
Port (en option)	Port (en option)
Région	Région (facultatif)
Activer SSL	Activer SSL
Activer le style de chemin	Clear Path Adresse qui vous a été attribuée

FTP	
Nom d'affichage	Nom d'affichage
Hôte	Adresse de l'hôte
Nom d'utilisateur	Nom d'utilisateur
Mot de passe	Mot de passe
Racine	Menu principal
Sécurisé ftps://	

SFTP	
Nom d'affichage	Nom d'affichage
Hôte	Adresse de l'hôte
Nom d'utilisateur	Nom de l'utilisateur
Mot de passe	Mot de passe
Racine	Menu principal

ownCloud	
Nom d'affichage	Nom d'affichage
URL	URL de ownCloud
Nom d'utilisateur	Nom d'utilisateur
Mot de passe	Mot de passe
Sous-dossier distant	Dossier standard
Sécuriser https://	

WebDAV	
Nom d'affichage	Nom d'affichage
URL	URL WebDAV
Nom d'utilisateur	Nom de l'utilisateur
Mot de passe	Mot de passe
Racine	Menu principal
Sécuriser https://	
Partage de Windows	La prise en charge de Windows Share sera bientôt disponible
SharePoint	La prise en charge de Microsoft SharePoint sera bientôt disponible

Journal d’audit

Vous trouverez ici un journal qui enregistre des informations sur les actions effectuées dans la console MDM.

L'icône de filtre permet d'appliquer des filtres à la liste affichée.

Le menu déroulant **Éléments par page** permet de sélectionner le nombre d'éléments à afficher sur une page de la liste.

Mesures prises / modification de la configuration	L'action qui a été entreprise / Le paramètre qui a été modifié
Valeur	Valeur de l'action entreprise / du paramètre modifié
Utilisateur	Le nom de l'utilisateur qui a effectué l'action / qui a modifié le paramètre
Date	L'heure à laquelle cette action a été entreprise / ce paramètre a été modifié.
Chemin d'accès / Type	Chemin d'accès à l'endroit où cette action a été effectuée / ce paramètre a été modifié

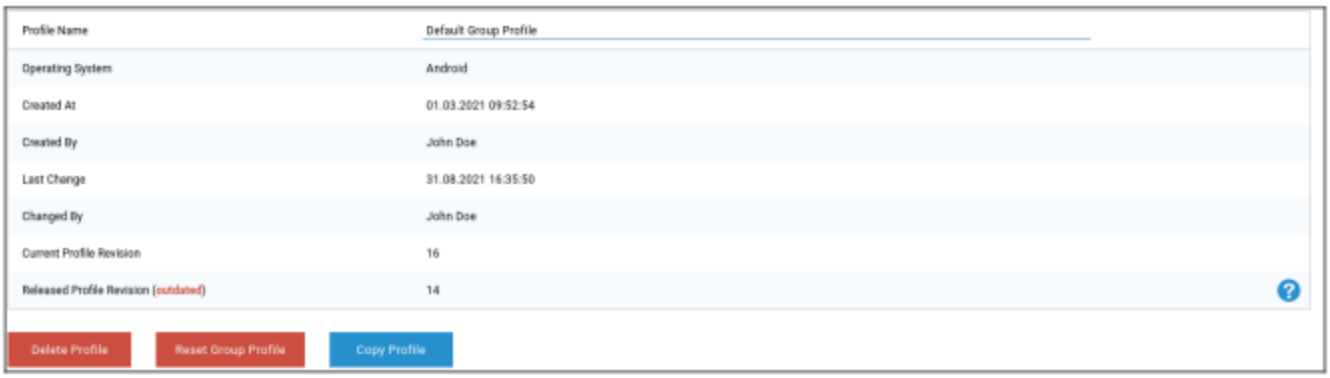
Configuration iOS

Général

Selon que vous avez sélectionné un groupe ou un appareil, l'affichage et les sous-points sont différents.

Aperçu du profil du groupe (uniquement au niveau du groupe)

Lorsque vous ouvrez un profil de groupe, vous obtenez une vue d'ensemble rapide du profil



Nom du profil	Nom du profil (peut être modifié ici)
Système d'exploitation	Système d'exploitation pour lequel le profil est établi
Créé à	Moment de la création
Créé par	Le créateur du profil
Dernier changement	Date de la dernière modification du profil
Modifié par	Compte ayant effectué les dernières modifications
Révision du profil actuel	Révision de l'état du profil sauvegardé
Révision du profil validé	Révision du profil attribué ("Attribuer maintenant"). Si l'étiquette affiche "(obsolète)" derrière le texte, cela signifie que vous avez enregistré le profil mais que vous ne l'avez pas encore attribué.

Informations générales

Si vous êtes directement sur l'appareil, vous recevrez un bref aperçu de l'appareil sélectionné.

Nom de l'appareil	Nom de l'appareil
Numéro de téléphone	Numéro de téléphone de l'appareil
Modèle	Numéro de modèle
Système d'exploitation	OS
Numéro de série	Numéro de série de l'appareil
Propriété des appareils	Dispositif d'entreprise ou privé Entreprise = appareil de l'entreprise Employé = dispositif privé
Type d'appareil	Type d'appareil (tablette ou téléphone)
Jailbroken	S'il y a un Jailbreak sur l'appareil
Supervisé	Indique s'il s'agit d'un dispositif supervisé
Conforme à la loi	Si des lignes directrices ont été violées
Dernière visite	État de la dernière communication de l'appareil avec le serveur AppTec360

Paramètres

Ces paramètres contiennent le nom de l'appareil et un arrière-plan prédéfini.

Nom de l'appareil en fonction du nom du système	Le nom qui sera émis dans la console AppTec360 (dans la structure hiérarchique de gauche), sera le même que sur l'appareil de l'utilisateur final respectif (peut être vu dans les paramètres de l'appareil).
Utiliser un fond d'écran personnalisé (appareils supervisés uniquement)	Vous pouvez ici prédéfinir l'arrière-plan qui doit être affiché sur l'appareil de l'utilisateur final (par exemple, pour un type de marque d'entreprise pour l'appareil). N'est disponible qu'en mode supervisé !
Mises à jour automatiques du système d'exploitation	Force les mises à jour du système d'exploitation si elles sont disponibles. Uniquement pour les appareils DEP en mode supervisé.
Polices personnalisées	Vous pouvez y ajouter des polices personnalisées.
Nom	Facultatif. Nom de la police visible par l'utilisateur. Ce champ est remplacé par le nom réel de la police après l'installation.
Police	Téléchargez le fichier de police (.otf ou .ttf).

Révision de la configuration

Vous obtiendrez ici un aperçu du profil de groupe attribué à l'appareil.

Si vous cliquez sur le profil du groupe, vous accédez directement au profil et vous pouvez effectuer des réglages.

Le symbole vous permet de rétablir les paramètres du profil de groupe pour les applications attribuées.

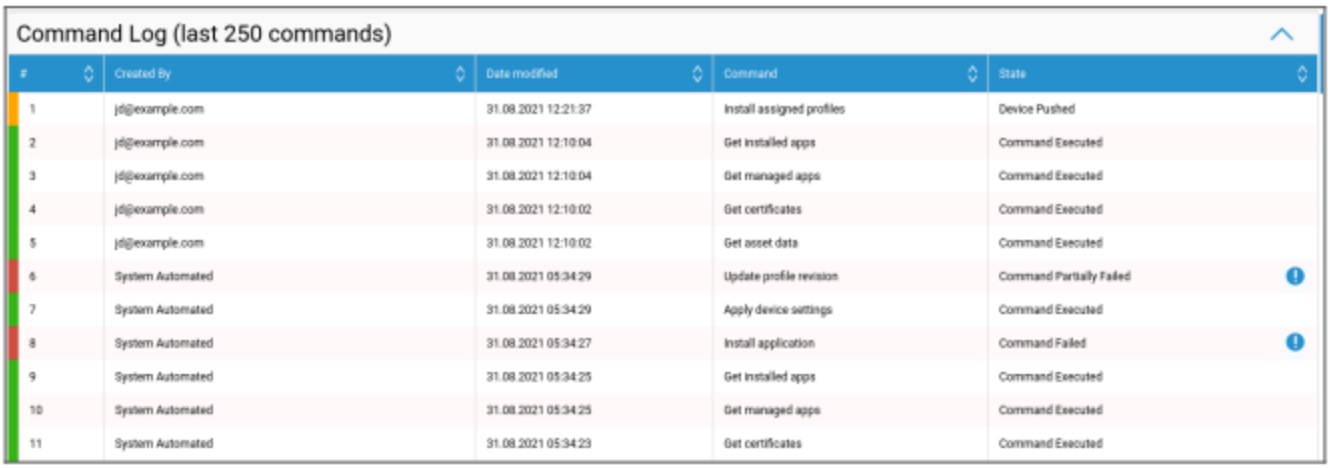
Le symbole permet de réinitialiser le profil de l'appareil pour qu'il ne comporte aucun paramètre.

La mention "Révision plus récente disponible" indique que le profil de groupe a été modifié et enregistré, mais qu'il n'a pas été attribué. Le profil de groupe doit être attribué avec "Attribuer maintenant" au niveau du groupe pour appliquer les changements aux appareils.

Journal de l’appareil (uniquement au niveau de l’appareil)

Journal des commandes

Vous pouvez voir ici quelles commandes ont été émises pour l'appareil et quel est leur état.



Les commandes créées par le "système automatisé" sont automatiquement créées par le système.

États possibles de la commande

Dispositif poussé	Une requête "push" a été envoyée au service "push" (par exemple APNS) pour demander à l'appareil de se reconnecter au serveur EMM.
Commande créée	La commande a été créée dans le système.
Commande envoyée	La commande a été envoyée à l'appareil après qu'il se soit connecté au serveur.
Commande exécutée	La commande a été exécutée avec succès.
Échec de la commande	La commande a échoué. *
Échec partiel de la commande	Selon le système d'exploitation de l'appareil, certaines commandes peuvent être regroupées. Dans ce cas, certaines parties de ce groupe de commande ont échoué. *
Commande exécutée, échec éventuel	La commande a été exécutée, mais peut-être qu'elle ne l'a pas été.
Commandement repoussé	La commande a été repoussée par un utilisateur.
Mise au rebut	La commande a été supprimée. Par exemple, parce qu'elle a été remplacée par une autre commande ou parce que l'appareil a été réenrôlé et que les anciennes commandes ont été supprimées.

Si le message est accompagné d'un point d'exclamation, vous pouvez obtenir plus d'informations en survolant l'icône avec votre curseur.

Gestion des actifs (uniquement au niveau de l’appareil)

Gestion des actifs (uniquement au niveau de l’appareil)

Informations sur l’appareil

Modèle	Numéro de modèle de l'appareil
Système d'exploitation	OS
Version OS	Version du système d'exploitation
Numéro de série	Numéro de série
UDID	Dispositif UDID
Nom de l'appareil	Nom de l'appareil
Supervisé	Indique si l'appareil est supervisé
État de la batterie	État de la batterie

Wi-Fi

Adresse IP	Adresse IP de l'appareil
WiFi MAC	Adresse MAC WiFi

Cellulaire

Statut	État (carte SIM présente)
Numéro de téléphone	Numéro de téléphone
État de l'itinérance	État actuel de l'itinérance
Itinérance (voix/données)	Statut d'itinérance pour la voix et les données
Adresse IP	Adresse IP
IMEI	Numéro IMEI
Opérateur/transporteur	Fournisseur de services cellulaires
Réseau de l'opérateur SIM	Réseau de l'opérateur SIM
Version transporteur	Version transporteur
Firmware du modem	Firmware du modem
Actuel MCC/MNC	Voir "SIM MCC/MNC"
SIM MCC/MNC	L'indicatif de pays du mobile est une identification de pays établie par l'UIT conformément à la norme E.212, qui, en conjonction avec le code de réseau mobile (MNC), est utilisé pour identifier un réseau cellulaire (=code de pays). Lorsque vous passez sur un autre réseau cellulaire, le "MCC/MNC actuel" et le "MCC/MNC SIM" sont donc différents.

Bluetooth

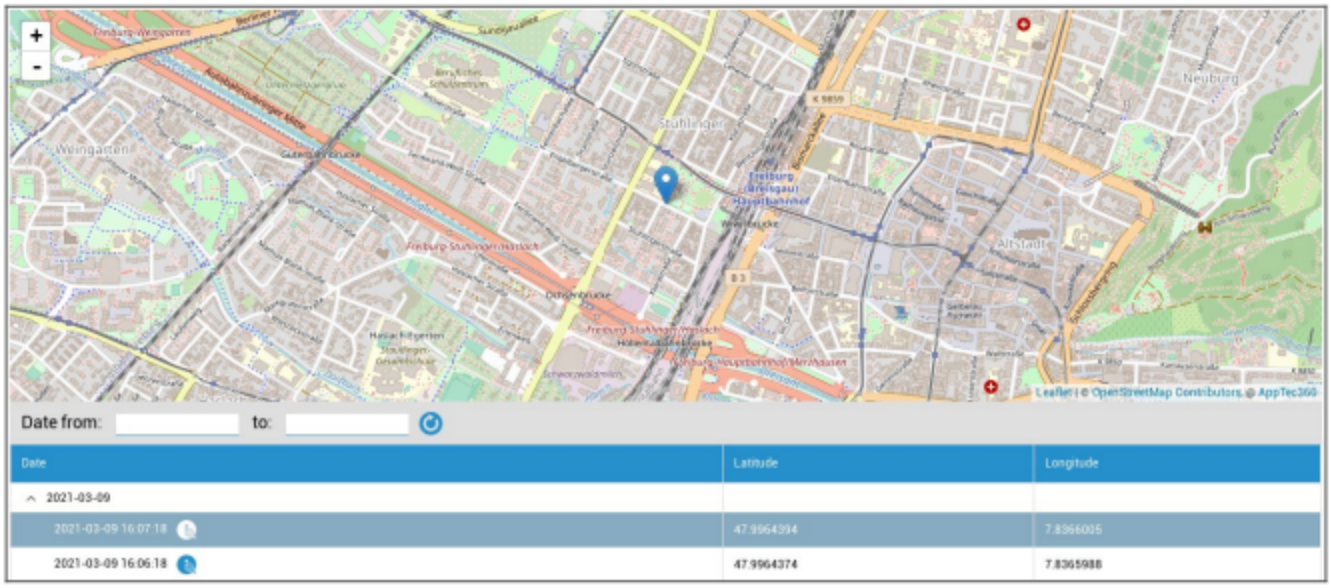
Bluetooth MAC	Adresse MAC Bluetooth

Gestion de la sécurité

Antivol (uniquement au niveau de l’appareil)

Informations GPS (uniquement au niveau de l’appareil)

Ici, vous pouvez évaluer l'emplacement actuel/dernier emplacement de l'appareil. La localisation peut être protégée par un ou deux mots de passe - Voir : Paramètres généraux - Confidentialité - Accès GPS



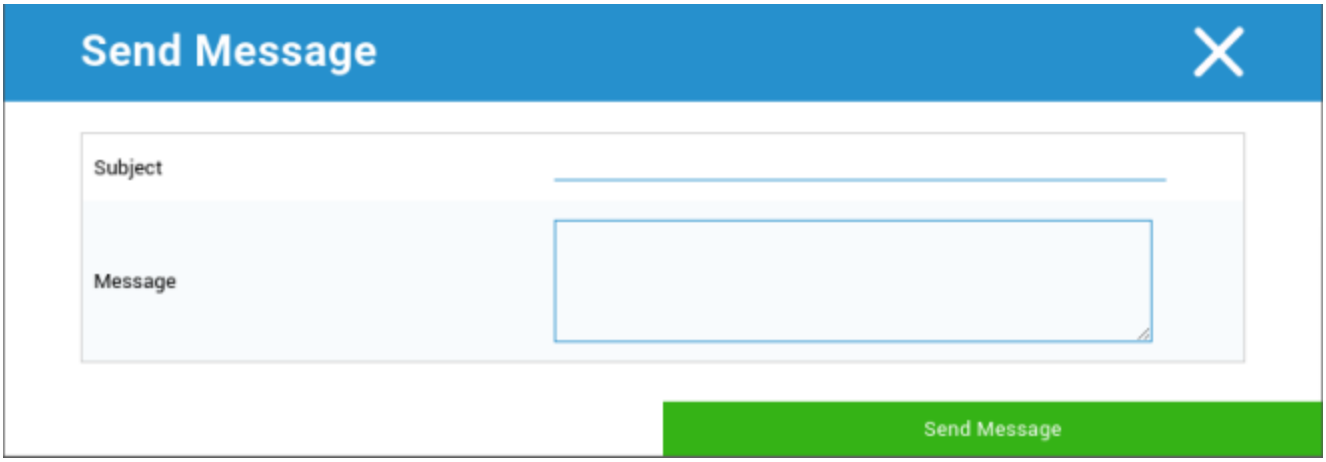
Effacement et verrouillage (uniquement au niveau de l’appareil)

Sous "Effacer et verrouiller", vous pouvez effectuer les trois actions suivantes :

Essuyage complet	L'appareil est restauré à ses paramètres d'usine (les données de l'entreprise et les données personnelles sont supprimées).
Nettoyage de l'entreprise	Seules les données de l'entreprise sont supprimées de l'appareil de l'utilisateur final (toutes les applications, données, etc. qui ont été fournies par AppTec).
Écran de verrouillage	Le verrouillage de l'écran est activé, il suffit de déverrouiller l'appareil avec le mot de passe/NIP de l'appareil.
Verrouillage judiciaire (dispositifs supervisés uniquement)	Si cette fonction est activée à l'aide du symbole  , l'appareil sera verrouillé en affichant un message qui ne pourra pas être fermé. L'employé ne peut pas non plus déverrouiller l'appareil. Seul l'administrateur peut déverrouiller l'appareil dans la console à l'aide du symbole de déverrouillage  .
Autoriser le verrouillage de l'activation (dispositifs supervisés uniquement)	Si cette fonction est activée, l'appareil sera verrouillé dès que la fonction "Trouver mon iPhone" sera activée dans les réglages iCloud.

Message (uniquement au niveau de l’appareil)

Dans la fenêtre suivante, vous pouvez remplir l'objet et un message et l'envoyer à un appareil d'utilisateur final :



Configuration de la sécurité

Code d’accès

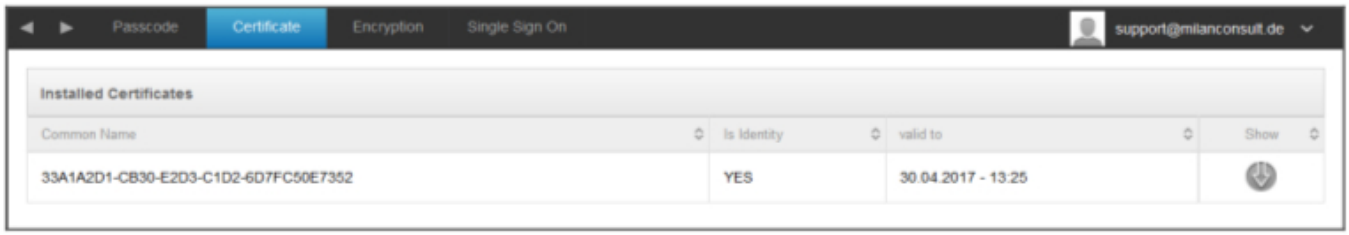
Vous définissez ici les paramètres du mot de passe de l'appareil

Désactivation du code autorisée	Lorsque ce paramètre est activé, il n'y a pas de demande de saisie d'un mot de passe Dès qu'un mot de passe est établi, il ne peut pas être désactivé
Autoriser une valeur simple	Permettre à l'utilisateur d'utiliser les mêmes chaînes de numéros, croissants et décroissants (ex. 1234, 1111).
Valeur alphanumérique requise	Les mots de passe doivent contenir au moins une lettre
Longueur minimale du code d'accès	Longueur minimale du mot de passe
Nombre minimum de caractères complexes	Nombre minimal de symboles alphanumériques dans le mot de passe
Âge maximal du code d'accès	Nombre de jours après lesquels le mot de passe doit être modifié
Verrouillage automatique maximal	Durée maximale après laquelle l'appareil est verrouillé
Délai de grâce maximum pour le verrouillage du dispositif	Après cette période, l'appareil passe en mode veille verrouillé.
Nombre maximal de tentatives infructueuses	Détermine le nombre de fois qu'un mot de passe peut être saisi de manière incorrecte avant qu'un effacement complet de l'appareil ne soit effectué.
Âge maximal du code d'accès (1-730 jours)	Âge maximal du mot de passe
Historique des codes d'accès (1-50 codes d'accès)	L'utilisation d'un ancien mot de passe est autorisée après ce nombre.

Un clic sur la corbeille ouvre la boîte de dialogue de réinitialisation du mot de passe, qui permet d'effacer un mot de passe oublié.

Certificat (uniquement au niveau de l’appareil)

Affiche les certificats disponibles sur l'appareil.


Passcode
Certificate
Encryption
Single Sign On
support@mlianconsult.de
Installed Certificates
Common Name
Is Identity
valid to
Show
33A1A2D1-CB30-E2D3-C1D2-6D7FC50E7352
YES
30.04.2017 - 13:25

Cryptage

Exiger le chiffrement du stockage	Activer la fonction de cryptage de l'appareil installé

Signature unique

Sous le point "Single Sign-On", vous pouvez configurer l'authentification Kerberos.

Ici, vous définissez les informations d'accès et les URL/applications respectives qui sont autorisées à utiliser les jetons Kerberos.

Disponible en mode supervisé	
Nom du compte	Nom du compte
Nom principal	Identité unique à laquelle les tickets Kerberos peuvent être distribués
Royaume	Votre royaume Kerberos, qui doit être utilisé (ex. votre domaine)

Avec le symbole, vous pouvez créer des URL supplémentaires.

Modèle d'URL utilisé pour limiter ce compte	URL à déterminer, vers lesquels les tickets Kerberos peuvent être distribués

Avec le symbole, vous pouvez créer des applications supplémentaires.

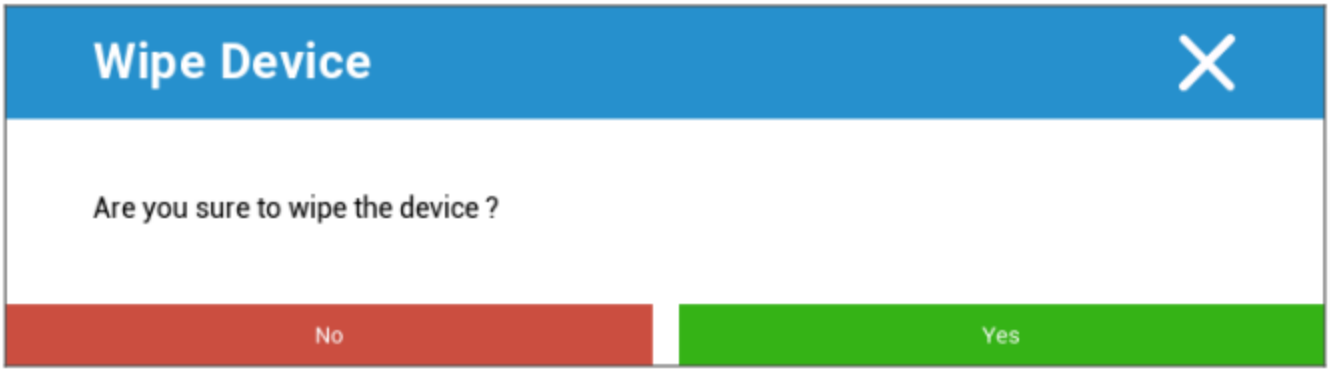
Applications pour limiter ce compte	Appels à déterminer, auxquels les tickets Kerberos peuvent être distribués

Fin de vie (uniquement au niveau de l’appareil)

Effacer (uniquement au niveau de l’appareil)

Sous "Effacer", vous pouvez rétablir les paramètres d'usine de l'appareil. Dans ce cas, les données de l'entreprise et les données privées sont supprimées sur l'appareil de l'utilisateur final.

En cliquant sur le "symbole moins", vous devriez recevoir le message suivant



Si vous répondez "Oui", vous pouvez procéder à l'effacement.

Sous "Rapport d'effacement", les éléments suivants peuvent être affichés

Effacé par	Historique de la personne qui a effectué l'essuyage
Date	Date
Statut	État (par exemple, si le nettoyage a été effectué avec succès)

Paramètres de restriction

Fonctionnalité de l’appareil

Ici, vous pouvez bloquer des fonctionnalités individuelles de l'appareil de l'utilisateur final.

Autoriser l'installation d'applications	Permettre l'installation d'applications
Autoriser l'appareil photo	Permettre l'utilisation de l'appareil photo
Autoriser FaceTime	Autoriser FaceTime
Permettre la capture d'écran	Permettre la capture d'écran
Autoriser la synchronisation automatique en cas d'itinérance	Autoriser la synchronisation automatique en cas d'itinérance
Autoriser Siri	Autoriser Siri
Autoriser la numérotation vocale	Autoriser la numérotation vocale
Permettre l'achat in-app	Permettre l'achat in-app
Exiger le mot de passe de l'iTunes Store pour tous les achats	Exiger le mot de passe de l'iTunes Store pour tous les achats
Permettre les jeux multijoueurs	Permettre les jeux multijoueurs
Permettre l'ajout d'amis Game Center	Permettre l'ajout d'amis Game Center
Permettre l'ouverture d'un système géré à un système non géré	Permettre l'ouverture de contenus d'applications gérées dans des applications non gérées
Permettre l'ouverture d'une zone non gérée à une zone gérée	Permettre l'ouverture de contenus dans des applications non gérées dans des applications gérées
Autoriser l'affichage du jour dans l'écran de verrouillage	Lorsque ce paramètre est activé, la vue "Aujourd'hui" s'affiche dans le centre de notification de l'écran de verrouillage.
Autoriser le centre de contrôle dans l'écran de verrouillage	Autoriser le Centre de contrôle sur l'écran de verrouillage
Autoriser TouchID	Autoriser TouchID
Autoriser les mises à jour de l'infrastructure de clés publiques (PKI) par voie hertzienne	Autoriser les mises à jour de l'infrastructure de clés publiques (PKI) par voie hertzienne

Autoriser le livret pendant le verrouillage	Autoriser le livret lorsque l'appareil est verrouillé
Limiter le suivi des publicités	Cette fonction désactive l'Ad Tracking (ex. les annonceurs ne peuvent pas utiliser l'Ad Tracking afin de distribuer des publicités personnalisées).
Autoriser le transfert	Autoriser le transfert
Permettre aux résultats de l'internet d'être mis en avant	Autoriser les résultats internet dans les spots (ex. Bing ou Wikipedia)
Exiger un code d'accès lors du premier appairage AirPlay	Exiger un code d'accès lors du premier appairage AirPlay
Protection du poignet de la montre Force	Si elle est activée, l'Apple Watch est forcée d'utiliser la "protection du poignet" (reconnaissance du poignet).
Autoriser la photothèque iCloud	Autorise la photothèque iCloud. Si vous ne l'autorisez pas, toutes les photos qui n'ont pas été entièrement téléchargées à partir d'iCloud seront effacées du stockage local.
Disponible en mode supervisé	
Autoriser la modification du compte	Autoriser la modification de "courrier, contacts, calendrier".
Autoriser AirDrop	Autoriser AirDrop
Autoriser la modification cellulaire de l'application	Ce paramètre bloque le réglage des applications autorisées à utiliser les données mobiles. Ce paramètre peut, par exemple, être défini manuellement sur l'appareil de l'utilisateur final et cette restriction peut alors être activée
Permettre à Siri d'interroger le contenu généré par l'utilisateur sur le web	La recherche sur certains sites web est bloquée, par exemple Wikipedia, parce que tout le monde peut y apporter des modifications à sa guise.
Activer le filtre de blasphèmes de Siri	Les injures adressées à Siri sont censurées.
Autoriser l'iBook Store	Autoriser l'iBook Store
Autoriser l'iBook Store Erotica	Autoriser l'iBook Store Erotica
Autoriser la modification des paramètres de Find my Friends	Autoriser la modification des paramètres de Find my Friends
Autoriser Game Center	Autoriser Game Center

Autoriser le couplage d'hôtes	Contrôle de l'appariement des ordinateurs
Permettre l'installation de profils de configuration	Permettre l'installation de profils de configuration
Autoriser Supprimer l'application	Suppression des applications de contrôle
Autoriser iMessage	Autoriser iMessage
Autoriser l'effacement de tous les contenus et paramètres	Permettre l'effacement de tous les contenus et paramètres
Permettre de configurer des restrictions	Permettre de configurer des restrictions
Permettre le podcast	Permettre le podcast
Autoriser la recherche de définition	Permettre la recherche de définitions
Autoriser le clavier prédictif	Autoriser le clavier prédictif
Autoriser la correction automatique	Autoriser la correction automatique
Autoriser l'installation d'applications d'interface utilisateur	Si elle est désactivée, aucune application ne peut être installée à partir de l'AppStore public (l'icône n'est plus affichée). Cependant, les applications peuvent toujours être installées via iTunes et le Configurateur.
Autoriser les raccourcis clavier	Autoriser les raccourcis clavier, si l'appareil est relié à un clavier physique.
Autoriser l'appairage de l'Apple Watch	Interdit l'appairage entre l'appareil et l'Apple Watch, les connexions existantes seront interrompues.
Autoriser la modification du code d'accès	S'il n'est pas autorisé, aucun mot de passe ne peut être ajouté, modifié ou supprimé.
Autoriser la modification du nom du périphérique	Lignes directrices pour déterminer si le nom de l'appareil peut être modifié
Permettre la modification du papier peint	Ligne directrice pour déterminer si le papier peint peut être changé
Autoriser le téléchargement automatique d'applications	Si elle est désactivée, une application achetée ne sera pas automatiquement installée sur d'autres appareils. Ne s'applique pas aux mises à jour des applications existantes.
Autoriser les nouvelles	Autoriser les actualités sur l'appareil iOS

Autoriser la confiance dans les applications d'entreprise	S'il est défini sur false, il empêche de faire confiance aux applications d'entreprise.

iCloud

Bloquer certaines fonctionnalités lors de l'appairage iCloud

Autoriser la sauvegarde	Autoriser la sauvegarde
Autoriser la synchronisation des documents	Autoriser la synchronisation des documents
Autoriser le flux de photos	Autoriser le flux de photos
Autoriser le partage de flux de photos	Autoriser le partage de flux de photos
Autoriser la synchronisation du trousseau dans le nuage	Autoriser la synchronisation du trousseau dans le nuage
Autoriser les applications gérées à stocker des données	Autoriser les applications gérées à stocker des données
Autoriser la synchronisation des notes et des surlignements pour les livres d'entreprise	Autoriser la synchronisation des notes et des surlignements pour les livres d'entreprise
Permettre la sauvegarde des livres d'entreprise	Permettre la sauvegarde des livres d'entreprise

Sécurité et vie privée

Bloquer ces fonctionnalités associées aux données de diagnostic

Permet d'envoyer des données de diagnostic à Apple	Permettre l'envoi de données de diagnostic à Apple
Autoriser l'utilisateur à accepter des certificats TLS non fiables	Autoriser l'utilisateur à accepter des certificats TLS non fiables
Forcer les sauvegardes cryptées	Forcer les sauvegardes cryptées

BYOD

Sécurité intégrée d’iOS (conteneur)

iOS a toujours été en mesure de faire la différence entre les réseaux gérés (professionnels) et les réseaux non gérés (privés). Tout ce qui provient du système MDM est traité comme géré. Par exemple, si vous installez une application via MDM ou si vous configurez un compte Exchange, celui-ci sera considéré comme géré par iOS.

Tout ce qui est configuré/installé manuellement sur l'appareil sera traité comme non géré. Par exemple, si l'utilisateur installe WhatsApp lui-même ou s'il ajoute un compte Exchange. Cependant, cette séparation n'a jamais affecté les contacts. Mais depuis iOS 11.3 (et les versions ultérieures), cette fonction a également été ajoutée pour les contacts.

Comme il s'agit d'une fonctionnalité de base du système d'exploitation, vous n'avez pas besoin d'installer quelque chose ou de configurer un conteneur spécial.

Activez la fonction intégrée pour séparer les applications/informations/fichiers privés et professionnels. Ce paramètre désactive également d'autres fonctions qui pourraient, par erreur, désactiver certaines parties de cette séparation.

Activation

Activer les solutions de conteneurs supportées par AppTec360

Activer le conteneur Google Divide	Activer le conteneur Google Divide
Activer le conteneur SecurePIM	Activer le conteneur SecurePIM

Si vous avez activé le SecurePIM Container, vous trouverez également le point suivant sous "Activation". En outre, quatre autres onglets s'ouvrent immédiatement, qui sont décrits ci-dessous.

Adresse électronique de l'assistance	Adresse électronique d'assistance à laquelle l'utilisateur peut s'adresser en cas de problème

Mot de passe SecurePIM

Sous "Mot de passe SecurePIM", vous pouvez définir les directives relatives à la force de sécurité du mot de passe.

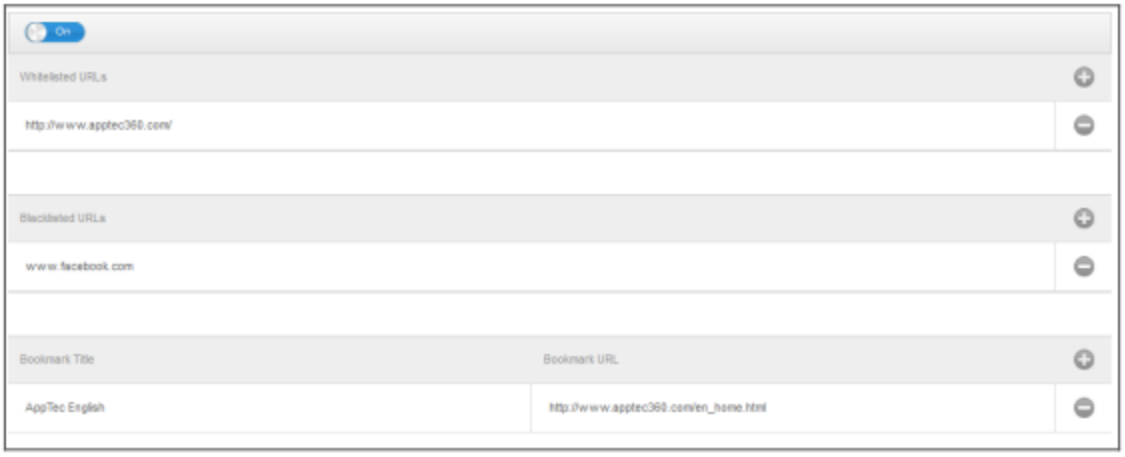
Délai d'attente de la session	Vous pouvez déterminer ici après combien de minutes un nouveau mot de passe doit être saisi une fois que SecurePIM fonctionne en arrière-plan.
Longueur du mot de passe	Longueur du mot de passe pour l'accès au SecurePIM Container
Caractères majuscules	Caractères majuscules minimum
Caractères minuscules	Minimum de caractères minuscules
Caractères spéciaux	Caractères spéciaux minimums
Chiffres	Chiffres minimums
Application par essuyage	Nombre de fois qu'un mot de passe peut être saisi de manière incorrecte avant que le contenu de SecurePIM ne soit supprimé. (L'application reste toutefois sur l'appareil de l'utilisateur final).

SecurePIM Sécurité

Sous "Sécurité SecurePIM", vous pouvez définir divers paramètres de sécurité.

Détecter les appareils Jailbreakés	Si ce paramètre est activé, l'accès au conteneur SecurePIM sera bloqué dès que l'appareil sera détecté comme étant jailbreaké.
Champs de texte sécurisés	Le contenu des champs de soumission est crypté, aucune information ne parvient au système d'exploitation (iOS). Remarque : Tant que ce paramètre est actif, la correction automatique n'est plus disponible.
Exporter les données de contact vers un appareil	Si ce paramètre est activé, l'utilisateur est autorisé à exporter les contacts Exchange sur son appareil local. Note : Seuls le nom et le numéro de téléphone sont exportés.
Lieu de l'événement	Si ce paramètre est activé, l'emplacement des événements à venir sera affiché dans la barre de notification.
Afficher le titre de l'événement	Si ce paramètre est activé, l'emplacement du titre de l'événement à venir sera affiché dans la barre de notification.

Navigateur SecurePIM



Vous pouvez ici configurer le navigateur de SecurePIM.

Le symbole permet de définir une nouvelle URL.

Le symbole vous permet de supprimer à nouveau un URL défini.

Les "Whitelisted URL" sont des URL qui peuvent être chargés.

Les "URL sur liste noire" sont des URL qui ne peuvent pas être chargés et sont donc bloqués.

Veuillez noter que les entrées de la liste blanche ont une priorité plus élevée que les entrées de la liste noire. Sous "Titre du signet", vous pouvez donner un titre. Avec "URL du signet", vous pouvez associer l'adresse URL au titre du signet - de cette façon, vous pouvez distribuer des signets individualisés aux utilisateurs respectifs.

Échange

Sous "Exchange", vous pouvez configurer un compte Exchange.

Adresse électronique ActiveSync	Adresse électronique de l'échange (prenez note des "Placeholders")
Connexion ActiveSync Exchange	Echangez les noms d'utilisateurs (prenez note des "Placeholders")
ActiveSync Exchange Server	Adresse du serveur Exchange (FQDN)
ActiveSync Domaine Exchange	Adresse du domaine Exchange
Certificat d'utilisateur	Certificat d'utilisateur
Authentification par certificat	L'utilisateur s'authentifie à l'aide d'un certificat
Autoriser le cryptage S/MIME	Permet à l'utilisateur de crypter son courrier
Autoriser la signature S/MIME	Permet à l'utilisateur de signer son courrier
Vérification de la CRL	S'il est actif, le certificat privé sera comparé à la CRL (Certificate Revocation List).

Gestion des connexions

Wi-Fi

Identificateur d'ensemble de services (SSID)	SSID du réseau à connecter
Jointure automatique	Activer la connexion automatique lors de l'adhésion à un réseau
Réseau caché	Activer, dans le cas où le point d'accès ne diffuse pas le SSID.

Configuration du proxy

Configuration d'un proxy pour chaque point d'accès

Aucun	Ne pas établir de procuration
Manuel	Établir une procuration manuelle
URL du serveur proxy	Adresse pour accéder aux paramètres du proxy
Port	Établir le port pour le Proxy
Authentification	Nom d'utilisateur pour l'authentification sur le Proxy
Mot de passe	Mot de passe pour l'authentification sur le Proxy
Automatique	Établir automatiquement un proxy
URL du serveur proxy	URL pour accéder aux paramètres du proxy

Type de sécurité

Établir le type de sécurité pour l'AP

WEP	
Mot de passe	Mot de passe pour l'AP

WPA/WPA2	
Mot de passe	Mot de passe pour l'AP

WEP Enterprise - WPA / WPA2 Enterprise - Any Enterprise			
	Protocoles		
	TLS	Activer/Désactiver	
	TTLS	Activer/Désactiver	
	LEAP	Activer/Désactiver	
	PEAP	Activer/Désactiver	
	EAP-FAST	Activer/Désactiver	
	EAP-SIM	Activer/Désactiver	
	Utiliser le PAC		Utilisation du PAC (Contrôle d'accès protégé)
	Provision PAC	Configuration du PAC de provision	
	Provisionner le PAC de manière anonyme	Fourniture anonyme de PAC	
	Authentifications internes	Protocole d'authentification à utiliser : PAP, CHAP, MSCHAP, MSCHAPv2	
	Nom d'utilisateur	Nom d'utilisateur pour l'authentification	
	N'utilisez pas de mot de passe par connexion	N'utilisez pas de mot de passe par connexion	
	Certificat d'identité	Télécharger/sélectionner le certificat d'authentification	
	Identité extérieure	Identité visible de l'extérieur	
	Confiance		
	Certificat de confiance 1	Télécharger le premier certificat de confiance	
	Certificat de confiance 2	Télécharger le deuxième certificat de confiance	
	Certificat de confiance 3	Télécharger un troisième certificat de confiance	
	Noms des certificats du serveur de confiance	Les noms des certificats de serveur attendus (dans une liste séparée par des virgules)	

Aucun	Ne pas établir de sécurité

VPN

Nom de la connexion	Nom du profil VPN

Type de VPN

VPN

Tout le trafic réseau de l'appareil sera acheminé via une connexion VPN.

Type de connexion		Établir le type de connexion VPN
	IPsec (cisco)	Protocole IPsec de Cisco
	PPTP	Protocole PPTP
	L2TP	Protocole L2TP
	Cisco AnyConnect	Protocole AnyConnect
	Juniper SSL	Protocole SSL de Juniper
	F5 SSL	Protocole SSL F5
	SonicWall mConnect	SonicWall mobile Connect
	Aruba VIA	Protocole Aruba VIA
	SSL personnalisé	Connexion via SSL personnalisé
	OpenVPN	Protocole OpenVPN

VPN par application

Lors de l'ouverture d'une application, une connexion VPN est établie.

Démarrer automatiquement la connexion VPN par application		Démarrer automatiquement la connexion VPN par application
Type de connexion		Établir le type de connexion VPN
	Cisco AnyConnect	Protocole AnyConnect
	Juniper SSL	Protocole SSL de Juniper
	F5 SSL	Protocole SSL F5
	SonicWall mConnect	SonicWall mobile Connect
	Aruba VIA	Protocole Aruba VIA
	SSL personnalisé	Connexion via SSL personnalisé
	OpenVPN	Protocole OpenVPN

Configuration du proxy

Configuration d'un proxy pour la connexion VPN

Aucun	Ne pas établir de procuration
Manuel	Établir manuellement un proxy
URL du serveur proxy	Adresse pour accéder aux paramètres du proxy
Port	Établir le port pour le Proxy
Authentification	Nom d'utilisateur pour l'authentification au Proxy
Mot de passe	Mot de passe pour l'authentification au Proxy
Automatique	Établir automatiquement un proxy
URL du serveur proxy	URL pour accéder aux paramètres du proxy

Afficher les espaces réservés	Affiche toutes les variables utilisateur disponibles, que l'AppTec360 peut utiliser.

APN

Nom du point d'accès	Nom du point d'accès
Nom d'utilisateur du point d'accès	Nom d'utilisateur du point d'accès
Mot de passe du point d'accès	Mot de passe du point d'accès
Serveur Proxy	Adresse du serveur proxy
Port	Le port Proxy respectif

Cellulaire

Activer l'itinérance des données	Activer l'itinérance des données
Activer l'itinérance vocale	Activer l'itinérance vocale
Activer le Hotspot	Activer le Hotspot

Proxy HTTP

Type de mandataire	
Manuel	Établir un proxy manuellement
URL du serveur proxy	Adresse d'accès aux paramètres du proxy
Port	Établir le port du proxy
Authentification	Nom d'utilisateur pour l'authentification au Proxy
Mot de passe	Mot de passe pour l'authentification au Proxy
Automatique	Établir automatiquement un proxy
Proxy PAC URL	Proxy PAC URL
Autoriser la connexion directe si le PAC est inaccessible	Autoriser la connexion directe (sans VPN), si le PAC est inaccessible
Permettre de contourner le proxy pour accéder aux réseaux captifs	Permettre de contourner le proxy pour accéder aux réseaux internes captifs

AirPrint

Adresse IP	Adresse IP de l'imprimante
Chemin d'accès aux ressources	Chemin d'accès défini au périphérique AirPrint

AirPlay

Nom de l'appareil	Nom de l'appareil
Mot de passe	Mot de passe de pairage
Liste blanche	Définissez une liste d'appareils avec lesquels l'appareil peut s'appairer exclusivement.

Gestion du PIM

Exchange Active Sync

Nom du compte	Nom du compte de messagerie
Hôte Exchange ActiveSync	Adresse/FQDN du serveur
Autoriser le déplacement	Permettre le déplacement de courriels
A utiliser uniquement dans le courrier	Les interactions ne peuvent avoir lieu que sur l'application Mail native.
Utiliser SSL	Utiliser le cryptage SSL
Domaine	Domaine du serveur
Utilisateur	Nom d'utilisateur
Adresse électronique	adresse électronique (uniquement au niveau de l'appareil)
Mot de passe (uniquement au niveau de l'appareil)	Mot de passe de l'utilisateur
Certificat d'identité	Sélectionnez le certificat correspondant pour l'authentification sur le serveur
Les jours précédents de Mail to Sync	Nombre de jours jusqu'à ce que les courriels soient synchronisés à nouveau. No Limit = illimité
Activer S/MIME	Activer le cryptage S/MIME
Certificat de signature	Téléchargez le certificat de signature correspondant
Certificat de cryptage	Téléchargez le certificat de cryptage correspondant

eMail

Mise en place de comptes POP3 / IMAP sur l'appareil de l'utilisateur final

Description du compte	Nom des comptes e-mail		
Type de compte	IMAP	Préfixe du chemin	Le préfixe de chemin pour les dossiers spéciaux
	POP		
Nom d'affichage de l'utilisateur	Nom d'affichage de l'utilisateur		
Adresse électronique	Adresse électronique de l'utilisateur		
Autoriser le déplacement	Permettre le déplacement de courriels		
Activer S/MIME	Activer le cryptage S/MIME		
Certificat de signature	Téléchargez le certificat de signature correspondant		
Certificat de cryptage	Téléchargez le certificat de cryptage correspondant		

Courrier entrant

Paramètres du serveur entrant

Adresse du serveur de messagerie	Adresse du serveur de messagerie
Port du serveur de messagerie	Port du serveur de messagerie
Nom de l'utilisateur	Nom d'utilisateur respectif
Type d'authentification	Type d'authentification
Aucun	Pas de type d'authentification
Mot de passe (uniquement au niveau de l'appareil)	Demande de mot de passe
Réponse au défi MDM	
NTLM	NTLM-Authentication
HTTP MD5 Digest	
Utiliser SSL	Utilisez SSL, si nécessaire

Courrier sortant

Paramètres du serveur sortant

Adresse du serveur de messagerie	Adresse du serveur de messagerie
Port du serveur de messagerie	Port du serveur de messagerie
Nom de l'utilisateur	Nom d'utilisateur respectif
Type d'authentification	
Aucun	Pas de méthode d'authentification
Mot de passe (uniquement au niveau de l'appareil)	Demande de mot de passe
Réponse au défi MDM	
NTLM	NTLM-Authentication
HTTP MD5 Digest	
Utiliser SSL	Utilisez SSL, si nécessaire
Mot de passe sortant identique au mot de passe entrant	Mot de passe sortant identique au mot de passe entrant
A utiliser uniquement dans le courrier	Activez cette option si tous les courriels sortants doivent être envoyés par l'intermédiaire de l'application Mail.

CalDav

Configurer la mise en place et la distribution d'un compte CalDav

Description du compte	Nom d'affichage du compte
Nom d'hôte	Nom d'hôte et/ou adresse IP
Port	Port du compte CalDav
URL principal	URL principal du compte
Nom d'utilisateur	Nom d'utilisateur CalDav respectif
Mot de passe (uniquement au niveau de l'appareil)	Mot de passe CalDav respectif
Utiliser SSL	Utilisez SSL, si nécessaire

Calendriers abonnés

Mise en place et distribution de calendriers abonnés

Description	Nom d'affichage du compte
URL	URL de la base de données du calendrier
Nom d'utilisateur	Nom d'utilisateur de l'abonnement au calendrier
Mot de passe (uniquement au niveau de l'appareil)	Mot de passe de l'abonnement au calendrier
Utiliser SSL	Utilisez SSL, si nécessaire

LDAP

Dans cette zone, établissez une connexion LDAP afin de permettre un échange dynamique de certificats entre l'appareil de l'utilisateur final et l'Active Directory.

Veuillez noter que l'utilisateur sélectionné doit disposer du droit de lecture correspondant.

Description du compte	Description du compte
Nom d'utilisateur du compte	Utilisateur pour l'accès LDAP
Mot de passe du compte	Mot de passe pour l'accès LDAP
Nom d'hôte du compte	Nom d'hôte/adresse IP du serveur LDAP
Utiliser SSL	Utilisez SSL, si nécessaire

Dans la deuxième partie, vous pouvez définir des filtres individuels pour la recherche dans le registre LDAP.

Description	Champ d'application	Base de recherche
Description du filtre	Niveau de recherche dans le registre LDAP	Définir le filtre individuel

Gestion du Web

Webclips

Cet emplacement permet de définir des signets, avec des liens vers des pages web, des portails intranet, etc., qui seront visibles en tant qu'application sur l'appareil de l'utilisateur final.

Étiquette	Nom de la connexion sur l'appareil de l'utilisateur final
URL	Lien vers le site web correspondant
Amovible	Si cette option est activée, l'utilisateur peut retirer le webclip.
Icône	Via ce dialogue, téléchargez un logo pour la connexion : Dimensions 180x180, format png
Icône précomposée	Si cette option est activée, aucun effet supplémentaire (ombre, reflet) ne sera affiché sur l'icône.
Plein écran	Lors de l'ouverture de clips web, le navigateur s'ouvre en mode plein écran.

Filtre de contenu web

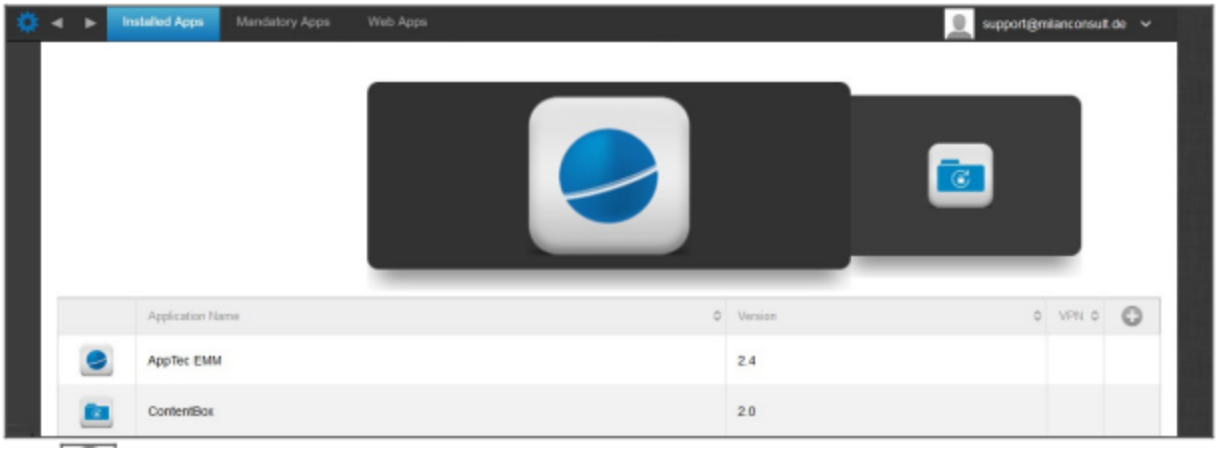
Le filtre de contenu Web permet de limiter l'accès à des pages Internet spécifiques.

Sites web autorisés	
Limiter le contenu pour adultes	Le filtre web est automatiquement appliqué pour les contenus adultes
URL autorisés	Le symbole + permet d'ajouter des pages autorisées
URL sur liste noire	Avec le symbole +, ajoutez des pages bloquées
Sites web spécifiques uniquement	Seul un contenu spécifique peut être affiché, que vous pouvez ajouter à l'aide du symbole +.

Gestion des applications

Gestionnaire d’applications d’entreprise

Applications installées (uniquement au niveau de l’appareil)



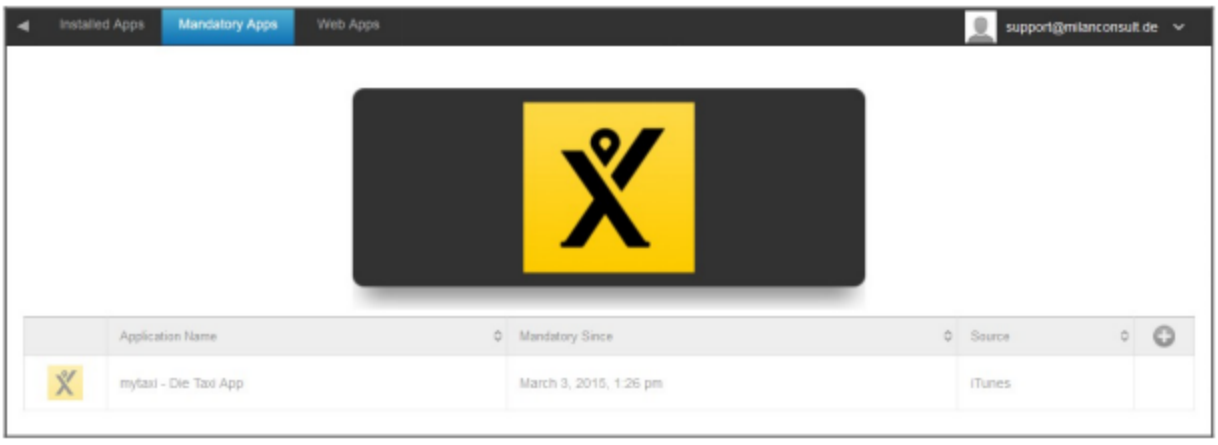
Ici, vous pouvez voir les applications qui sont actuellement installées sur l'appareil.

Applications obligatoires

Sous Apps obligatoires, vous pouvez mandater les apps nécessaires.

L'utilisateur se verra continuellement rappeler d'installer l'application mentionnée.

Grâce au , l'application obligatoire peut être définie.



Il peut s'agir d'une application Apple App Store, mais aussi d'une application interne.

S'il s'agit d'un appareil surveillé, l'application sera installée automatiquement.

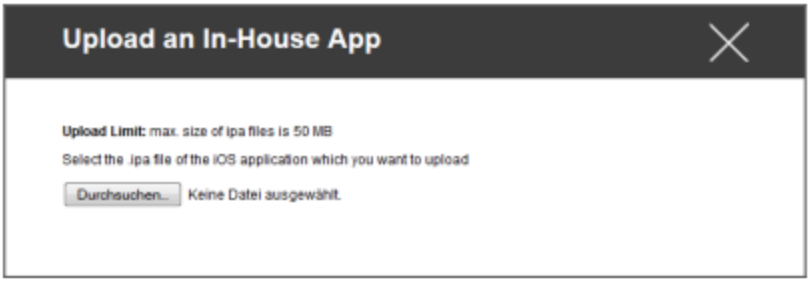
Vous pouvez pousser une application "Apple AppStore" de l'AppStore public sur l'appareil, ainsi qu'une application interne développée en interne.

Vous pouvez également sélectionner la catégorie "Applications maison iOS" et choisir une application maison que vous avez téléchargée dans les paramètres généraux.

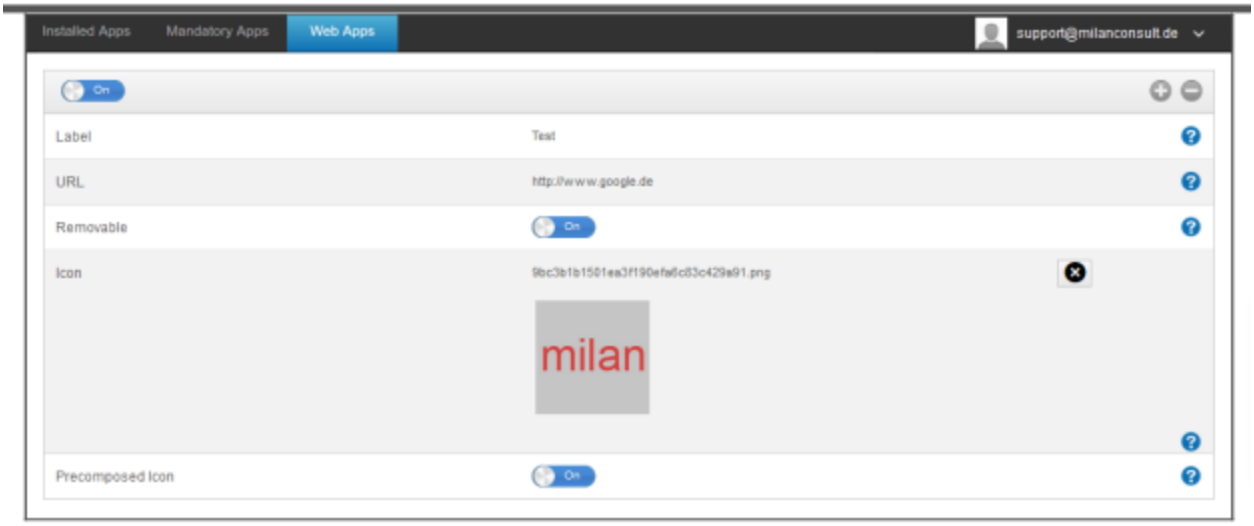
Options d'installation

Tenir à jour (uniquement pour les VPP par appareil)	Une fois par semaine, il sera déterminé s'il existe une mise à jour pour l'application. Si c'est le cas, cette mise à jour sera installée Pour les applications internes, la cible de mise à jour que vous avez configurée dans les paramètres généraux sera utilisée pour le processus de mise à jour.
Dépassement en l'absence de gestion	Si l'application est déjà installée, le MDM prendra en charge l'application et la gérera.
Supprimer l'application lorsque le profil MDM est supprimé	Dans le cas d'une suppression de la gestion de l'appareil, l'application sera désinstallée.
Empêcher la sauvegarde des données de l'application	Une sauvegarde des données spécifiques à l'application ne sera pas créée.
Paramétrage de l'application	Sous "App Settings", vous pouvez attribuer à l'application certaines valeurs au premier plan (pour autant que l'application le permette, si nécessaire, demandez au développeur de l'application).

Vous pouvez également sélectionner et télécharger directement un fichier ipa, via "Télécharger une application interne".



Applications Web



Sous le point "Web Apps", vous pouvez, comme avec "Web Clips", pousser des pages internet ou des portails intranet en tant qu'application sur l'appareil de l'utilisateur final, dans le domaine de la gestion web. Par défaut, les applications Web s'affichent en mode plein écran, qui peut être configuré sous Webclips.

Étiquette	Nom de la connexion sur l'appareil de l'utilisateur final
URL	Lien vers le site web correspondant
Amovible	Si cette option est activée, l'utilisateur peut retirer le Webclip
Icône	Via ce dialogue, téléchargez un logo pour la connexion : Dimensions 180x180, format png
Icône précomposée	Si cette option est activée, aucun effet supplémentaire (ombre, reflet) ne sera affiché sur l'icône.

Restrictions et réglages

Apps sur liste noire / liste blanche

Ici, vous pouvez définir les applications qui sont bloquées (ou autorisées) en fonction de vos paramètres dans "Paramètres généraux". Un clic sur ce bouton fait apparaître la recherche d'applications connues. Vous pouvez y rechercher les applications que vous souhaitez ajouter.

Notez qu'un dispositif supervisé est nécessaire pour cette fonction.

Restrictions SysApp

Bloquer des applications ou des fonctions spécifiques de votre appareil

Autoriser l'utilisation de YouTube	Autoriser l'utilisation de YouTube
Permettre l'utilisation de l'iTunes Store	Permettre l'utilisation de l'iTunes Store
Autoriser l'utilisation de Safari	Autoriser l'utilisation de Safari
Activer le remplissage automatique	Permet le remplissage automatique
Avertissement de la police en cas de fraude	Force l'avertissement de fraude
Activer JavScript	Permet l'utilisation de JavaScript
Bloquer les pop-ups	Bloque tous les types de pup-ups
Autoriser les cookies	Choisissez quand Safari accepte les cookies

App-VPN

Le symbole permet de définir les applications qui lanceront automatiquement la connexion VPN sélectionnée au démarrage.

Paramètres de l’application

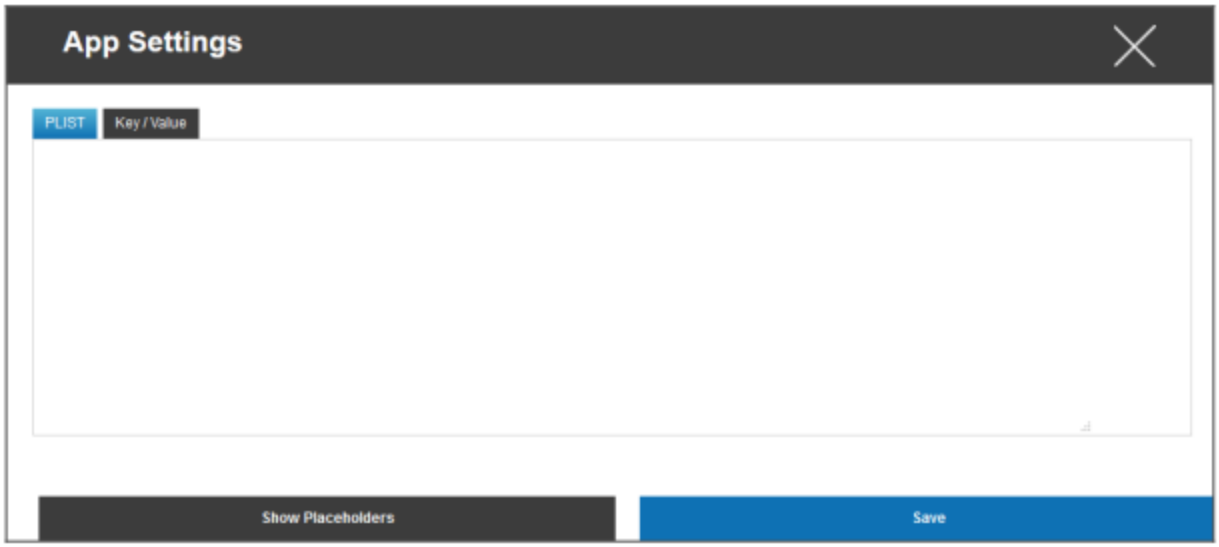
Sous "App Settings", vous pouvez attribuer à l'application certaines valeurs au premier plan (pour autant que l'application le permette, si nécessaire, demandez au développeur de l'application).

Via le symbole, vous ajoutez une application (supplémentaire). Vous trouverez, une fois de plus, la représentation familière d'AppTec360 d'une importation d'application.

Recherchez ici l'application que vous souhaitez configurer et sélectionnez-la. Les paramètres ne s'appliquent qu'aux applications gérées.

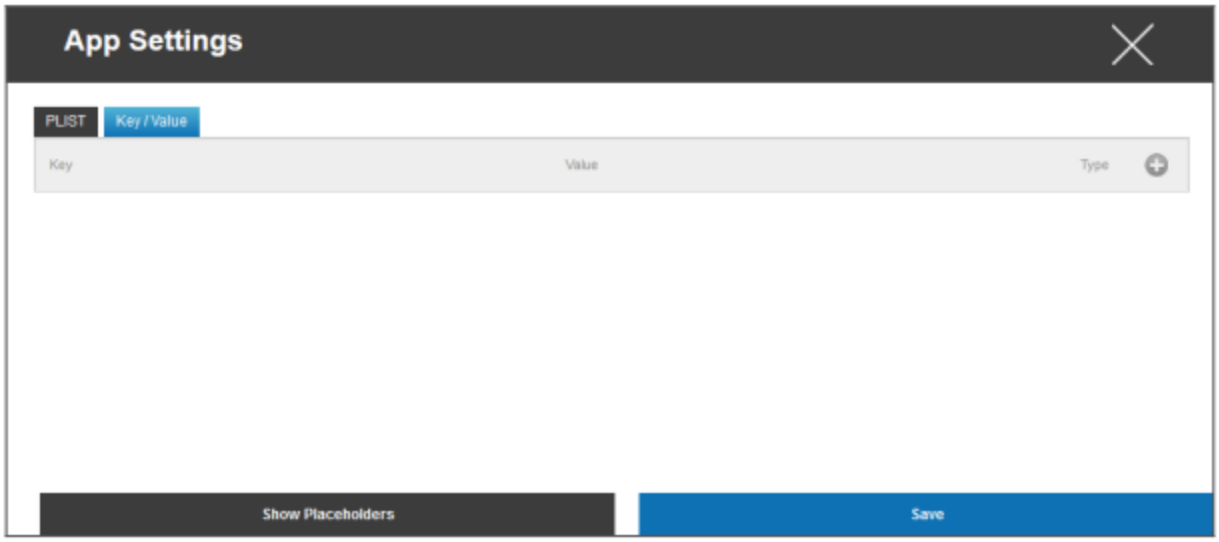
Si l'importation a réussi, l'écran suivant s'affiche :

Désormais, d'un simple clic sur , vous pouvez effectuer toute une série de configurations. Vous recevrez ensuite l'aperçu suivant :

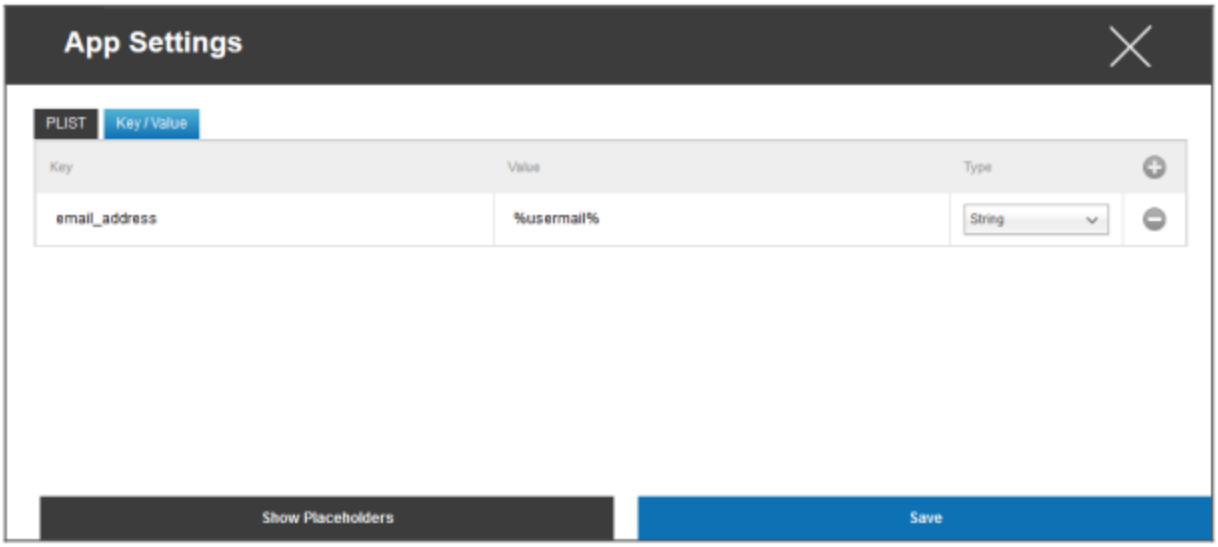


Si vous avez déjà une PLIST (texte source de la configuration), vous pouvez l'ajouter ici et sauvegarder le tout avec "Save".

Sous "Clé / Valeur", vous pouvez attacher des configurations spécifiques à l'application.



Ici, vous pouvez établir une nouvelle clé et sa valeur avec le symbole.



Bien entendu, tous les espaces réservés d'AppTec sont à votre disposition

Explication du "type" :

Chaîne	Texte
Booléen	Vrai/Faux
Nombre	Nombre

Le symbole vous permet de supprimer à nouveau une application.

App Store d’entreprise

Applications iTunes

Dans ce cadre, vous pouvez distribuer des applications optionnelles à votre utilisateur.

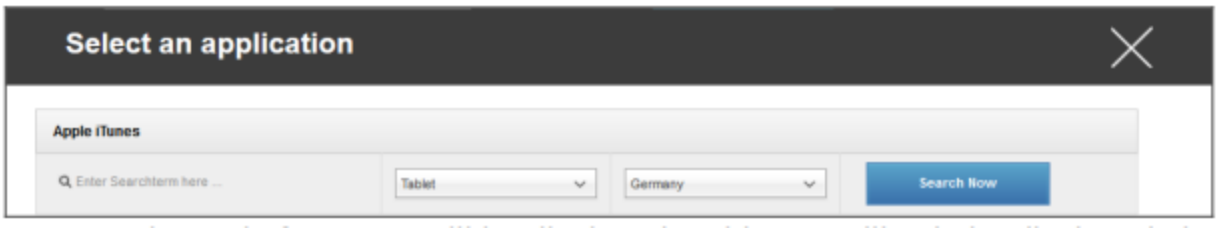
S'il y a une application ici, elle sera installée automatiquement sur l'appareil de l'utilisateur final de la boutique AppTec360.

Il s'agit simplement de liens vers l'App Store officiel d'Apple. C'est pourquoi chaque appareil de l'utilisateur final doit être équipé d'un identifiant Apple.

À ce stade, nous recommandons que chaque utilisateur dispose de son propre identifiant Apple.

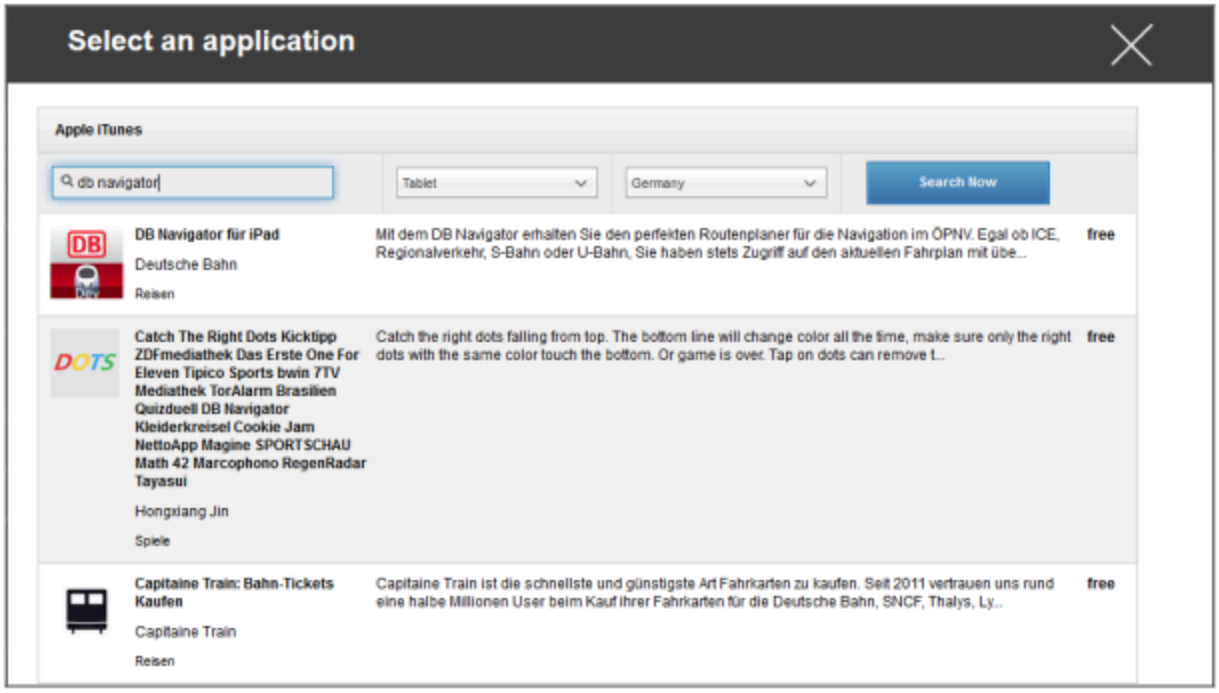
Avec le symbole, vous pouvez ajouter des applications supplémentaires.

Une fenêtre s'ouvre alors avec l'aperçu suivant.



Veuillez noter que seules les applications gratuites seront affichées, les applications payantes ne seront affichées que via VPN.

Sous "Enter Search Term here ...", vous pouvez rechercher une application qui se trouve dans l'App Store d'Apple.



Une fois que vous avez cliqué sur l'icône ou sur le nom de l'application, il vous sera à nouveau demandé d'effectuer des configurations supplémentaires.

Restez informé	Une fois par semaine, il sera déterminé s'il existe une mise à jour pour l'application. Si c'est le cas, cette mise à jour sera installée
Supprimer l'application lorsque le profil MDM est supprimé	Dans le cas d'une suppression de la gestion de l'appareil, l'application sera désinstallée.
Empêcher la sauvegarde des données de l'application	Une sauvegarde des données spécifiques à l'application ne sera pas créée.
App-VPN	Sélectionnez une connexion VPN, qui se lancera à l'ouverture de l'application.

Après avoir cliqué sur "Installer", l'application sera ajoutée à l'App Store de l'entreprise et pourra ensuite être installée sur l'appareil de l'utilisateur final, via l'AppStore AppTec360.

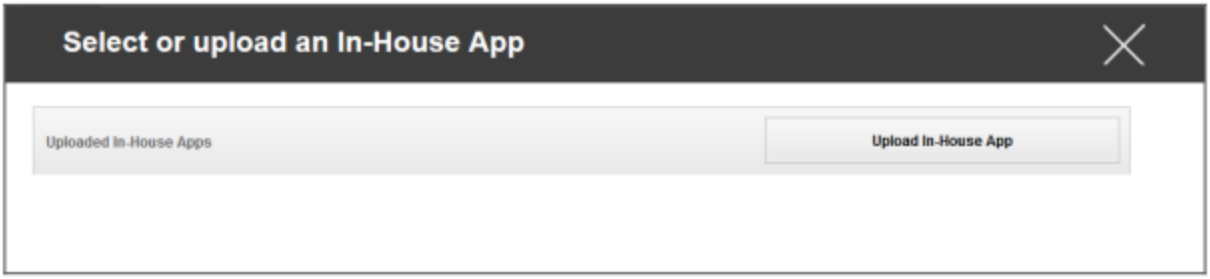
Si l'importation dans l'App-Store a été effectuée avec succès, vous recevrez l'aperçu suivant :

En interne

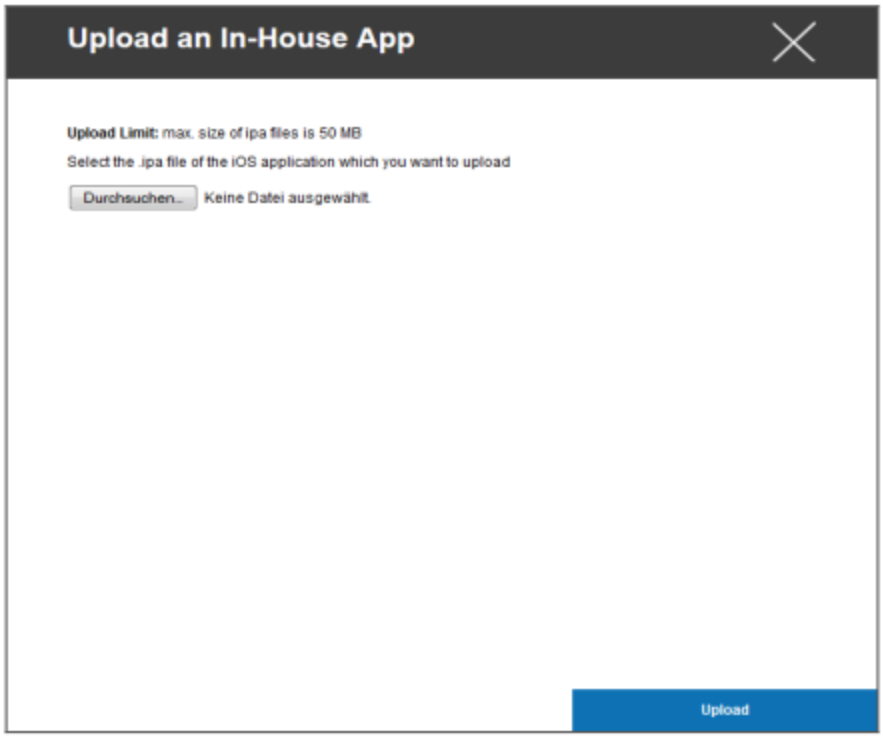
Sous le point "In-House", vous pouvez télécharger des applications développées en interne et les distribuer.

Avec le symbole, vous pouvez distribuer des applications internes supplémentaires.

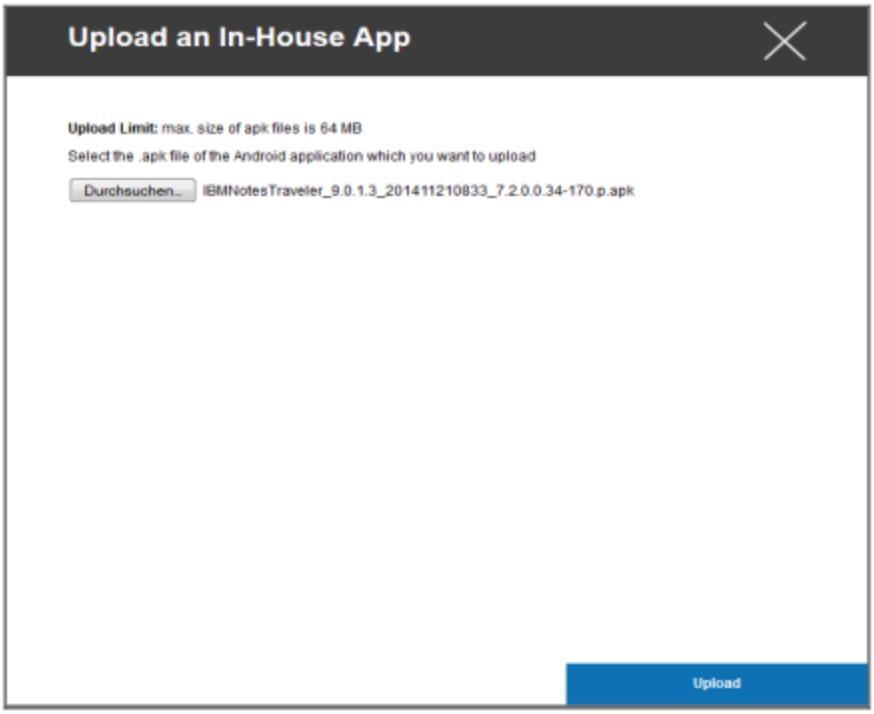
Si vous n'avez jamais distribué In-House App, vous recevrez alors la présentation suivante :



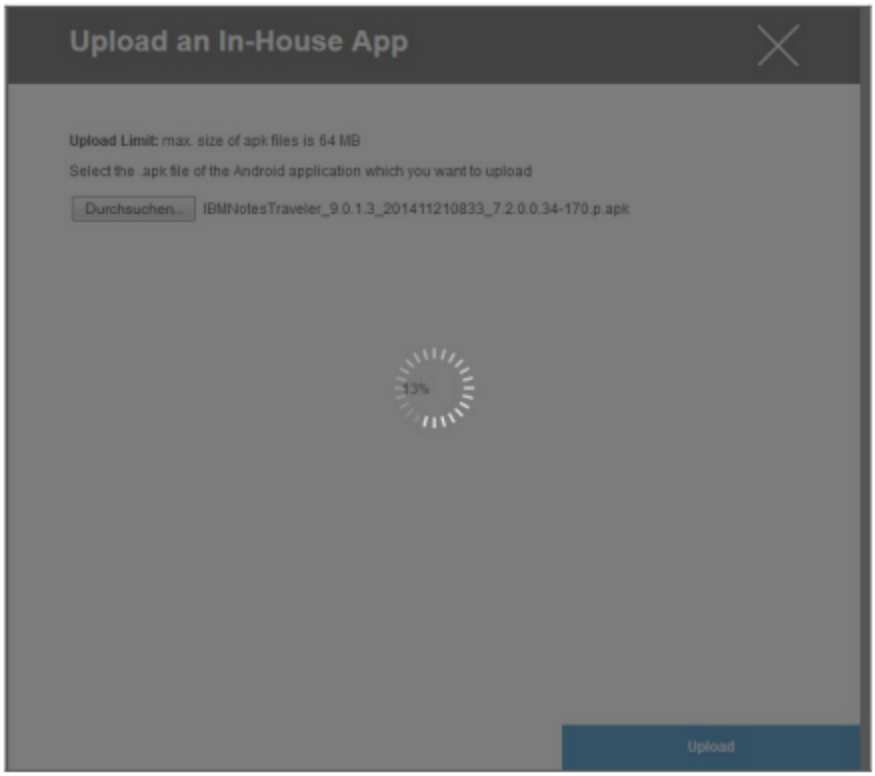
Pour cela, cliquez sur "Upload In-House App", vous obtiendrez alors l'aperçu suivant :



Sélectionnez ensuite avec "Search..." un fichier .ipa et cliquez sur "Upload"



Votre application est maintenant téléchargée. Au milieu du cercle, vous pouvez voir le pourcentage de votre application qui a déjà été téléchargé.



Si le téléchargement de l'application interne a été effectué avec succès, vous verrez l'application nouvellement téléchargée dans votre catalogue d'applications.

L'utilisateur a maintenant la possibilité de voir et d'installer cette application dans la boutique AppTec360 sur l'appareil de l'utilisateur final, dans la catégorie "In-House".

Comme il ne s'agit pas d'une application publique de l'AppStore d'Apple, l'utilisateur n'a pas besoin d'un identifiant Apple stocké sur l'appareil de l'utilisateur final.

Mode kiosque

Le mode kiosque iOS n'est disponible qu'en mode supervisé

Le mode kiosque vous permet de prédéfinir une application ou une URL, de sorte qu'il sera possible d'exécuter/de visiter cette application/URL exclusivement.

En outre, vous pouvez désactiver divers boutons matériels en mode kiosque.

Type d’application

Paquet

Si vous souhaitez lancer l'application en mode kiosque, sélectionnez "Package" sous "Type d'application"

Application kiosque	Cliquez ici pour sélectionner une application qui doit être lancée en mode kiosque. Vous y trouverez l'aperçu actuel de la gestion de l'application Vous pouvez choisir entre "Apple iTunes Apps" et "iOS In-House Apps"

URL

Si vous souhaitez lancer une URL en mode kiosque, sélectionnez "URL" sous "Type d'application"

URL	Définissez maintenant l'adresse URL souhaitée
Politique de la même origine	Si cette fonction est activée, l'utilisateur ne peut alors surfer que sur les sous-pages de l'URL prédéfini. Par exemple, si vous avez défini l'URL suivante : www.mypage.com, l'utilisateur peut alors surfer sur www.mypage.com/subpage
URL sur liste blanche	Ici, vous pouvez maintenir une liste blanche, tous ces URL sont autorisés. Maximum 1 URL par ligne Un URL doit commencer par http:/ ou https://.
URL sur liste noire	Ici, vous pouvez maintenir une liste noire, tous ces URL sont interdits. Maximum 1 URL par ligne Un URL doit commencer par http:/ ou https://.
Effacer le navigateur après inactivité	Après une période d'inactivité, le cache du navigateur sera vidé.
Mot de passe de sortie activé	Si vous activez cette fonction, l'utilisateur a la possibilité de terminer le mode kiosque avec un mot de passe que vous avez prédéfini.
Quitter le mot de passe	Il s'agit du mot de passe que vous avez prédéfini.

Paramètres du mode kiosque

Mode kiosque programmé	En fonction de l'heure de la journée, vous pouvez régler le mode kiosque de manière à ce que le mode démarre et s'arrête automatiquement à une heure prédéterminée.
Heure de début	Heure de début
Temps en minutes	Temps en minutes après lequel le mode kiosque doit être terminé à nouveau.
Désactiver le toucher	Si elle est activée, l'écran tactile est désactivé.
Désactiver la rotation des appareils	Si elle est activée, l'adaptation automatique de l'écran est désactivée.
Interrupteur de désactivation de la sonnerie	S'il est activé, le commutateur de sonnerie est alors désactivé. A partir de ce moment, le comportement dépend de la fonction réglée précédemment.
Désactiver les boutons de volume	Si cette option est activée, les boutons de volume seront désactivés.
Désactiver le bouton Veille-Sommeil	Si elle est activée, l'interrupteur marche/arrêt sera désactivé.
Désactiver le verrouillage automatique	Si cette option est activée, l'appareil ne sera pas mis en veille.
Activer la voix sur	Si l'option est activée, l'assistant vocal sera activé.
Activer le zoom	Si elle est activée, le zoom sera activé
Activer l'inversion des couleurs	Si cette option est activée, le mode d'affichage inversé est activé.
Activer l'assistance tactile	Si elle est activée, l'AssistiveTouch sera activée.
Activer la sélection de la parole	Si elle est activée, la sélection de la parole sera activée
Activer l'audio mono	Si cette option est activée, le son mono sera activé.
VoiceOver	Si cette option est activée, l'utilisateur peut activer VoiceOver
Zoom	Si cette option est activée, l'utilisateur peut activer la fonction Zoom
Inverser les couleurs	Si cette option est activée, l'utilisateur peut activer les couleurs inversées.
Toucher assisté	Si cette option est activée, l'utilisateur peut activer l'assistance tactile.

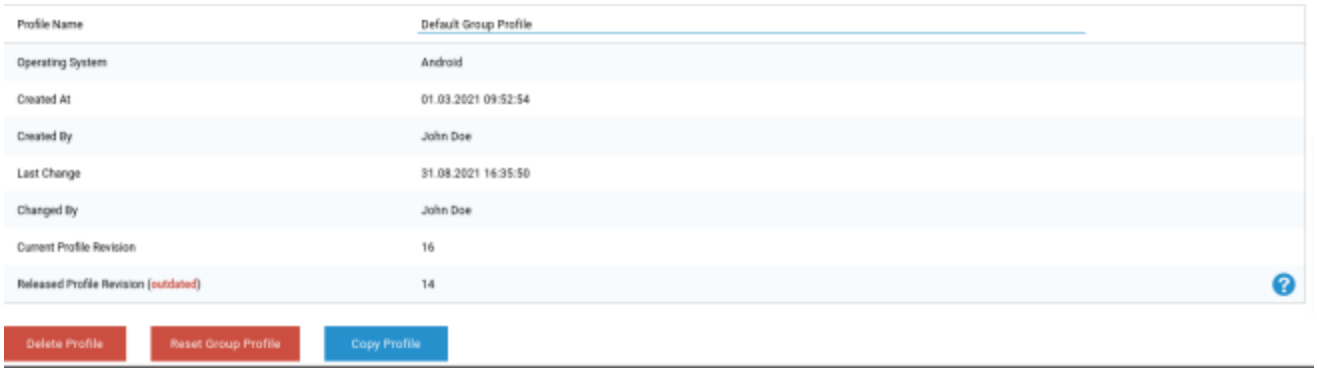
Android Enterprise – Configuration des appareils entièrement gérée

Selon que vous avez sélectionné un profil de groupe ou un appareil, la vue d'ensemble et ses sous-points diffèrent.

Général

Aperçu du profil du groupe (uniquement au niveau du groupe)

Lorsque vous ouvrez un profil de groupe, vous obtenez un aperçu rapide du profil.



Nom du profil	Nom du profil (peut être modifié ici)
Système d'exploitation	Système d'exploitation pour lequel le profil est établi
Créé à	Moment de la création
Créé par	Le créateur du profil
Dernier changement	Date de la dernière modification du profil
Modifié par	Compte ayant effectué les dernières modifications
Révision du profil actuel	Révision de l'état du profil sauvegardé
Révision du profil validé	Révision du profil attribué ("Attribuer maintenant"). Si l'étiquette affiche "(obsolète)" derrière le texte, cela signifie que vous avez enregistré le profil mais que vous ne l'avez pas encore attribué.

Aperçu de l’appareil (uniquement au niveau de l’appareil)

Si vous vous trouvez sur un appareil, vous recevrez un récapitulatif de l'appareil sélectionné, qui contient les informations suivantes :

Nom de l'appareil	Nom de l'appareil
Localisation	Coordonnées du lieu
Numéro de téléphone	Numéro de téléphone
Apps obligatoires assignées	Nombre d'applications obligatoires attribuées
Version OS	Version du système d'exploitation de l'appareil
Système d'exploitation	Système d'exploitation (Android Enterprise)
Numéro de série	Numéro de série de l'appareil
Propriété des appareils	Dispositif d'entreprise ou privé
Type d'appareil	Dispositif géré par AE Work
Enraciné	Statut, indiquant si l'appareil a été enraciné
Conforme à la loi	Conforme aux lignes directrices
Adresse IP	Adresse IP de l'appareil
Dernière visite	Moment où le dispositif s'est connecté pour la dernière fois à AppTec
Dernière poussée	Moment où la dernière impulsion a été envoyée à l'appareil.
Mode propriétaire de l'appareil AE	Oui
Affectation des utilisateurs	L'utilisateur ou le groupe auquel ce dispositif est affecté

Révision de la configuration (uniquement au niveau de l’appareil)

Vous obtenez ici une vue d'ensemble du profil de groupe attribué à l'appareil.

Si vous cliquez sur le profil du groupe, vous aurez un accès direct à ce profil et vous pourrez effectuer des réglages.

Ce symbole permet de rétablir les paramètres du profil de groupe pour les applications distribuées.

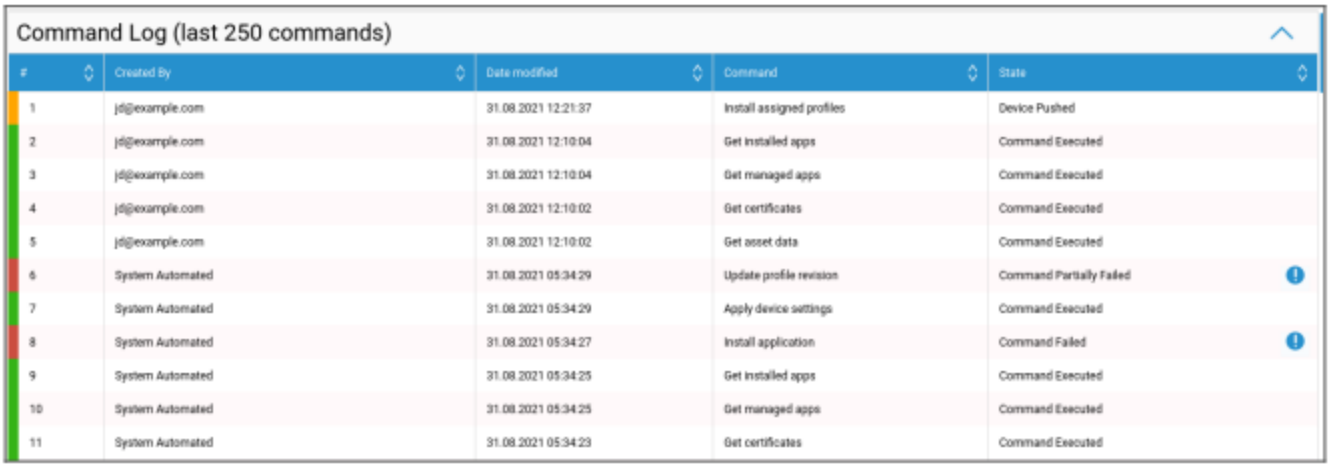
Ce symbole vous permet de rétablir les paramètres du profil de groupe pour toutes les applications utilisées.

La mention "Révision plus récente disponible" indique que le profil de groupe a été modifié et enregistré, mais qu'il n'a pas été attribué. Le profil de groupe doit être attribué avec "Attribuer maintenant" au niveau du groupe pour appliquer les changements aux appareils.

Journal de l’appareil (uniquement au niveau de l’appareil)

Journal des commandes

Vous pouvez voir ici quelles commandes ont été émises pour l'appareil et quel est leur état.



Les commandes créées par le "système automatisé" sont automatiquement créées par le système.

États possibles de la commande

Dispositif poussé	Une requête "push" a été envoyée au service "push" (par exemple APNS) pour demander à l'appareil de se reconnecter au serveur EMM.
Commande créée	La commande a été créée dans le système.
Commande envoyée	La commande a été envoyée à l'appareil après qu'il se soit connecté au serveur.
Commande exécutée	La commande a été exécutée avec succès.
Échec de la commande	La commande a échoué. *
Échec partiel de la commande	Selon le système d'exploitation de l'appareil, certaines commandes peuvent être regroupées. Dans ce cas, certaines parties de ce groupe de commande ont échoué. *
Commande exécutée, échec éventuel	La commande a été exécutée, mais peut-être qu'elle ne l'a pas été.
Commandement repoussé	La commande a été repoussée par un utilisateur.
Mise au rebut	La commande a été supprimée. Par exemple, parce qu'elle a été remplacée par une autre commande ou parce que l'appareil a été réenrôlé et que les anciennes commandes ont été supprimées.

Si le message est accompagné d'un point d'exclamation, vous pouvez obtenir plus d'informations en survolant l'icône avec votre curseur.

Paramètres de l’appareil

Configuration du client

Ici, vous pouvez effectuer les configurations suivantes sur votre appareil Android :

Temps de non-conformité	Délai d'attente de la réponse de l'utilisateur après lequel la mesure d'exécution est appliquée.
Mesures d'exécution après l'expiration du délai de mise en conformité	Action de mise en application lorsqu'un utilisateur n'effectue pas les actions qui conduisent à un statut d'appareil conforme.
Fréquence de la collecte des données	Fréquence à laquelle les informations relatives à l'appareil/au GPS doivent être collectées
Fréquence de battement de cœur du dispositif	Intervalle dans lequel le dispositif doit contacter le serveur AppTec360 Min. 1 minute Max. 24 heures
Activer les mises à jour de localisation	Si cette option est activée, l'appareil envoie des mises à jour de l'emplacement au serveur AppTec360.
Lieu Heure de mise à jour	Détermine dans quels intervalles de temps l'appareil envoie des mises à jour de localisation à AppTec360
Utilisez la précision de localisation de Google pour la mise à jour de l'emplacement	S'il est activé, l'emplacement du réseau sera utilisé pour les mises à jour de l'emplacement (si ce paramètre a été désactivé dans "Restrictions", il n'aura aucune incidence).
Utiliser la localisation GPS pour la mise à jour de l'emplacement	Si cette option est activée, le GPS sera utilisé pour les mises à jour de la position.
Autoriser les faux emplacements	Permet de falsifier les informations de localisation via des applications tierces
Action en cas de perte de connexion	Si cette option est activée, vous pouvez spécifier une action pour le cas où un appareil n'obtient pas de connexion au serveur MDM dans l'intervalle de battement de cœur. Par exemple, si l'appareil a un intervalle de battement de cœur de 5 minutes, il se connecte au serveur à 10:35 AM. Ensuite, l'appareil quitte la zone Wi-Fi. Le prochain battement de cœur à 10:40 AM échouera et l'action spécifiée sera exécutée.
Action	L'action à entreprendre dès qu'un dispositif devient non conforme.

	• Dispositif de verrouillage = dispositif de verrouillage • Effacer l'appareil = l'appareil sera restauré aux paramètres d'usine • Effacer l'appareil et la carte SD = l'appareil sera restauré aux paramètres d'usine et le stockage sur la carte SD sera supprimé.
Seuil	Vous pouvez spécifier un seuil de battements cardiaques défaillants nécessaires pour déclencher l'action spécifiée.

Mode d'application de la politique	Par défaut :	Les utilisateurs seront invités périodiquement à exécuter les actions en cours.
	Application paresseuse de la politique :	Les utilisateurs ne seront jamais invités à exécuter les actions en cours. Toutes les actions en cours seront affichées dans le client AppTec360.
	Application agressive de la politique :	Les utilisateurs seront invités en permanence à exécuter les actions en cours.
Verrouillage de la version d'AppTec360	Si cette option est activée, un code de version pour le client MDM AppTec360 peut être spécifié. Le client AppTec360 ne sera mis à jour qu'avec la version spécifiée. Les versions plus récentes seront ignorées. Une rétrogradation n'est PAS possible.	
Code de la version	Code de version du client MDM AppTec360 à verrouiller.	
Désactiver la notification AppTec360	S'il est désactivé, le client AppTec360 n'affichera pas de notification dans la barre de notification. Les utilisateurs peuvent donc fermer le client AppTec360 via le gestionnaire des tâches. Si le client AppTec360 est fermé, plusieurs fonctionnalités, y compris le mode kiosque et la liste noire/blanche des applications, ne fonctionneront pas correctement. Les appareils Samsung offrent un mécanisme de protection pour le client AppTec360. La notification est désactivée par défaut sur les appareils Samsung qui prennent en charge les API KNOX. La notification ne devrait pas être désactivée sur les appareils équipés d'Android 8.0 ou d'une version ultérieure.	

Papier peint

Définir un fond d'écran personnalisé	Activer/désactiver le fond d'écran personnalisé
Papier peint	Définissez le mode de fond d'écran pour utiliser un code couleur ou une image.
Spécifiez une couleur	Spécifiez une couleur de fond sous forme de valeur hexagonale, par exemple #000000 pour le noir ou #ffffff pour le blanc.
Définir l'image comme fond d'écran	Téléchargez le fichier image que vous souhaitez utiliser comme fond d'écran.

Gestion des actifs (uniquement au niveau de l’appareil)

Informations sur l’appareil

Modèle	Désignation du modèle de l'appareil
Système d'exploitation	OS
Version OS	Version du système d'exploitation
Numéro de série	Numéro de série
Nom de l'appareil	Nom de l'appareil
État de la batterie	État de la batterie
Mémoire libre / totale	Mémoire libre / totale
Coffre-fort Samsung	Interface Samsung SAFE, nécessaire pour une variété d'options de réglage
Carte SD disponible	Carte SD disponible
Carte SD émulée	Carte SD émulée
Carte SD amovible	Carte SD amovible
SD Mémoire libre / totale	SD Libre / Mémoire totale de la carte SD

Wi-Fi

Adresse IP	Adresse IP de l'appareil
WiFi MAC	Adresse MAC du WiFi

Cellulaire

Statut	État (carte SIM installée)
Numéro de téléphone	Numéro de téléphone
Itinérance (voix/données)	Itinérance pour la voix et les données
État de l'itinérance	État actuel de l'itinérance
Adresse IP	Adresse IP
Opérateur/transporteur	Opérateur/transporteur
Technologie cellulaire	Technologie cellulaire
IMEI	Numéro IMEI
ICCID	Il s'agit de l'identifiant de la carte SIM, qui est souvent aussi une carte à puce ou une carte à circuit intégré (ICC).
IMSI	L'International Mobile Subscriber Identity (IMSI) permet, dans les réseaux mobiles GSM et UMTS, une identification précise des utilisateurs du réseau. L'IMSI est composé d'un maximum de 15 chiffres et est configuré de la manière suivante : • Indicatif de pays du mobile (MCC), 3 chiffres • Code de réseau mobile (MNC), 2 ou 3 chiffres • Numéro d'identification de l'abonné mobile (MSIN), 1 à 10 chiffres
Actuel MCC/MNC	Voir "SIM MCC/MNC"
SIM MCC/MNC	L'indicatif de pays du mobile est un identificateur de pays établi par l'UIT selon la norme E.212. Il est associé au code de réseau mobile (MNC) pour l'identification du réseau mobile. Signifie le code de pays/réseau mobile de la carte SIM. Si vous vous rendez sur un autre réseau mobile, il est logique que le "MCC/MNC actuel" et le "MCC/MNC SIM" soient différents.

Bluetooth

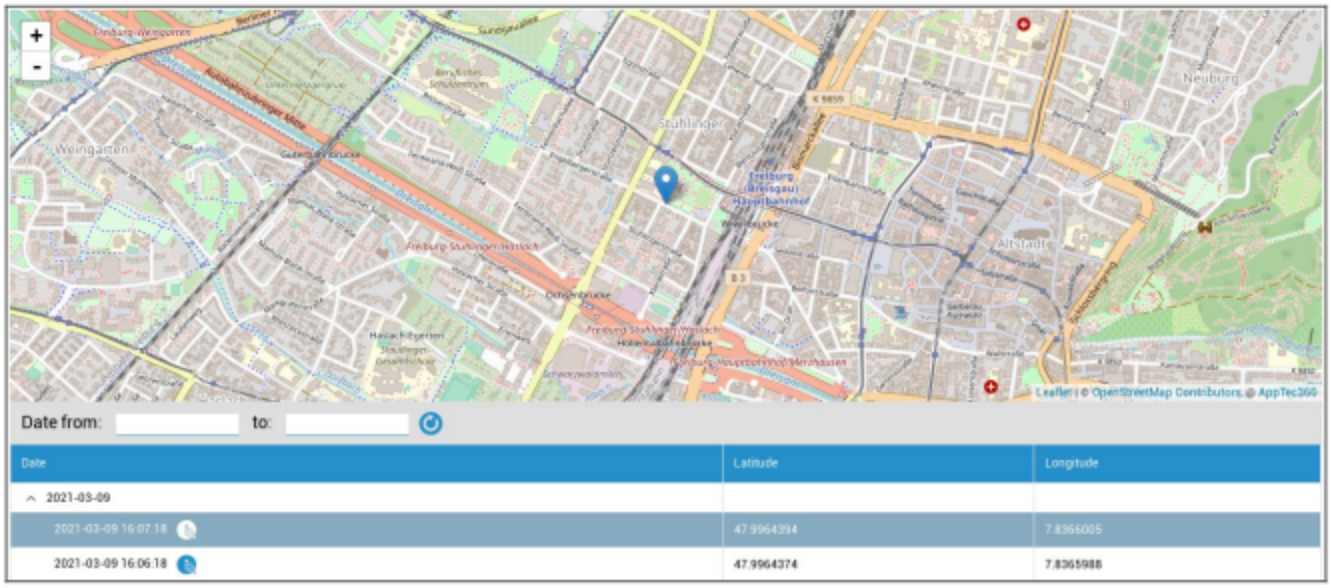
Bluetooth MAC	Adresse MAC Bluetooth

Gestion de la sécurité

Antivol (uniquement au niveau de l’appareil)

Informations GPS (uniquement au niveau de l’appareil)

Vous pouvez ici déterminer l'emplacement actuel/dernier emplacement de l'appareil. La localisation peut être protégée par un ou deux mots de passe - Voir : Paramètres généraux - Confidentialité - Accès GPS



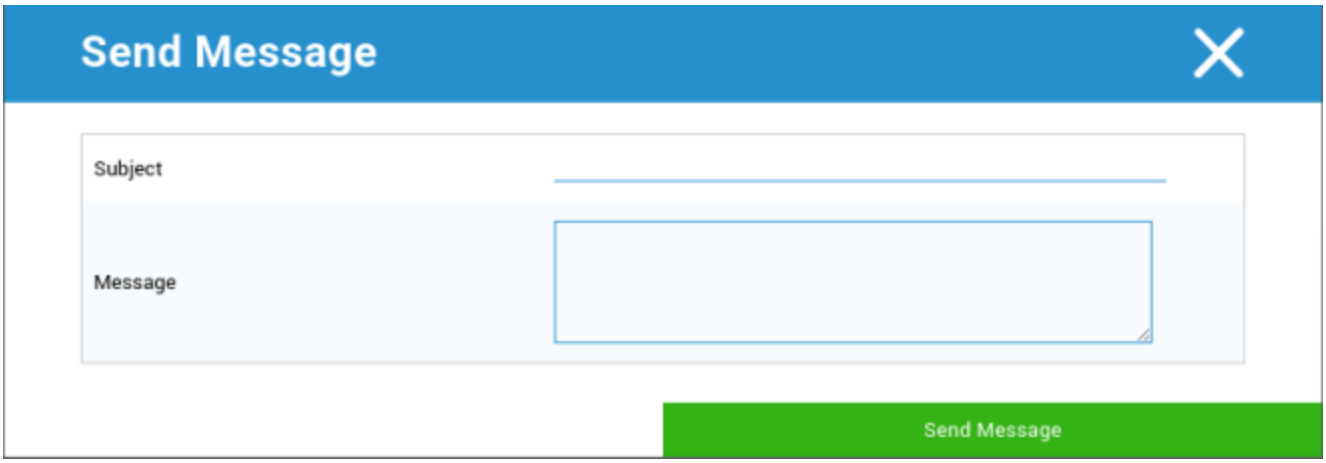
Effacement et verrouillage (uniquement au niveau de l’appareil)

Sous "Effacer et verrouiller", vous pouvez effectuer les trois actions suivantes :

Essuyage complet	L'appareil est restauré à ses paramètres d'usine (les données de l'entreprise et les données personnelles sont supprimées).
Nettoyage de l'entreprise	Seules les données de l'entreprise sont supprimées de l'appareil de l'utilisateur final (toutes les applications, données, etc. qui ont été fournies par AppTec360).
Écran de verrouillage	Le verrouillage de l'écran est activé, il suffit de déverrouiller l'appareil avec le mot de passe/NIP de l'appareil.

Message (uniquement au niveau de l’appareil)

Ici, vous pouvez remplir l'objet et un message et l'envoyer à un appareil de l'utilisateur final.



Configuration de la sécurité

Code de l’appareil

Sous "Passcode", vous pouvez mandater un mot de passe pour l'appareil, les options de réglage suivantes sont disponibles

Longueur minimale du mot de passe	Fixe le nombre minimum de symboles que doit comporter un mot de passe	
Qualité du mot de passe	Non spécifié	Cette politique ne prévoit aucune exigence concernant le mot de passe.
	Biométrique Faible	Cette politique autorise les technologies de reconnaissance biométrique à faible niveau de sécurité. Il s'agit de technologies capables de reconnaître l'identité d'une personne à l'aide d'un code PIN à trois chiffres environ (le taux de fausse détection est inférieur à 1 sur 1 000).
	Quelque chose	Cette politique exige la définition d'un mot de passe ou d'un modèle, mais n'impose pas de règles spécifiques.
	Alphabétique	L'utilisateur doit avoir introduit un mot de passe contenant au moins des caractères alphabétiques (ou d'autres symboles).
	Alphanumérique	L'utilisateur doit avoir saisi un mot de passe contenant au moins des caractères numériques et alphabétiques (ou d'autres symboles).
	Complexe	L'utilisateur doit avoir saisi un mot de passe contenant au moins une lettre, un chiffre et un symbole spécial, par défaut. Avec cette qualité de mot de passe, les mots de passe peuvent être restreints pour contenir différents ensembles de caractères, comme au moins une lettre majuscule, etc.
Longueur minimale du mot de passe	Définissez le nombre de caractères requis pour le mot de passe. Par exemple, vous pouvez exiger que les codes PIN ou les mots de passe comportent au moins six caractères.	
Nombre minimum de chiffres requis pour le mot de passe	Nombre minimum de chiffres requis pour le mot de passe	

Minimum de lettres minuscules requis dans le mot de passe	Minimum de lettres minuscules requis dans le mot de passe
Minimum de lettres majuscules requis dans le mot de passe	Minimum de lettres majuscules requis dans le mot de passe
Nombre minimum de caractères non alphabétiques requis dans le mot de passe	Nombre minimum de caractères non alphabétiques requis dans le mot de passe
Symboles minimums requis dans le mot de passe	Symboles minimums requis dans le mot de passe

Verrouillage du temps d'inactivité maximum	Inactivité maximale de l'utilisateur jusqu'au verrouillage de l'heure
Délai d'expiration du mot de passe	Établit, après quoi le mot de passe expire et un nouveau mot de passe doit être délivré.
Restriction de l'historique des mots de passe	Nombre de mots de passe précédemment utilisés qui ne sont pas autorisés
Nombre maximal d'échecs de tentatives de saisie du mot de passe	Détermine le nombre de fois qu'un mot de passe peut être saisi de manière incorrecte avant qu'un effacement complet de l'appareil ne soit effectué.
Autoriser l'authentification biométrique	Permet l'authentification par empreinte digitale ou par balayage de l'iris. Uniquement pour Samsung KNOX 2.1 et plus.

AntiVirus

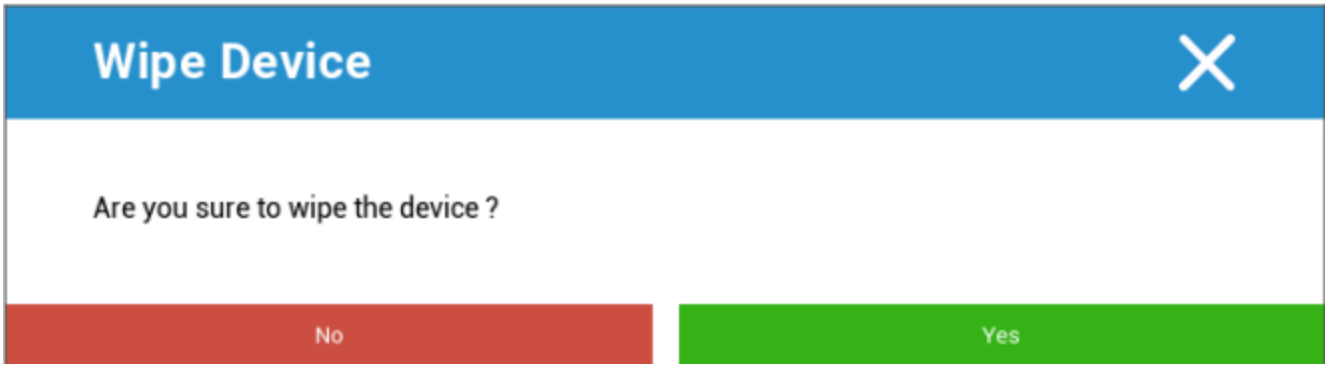
Scan automatique	Activer les balayages automatiques périodiques
Intervalle de balayage	Intervalle d'examen (rapide / complet)
Scan automatique complet	Activer les analyses automatiques complètes
Mises à jour automatiques	Activer les mises à jour automatiques
Intervalle de vérification de la mise à jour	A quelle fréquence l'application et sa base de données doivent-elles être mises à jour (virus / code endommagé) ?
Protection des applications	Activer l'analyse automatique des applications
Protection de la carte SD	Activer l'analyse automatique de la carte SD
Mise à jour Wi-Fi uniquement	Lorsque cette option est activée, les mises à jour ne sont appliquées que lorsque l'appareil est connecté avec succès à un réseau Wi-Fi.

Fin de vie (uniquement au niveau de l’appareil)

Effacer (uniquement au niveau de l’appareil)

Sous "Effacer", vous pouvez rétablir les paramètres d'usine de l'appareil. Dans ce cas, les données de l'entreprise et les données privées sont supprimées sur l'appareil de l'utilisateur final.

En cliquant sur le "symbole moins", vous obtenez le message suivant :



Si vous répondez "Oui", vous pouvez procéder à l'effacement.

Sous "Rapport d'effacement", les éléments suivants peuvent être affichés

Effacé par	Historique de la personne qui a effectué l'essuyage
Date	Date
Statut	État (par exemple, si le nettoyage a été effectué avec succès)

Paramètres de restriction

Restrictions

Ici, il est possible de restreindre et de bloquer toute une série de choses.

Activer la caméra	Permettre l'utilisation de l'appareil photo	
Forcer la synchronisation automatique	Sur	La synchronisation est activée en permanence
	Arrêt	La synchronisation est désactivée de façon permanente
	Choix de l'utilisateur	Sélectionné par l'utilisateur
Force Bluetooth	Sur	Bluetooth est activé en permanence
	Arrêt	Bluetooth est désactivé de façon permanente
	Choix de l'utilisateur	Sélectionné par l'utilisateur
Force GPS	Sur	Le GPS est activé en permanence
	Arrêt	Le GPS est désactivé en permanence
	Choix de l'utilisateur	Sélectionné par l'utilisateur
Emplacement du réseau de forces	Sur	Localisation permanente sur l'internet
	Arrêt	Désactivation permanente de la localisation sur internet
	Choix de l'utilisateur	Sélectionné par l'utilisateur

Sécurité		
Interdire l'emplacement du partage	Indique si un utilisateur n'est pas autorisé à activer le partage de la localisation.	
Interdire le démarrage sécurisé	Indique si l'utilisateur n'est pas autorisé à redémarrer l'appareil en mode de démarrage sécurisé.	
Interdire la réinitialisation du réseau	Indique si un utilisateur n'est pas autorisé à réinitialiser les paramètres du réseau à partir des paramètres.	
Interdire la réinitialisation d'usine	Indique si un utilisateur n'est pas autorisé à réinitialiser l'appareil.	
Activer ADB	Permet la connexion à un PC via ADB	
Désactiver le Keyguard	Désactive le Keyguard	
Propriétaire de l'appareil Informations sur l'écran de verrouillage	Définit les informations relatives au propriétaire de l'appareil à afficher sur l'écran de verrouillage.	
Contrôle de la conformité	Mode Prompt User	L'utilisateur sera invité à effectuer les actions nécessaires.
	Mode Lock-Down Container	Masquer toutes les applications jusqu'à ce que toutes les conditions soient remplies

Gestion des applications	
Autoriser l'établissement de liens entre les applications d'un même profil	Permet aux applications du profil parent de gérer les liens web du profil géré.
Interdire le contrôle des applications	Indique si un utilisateur n'est pas autorisé à modifier les applications dans les paramètres ou les lanceurs.
Interdire l'installation d'une application	Indique si un utilisateur n'est pas autorisé à installer des applications.
Désactiver les applications de désinstallation	Indique si un utilisateur n'est pas autorisé à désinstaller des applications.
Politique d'autorisation d'exécution	Indique comment les nouvelles demandes d'autorisation des applications seront traitées.
Autoriser les sources inconnues	Si cette option est activée, les utilisateurs peuvent charger des applications de manière latérale en installant un fichier .apk.

Connectivité	
Désactiver la configuration du réseau mobile	Indique si un utilisateur n'est pas autorisé à configurer des réseaux mobiles.
Disallow Tethering Config	Indique si un utilisateur n'est pas autorisé à configurer le Tethering et les points d'accès portables.
Interdire la configuration du VPN	Indique si un utilisateur n'est pas autorisé à configurer un VPN.
Désactiver la configuration Wifi	Indique si un utilisateur n'est pas autorisé à modifier les points d'accès WiFi.
Interdire les faisceaux NFC sortants	Indique si l'utilisateur n'est pas autorisé à utiliser la technologie NFC pour transmettre des données à partir d'applications.
Verrouiller la configuration WiFi	Ce paramètre détermine si les configurations WiFi créées par une application du propriétaire de l'appareil doivent être verrouillées (c'est-à-dire qu'elles ne peuvent être modifiées ou supprimées que par l'application du propriétaire de l'appareil, même pas par l'application Paramètres).
Activer l'itinérance des données	Active l'itinérance des données

Bluetooth	
Désactiver le Bluetooth	Indique si le Bluetooth est interdit sur l'appareil. Nécessite Android 8.0
Désactiver le partage Bluetooth	Spécifie si le partage Bluetooth sortant est interdit sur l'appareil. Nécessite Android 8.0
Désactiver la configuration Bluetooth	Indique si un utilisateur n'est pas autorisé à configurer Bluetooth.

Gestion des comptes	
Interdire l'ajout d'un profil géré	Spécifie si un utilisateur n'est pas autorisé à ajouter des profils gérés. Nécessite Android 8.0
Interdire l'ajout d'utilisateurs	Indique si un utilisateur n'est pas autorisé à ajouter de nouveaux utilisateurs.
Désactiver Supprimer le profil géré	Spécifie si les profils gérés de cet utilisateur peuvent être supprimés, sauf par le propriétaire du profil. Nécessite Android 8.0
Interdire la modification du compte	Indique si un utilisateur n'a pas le droit d'ajouter ou de supprimer des comptes, à moins qu'ils ne soient ajoutés par programme par Authenticator.

Téléphonie	
Interdire les appels sortants	Spécifie que l'utilisateur n'est pas autorisé à passer des appels téléphoniques sortants.
Interdire les SMS	Spécifie que l'utilisateur n'est pas autorisé à envoyer ou à recevoir des messages SMS.

Système	
Interdire la création de fenêtres	Spécifie que les fenêtres autres que les fenêtres d'application ne doivent pas être créées.
Désactiver l'icône de l'utilisateur	Indique si un utilisateur n'est pas autorisé à modifier son icône.
Disallow Set Wallpaper	Restriction de l'utilisateur pour interdire la définition d'un fond d'écran.
Désactiver la barre d'état	La désactivation de la barre d'état bloque les notifications, les réglages rapides et autres superpositions d'écran qui permettent de s'échapper d'un appareil à usage unique.
Activer l'heure automatique	Règle l'heure automatiquement.
Activer le fuseau horaire automatique	Définit automatiquement le fuseau horaire.
Reste allumé lorsqu'il est branché	L'appareil reste actif lorsqu'il est connecté à une source d'alimentation.

Stockage	
Désactiver la vérification des applications	Indique si un utilisateur n'est pas autorisé à désactiver la vérification des applications.
Interdire le montage de supports physiques	Indique si un utilisateur n'est pas autorisé à monter des supports physiques externes.
Activer le service de sauvegarde	Le service de sauvegarde gère tous les mécanismes de sauvegarde et de restauration sur l'appareil. Si vous réglez ce paramètre sur faux, les données ne pourront pas être sauvegardées ou restaurées. Le service de sauvegarde est désactivé par défaut. Nécessite Android 8.0
Activer la mémoire de masse USB	Active l'utilisation de la mémoire de masse USB.

Clavier	
Interdire le remplissage automatique	Spécifie si un utilisateur n'est pas autorisé à utiliser les services de remplissage automatique. Nécessite Android 8.0
Interdire le copier-coller entre profils	Spécifie si ce qui est copié dans le presse-papiers de ce profil peut être collé dans des profils connexes.

Son	
Refuser l'ajustement des volumes	Indique si un utilisateur n'est pas autorisé à régler le volume principal.
Désactiver Désactiver le microphone	Indique si un utilisateur n'est pas autorisé à régler le volume du microphone.
Dispositif de mise en sourdine	Dispositif de mise en sourdine.

Gestion des certificats

Vous pouvez y distribuer des certificats de confiance et des certificats d'identité à vos appareils.

Android 8 ou une version plus récente est nécessaire pour distribuer des certificats de confiance et Android 9 ou une version plus récente est nécessaire pour distribuer des certificats d'identité.

Avec le "+", vous pouvez ajouter plusieurs certificats.

Les certificats de confiance doivent être au format PEM.

Les certificats d'identité doivent être au format PKCS12.

Gestion des connexions

Wifi

Pour ce paramètre, effectuez la préconfiguration des dispositifs de l'utilisateur final, pour l'accès aux points d'accès internes

.

Identificateur d'ensemble de services (SSID)	SSID du réseau à connecter
Réseau caché	Activer, dans le cas où le point d'accès ne diffuse pas le SSID.

Type de sécurité

Établir le type de sécurité de l'AP

WEP

Mot de passe	Mot de passe pour l'AP

WPA/WPA2

Mot de passe	Mot de passe pour l'AP

802.1x EAP

Méthode EAP

PWD	Identité	Identité
	Mot de passe	Mot de passe

PEAP	Protocole d'authentification de phase 2	aucun	Pas de protocole supplémentaire
		MSCHAPV2	Protocole MSCHAPV2
		CTG	Protocole GTC
	Certificat CA	Certificat CA	
	Identité	Identité	
	Identité anonyme	Identité anonyme	
	Mot de passe	Mot de passe	

TTLS	Protocole d'authentification de phase 2	aucun	Pas de protocole supplémentaire
		PAP	Protocole PAP
		MSCHAP	Protocole MSCHAP
		MSCHAPV2	Protocole MSCHAPV2
		CTG	Protocole GTC
	Certificat CA	Certificat CA	
	Identité	Identité	
	Identité anonyme	Identité anonyme	
	Mot de passe	Mot de passe	

TLS	Certificat CA	Certificat CA
	Identité	Identité
	Mot de passe	Mot de passe

VPN

Nom de la connexion	Nom de la connexion VPN

Type de VPN

VPN

Client VPN

Client VPN AppTec360	
Configuration de la passerelle	Sélectionnez la configuration VPN de la passerelle (voir **Paramètres généraux > Passerelle universelle > Paramètres VPN**).
VPN toujours actif	Activer le verrouillage natif
Activer le verrouillage d'AppTec360	Activer le verrouillage d'AppTec360

Intégré (disponible uniquement sur les appareils Samsung)			
Type de connexion	PPTP	Serveur	Serveur
		Activer le cryptage PPTP	Activer le cryptage PPTP
	L2TP / IPSec PSK	Serveur	Serveur
		Clé pré-partagée IPSec	Clé pré-partagée IPSec
		Activer le secret L2TP	Activer le secret L2TP
		L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Serveur	Serveur
		Identifiant IPSec	Identifiant IPSec
		Clé pré-partagée IPSec	Clé pré-partagée IPSec
Domaines de recherche DNS	Domaines de recherche DNS		
Paramètres experts	Serveurs DNS	Serveurs DNS	
	Routes de transfert	Routes de transfert	

VPN ouvert		
Serveur	Serveur	
Profil OpenVPN	Profil OpenVPN	
Application OpenVPN	OpenVPN pour Android (recommandé)	
	Connexion OpenVPN	
Paramètres experts	Serveurs DNS	Serveurs DNS
	Routes de transfert	Routes de transfert

Samsung / Strong Swan			
Type de connexion	PPTP	Serveur	Serveur
		Nom d'utilisateur	Nom d'utilisateur
		Mot de passe	Mot de passe
		Activer le cryptage PPTP	Activer le cryptage PPTP
	L2TP / IPSec PSK	Serveur	Serveur
		Clé pré-partagée IPSec	Clé pré-partagée IPSec
		Nom d'utilisateur	Nom d'utilisateur
		Mot de passe	Mot de passe
		Activer le secret L2TP	L2TP Secret
	IPSec XAuth PSK	Serveur	Serveur
		Identifiant IPSec	Identifiant IPSec
		Clé pré-partagée IPSec	Clé pré-partagée IPSec
		Nom d'utilisateur	Nom d'utilisateur
		Mot de passe	Mot de passe
Paramètres experts	Serveurs DNS	Serveurs DNS	
	Routes de transfert	Routes de transfert	

Cisco Any Connect		
Serveur	Serveur	
Mode certificat	Handicapés	Handicapés
	Automatique	Automatique
Paramètres experts	Serveurs DNS	Serveurs DNS
	Routes de transfert	Routes de transfert

VPN par application

Client VPN

Client VPN AppTec360		
Configuration de la passerelle	Sélectionnez la configuration VPN de la passerelle (voir **Paramètres généraux > Passerelle universelle > Paramètres VPN**).	
Applications VPN	Applications VPN	
VPN toujours actif	Activer le verrouillage natif	VPN toujours actif
Activer le verrouillage d'AppTec360	Activer le verrouillage d'AppTec360	

Samsung / Strong Swan			
Type de connexion	PPTP	Serveur	Serveur
		Applications VPN	Applications VPN
		Nom d'utilisateur	Nom d'utilisateur
		Mot de passe	Mot de passe
		Activer le cryptage PPTP	Activer le cryptage PPTP
	L2TP / IPSec PSK	Serveur	Serveur
		Applications VPN	Applications VPN
		Clé pré-partagée IPSec	Clé pré-partagée IPSec
		Nom d'utilisateur	Nom d'utilisateur
		Mot de passe	Mot de passe
		Activer le secret L2TP	L2TP Secret
	IPSec XAuth PSK	Serveur	Serveur
		Applications VPN	Applications VPN
		Identifiant IPSec	Identifiant IPSec
		Clé pré-partagée IPSec	Clé pré-partagée IPSec
		Nom d'utilisateur	Nom d'utilisateur
		Mot de passe	Mot de passe
Paramètres experts	Serveurs DNS	Serveurs DNS	
	Routes de transfert	Routes de transfert	

Restrictions

Vous pouvez ici définir les restrictions relatives à la gestion des connexions.

Autoriser l'itinérance des données	Autoriser les données mobiles en itinérance
Forcer l'itinérance des données	Si elle est activée, l'itinérance pour les données mobiles est activée en permanence (non recommandé !). Ce paramètre écrase le paramètre "Allow Data Roaming" (autoriser l'itinérance des données) !
Les paramètres suivants ne sont disponibles que sur SAFE 2.x ou supérieur	
Autoriser les appels d'urgence uniquement	Autoriser les appels d'urgence uniquement
Autoriser le WiFi	Autoriser le WiFi
Niveau de sécurité minimum du réseau WiFi	Niveau de sécurité minimum du réseau WiFi Ouvert = tous les types de WiFi sont autorisés
Interdire à l'utilisateur d'ajouter des réseaux WiFi	L'utilisateur ne peut pas ajouter lui-même un réseau WiFi Ce réglage n'est possible que si un profil WiFi a été défini sous "Gestion des connexions"
Autoriser les SMS et MMS	Tous = Tout le trafic SMS et MMS est autorisé SMS entrants uniquement = Seuls les SMS entrants sont autorisés. SMS sortants uniquement = Seuls les SMS sortants sont autorisés. Aucun = Aucun trafic SMS / MMS n'est autorisé
Autoriser la synchronisation en itinérance	Autoriser la synchronisation en itinérance Allumé = activé Désactivé = désactivé Choix de l'utilisateur = choix de l'utilisateur
Autoriser l'itinérance vocale	Autoriser l'itinérance vocale Allumé = activé Désactivé = désactivé Choix de l'utilisateur = choix de l'utilisateur
Utiliser le serveur proxy http du système	L'utilisation d'un serveur proxy HTTP, qui est fourni par les paramètres du système dans les réglages, dépend du réseau connecté (WiFi ou APN).

Gestion du PIM

Gmail Exchange

Info : Cette configuration sera appliquée à l'application Gmail. Vous devez donc approuver et installer Gmail.

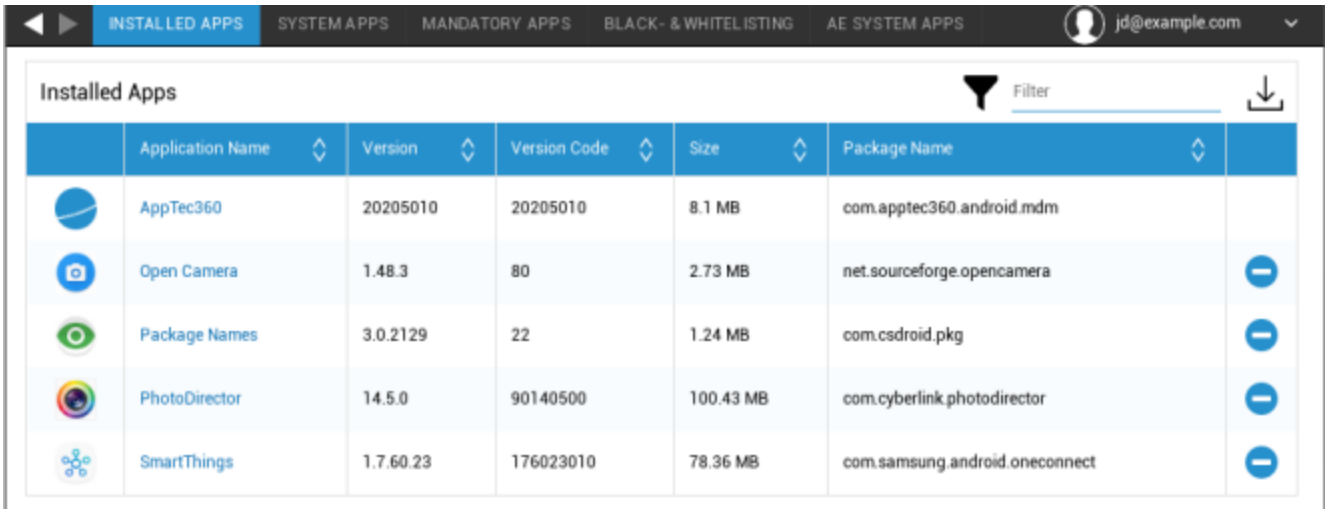
Adresse électronique	L'adresse électronique de l'utilisateur fourni Veuillez noter les "Placeholders", que vous pouvez utiliser pour travailler avec les informations d'identification et que vous ne devez pas modifier manuellement sur chaque appareil. En un clic, vous pouvez les visualiser par vous-même.
Nom d'hôte du serveur	Adresse de votre serveur Exchange
Nom de connexion	Le nom de connexion pour l'appareil de l'utilisateur final respectif, veuillez également noter les "Placeholders here".
Signature	Une signature peut être jointe (Remarque : certains appareils exigent un formatage HTML pour la signature).
Nombre de jours précédents à synchroniser	Nombre de jours déterminant le moment où les courriels sont synchronisés à nouveau
Identifiant de l'appareil	Chaîne contenant le DeviceID de l'EAS. Cette chaîne fait partie du protocole EAS et peut être utilisée dans certains environnements.
Utilisez le protocole SSL (Secure Sockets Layer)	Utiliser une connexion SSL
Accepter tous les certificats	Tous les certificats sont acceptés. Veuillez sélectionner cette option si votre serveur Exchange utilise un certificat auto-signé.

Gestion des applications

Gestionnaire d’applications d’entreprise

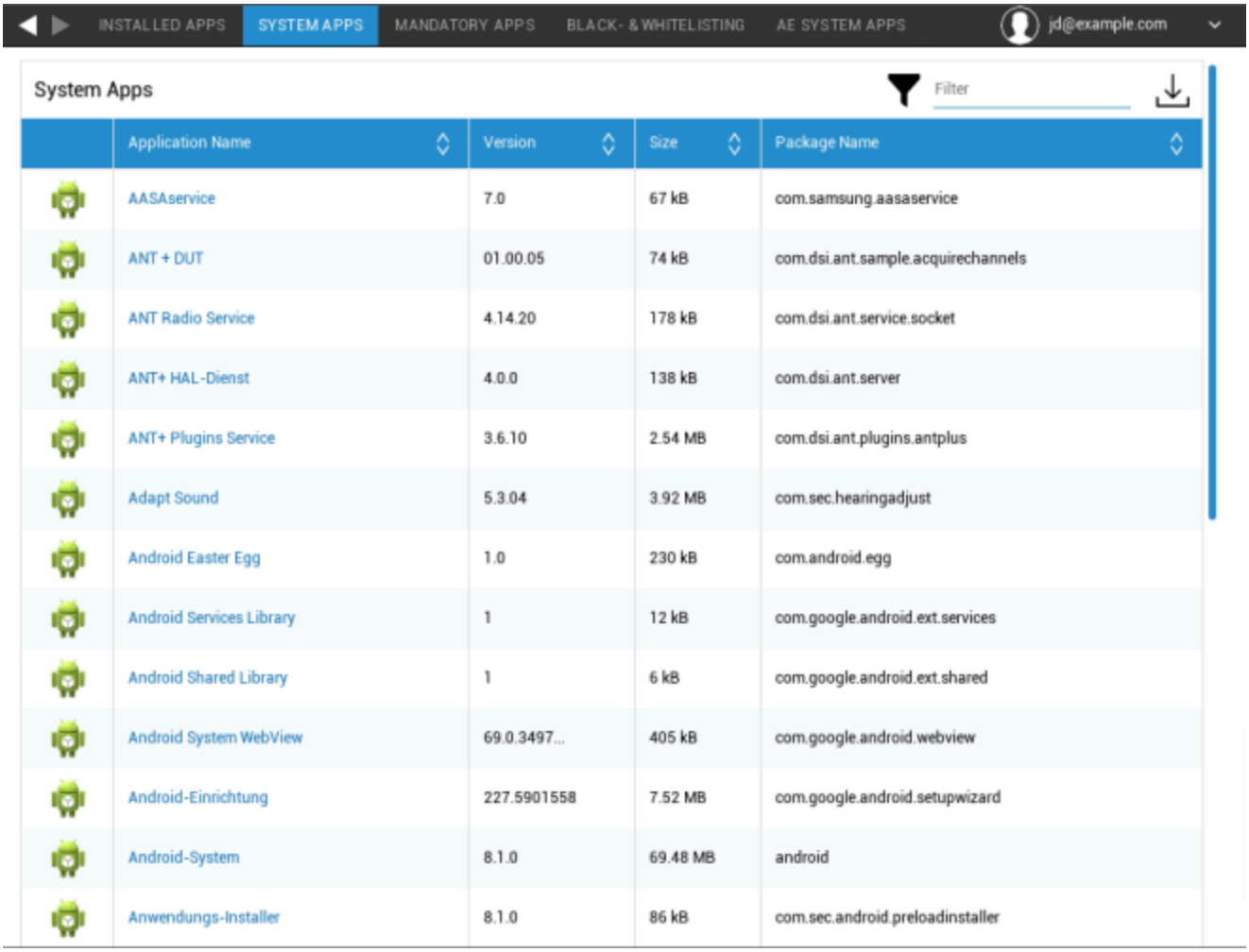
Applications installées (uniquement au niveau de l’appareil)

Toutes les applications actuellement installées sur l'appareil de l'utilisateur final s'affichent ici.



Apps système (uniquement au niveau de l’appareil)

Sous "Apps système", toutes les apps et tous les services qui ont déjà été installés sur l'appareil de l'utilisateur final par le fabricant de l'appareil sont répertoriés pour vous.

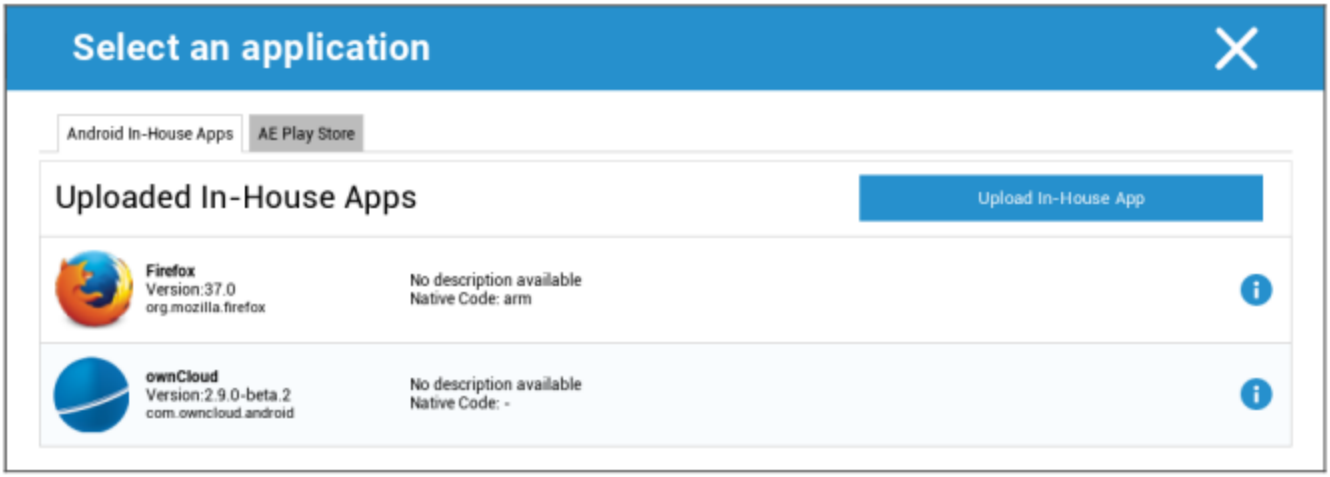


Applications obligatoires

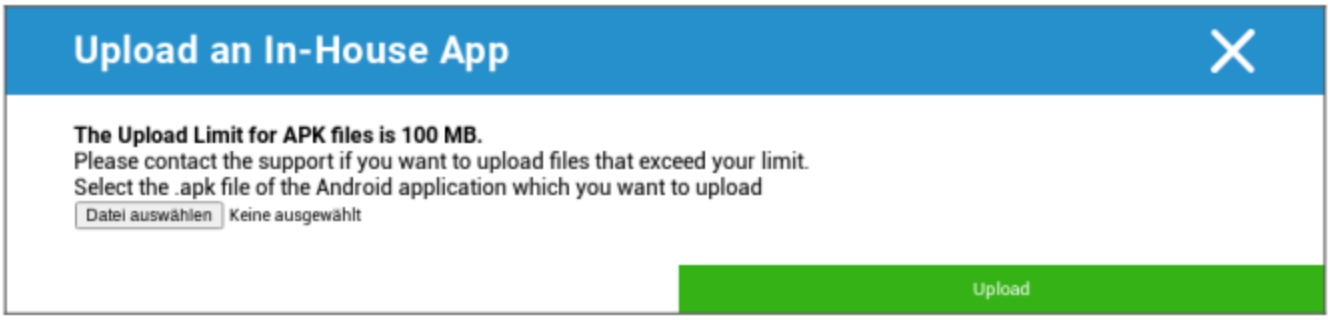
Sous la rubrique Applications obligatoires, vous pouvez définir les applications obligatoires requises. L'utilisateur sera continuellement invité à installer cette application désignée.

L'application obligatoire peut être définie à l'aide de l'application obligatoire.

Il peut s'agir d'une application interne figurant dans la liste des "applications internes Android" que vous avez téléchargée dans les paramètres généraux.

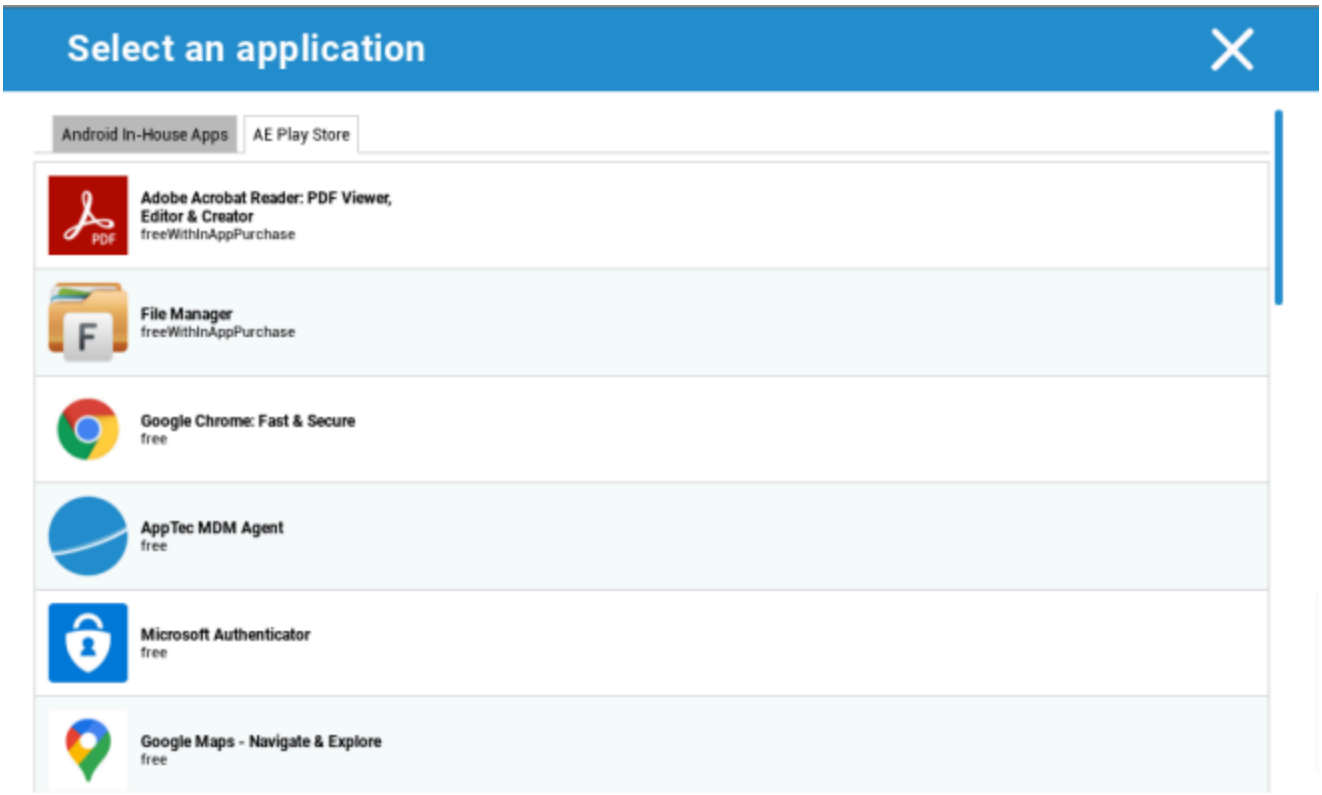


Vous pouvez également sélectionner et télécharger directement un fichier apk avec "Upload In-House App".



Si vous installez une application interne, vous aurez la possibilité d'activer l'option "Tenir à jour". Si cette option est activée et que vous avez défini une version plus récente dans la base de données des applications internes, l'application sera mise à jour sur l'appareil.

Il peut également s'agir d'une application "AE Play Store" du Google Work Play Store.



Seules les "applications AE Play Store" approuvées seront affichées dans cet onglet.

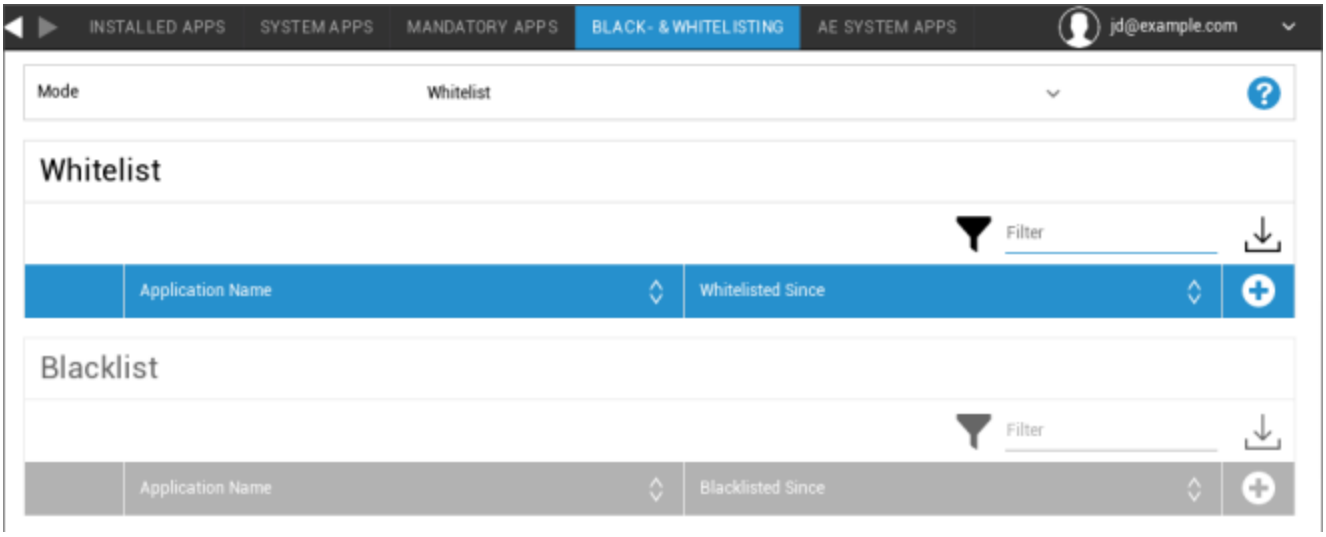
Pour approuver une "AE Play Store App", veuillez vous rendre dans "General Settings" > "App Management" > "AE Play

Store" et ajoutez une application via le bouton qui vous redirigera vers l'onglet "Play Store Apps" (ou vous
peut aller directement à l'onglet "Play Store Apps").

Dans l'onglet "Play Store Apps", vous pouvez rechercher des applications. Lorsque vous cliquez sur une application, la page de l'application s'ouvre
et vous pouvez approuver l'application en cliquant sur "Approuver".

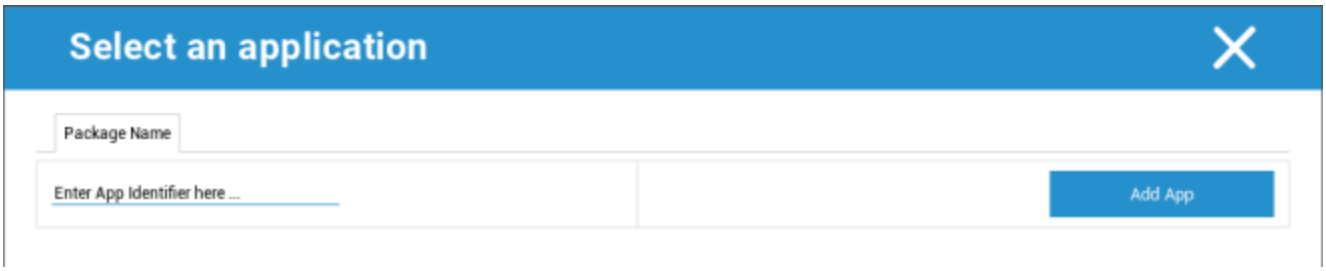
Liste noire et liste blanche

Sous "Liste noire et liste blanche", vous pouvez choisir entre le mode "Liste blanche" et le mode "Liste noire".



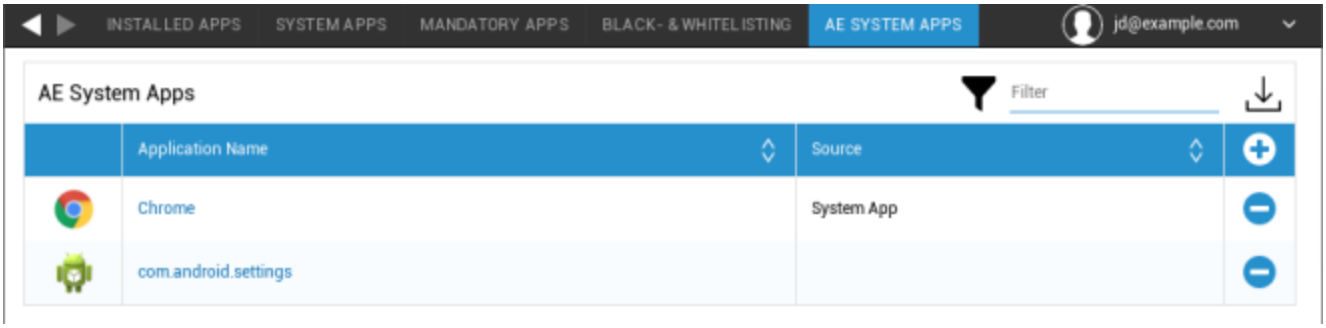
Liste blanche	Seuls les applications et services ajoutés à la liste peuvent être installés sur l'appareil de l'utilisateur final. S'ils sont déjà préinstallés sur l'appareil de l'utilisateur final, ils seront activés et configurés pour que l'utilisateur puisse les exécuter.
	Toutes les autres applications qui ne sont pas ajoutées à la liste ne peuvent pas être installées sur l'appareil de l'utilisateur final. Si elles sont déjà préinstallées sur l'appareil de l'utilisateur final, elles seront désactivées et paramétrées de sorte que l'utilisateur ne puisse pas les exécuter.
Liste noire	Les applications et services ajoutés à la liste ne peuvent pas être installés sur l'appareil de l'utilisateur final. S'ils sont déjà préinstallés sur l'appareil de l'utilisateur final, ils seront désactivés et configurés de manière à ce que l'utilisateur ne puisse pas les exécuter.
	Toutes les autres applications qui ne sont pas ajoutées à la liste peuvent être installées sur l'appareil de l'utilisateur final. Si elles sont déjà préinstallées sur l'appareil de l'utilisateur final, elles seront activées et paramétrées pour que l'utilisateur puisse les exécuter.

Via le , vous ajoutez des applications ou des services supplémentaires à la liste actuellement utilisée.
Via le , vous ajoutez des applications ou des services supplémentaires à la liste actuellement inactive.
Vous pouvez définir un "Packagename" :

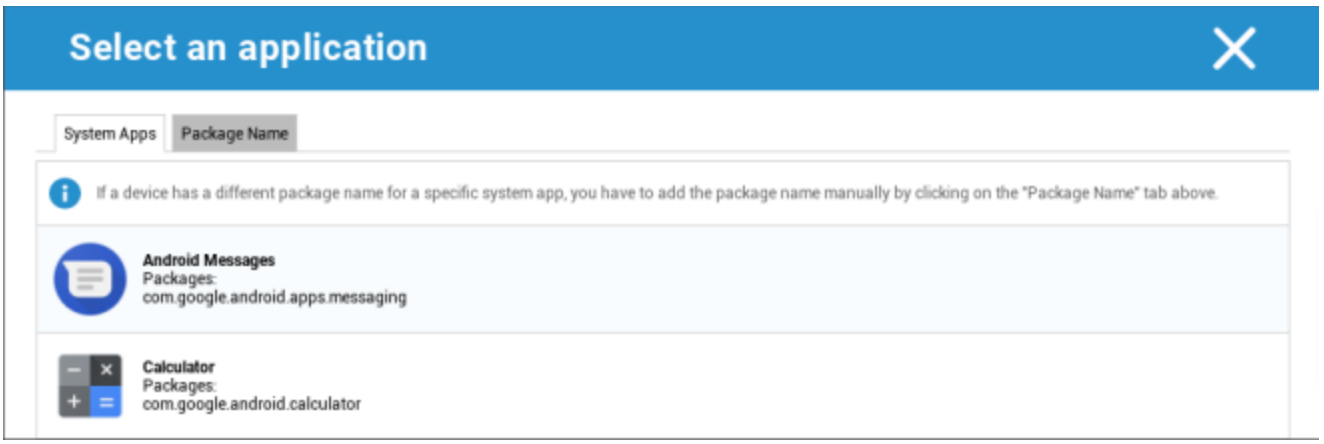

Select an application
Package Name
Enter App Identifier here ...
Add App

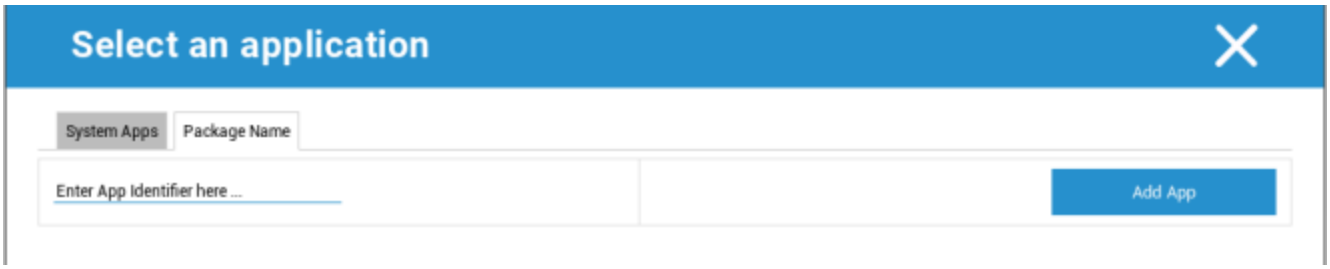
Applications du système AE

Vous pouvez définir ici une liste contenant des applications système spécifiques qui doivent être activées sur les appareils.



Si vous cliquez sur le bouton, vous pouvez choisir dans une liste d'applications système possibles fournie par Google ou saisir directement le nom du paquet d'une application système qui doit être activée.





N'oubliez pas que les applications système figurant dans la liste fournie par Google sont uniquement des applications qui peuvent être des applications système, mais qu'elles ne doivent pas nécessairement être des applications système sur vos appareils.

Toutefois, cette liste ne concerne que les applications déjà préinstallées.

L'ajout d'applications qui ne sont pas préinstallées sur vos appareils ne les affectera pas, que l'application figure dans la liste fournie par Google ou que le nom du paquet de l'application soit saisi directement.

Restrictions et paramètres

Paramètres de gestion des applications

Vous pouvez ici configurer le comportement de l'appareil en ce qui concerne les mises à jour d'applications.

Fréquence des contrôles de mise à jour	Spécifiez l'intervalle dans lequel le client AppTec360 recherchera les mises à jour de l'application. La valeur par défaut est de 24 heures.
Seuil Wi-Fi	Les applications dont la taille est supérieure à celle spécifiée seront téléchargées par Wi-Fi. Si vous sélectionnez "Wi-Fi uniquement", toutes les applications seront téléchargées par Wi-Fi.

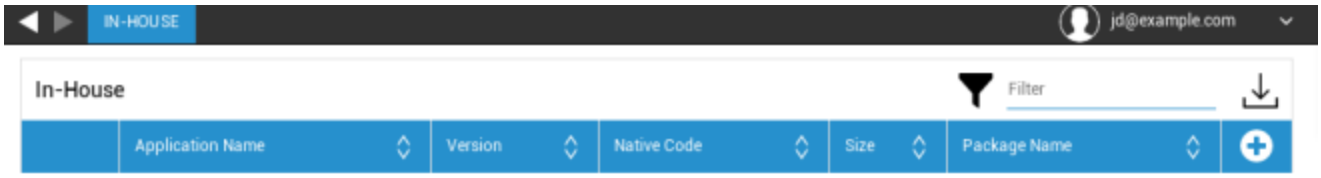
App Store d’entreprise

En interne

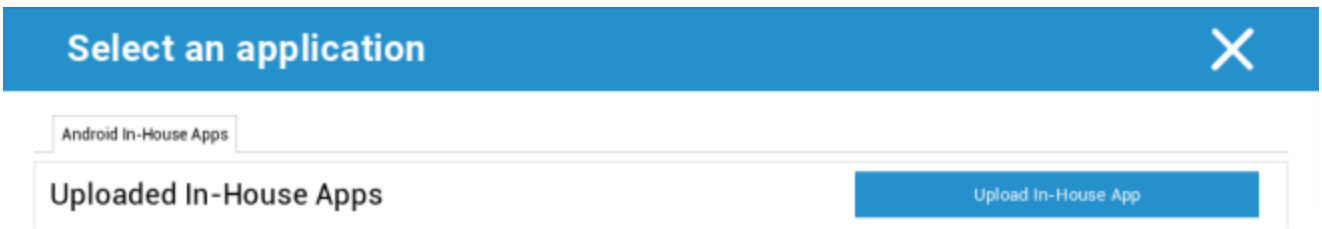
Sous le point "In-House", vous pouvez télécharger et distribuer des applications développées en interne.

Avec le symbole, vous pouvez distribuer des applications internes supplémentaires.

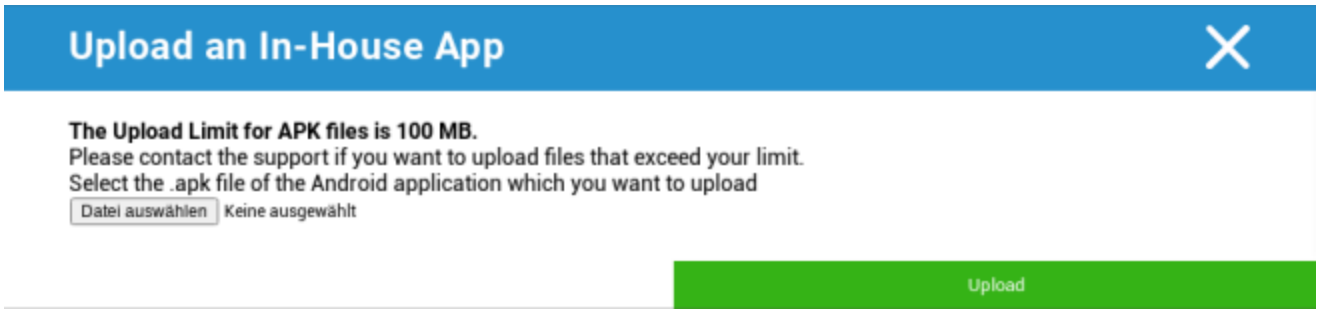
Si vous installez une application interne, vous aurez la possibilité d'activer l'option "Tenir à jour". Si est activée et que vous avez défini une version plus récente dans la base de données des applications internes, l'application sera activée.
mis à jour sur l'appareil.



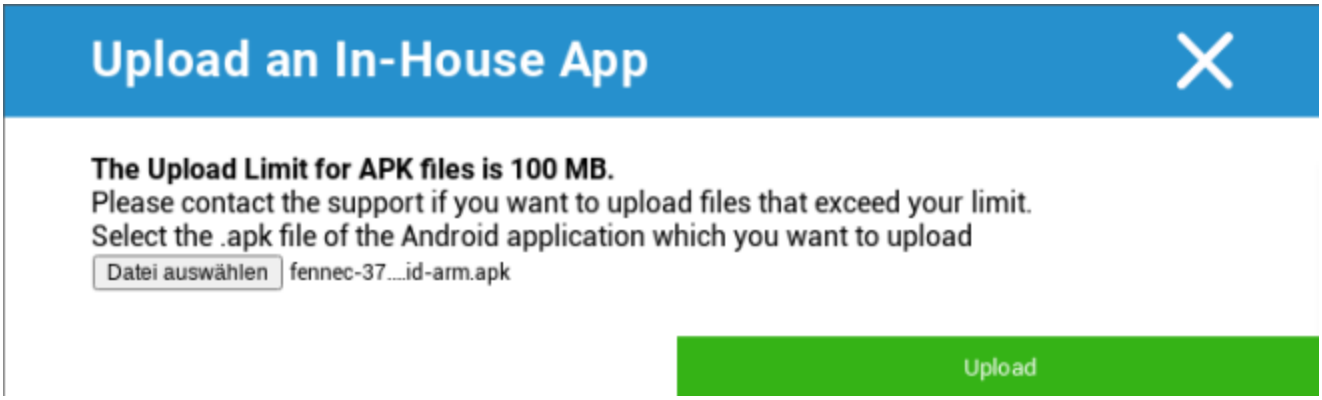
Si vous n'avez pas distribué d'applications internes, vous recevrez alors l'aperçu suivant :



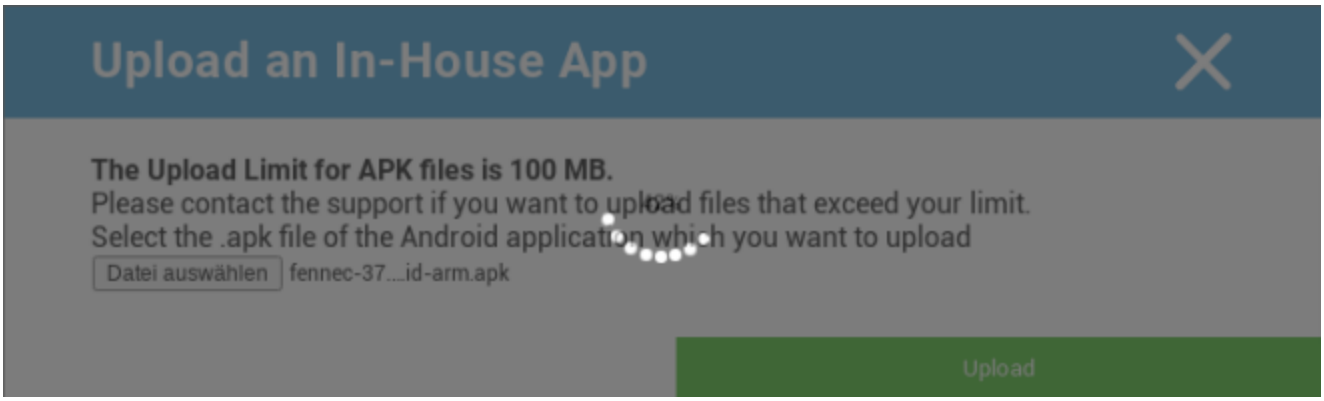
Pour ce faire, cliquez sur "Upload In-House App", vous obtiendrez alors l'aperçu suivant :



Maintenant, choisissez avec "Search..." un fichier .apk et cliquez sur "Upload".



Votre application va maintenant être téléchargée. Au milieu du cercle, vous verrez un indicateur de pourcentage,
indiquant la part de votre application qui a déjà été téléchargée.



Si le téléchargement de votre application interne a été effectué avec succès, vous pouvez alors trouver l'application téléchargée.
dans votre catalogue d'applications.

L'utilisateur a maintenant la possibilité de voir et d'installer cette application dans la boutique AppTec360 sur l'utilisateur final.
dans la catégorie "In-House".

Comme il ne s'agit pas d'une application Google PlayStore, l'utilisateur n'a pas besoin d'un mot de passe enregistré sur Google.
sur leur appareil d'utilisateur final respectif.

Entreprise Play Store

AE Play Store

Ici, vous pouvez ajouter des applications à la boutique Android Enterprise Playstore. Veuillez noter que vous devez approuver
Apps avec votre compte administrateur AE avant de pouvoir les ajouter.

Pour approuver une application, veuillez consulter les instructions de la section Applications obligatoires.

Mode kiosque et lanceur

Mode kiosque

Le mode kiosque vous permet de prédéfinir une application ou une URL. Il sera alors exclusivement possible de
exécuter/visiter cette application et/ou URL.

De même, divers boutons matériels peuvent être désactivés dans le mode kiosque.

Démarrage automatique	Lance automatiquement le mode kiosque dès que le profil atteint l'appareil de l'utilisateur final.
Mode kiosque programmé ?	Vous pouvez planifier une durée pour le mode kiosque, qui commencera et s'achèvera automatiquement à l'heure que vous aurez fixée.
Heure de début	Heure de début
Temps en minutes	Temps en minutes après lequel le mode kiosque doit se terminer à nouveau

Type d'application

Application unique	Si vous souhaitez démarrer l'application en mode kiosque, sélectionnez "Package" sous "Type d'application"
Application kiosque	Cliquez ici pour sélectionner une application qui doit être lancée en mode kiosque. Vous trouverez l'aperçu habituel de la gestion des applications Vous pouvez choisir entre "Google Play Store", "Android In-House Apps" et "Packagename"

Type d'application	
URL	Si vous souhaitez lancer une URL en mode kiosque, sélectionnez "URL" sous "Type d'application" Définissez ensuite l'adresse URL souhaitée
Effacer le navigateur après l'inactivité	Vous pouvez définir ici un intervalle de temps en minutes, après lequel le mode kiosque doit être relancé.
Effacer le cache et les cookies	Si vous activez cette fonction, après un redémarrage du mode kiosque, le cache Web (cookies et images en cache) sera effacé.
Politique de la même origine	Si cette fonction est activée, l'utilisateur ne peut naviguer que sur les sous-pages d'un URL défini. Par exemple, vous avez défini l'URL suivante: www.mypage.com Ensuite, l'utilisateur peut surfer sur : www.mypage.com/subpage
URL sur liste blanche	Ici, vous pouvez maintenir une liste blanche, tous ces URL sont autorisés. Maximum 1 URL par ligne Un URL doit commencer par http:/ ou https://.
URL sur liste noire	Ici, vous pouvez maintenir une liste noire, tous ces URL ne sont pas autorisés. Maximum 1 URL par ligne Un URL doit commencer par http:/ ou https://.
Orientation de l'écran	Ce paramètre concerne les réglages de l'écran Automatique = automatique Portrait = format vertical Paysage = mode paysage

Multi App	Si vous sélectionnez le mode kiosque "Multi App", l'utilisation du lanceur AppTec360 sera obligatoire.
Applications	Application : Sélectionnez une application Playstore ou une application interne comme application kiosque. Il est également possible de saisir un nom de pack. L'application kiosque sélectionnée doit être installée sur l'appareil. N'oubliez pas de rendre l'application kiosque obligatoire. Raccourci sur l'écran d'accueil : Si ce paramètre est réglé sur "On", un raccourci sera créé sur l'écran d'accueil. S'il est réglé sur "Off", l'application s'affichera toujours dans la liste des applications.

Mot de passe de sortie activé	Si vous activez cette fonction, l'utilisateur peut quitter le mode kiosque avec un mot de passe que vous avez prédéfini.
Quitter le mot de passe	Il s'agit du mot de passe que vous avez prédéfini.
Réduction automatique de la barre d'état	Si cette option est activée, la barre d'état sera automatiquement mise en surbrillance. Avec cette option, les utilisateurs peuvent voir les informations de la barre d'état, mais ne peuvent pas accéder à ses fonctions.
Désactiver la barre d'état	La barre d'état contient des notifications, des raccourcis et des informations. Uniquement disponible pour les appareils Samsung équipés de SAFE 4.0 ou supérieur.
Désactiver les touches de volume	Désactiver les touches de volume (disponible uniquement sur les appareils Samsung avec SAFE 3.0 ou supérieur)
Désactiver l'interrupteur marche/arrêt	Désactiver l'interrupteur marche/arrêt (disponible uniquement sur les appareils Samsung équipés de SAFE 3.0 ou d'une version plus récente)
Désactiver le bouton d'accueil	Désactiver le bouton Home. Si cette fonction a été activée, le mode kiosque ne peut être interrompu que dans la console AppTec360. (disponible uniquement sur les appareils Samsung équipés de SAFE 3.0 ou supérieur)
Désactiver la barre de navigation	Cette option vous permet de désactiver la barre de navigation (Retour / Menu). Si cette fonction a été activée, le mode kiosque ne peut être interrompu que dans la console AppTec360. (disponible uniquement sur les appareils Samsung équipés de SAFE 3.0 ou supérieur)

AppTec360 Launcher

Activer le lanceur AppTec360	Activé : Active le lanceur AppTec360. L'utilisateur doit le définir comme lanceur par défaut une fois. Note : Si le mode kiosque est activé et que le mode kiosque est réglé sur "Multi App", l'utilisation du lanceur AppTec360 sera imposée.
Grandes icônes	Allumé : Affiche une version plus grande des icônes des applications dans le lanceur.
Cacher l'icône de l'application AppTec360	Activé : Masque complètement l'application AppTec360
Cacher l'icône de la boutique AppTec360	Activé : Masque complètement l'AppStore AppTec360 Enterprise

Paramètres AppTec360

Activer l'application AppTec360 Settings	L'application AppTec360 Settings permet de contrôler les connexions WiFi et Bluetooth.
Activer les paramètres dans les applications multiples Mode kiosque	Si cette option est activée, les utilisateurs peuvent accéder à l'application de paramétrage AppTec360 lorsque le mode kiosque multi-applications est actif.

Télécommande

Splashtop

Pour démarrer une session de contrôle à distance sur votre appareil, l'application "Splashtop Streamer" doit être installée sur l'appareil en ajoutant l'application à **App Management → Enterprise App Manager → Mandatory Apps**.

Ensuite, configurez les paramètres suivants pour Splashtop :

Activer Splashtop	Si cette option est activée, AppTec360 configurera l'application Splashtop pour permettre le contrôle à distance.
Déployer le code	Allez sur https://my.splashtop.com et connectez-vous à votre compte Splashtop. Cliquez sur "Ajouter un ordinateur" et copiez le code de déploiement à 12 chiffres de la page qui s'affiche.
Définir une passerelle de déploiement personnalisée ?	Déployer la passerelle
Déployer le domaine / l'hôte de la passerelle	Déployer la passerelle
Vérification des certificats	Vérification des certificats

Vous pouvez ensuite utiliser l'option Splashtop Remote Control du menu contextuel (engrenage à côté de la barre de recherche, lorsque l'appareil est sélectionné ou clic droit sur l'appareil dans l'arborescence) pour démarrer la session de contrôle à distance.

TeamViewer

Pour démarrer une session de contrôle à distance sur votre appareil, l'application "TeamViewer QuickSupport" doit être installée sur l'appareil en ajoutant l'application à **App Management → Enterprise App Manager → Mandatory Apps**.

Vous pouvez ensuite utiliser l'option **TeamViewer Remote Control** du menu contextuel (engrenage à côté de la barre de recherche, lorsque l'appareil est sélectionné ou clic droit sur l'appareil dans l'arborescence) pour démarrer la session de contrôle à distance.

Gestion du contenu

ContentBox

Ici, vous pouvez activer la boîte de contenu.

Dès que l'option "Activer ContentBox" est activée, une application ContentBox distincte est installée. automatiquement sur l'appareil de l'utilisateur final.

Navigateur sécurisé

Vous pouvez ici configurer les paramètres du AppTec360 Secure Browser.

Dès que vous activez la section "Secure Browser", une application de navigation distincte est automatiquement installée sur l'appareil de l'utilisateur final à l'adresse
.

Demande de mot de passe	Exiger de l'utilisateur qu'il définisse et utilise un mot de passe pour accéder au navigateur.
Longueur minimale du mot de passe	Définissez le nombre de caractères requis pour le mot de passe
Qualité requise du mot de passe	Définissez la qualité du mot de passe requis
Restreindre les téléchargements / Ouvrir en	
Limiter les téléchargements	
Télécharger la liste blanche	Une liste d'URL pour lesquelles le téléchargement sera toujours autorisé.
Autoriser la copie	Permettre de copier, de couper ou de partager du texte à l'intérieur des pages web.
Autoriser la capture d'écran	Permettre la réalisation de captures d'écran.
Fréquence de nettoyage des données	Sélectionnez la fréquence à laquelle TOUTES les données de l'utilisateur (historique, cache, etc.) doivent être automatiquement supprimées.
Signets d'entreprise	Les signets apparaîtront dans le dossier "Signets de l'entreprise" des signets du navigateur. Ils ne sont pas modifiables par l'utilisateur.
Masquer la barre d'adresse	

Liste blanche dans le navigateur (sans passerelle universelle)	Active la liste blanche d'URL côté client. • Les signets d'entreprise sont toujours inscrits sur la liste blanche • Pris en charge pour 100 URL seulement • Veuillez utiliser la passerelle universelle pour un nombre illimité de listes noires et blanches.
URL sur liste blanche	Une liste d'URL autorisés.
Liste noire et liste blanche basées sur la passerelle	L'inscription sur liste noire est soumise aux exigences suivantes : • Une passerelle universelle AppTec360 fonctionnelle ("Paramètres généraux" → "Passerelle universelle") • Une configuration VPN fonctionnelle avec un serveur DNS spécifié ("Paramètres généraux" → "Passerelle universelle" → "Paramètres VPN") • Une configuration de liste noire ("General Settings" → "Universal Gateway" → "Domain Blacklist") • Une connexion VPN valide dans le profil ("Gestion des connexions" → "VPN")

API supplémentaire

Samsung KNOX

Restrictions

Autoriser la carte SD	
Autoriser l'écriture sur la carte SD	
Autoriser la capture d'écran	
Autoriser le presse-papiers	
Sauvegarde des paramètres et des données de l'application dans Google Cloud	
Restauration des paramètres à partir de Google Cloud lors de la réinstallation d'une application	
Autoriser le débogage USB	
Autoriser le rapport d'accident de Google	
Autoriser la réinitialisation d'usine	
Autoriser la mise à jour OTA	
Autoriser le stockage hôte USB	Si cette option est activée, l'utilisateur peut connecter une clé USB portable, un disque dur externe ou un lecteur de carte Secure Digital (SD), qui sera alors monté en tant que disque de stockage sur l'appareil.
Autoriser le lecteur multimédia USB (MTP, PTP)	
Autoriser le microphone	Désactive le microphone pour les applications tierces
Autoriser la NFC (Near Field Communication)	
Autoriser les sources inconnues (APK Sideloading)	Si cette option est activée, le chargement latéral d'applications (fichiers APK) est autorisé. Une fois ce paramètre désactivé, l'utilisateur doit l'activer manuellement lorsque vous autorisez à nouveau l'installation d'APK provenant de sources inconnues.

Autoriser la création d'un utilisateur	Si cette option est activée, l'utilisateur est autorisé à créer plusieurs comptes sur l'appareil, par exemple des comptes d'invité.

Courriel

Adresse électronique	
Protocole du serveur entrant	
Adresse du serveur entrant	
Port du serveur entrant	
Nom d'utilisateur du serveur entrant	
Mot de passe du serveur entrant	
Le serveur entrant utilise SSL	
Le serveur entrant utilise TLS	
Le serveur entrant accepte tous les certificats	
Protocole du serveur sortant	
Adresse du serveur sortant	
Port du serveur sortant	
Le serveur sortant utilise des informations d'identification supplémentaires	Si cette option est désactivée, le système utilise les informations d'identification entrantes pour le serveur sortant également.
Nom d'utilisateur du serveur sortant	
Mot de passe du serveur sortant	
Le serveur sortant utilise SSL	
Le serveur sortant utilise TLS	
Le serveur sortant accepte tous les certificats	
Signature de l'ensemble	
Signature	Note : Pour certains appareils, la signature doit être spécifiée au format HTML.
Notifier l'utilisateur lors de la réception d'un nouvel e-mail	

Échange

Adresse électronique	
Nom d'hôte du serveur	Le nom d'hôte du serveur Exchange
Nom de connexion	Le nom d'utilisateur utilisé pour se connecter au serveur Exchange.
Domaine	Si une configuration de passerelle ACL est activée et que le champ Domaine n'est pas vide, la passerelle universelle AppTec360 authentifiera l'appareil avec le nom suivant : "Nom de domaine".
Mot de passe	
Nombre de jours précédents à synchroniser	
Fréquence de synchronisation de l'eMail	
Synchronisation en itinérance	
Signature de l'ensemble	
Signature	Note : Pour certains appareils, la signature doit être spécifiée au format HTML.
Compte par défaut	
Utilisez le protocole SSL (Secure Sockets Layer)	
Utiliser la sécurité de la couche transport (TLS)	
Accepter tous les certificats	

APN

Nom d'affichage de l'APN	
Nom du point d'accès	Nom de l'APN
Protocole du serveur sortant	
MCC - Indicatif de pays de téléphonie mobile	Laissez vide pour utiliser le mmc de la carte SIM installée
MNC - Code de réseau mobile	Laissez vide pour utiliser le mnc de la carte SIM installée
Adresse du serveur	
Numéro de port du serveur	
Adresse proxy du serveur	
Adresse du serveur MMS	Laissez vide pour la valeur par défaut
Numéro de port MMS	Laissez vide pour la valeur par défaut
Adresse proxy MMS	Laissez vide pour la valeur par défaut
Nom d'utilisateur	
Mot de passe	
Type de point d'accès	Les types acceptés sont "default", "mms", "supl".
	Si null ou empty est transmis, par défaut "default,supl,mms" est utilisé.
	Laissez vide pour la valeur par défaut.
APN préféré	

Bluetooth

Autoriser la découverte de l'appareil via Bluetooth	
Autoriser l'appairage Bluetooth	
Autoriser les oreillettes Bluetooth	
Autoriser les dispositifs mains libres Bluetooth	
Autoriser les périphériques Bluetooth A2DP	A2DP, Advanced Audio Distribution Profile (profil de distribution audio avancée) permet la diffusion audio entre les appareils
Autoriser les appels sortants	
Autoriser le transfert de données via Bluetooth	
Autoriser le Bluetooth Tethering	
Autoriser la connexion à l'ordinateur via Bluetooth	

Connexion

Autoriser les appels d'urgence uniquementAutoriser le Wi-Fi	
Niveau de sécurité minimum du réseau Wi-Fi	
Interdire à l'utilisateur d'ajouter des réseaux Wi-Fi	Cette restriction ne peut être activée que si au moins un profil Wi-Fi actif est défini sous Gestion des connexions.
Autoriser les SMS et MMS	
Autoriser la synchronisation en itinérance	
Autoriser l'itinérance vocale	

Android Enterprise – Dispositif entièrement géré avec profil de travail (COPE)

Explication générale du COPE

COPE est l'abréviation de **Corporate Owned Personally Enabled**.

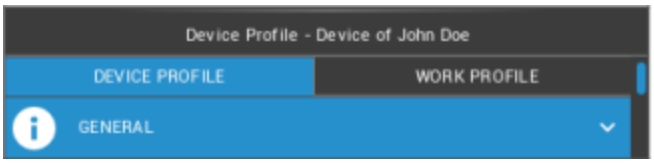
Le mode COPE permet à un appareil Android d'être enregistré en tant qu'**appareil Android Enterprise - Entièrement géré** avec le profil **Android Enterprise - Conteneur** intégré.

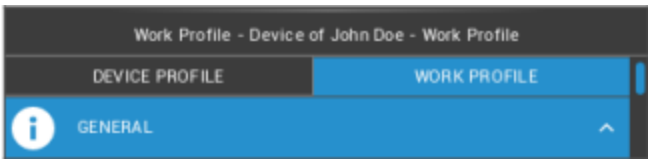
Il peut s'agir d'un appareil Android qui est déjà enregistré en tant qu'appareil **Android Enterprise - Dispositif entièrement géré** et sur lequel le **Android Enterprise - Conteneur** est également configuré, ou un appareil Android nouvellement inscrit qui est directement inscrit en tant qu'appareil **Android Enterprise - Dispositif entièrement géré** en collaboration avec le **Android Enterprise - Conteneur** sur le dessus.

Le mode COPE n'est disponible que pour les appareils équipés d'Android 8, 9 et 10.

Configuration des profils pour les dispositifs COPE

Comme il n'existe pas de profil de configuration pour le mode COPE lui-même, la configuration d'**Android Enterprise - dispositif entièrement géré** et d' **Android Enterprise - conteneur** est séparée en deux profils au sein du profil COPE. Il est possible de passer d'un profil à l'autre pour la configuration de chaque profil en cliquant sur le bouton correspondant sur le côté gauche de la console :





Les deux profils peuvent être configurés comme décrit pour chaque profil individuel :

Android Enterprise - Dispositif entièrement géré

Android Enterprise - Conteneur

Revenir à un dispositif entièrement géré par l'AE

Le profil **Android Enterprise - Container** peut être supprimé comme décrit dans la section **Gestion des mobiles**.

En supprimant le profil de conteneur, le profil COPE sera transformé en profil **Android Enterprise - Fully Managed Device**.

Android Enterprise – Configuration des conteneurs

Selon que vous avez sélectionné un profil de groupe ou un appareil, la vue d'ensemble et ses sous-points diffèrent.

Général

Aperçu du profil (uniquement au niveau du profil)

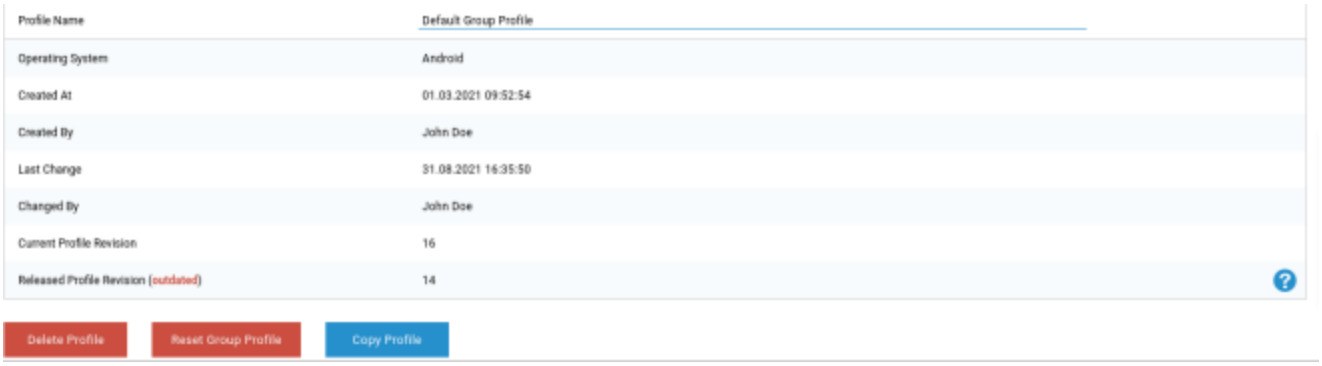
Si vous vous trouvez dans un profil, vous recevrez un bref aperçu du profil, en ce qui concerne le nom, le système d'exploitation, la date de création, l'auteur, etc.

Nom du profil	Nom du profil - peut être renommé directement ici
Système d'exploitation	Système d'exploitation valide pour le profil
Créé à	Date de création
Créé par	Créé par
Dernier changement	Date de la dernière modification
Modifié par	L'utilisateur qui a effectué les dernières modifications de ce profil
Révision du profil actuel	Nombre de fois où le profil a déjà été mis à jour
Révision du profil validé	Nombre de fois où le profil a déjà été mis à jour et où des appareils lui ont été attribués

Supprimer le profil	Supprimer le profil
Réinitialiser le profil du groupe	Réinitialiser le profil du groupe
Profil de la copie	Profil de la copie

Aperçu du profil du groupe (uniquement au niveau du groupe)

Lorsque vous ouvrez un profil de groupe, vous obtenez un aperçu rapide du profil.



Nom du profil	Nom du profil (peut être modifié ici)
Système d'exploitation	Système d'exploitation pour lequel le profil est établi
Créé à	Moment de la création
Créé par	Le créateur du profil
Dernier changement	Date de la dernière modification du profil
Modifié par	Compte ayant effectué les dernières modifications
Révision du profil actuel	Révision de l'état du profil sauvegardé
Révision du profil validé	Révision du profil attribué ("Attribuer maintenant"). Si l'étiquette affiche "(obsolète)" derrière le texte, cela signifie que vous avez enregistré le profil mais que vous ne l'avez pas encore attribué.

Aperçu de l’appareil (uniquement au niveau de l’appareil)

Si vous vous trouvez sur un appareil, vous recevrez un récapitulatif de l'appareil sélectionné, qui contient les informations suivantes :

Nom de l'appareil	Nom de l'appareil
Localisation	Coordonnées du lieu
Numéro de téléphone	Numéro de téléphone
Apps obligatoires assignées	Nombre d'applications obligatoires attribuées
Version OS	Version du système d'exploitation de l'appareil
Système d'exploitation	Système d'exploitation (Android Enterprise)
Numéro de série	Numéro de série de l'appareil
Propriété des appareils	Dispositif d'entreprise ou privé
Type d'appareil	Dispositif géré par AE Work
Enraciné	Statut, indiquant si l'appareil a été enraciné
Conforme à la loi	Conforme aux lignes directrices
Adresse IP	Adresse IP de l'appareil
Dernière visite	Moment où le dispositif s'est connecté pour la dernière fois à AppTec
Dernière poussée	Moment où la dernière impulsion a été envoyée à l'appareil.
Affectation des utilisateurs	L'utilisateur ou le groupe auquel ce dispositif est affecté

Révision de la configuration

Vous obtenez ici une vue d'ensemble du profil de groupe attribué à l'appareil.

Si vous cliquez sur le profil du groupe, vous aurez un accès direct à ce profil et vous pourrez effectuer des réglages.

Ce symbole permet de rétablir les paramètres du profil de groupe pour les applications distribuées.

Ce symbole vous permet de rétablir les paramètres du profil de groupe pour toutes les applications utilisées.

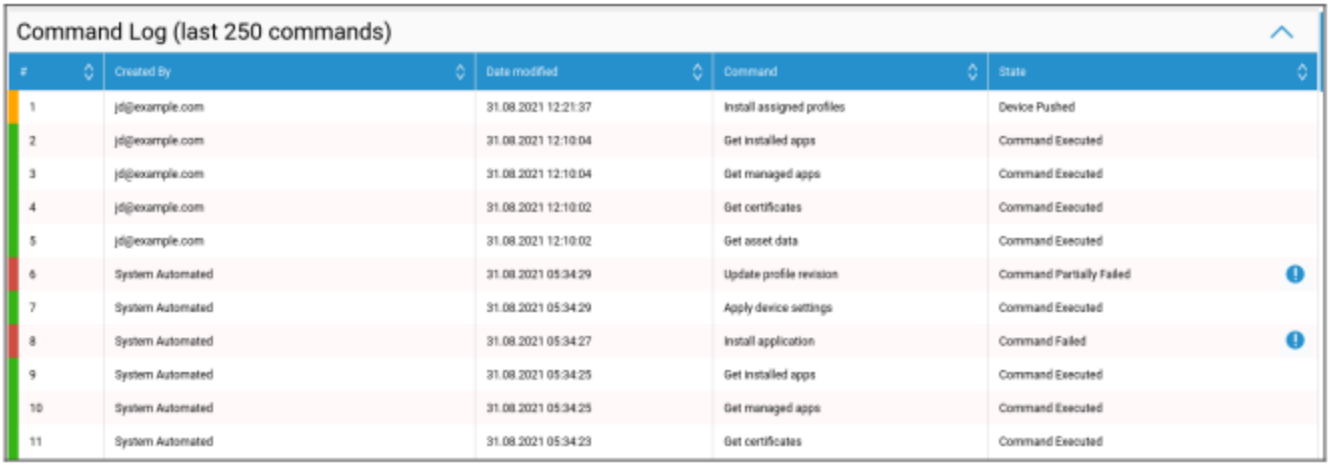
La mention "Révision plus récente disponible" indique que le profil de groupe a été modifié et enregistré, mais qu'il n'a pas été attribué. Le profil de groupe doit être attribué avec "Attribuer maintenant" au niveau du groupe pour appliquer les changements aux appareils.

Journal de l’appareil (uniquement au niveau de l’appareil)

Vous y recevrez différents journaux de bord. Si nécessaire, vous pouvez directement trouver la cause d'une erreur ici.

Journal des commandes

Vous pouvez voir ici quelles commandes ont été émises pour l'appareil et quel est leur état.



États possibles de la commande

Dispositif poussé	Une requête "push" a été envoyée au service "push" (par exemple APNS) pour demander à l'appareil de se reconnecter au serveur EMM.
Commande créée	La commande a été créée dans le système.
Commande envoyée	La commande a été envoyée à l'appareil après qu'il se soit connecté au serveur.
Commande exécutée	La commande a été exécutée avec succès.
Échec de la commande	La commande a échoué. *
Échec partiel de la commande	Selon le système d'exploitation de l'appareil, certaines commandes peuvent être regroupées. Dans ce cas, certaines parties de ce groupe de commande ont échoué. *
Commande exécutée, échec éventuel	La commande a été exécutée, mais peut-être qu'elle ne l'a pas été.
Commandement repoussé	La commande a été repoussée par un utilisateur.
Mise au rebut	La commande a été supprimée. Par exemple, parce qu'elle a été remplacée par une autre commande ou parce que l'appareil a été réenrôlé et que les anciennes commandes ont été supprimées.

*Si le message est accompagné d'un point d'exclamation, vous pouvez obtenir plus d'informations en survolant l'icône avec votre curseur.

Paramètres de l’appareil

Configuration du client

Ici, vous pouvez effectuer les configurations suivantes sur votre appareil Android :

Temps de non-conformité	Délai d'attente de la réponse de l'utilisateur après lequel la mesure d'exécution est appliquée.
Mesures d'exécution après l'expiration du délai de mise en conformité	Action de mise en application lorsqu'un utilisateur n'effectue pas les actions qui conduisent à un statut d'appareil conforme.
Fréquence de la collecte des données	Fréquence à laquelle les informations relatives à l'appareil/au GPS doivent être collectées
Fréquence de battement de cœur du dispositif	Intervalle dans lequel l'appareil doit contacter le serveur AppTec Min. 1 minute Max. 24 heures
Activer les mises à jour de localisation	Si cette option est activée, l'appareil envoie des mises à jour de localisation au serveur AppTec.
Lieu Heure de mise à jour	Détermine dans quels intervalles de temps l'appareil envoie des mises à jour de localisation à AppTec
Utilisez la précision de localisation de Google pour la mise à jour de l'emplacement	S'il est activé, l'emplacement du réseau sera utilisé pour les mises à jour de l'emplacement (si ce paramètre a été désactivé dans "Restrictions", il n'aura aucune incidence).
Utiliser la localisation GPS pour la mise à jour de l'emplacement	Si cette option est activée, le GPS sera utilisé pour les mises à jour de la position.
Autoriser les faux emplacements	Permet de falsifier les informations de localisation via des applications tierces
Action en cas de perte de connexion	Si cette option est activée, vous pouvez spécifier une action pour le cas où un appareil n'obtient pas de connexion au serveur MDM dans l'intervalle de battement de cœur. Par exemple, si l'appareil a un intervalle de battement de cœur de 5 minutes, il se connecte au serveur à 10:35 AM. Ensuite, l'appareil quitte la zone Wi-Fi. Le prochain battement de cœur à 10:40 AM échouera et l'action spécifiée sera exécutée.
Action	L'action à entreprendre dès qu'un dispositif devient non conforme.

		• Lock Device = dispositif de verrouillage • Effacer l'appareil = l'appareil sera restauré aux paramètres d'usine • Effacer l'appareil et la carte SD = l'appareil sera restauré aux paramètres d'usine et le stockage sur la carte SD sera supprimé.
	Seuil	Vous pouvez spécifier un seuil de battements de cœur défaillants nécessaires pour déclencher l'action spécifiée.

Mode d'application de la politique	Par défaut :	Les utilisateurs seront invités périodiquement à exécuter les actions en cours.
	Application paresseuse de la politique :	Les utilisateurs ne seront jamais invités à exécuter les actions en cours. Toutes les actions en cours seront affichées dans le client AppTec.
	Application agressive de la politique :	Les utilisateurs seront invités en permanence à exécuter les actions en cours.
Verrouillage de la version d'AppTec	Si cette option est activée, il est possible de spécifier un code de version pour l'application AppTec. Le client AppTec ne sera mis à jour qu'avec la version spécifiée. Les versions plus récentes seront ignorées. Une rétrogradation n'est PAS possible.	
Code de la version	Code de la version de l'application AppTec sur laquelle il faut se verrouiller.	
Désactiver la notification d'AppTec	S'il est désactivé, le client AppTec n'affichera pas de notification dans la barre de notification. Les utilisateurs peuvent donc fermer le client AppTec via le gestionnaire des tâches. Si le client AppTec est fermé, plusieurs fonctionnalités, y compris le mode Kiosque et la liste noire/blanchie des applications, ne fonctionneront pas correctement. Les appareils Samsung offrent un mécanisme de protection pour le client AppTec. La notification est désactivée par défaut sur les appareils Samsung qui prennent en charge les API KNOX. La notification ne devrait pas être désactivée sur les appareils équipés d'Android 8.0 ou d'une version ultérieure.	

Papier peint

Définir un fond d'écran personnalisé	Activer/désactiver le fond d'écran personnalisé
Papier peint	Définissez le mode de fond d'écran pour utiliser un code couleur ou une image.
Spécifiez une couleur	Spécifiez une couleur d'arrière-plan sous forme de valeur hexagonale, par exemple #000000 pour le noir ou #ffffff pour le blanc.
Définir l'image comme fond d'écran	Téléchargez le fichier image que vous souhaitez utiliser comme fond d'écran.

Gestion des actifs (uniquement au niveau de l’appareil)

Informations sur l’appareil

Modèle	Désignation du modèle de l'appareil
Système d'exploitation	OS
Version OS	Version du système d'exploitation
Numéro de série	Numéro de série
Nom de l'appareil	Nom de l'appareil
État de la batterie	État de la batterie
Mémoire libre / totale	Mémoire libre / totale
Coffre-fort Samsung	Interface Samsung SAFE, nécessaire pour une variété d'options de réglage
Carte SD disponible	Carte SD disponible
Carte SD émulée	Carte SD émulée
Carte SD amovible	Carte SD amovible
SD Mémoire libre / totale	SD Libre / Mémoire totale de la carte SD

Wi-Fi

Adresse IP	Adresse IP de l'appareil
WiFi MAC	Adresse MAC du WiFi

Cellulaire

Statut	État (carte SIM installée)
Numéro de téléphone	Numéro de téléphone
Itinérance (voix/données)	Itinérance pour la voix et les données
État de l'itinérance	État actuel de l'itinérance
Adresse IP	Adresse IP
Opérateur/transporteur	Opérateur/transporteur
Technologie cellulaire	Technologie cellulaire
IMEI	Numéro IMEI
ICCID	Il s'agit de l'identifiant de la carte SIM, qui est souvent aussi une carte à puce ou une carte à circuit intégré (ICC).
IMSI	L'International Mobile Subscriber Identity (IMSI) permet, dans les réseaux mobiles GSM et UMTS, une identification précise des utilisateurs du réseau. L'IMSI est composé d'un maximum de 15 chiffres et est configuré de la manière suivante : • Indicatif de pays du mobile (MCC), 3 chiffres • Code de réseau mobile (MNC), 2 ou 3 chiffres • Numéro d'identification de l'abonné mobile (MSIN), 1 à 10 chiffres
Actuel MCC/MNC	Voir "SIM MCC/MNC"
SIM MCC/MNC	L'indicatif de pays du mobile est un identificateur de pays établi par l'UIT selon la norme E.212. Il est associé au code de réseau mobile (MNC) pour l'identification du réseau mobile. Signifie le code de pays/réseau mobile de la carte SIM. Si vous vous rendez sur un autre réseau mobile, il est logique que le "MCC/MNC actuel" et le "MCC/MNC SIM" soient différents.

Bluetooth

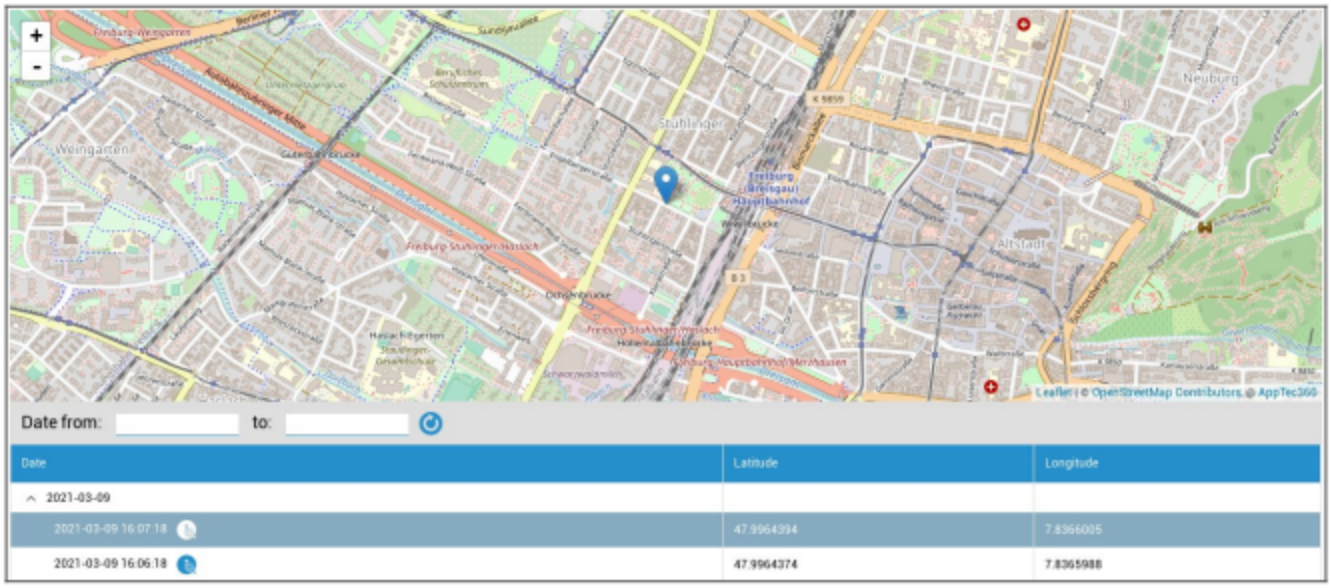
Bluetooth MAC	Adresse MAC Bluetooth

Gestion de la sécurité

Antivol (uniquement au niveau de l’appareil)

Informations GPS (uniquement au niveau de l’appareil)

Vous pouvez ici déterminer l'emplacement actuel/dernier emplacement de l'appareil. La localisation peut être protégée par un ou deux mots de passe - Voir : Paramètres généraux - Confidentialité - Accès GPS



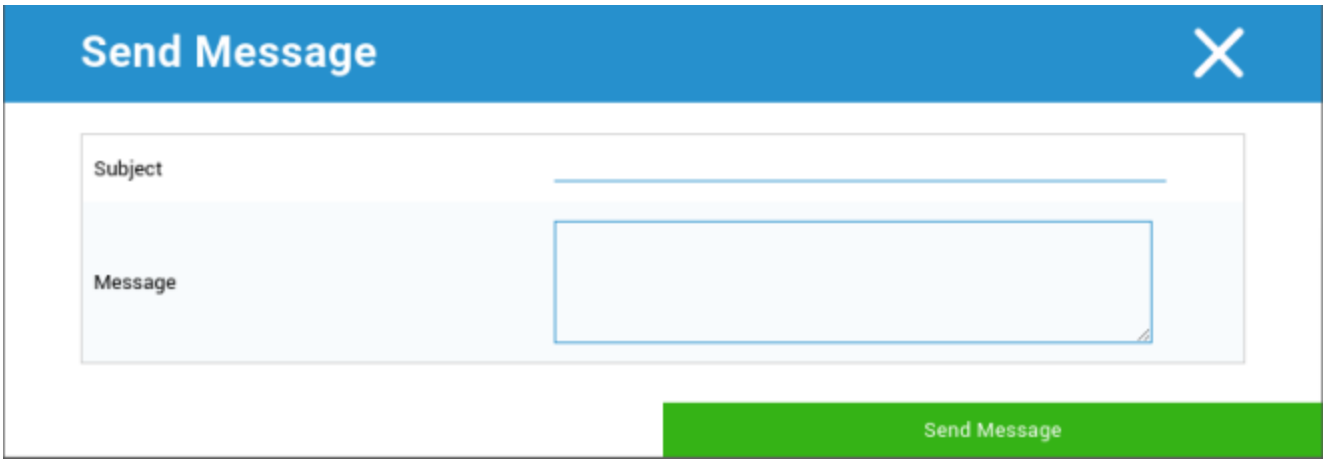
Effacement et verrouillage (uniquement au niveau de l’appareil)

Sous "Effacer et verrouiller", vous pouvez effectuer les trois actions suivantes :

Essuyage complet	L'appareil est restauré dans ses paramètres d'usine (les données de l'entreprise et les données personnelles sont supprimées). Ne fonctionne que pour le profil de travail amélioré
Nettoyage de l'entreprise	Seules les données de l'entreprise sont supprimées de l'appareil de l'utilisateur final (toutes les applications, données, etc. qui ont été fournies par AppTec).
Écran de verrouillage	Le verrouillage de l'écran est activé, il suffit de déverrouiller l'appareil avec le mot de passe/NIP de l'appareil.

Message (uniquement au niveau de l’appareil)

Ici, vous pouvez remplir l'objet et un message et l'envoyer à un appareil d'utilisateur final.



Configuration de la sécurité

Code de l’appareil

Sous "Passcode", vous pouvez mandater un mot de passe pour l'appareil, les options de réglage suivantes sont disponibles

Longueur minimale du mot de passe	Fixe le nombre minimum de symboles que doit comporter un mot de passe	
Qualité du mot de passe	Non spécifié	Cette politique ne prévoit aucune exigence concernant le mot de passe.
	Biométrique Faible	Cette politique autorise les technologies de reconnaissance biométrique à faible niveau de sécurité. Il s'agit de technologies capables de reconnaître l'identité d'une personne à l'aide d'un code PIN à trois chiffres environ (le taux de fausse détection est inférieur à 1 sur 1 000).
	Quelque chose	Cette politique exige la définition d'un mot de passe ou d'un modèle, mais n'impose pas de règles spécifiques.
	Alphabétique	L'utilisateur doit avoir introduit un mot de passe contenant au moins des caractères alphabétiques (ou d'autres symboles).
	Alphanumérique	L'utilisateur doit avoir saisi un mot de passe contenant au moins des caractères numériques et alphabétiques (ou d'autres symboles).
	Complexe	L'utilisateur doit avoir saisi un mot de passe contenant au moins une lettre, un chiffre et un symbole spécial, par défaut. Avec cette qualité de mot de passe, les mots de passe peuvent être restreints pour contenir différents ensembles de caractères, comme au moins une lettre majuscule, etc.
Longueur minimale du mot de passe	Définissez le nombre de caractères requis pour le mot de passe. Par exemple, vous pouvez exiger que les codes PIN ou les mots de passe comportent au moins six caractères.	
Nombre minimum de chiffres requis pour le mot de passe	Nombre minimum de chiffres requis pour le mot de passe	

Minimum de lettres minuscules requis dans le mot de passe	Minimum de lettres minuscules requis dans le mot de passe
Minimum de lettres majuscules requis dans le mot de passe	Minimum de lettres majuscules requis dans le mot de passe
Nombre minimum de caractères non alphabétiques requis dans le mot de passe	Nombre minimum de caractères non alphabétiques requis dans le mot de passe
Symboles minimums requis dans le mot de passe	Symboles minimums requis dans le mot de passe

Verrouillage du temps d'inactivité maximum	Inactivité maximale de l'utilisateur jusqu'au verrouillage de l'heure
Délai d'expiration du mot de passe	Établit, après quoi le mot de passe expire et un nouveau mot de passe doit être délivré.
Restriction de l'historique des mots de passe	Nombre de mots de passe précédemment utilisés qui ne sont pas autorisés
Nombre maximal d'échecs de tentatives de saisie du mot de passe	Détermine le nombre de fois qu'un mot de passe peut être saisi de manière incorrecte avant qu'un effacement complet de l'appareil ne soit effectué.
Autoriser l'authentification biométrique	Permet l'authentification par empreinte digitale ou par balayage de l'iris. Uniquement pour Samsung KNOX 2.1 et plus.

Code d’accès au conteneur

Sous "Passcode", vous pouvez mandater un mot de passe de conteneur, les options de réglage suivantes sont disponibles sur

.

Longueur minimale du mot de passe	Fixe le nombre minimum de symboles que doit comporter un mot de passe	
Qualité du mot de passe	Non spécifié	Cette politique ne prévoit aucune exigence concernant le mot de passe.
	Biométrique Faible	Cette politique autorise les technologies de reconnaissance biométrique à faible niveau de sécurité. Il s'agit de technologies capables de reconnaître l'identité d'une personne à l'aide d'un code PIN à trois chiffres environ (le taux de fausse détection est inférieur à 1 sur 1 000).
	Quelque chose	Cette politique exige la définition d'un mot de passe ou d'un modèle, mais n'impose pas de règles spécifiques.
	Alphabétique	L'utilisateur doit avoir introduit un mot de passe contenant au moins des caractères alphabétiques (ou d'autres symboles).
	Alphanumérique	L'utilisateur doit avoir saisi un mot de passe contenant au moins des caractères numériques et alphabétiques (ou d'autres symboles).
	Complexe	L'utilisateur doit avoir saisi un mot de passe contenant au moins une lettre, un chiffre et un symbole spécial, par défaut. Avec cette qualité de mot de passe, les mots de passe peuvent être restreints pour contenir différents ensembles de caractères, comme au moins une lettre majuscule, etc.
Longueur minimale du mot de passe	Définissez le nombre de caractères requis pour le mot de passe. Par exemple, vous pouvez exiger que les codes PIN ou les mots de passe comportent au moins six caractères.	
Nombre minimum de chiffres requis pour le mot de passe	Nombre minimum de chiffres requis pour le mot de passe	

Minimum de lettres minuscules requis dans le mot de passe	Minimum de lettres minuscules requis dans le mot de passe
Minimum de lettres majuscules requis dans le mot de passe	Minimum de lettres majuscules requis dans le mot de passe
Nombre minimum de caractères non alphabétiques requis dans le mot de passe	Nombre minimum de caractères non alphabétiques requis dans le mot de passe
Symboles minimums requis dans le mot de passe	Symboles minimums requis dans le mot de passe

Verrouillage du temps d'inactivité maximum	Inactivité maximale de l'utilisateur jusqu'au verrouillage de l'heure
Délai d'expiration du mot de passe	Établit, après quoi le mot de passe expire et un nouveau mot de passe doit être délivré.
Restriction de l'historique des mots de passe	Nombre de mots de passe précédemment utilisés qui ne sont pas autorisés
Nombre maximal d'échecs de tentatives de saisie du mot de passe	Détermine le nombre de fois qu'un mot de passe peut être saisi de manière incorrecte avant qu'un effacement complet de l'appareil ne soit effectué.

AntiVirus

Scan automatique	Activer les balayages automatiques périodiques
Intervalle de balayage	Intervalle d'examen (rapide / complet)
Scan automatique complet	Activer les analyses automatiques complètes
Mises à jour automatiques	Activer les mises à jour automatiques
Intervalle de vérification de la mise à jour	A quelle fréquence l'application et sa base de données doivent-elles être mises à jour (virus / code endommagé) ?
Protection des applications	Activer l'analyse automatique des applications
Protection de la carte SD	Activer l'analyse automatique de la carte SD
Mise à jour Wi-Fi uniquement	Lorsque cette option est activée, les mises à jour ne sont appliquées que lorsque l'appareil est connecté avec succès à un réseau Wi-Fi.

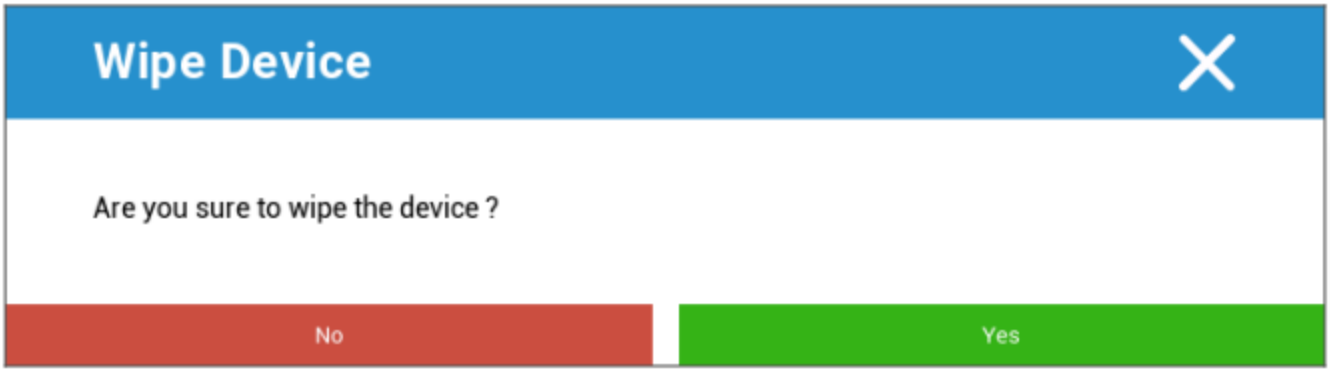
Fin de vie (uniquement au niveau de l’appareil)

Effacer (uniquement au niveau de l’appareil)

Sous "Effacer", vous pouvez rétablir les paramètres d'usine de l'appareil (uniquement pour le profil de travail amélioré).

Dans ce cas, les données de l'entreprise et les données privées sont supprimées sur l'appareil de l'utilisateur final.

En cliquant sur le "symbole moins", vous obtenez le message suivant :



Si vous répondez "Oui", vous pouvez procéder à l'effacement.

Sous "Rapport d'effacement", les éléments suivants peuvent être affichés

Effacé par	Historique de la personne qui a effectué l'essuyage
Date	Date
Statut	État (par exemple, si le nettoyage a été effectué avec succès)

Paramètres de restriction

Restrictions

Ici, il est possible de restreindre et de bloquer toute une série de choses.

Contrôle de la conformité	Mode Inviter l'utilisateur - L'utilisateur sera invité à effectuer les actions nécessaires. Mode Lock-Down Container - Masquer toutes les applications jusqu'à ce que toutes les conditions soient remplies
Politique d'autorisation d'exécution	Inviter l'utilisateur à demander de nouvelles autorisations Accordez toujours les nouvelles demandes d'autorisation Refusez toujours les nouvelles demandes d'autorisation Attention : Certaines applications ont des difficultés à reconnaître les autorisations si celles-ci sont définies automatiquement. Si vous accordez toujours les autorisations et que vous rencontrez des problèmes avec des applications qui disent que les autorisations sont manquantes, réglez ce paramètre sur "demander à l'utilisateur" et réinstallez l'application.
Autoriser le presse-papiers sortant	Permet de faire des copier-coller de l'intérieur du conteneur vers l'extérieur.
Autoriser la résolution de l'identification de l'appelant	Affiche le nom d'un appel entrant en fonction des contacts présents dans le conteneur.
Autoriser la résolution de la recherche de contacts	Permet de rechercher des noms dans les contacts du conteneur lors des appels.
Autoriser le partage des contacts par Bluetooth	Permet d'accéder au contact des conteneurs dans une voiture
Interdire les faisceaux NFC sortants	Désactive le NFC pour le conteneur
Autoriser les sources inconnues	Si cette option est activée, les utilisateurs peuvent charger des applications de manière latérale en installant un fichier .apk.

Autoriser le débogage USB	Si cette option est activée, les utilisateurs peuvent activer le débogage USB.
Interdire la modification du compte	Interdit la création, la suppression et la modification des comptes dans le conteneur. N'oubliez pas que certaines applications ont besoin de créer ou de modifier des comptes pour fonctionner correctement.

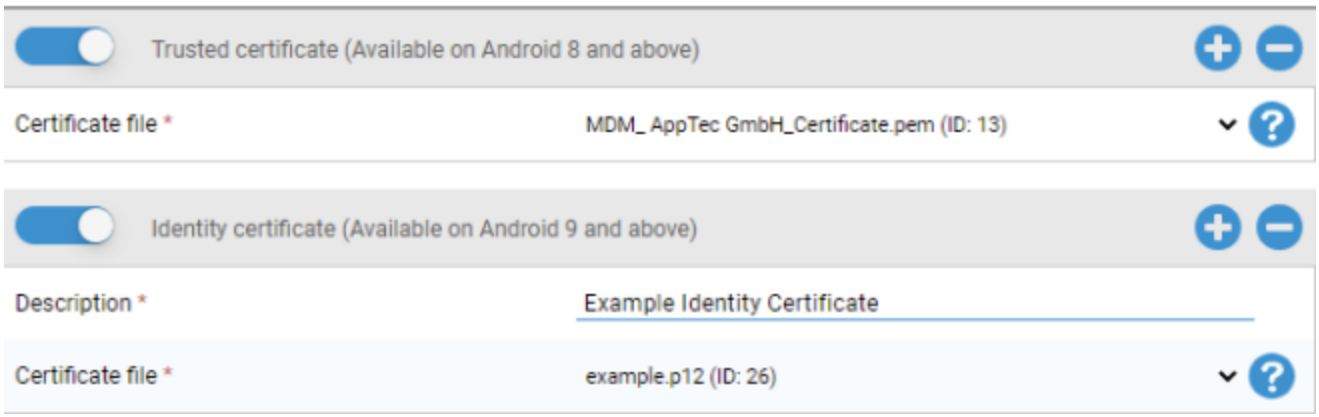
Restrictions du profil de travail. Disponible uniquement sur les appareils Android 11 et plus, avec le profil de travail amélioré.	
Désactiver l'appareil photo	Indique si la caméra est interdite dans le profil de travail.
Désactiver le Bluetooth	Indique si le Bluetooth est interdit dans le profil de travail.
Activer la protection contre la réinitialisation d'usine	Activez cette option pour remplacer la protection contre la réinitialisation d'usine d'Android par le compte Google que vous avez défini dans "Paramètres généraux" → "Configuration Android" → "Android Enterprise" → "Protection contre la réinitialisation d'usine" Si cette option est activée et que vous réinitialisez l'appareil, vous devrez fournir le compte Google configuré pour configurer à nouveau l'appareil.
Contrôlez la mise à jour du système d'exploitation	Activez cette option pour définir le comportement de la mise à jour : automatique, fenêtré ou différé.
Politique de mise à jour	Automatique : Installation automatique dès qu'une mise à jour est disponible. Fenêtre : Installation automatique dans une fenêtre de maintenance quotidienne. Cette option configure également les applications Play pour qu'elles soient mises à jour dans la fenêtre. Cette option est fortement recommandée pour les appareils kiosques, car c'est la seule façon pour Play de mettre à jour les applications épinglées en permanence au premier plan. Reporter : Reporte l'installation automatique jusqu'à un maximum de 30 jours.

Restrictions du profil personnel. Disponible uniquement sur les appareils Android 11 et plus, avec le profil de travail amélioré.	
Désactiver l'appareil photo	Indique si la caméra est interdite dans le profil personnel.
Désactiver le Bluetooth	Indique si le Bluetooth est interdit dans le profil personnel.

Autoriser les sources inconnues	Si cette option est activée, les utilisateurs de profils professionnels peuvent charger des applications de manière latérale en installant un fichier .apk.

Gestion des certificats

Vous pouvez y distribuer des certificats de confiance et des certificats d'identité à vos appareils. Android 8 ou une version plus récente est nécessaire pour distribuer des certificats de confiance et Android 9 ou une version plus récente est nécessaire pour distribuer des certificats d'identité.



Avec le "+", vous pouvez ajouter plusieurs certificats.

Les certificats de confiance doivent être au format PEM.

Les certificats d'identité doivent être au format PKCS12.

Gestion des connexions

Wifi

Pour ce paramètre, effectuez la préconfiguration des dispositifs de l'utilisateur final, pour l'accès aux points d'accès internes

.

Identificateur d'ensemble de services (SSID)	SSID du réseau à connecter
Réseau caché	Activer, dans le cas où le point d'accès ne diffuse pas le SSID.

Type de sécurité

Établir le type de sécurité de l'AP

WEP

Mot de passe	Mot de passe pour l'AP

WPA/WPA2

Mot de passe	Mot de passe pour l'AP

802.1x EAP

Méthode EAP

PWD	Identité	Identité
	Mot de passe	Mot de passe

PEAP	Protocole d'authentification de phase 2	aucun	Pas de protocole supplémentaire
		MSCHAPV2	Protocole MSCHAPV2
		CTG	Protocole GTC
	Certificat CA	Certificat CA	
	Identité	Identité	
	Identité anonyme	Identité anonyme	
	Mot de passe	Mot de passe	

TTLS	Protocole d'authentification de phase 2	aucun	Pas de protocole supplémentaire
		PAP	Protocole PAP
		MSCHAP	Protocole MSCHAP
		MSCHAPV2	Protocole MSCHAPV2
		CTG	Protocole GTC
	Certificat CA	Certificat CA	
	Identité	Identité	
	Identité anonyme	Identité anonyme	
	Mot de passe	Mot de passe	

TLS	Certificat CA	Certificat CA
	Identité	Identité
	Mot de passe	Mot de passe

VPN

Nom de la connexion	Nom de la connexion VPN

Type de VPN

VPN

Client VPN

AppTec VPN Client	
Configuration de la passerelle	Sélectionnez la configuration VPN de la passerelle (voir **Paramètres généraux > Passerelle universelle > Paramètres VPN**).
VPN toujours actif	Activer le verrouillage natif
Activer le verrouillage AppTec	Activer le verrouillage AppTec

Intégré (disponible uniquement sur les appareils Samsung)			
Type de connexion	PPTP	Serveur	Serveur
		Activer le cryptage PPTP	Activer le cryptage PPTP
	L2TP / IPSec PSK	Serveur	Serveur
		Clé pré-partagée IPSec	Clé pré-partagée IPSec
		Activer le secret L2TP	Activer le secret L2TP
		L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Serveur	Serveur
		Identifiant IPSec	Identifiant IPSec
		Clé pré-partagée IPSec	Clé pré-partagée IPSec
Domaines de recherche DNS	Domaines de recherche DNS		
Paramètres experts	Serveurs DNS	Serveurs DNS	
	Routes de transfert	Routes de transfert	

VPN ouvert		
Serveur	Serveur	
Profil OpenVPN	Profil OpenVPN	
Application OpenVPN	OpenVPN pour Android (recommandé)	
	Connexion OpenVPN	
Paramètres experts	Serveurs DNS	Serveurs DNS
	Routes de transfert	Routes de transfert

Samsung / Strong Swan			
Type de connexion	PPTP	Serveur	Serveur
		Nom d'utilisateur	Nom d'utilisateur
		Mot de passe	Mot de passe
		Activer le cryptage PPTP	Activer le cryptage PPTP
	L2TP / IPSec PSK	Serveur	Serveur
		Clé pré-partagée IPSec	Clé pré-partagée IPSec
		Nom d'utilisateur	Nom d'utilisateur
		Mot de passe	Mot de passe
		Activer le secret L2TP	L2TP Secret
	IPSec XAuth PSK	Serveur	Serveur
		Identifiant IPSec	Identifiant IPSec
		Clé pré-partagée IPSec	Clé pré-partagée IPSec
		Nom d'utilisateur	Nom d'utilisateur
		Mot de passe	Mot de passe
Paramètres experts	Serveurs DNS	Serveurs DNS	
	Routes de transfert	Routes de transfert	

Cisco Any Connect		
Serveur	Serveur	
Mode certificat	Handicapés	Handicapés
	Automatique	Automatique
Paramètres experts	Serveurs DNS	Serveurs DNS
	Routes de transfert	Routes de transfert

VPN par application

Client VPN

AppTec VPN Client		
Configuration de la passerelle	Sélectionnez la configuration VPN de la passerelle (voir **Paramètres généraux > Passerelle universelle > Paramètres VPN**).	
Applications VPN	Applications VPN	
VPN toujours actif	Activer le verrouillage natif	VPN toujours actif
Activer le verrouillage AppTec	Activer le verrouillage AppTec	

Samsung / Strong Swan			
Type de connexion	PPTP	Serveur	Serveur
		Applications VPN	Applications VPN
		Nom d'utilisateur	Nom d'utilisateur
		Mot de passe	Mot de passe
		Activer le cryptage PPTP	Activer le cryptage PPTP
	L2TP / IPSec PSK	Serveur	Serveur
		Applications VPN	Applications VPN
		Clé pré-partagée IPSec	Clé pré-partagée IPSec
		Nom d'utilisateur	Nom d'utilisateur
		Mot de passe	Mot de passe
		Activer le secret L2TP	L2TP Secret
	IPSec XAuth PSK	Serveur	Serveur
		Applications VPN	Applications VPN
		Identifiant IPSec	Identifiant IPSec
		Clé pré-partagée IPSec	Clé pré-partagée IPSec
		Nom d'utilisateur	Nom d'utilisateur
		Mot de passe	Mot de passe
Paramètres experts	Serveurs DNS	Serveurs DNS	
	Routes de transfert	Routes de transfert	

Restrictions

Vous pouvez ici définir les restrictions relatives à la gestion des connexions.

Autoriser l'itinérance des données	Autoriser les données mobiles en itinérance
Forcer l'itinérance des données	Si elle est activée, l'itinérance pour les données mobiles est activée en permanence (non recommandé !). Ce paramètre écrase le paramètre "Allow Data Roaming" (autoriser l'itinérance des données) !
Utiliser le serveur proxy http du système	L'utilisation d'un serveur proxy HTTP, qui est fourni par les paramètres du système dans les réglages, dépend du réseau connecté (WiFi ou APN).

Gestion du PIM

Gmail Exchange

Info : Cette configuration sera appliquée à l'application Gmail. Vous devez donc approuver et installer Gmail.

Adresse électronique	L'adresse électronique de l'utilisateur fourni Veuillez noter les "Placeholders", que vous pouvez utiliser pour travailler avec les informations d'identification et que vous ne devez pas modifier manuellement sur chaque appareil. En un clic, vous pouvez les visualiser par vous-même.
Nom d'hôte du serveur	Adresse de votre serveur Exchange
Nom de connexion	Le nom de connexion pour l'appareil de l'utilisateur final respectif, veuillez également noter les "Placeholders here".
Signature	Une signature peut être jointe (Remarque : certains appareils exigent un formatage HTML pour la signature).
Nombre de jours précédents à synchroniser	Nombre de jours déterminant le moment où les courriels sont synchronisés à nouveau
Identifiant de l'appareil	Chaîne contenant le DeviceID de l'EAS. Cette chaîne fait partie du protocole EAS et peut être utilisée dans certains environnements.
Utilisez le protocole SSL (Secure Sockets Layer)	Utiliser une connexion SSL
Accepter tous les certificats	Tous les certificats sont acceptés. Veuillez sélectionner cette option si votre serveur Exchange utilise un certificat auto-signé.
Autoriser les comptes non gérés	Autoriser les utilisateurs à ajouter ou supprimer tout compte Exchange, autre que le compte spécifié dans cette configuration gérée. Si ce paramètre est activé, vous ne pouvez pas empêcher les utilisateurs d'ajouter d'autres comptes Exchange à Gmail. Vous ne pouvez pas non plus contrôler le partage des données entre d'autres applications et les comptes Exchange ajoutés par les utilisateurs. Ce paramètre ne doit être activé que si vos utilisateurs doivent gérer plus d'un compte Exchange professionnel dans Gmail.

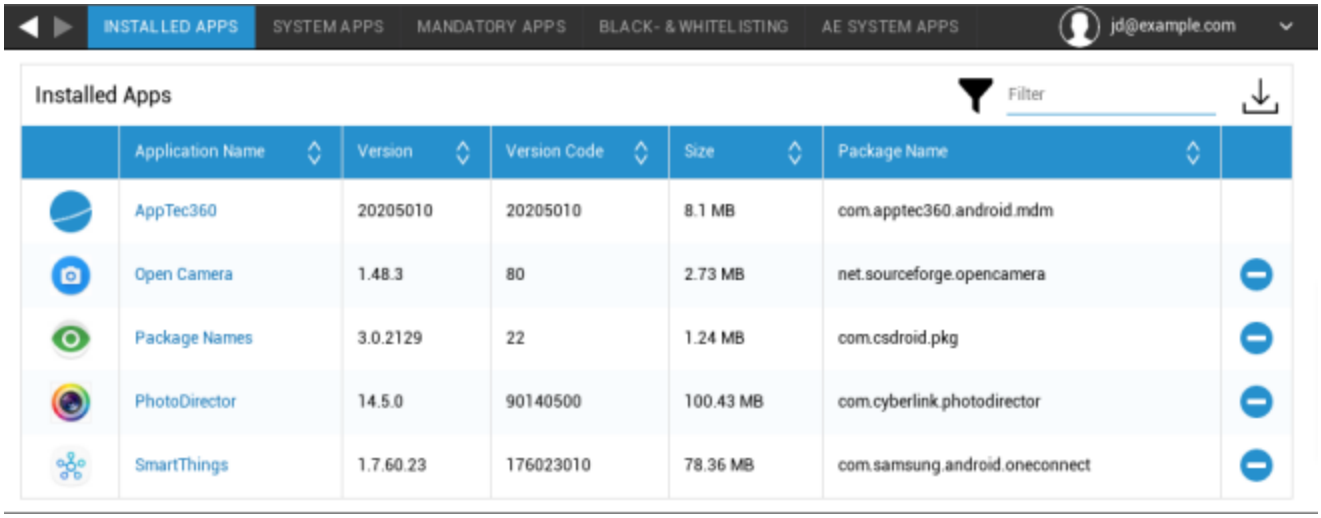
Certificat de client	Certificat du client. Nécessaire uniquement si votre serveur de messagerie s'attend à ce qu'il soit présent.

Gestion des applications

Gestionnaire d’applications d’entreprise

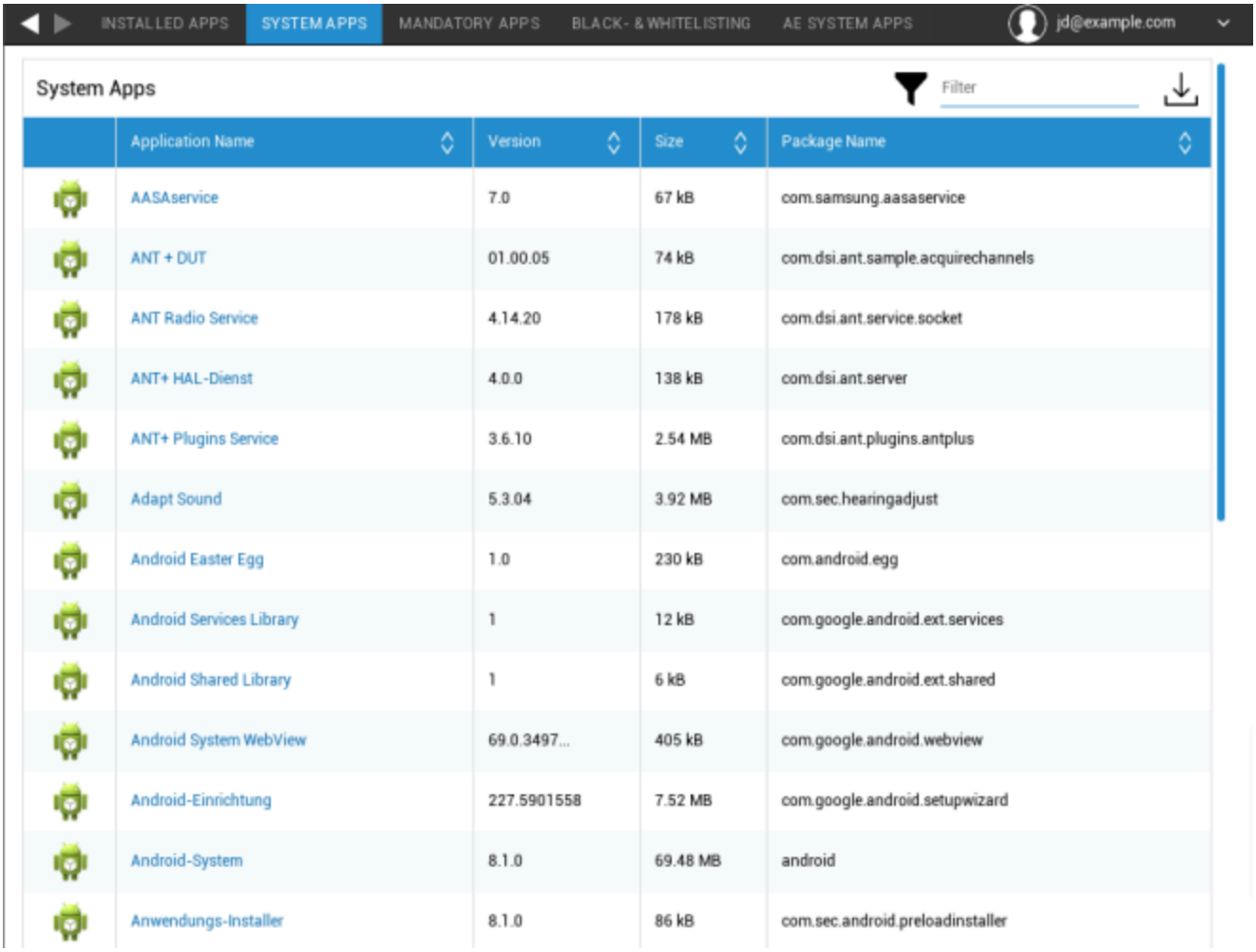
Applications installées (uniquement au niveau de l’appareil)

Toutes les applications actuellement installées dans le conteneur s'affichent ici.



Apps système (uniquement au niveau de l’appareil)

Sous "Apps système", toutes les apps et tous les services qui ont déjà été installés sur l'appareil de l'utilisateur final par le fabricant de l'appareil sont répertoriés pour vous.

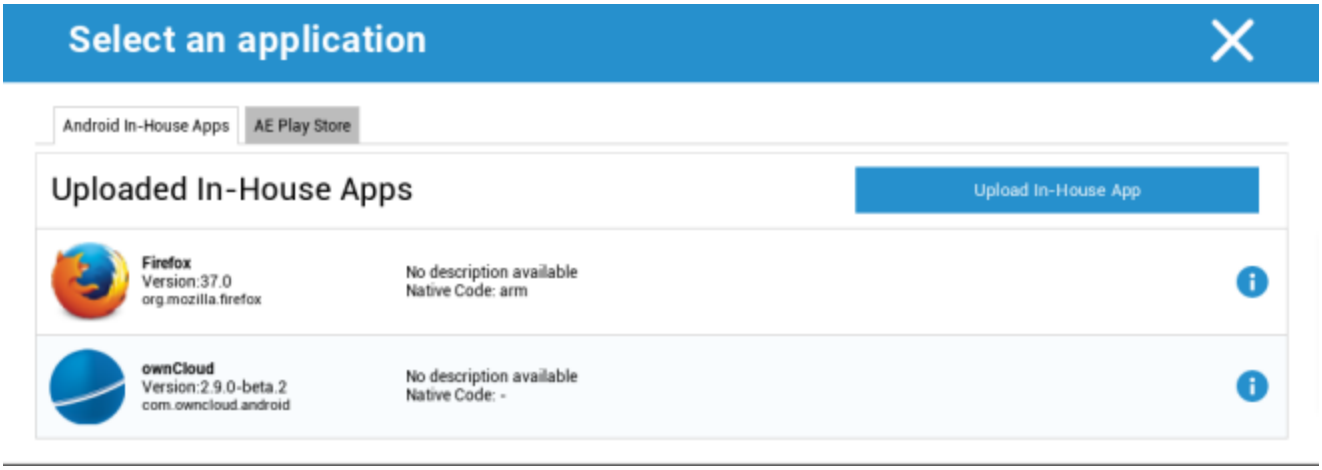


Applications obligatoires

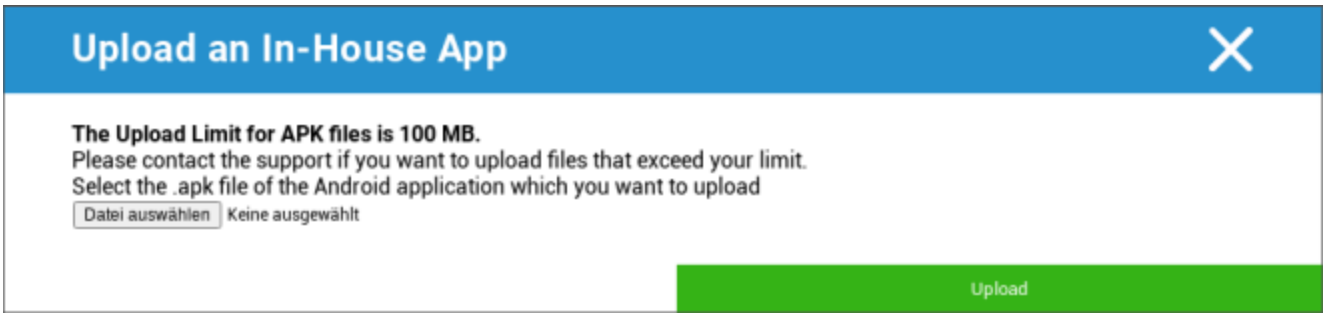
Sous la rubrique Applications obligatoires, vous pouvez définir les applications obligatoires requises. L'utilisateur sera continuellement invité à installer l'application désignée, s'il s'agit d'une application InHouse. Les applications du Play Store seront installées automatiquement.

L'application obligatoire peut être définie à l'aide de l'application obligatoire.

Il peut s'agir d'une application interne figurant dans la liste des "applications internes Android" que vous avez téléchargée dans les paramètres généraux.

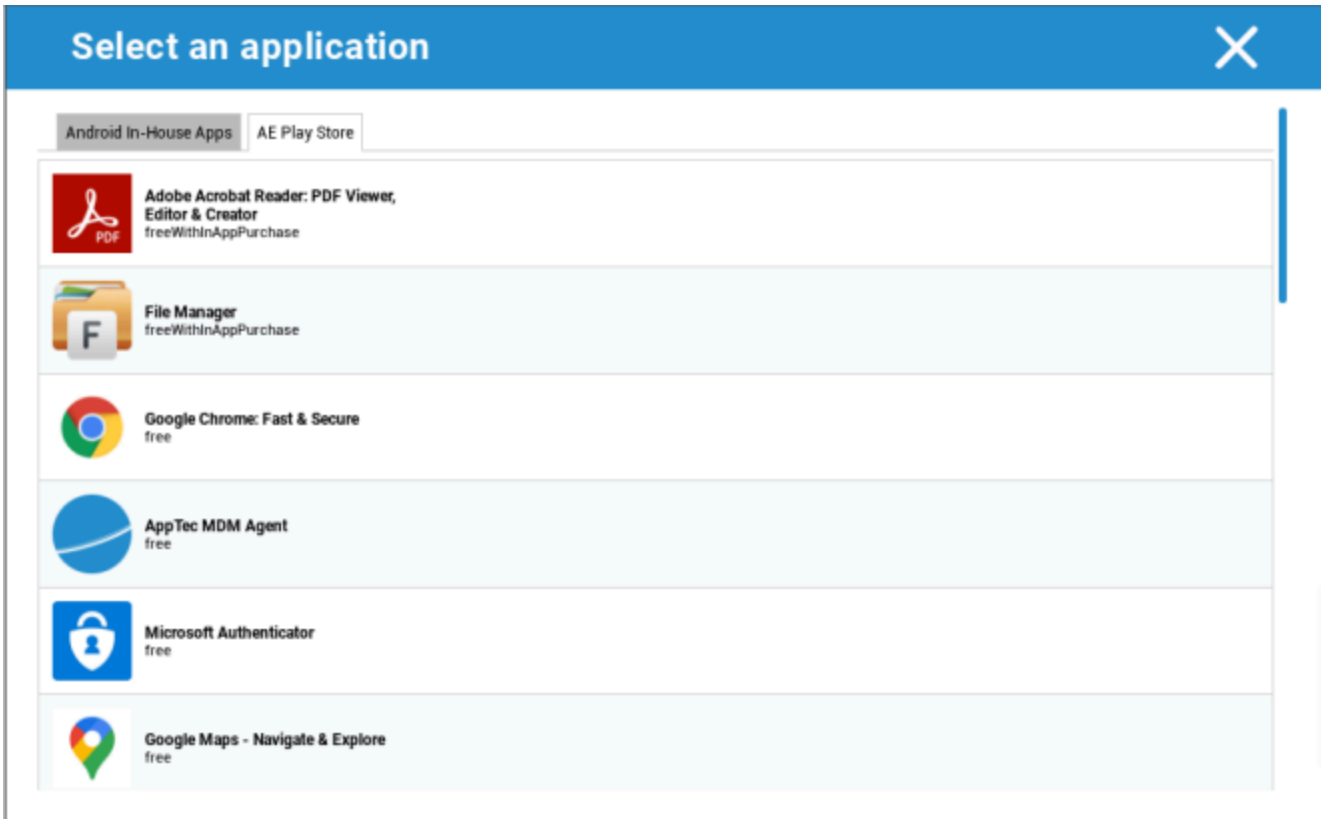


Vous pouvez également sélectionner et télécharger directement un fichier apk avec "Upload In-House App".



Si vous installez une application interne, vous aurez la possibilité d'activer l'option "Tenir à jour". Si cette option est activée et que vous avez défini une version plus récente dans la base de données des applications internes, l'application sera mise à jour sur l'appareil.

Il peut également s'agir d'une application "AE Play Store" du Google Work Play Store.



Seules les "applications AE Play Store" approuvées seront affichées dans cet onglet.

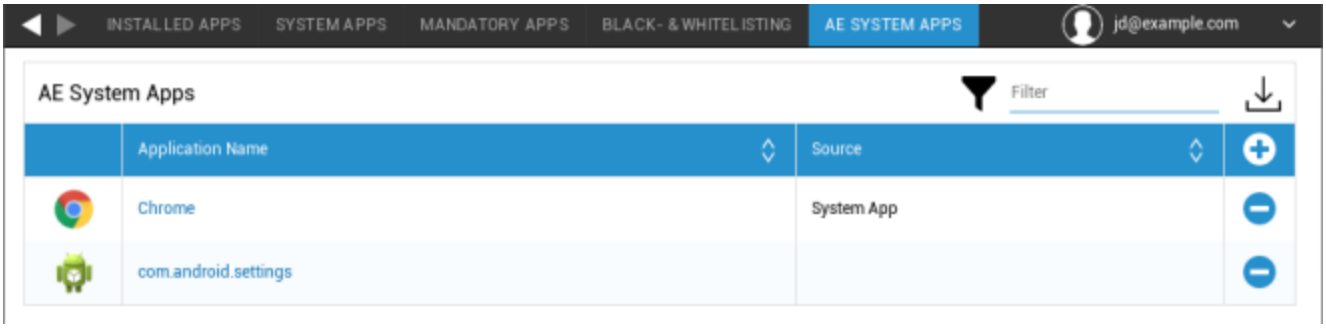
Pour approuver une "AE Play Store App", veuillez vous rendre dans "General Settings" > "App Management" > "AE Play

Store" et ajoutez une application en cliquant sur le bouton qui vous redirigera vers l'onglet "Play Store Apps" (ou vous pouvez aller directement à l'onglet "Play Store Apps").

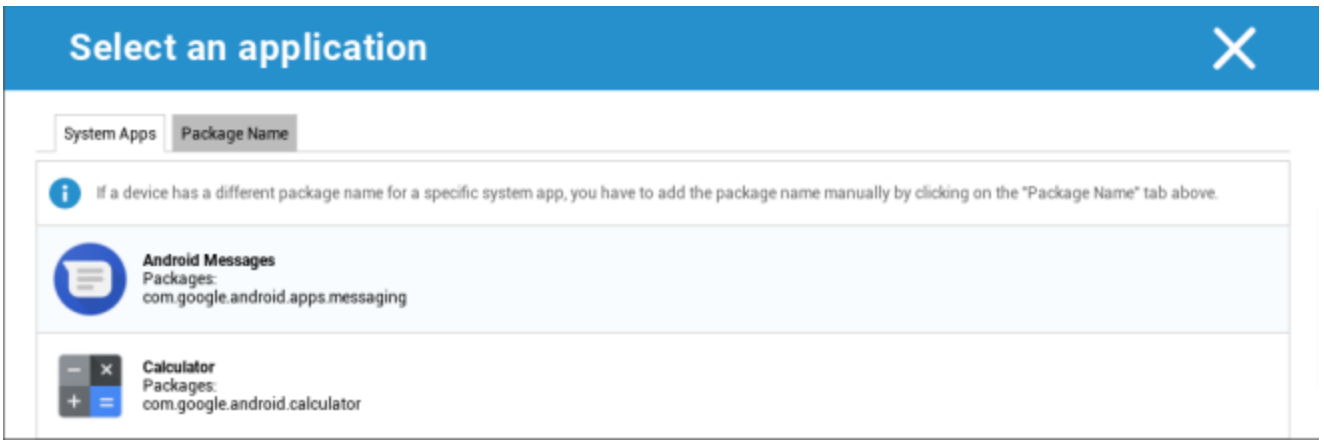
Dans l'onglet "Play Store Apps", vous pouvez rechercher des applications. Lorsque vous cliquez sur une application, la page de l'application s'ouvre et vous pouvez approuver l'application en cliquant sur "Approuver".

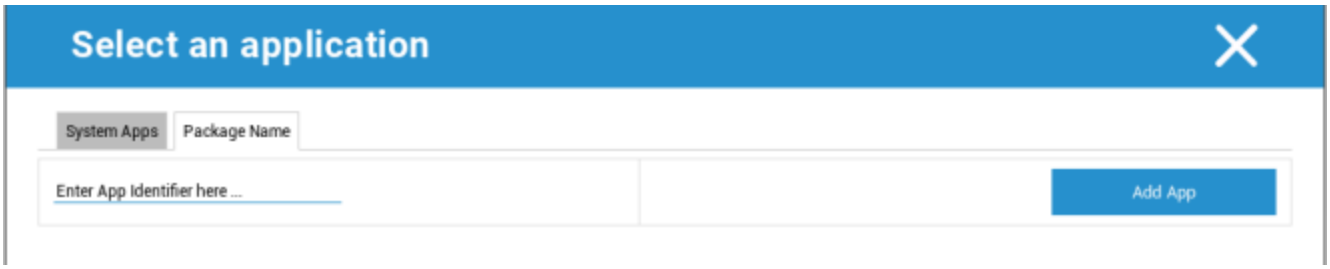
Applications du système AE

Vous pouvez définir ici une liste contenant des applications système spécifiques qui doivent être activées sur les appareils.



Si vous cliquez sur le bouton, vous pouvez choisir dans une liste d'applications système possibles fournie par Google ou saisir directement le nom du paquet d'une application système qui doit être activée.





N'oubliez pas que les applications système figurant dans la liste fournie par Google sont uniquement des applications qui peuvent être des applications système, mais qu'elles ne doivent pas nécessairement être des applications système sur vos appareils.

Toutefois, cette liste ne concerne que les applications déjà préinstallées.

L'ajout d'applications qui ne sont pas préinstallées sur vos appareils ne les affectera pas, que l'application figure dans la liste fournie par Google ou que le nom du paquet de l'application soit saisi directement.

Restrictions et paramètres

Paramètres de gestion des applications

Vous pouvez ici configurer le comportement de l'appareil en ce qui concerne les mises à jour d'applications.

Fréquence des contrôles de mise à jour	Spécifiez l'intervalle dans lequel le client AppTec recherchera les mises à jour de l'application. La valeur par défaut est de 24 heures.
Seuil Wi-Fi	Les applications dont la taille est supérieure à celle spécifiée seront téléchargées par Wi-Fi. Si vous sélectionnez "Wi-Fi uniquement", toutes les applications seront téléchargées par Wi-Fi.

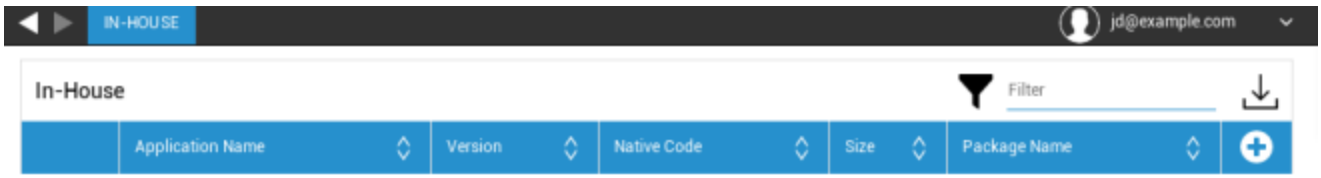
App Store d’entreprise

En interne

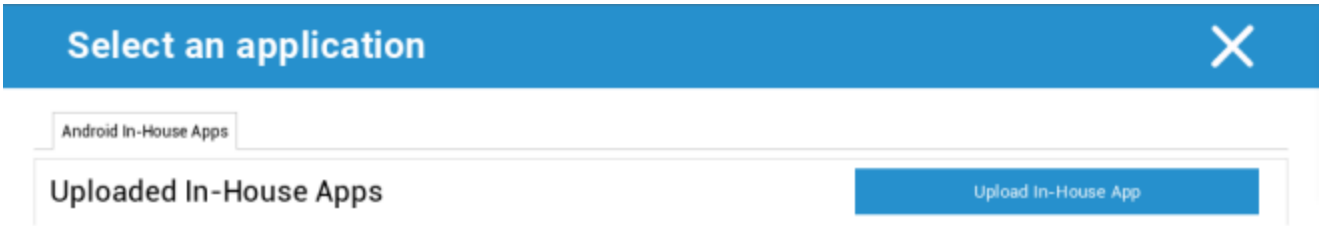
Sous le point "In-House", vous pouvez télécharger et distribuer des applications développées en interne.

Avec le symbole, vous pouvez distribuer des applications internes supplémentaires.

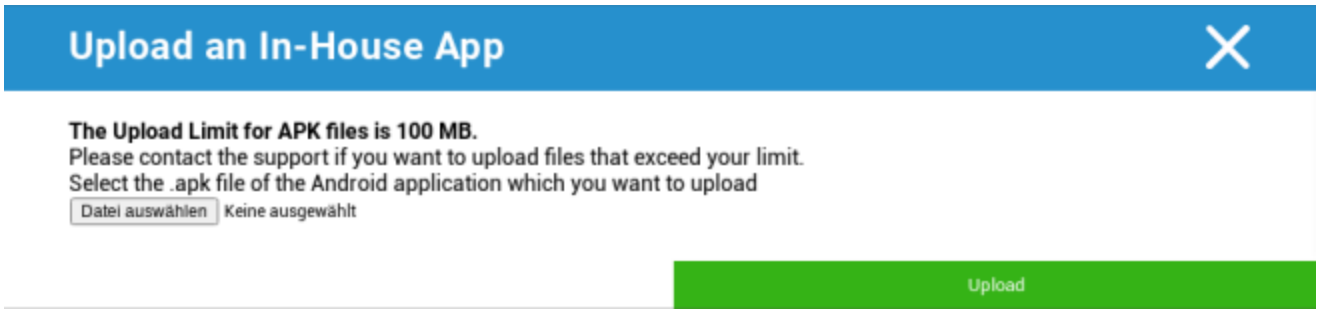
Si vous installez une application interne, vous aurez la possibilité d'activer l'option "Tenir à jour". Si cette option est activée et que vous avez défini une version plus récente dans la base de données des applications internes, l'application sera mise à jour sur l'appareil.



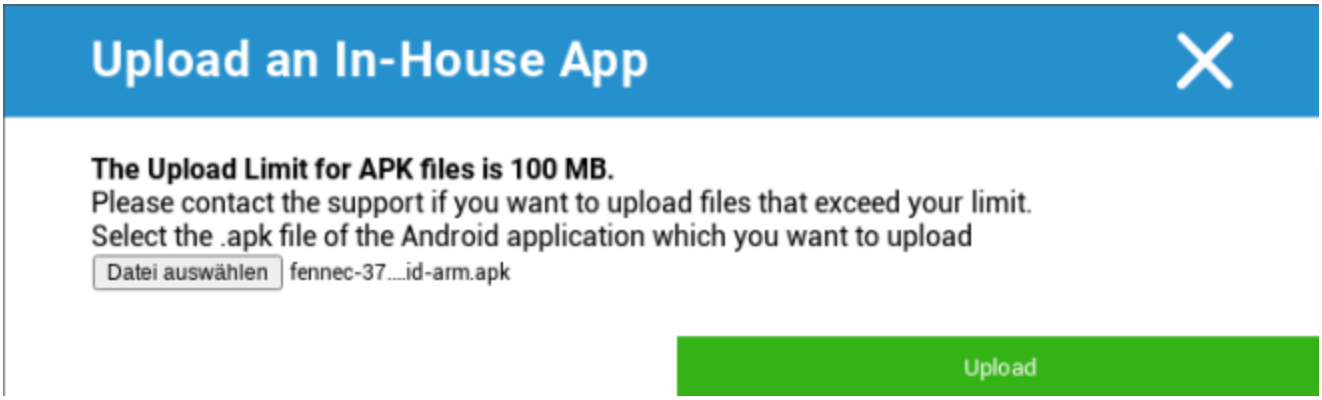
Si vous n'avez pas distribué d'applications internes, vous recevrez alors l'aperçu suivant :



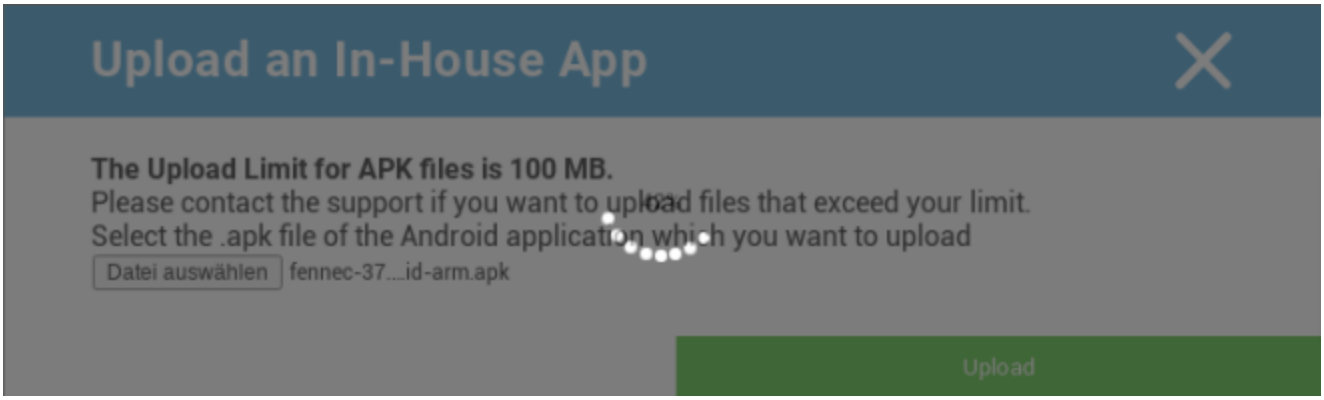
Pour ce faire, cliquez sur "Upload In-House App", vous obtiendrez alors l'aperçu suivant :



Maintenant, choisissez avec "Search..." un fichier .apk et cliquez sur "Upload".



Votre application va maintenant être téléchargée. Au milieu du cercle, vous verrez un indicateur de pourcentage, montrant la part de votre application qui a déjà été téléchargée.



Si le téléchargement de votre application interne a réussi, vous pouvez alors trouver l'application téléchargée dans votre catalogue d'applications.

L'utilisateur a maintenant la possibilité de voir et d'installer cette application dans l'AppTec Store sur l'appareil de l'utilisateur final, dans la catégorie "In-House".

Comme il ne s'agit pas d'une application Google PlayStore, l'utilisateur n'a pas besoin d'un identifiant Google stocké sur son appareil.

Entreprise Play Store

AE Play Store

Ici, vous pouvez ajouter des applications à la boutique Android Enterprise Playstore. Veuillez noter que vous devez approuver les applications avec votre compte d'administrateur AE avant de pouvoir les ajouter.

Pour approuver une application, veuillez consulter les instructions de la section Applications obligatoires.

Gestion du contenu

ContentBox

Ici, vous pouvez activer la boîte de contenu.

Dès que vous activez l'option "Enable ContentBox", une application ContentBox distincte est automatiquement installée sur l'appareil de l'utilisateur final.

Navigateur sécurisé

Vous pouvez ici configurer les paramètres du AppTec Secure Browser.

Dès que la section "Secure Browser" est activée, une application de navigation distincte est automatiquement installée sur l'appareil de l'utilisateur final.

Demande de mot de passe	Exiger de l'utilisateur qu'il définisse et utilise un mot de passe pour accéder au navigateur.
Longueur minimale du mot de passe	Définissez le nombre de caractères requis pour le mot de passe
Qualité requise du mot de passe	Définissez la qualité du mot de passe requis
Restreindre les téléchargements / Ouvrir en	
Limiter les téléchargements	
Télécharger la liste blanche	Une liste d'URL pour lesquelles le téléchargement sera toujours autorisé.
Autoriser la copie	Permettre de copier, de couper ou de partager du texte à l'intérieur des pages web.
Autoriser la capture d'écran	Permettre la réalisation de captures d'écran.
Fréquence de nettoyage des données	Sélectionnez la fréquence à laquelle TOUTES les données de l'utilisateur (historique, cache, etc.) doivent être automatiquement supprimées.
Signets d'entreprise	Les signets apparaîtront dans le dossier "Signets de l'entreprise" des signets du navigateur. Ils ne sont pas modifiables par l'utilisateur.
Masquer la barre d'adresse	
Liste blanche dans le navigateur (sans passerelle universelle)	Active la liste blanche d'URL côté client. • Les signets d'entreprise sont toujours inscrits sur la liste blanche • Pris en charge pour 100 URL seulement • Veuillez utiliser la passerelle universelle pour un nombre illimité de listes noires et blanches.

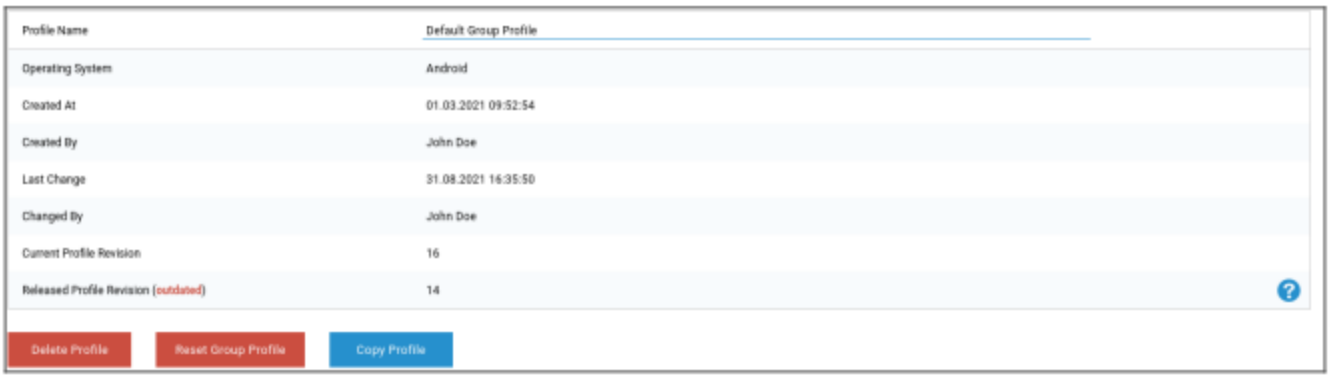
URL sur liste blanche	Une liste d'URL autorisés.
Liste noire et liste blanche basées sur la passerelle	L'inscription sur liste noire est soumise aux exigences suivantes : • Une passerelle universelle AppTec opérationnelle ("Paramètres généraux" → "Passerelle universelle") • Une configuration VPN fonctionnelle avec un serveur DNS spécifié ("Paramètres généraux" → "Passerelle universelle" → "Paramètres VPN") • Une configuration de liste noire ("General Settings" → "Universal Gateway" → "Domain Blacklist") • Une connexion VPN valide dans le profil ("Gestion des connexions" → "VPN")

Configuration Android

Général

Aperçu du profil du groupe (uniquement au niveau du groupe)

Lorsque vous ouvrez un profil de groupe, vous obtenez un aperçu rapide du profil.



Nom du profil	Nom du profil (peut être modifié ici)
Système d'exploitation	Système d'exploitation pour lequel le profil est établi
Créé à	Moment de la création
Créé par	Le créateur du profil
Dernier changement	Date de la dernière modification du profil
Modifié par	Compte ayant effectué les dernières modifications
Révision du profil actuel	Révision de l'état du profil sauvegardé
Révision du profil validé	Révision du profil attribué ("Attribuer maintenant"). Si l'étiquette affiche "(obsolète)" derrière le texte, cela signifie que vous avez enregistré le profil mais que vous ne l'avez pas encore attribué.

Aperçu de l’appareil (uniquement au niveau de l’appareil)

Si vous vous trouvez sur un appareil, vous recevrez un récapitulatif de l'appareil sélectionné, qui contient les informations suivantes :

Nom de l'appareil	Nom de l'appareil
Dernier lieu connu	Dernières coordonnées GPS connues
Numéro de téléphone	Numéro de téléphone
Apps obligatoires assignées	Le nombre d'applications obligatoires attribuées
Version OS	Version du système d'exploitation de l'appareil
Système d'exploitation	Système d'exploitation (Android / iOS / Windows Phone)
Numéro de série	Numéro de série de l'appareil
Propriété des appareils	Dispositif d'entreprise ou privé
Type d'appareil	Téléphone ou tablette
Enraciné	Statut, indiquant si l'appareil a été enraciné
Conforme à la loi	Conforme aux lignes directrices
Adresse IP	Adresse IP
Dernière visite	Moment où le dispositif s'est connecté pour la dernière fois à AppTec
Dernière poussée	Moment où le serveur a envoyé un message à l'appareil.
Affectation des utilisateurs	Une liste déroulante permettant d'attribuer l'appareil à un autre utilisateur

Révision de la configuration (uniquement au niveau de l’appareil)

Vous obtiendrez ici une vue d'ensemble du profil de groupe attribué à l'appareil.

Si vous cliquez sur le profil du groupe, vous accédez directement au profil et vous pouvez effectuer des réglages.

Le symbole vous permet de rétablir les paramètres du profil de groupe pour les applications attribuées.

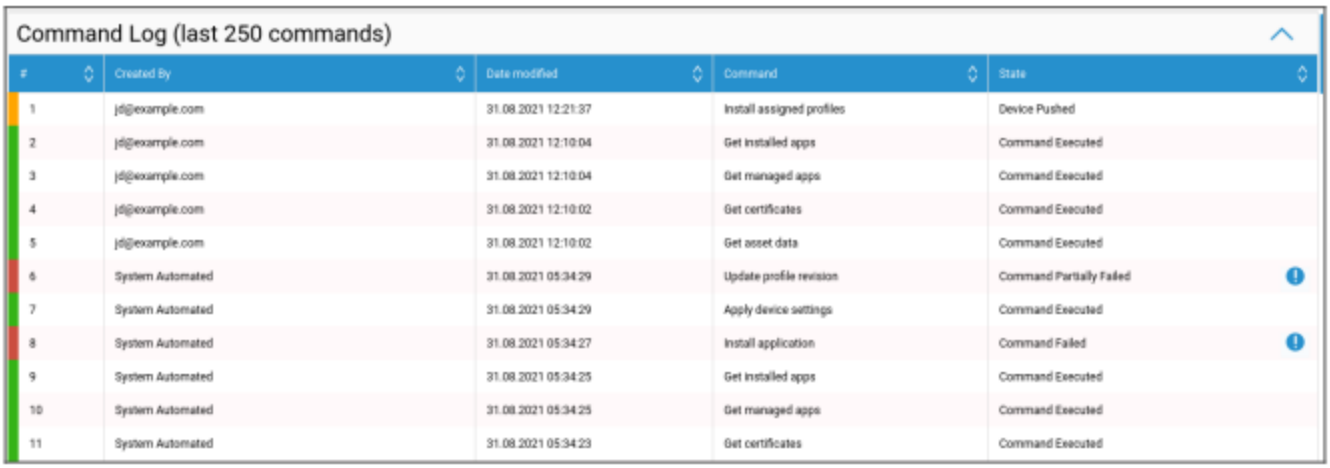
Le symbole permet de réinitialiser le profil de l'appareil pour qu'il ne comporte aucun paramètre.

La mention "Révision plus récente disponible" indique que le profil de groupe a été modifié et enregistré, mais qu'il n'a pas été attribué. Le profil de groupe doit être attribué avec "Attribuer maintenant" au niveau du groupe pour appliquer les changements aux appareils.

Journal de l’appareil (uniquement au niveau de l’appareil)

Journal des commandes

Vous pouvez voir ici quelles commandes ont été émises pour l'appareil et quel est leur état.



Les commandes créées par le "système automatisé" sont automatiquement créées par le système.

États possibles de la commande

Dispositif poussé	Une requête "push" a été envoyée au service "push" (par exemple APNS) pour demander à l'appareil de se reconnecter au serveur EMM.
Commande créée	La commande a été créée dans le système.
Commande envoyée	La commande a été envoyée à l'appareil après qu'il se soit connecté au serveur.
Commande exécutée	La commande a été exécutée avec succès.
Échec de la commande	La commande a échoué. *
Échec partiel de la commande	Selon le système d'exploitation de l'appareil, certaines commandes peuvent être regroupées. Dans ce cas, certaines parties de ce groupe de commande ont échoué. *
Commande exécutée, échec éventuel	La commande a été exécutée, mais peut-être qu'elle ne l'a pas été.
Commandement repoussé	La commande a été repoussée par un utilisateur.
Mise au rebut	La commande a été supprimée. Par exemple, parce qu'elle a été remplacée par une autre commande ou parce que l'appareil a été réenrôlé et que les anciennes commandes ont été supprimées.

*Si le message est accompagné d'un point d'exclamation, vous pouvez obtenir plus d'informations en survolant l'icône avec votre curseur.

Paramètres de l’appareil

Configuration du client

Ici, vous pouvez effectuer les configurations suivantes sur votre appareil Android :

Message d'avertissement après la désactivation de la gestion des périphériques	Message d'avertissement établi après la désactivation de la gestion des appareils
Temps de non-conformité	Délai à l'issue duquel la "mesure d'exécution après mise en conformité" sera exécutée si le dispositif n'est pas conforme. Min. 1 minute Max. 24 heures
Mesures d'exécution après l'expiration du délai de mise en conformité	L'action à entreprendre dès qu'un dispositif devient non conforme. • ne rien faire = pas d'action • Dispositif de verrouillage = dispositif de verrouillage • Effacer l'appareil = l'appareil sera restauré aux paramètres d'usine
Fréquence de la collecte des données	Fréquence à laquelle les informations relatives à l'appareil/au GPS doivent être collectées
Fréquence de battement de cœur du dispositif	Intervalle dans lequel le dispositif doit contacter le serveur AppTec360 Min. 1 minute Max. 24 heures
Activer les mises à jour de localisation	Si cette option est activée, l'appareil envoie des mises à jour de l'emplacement au serveur AppTec360.
Lieu Heure de mise à jour	Détermine dans quels intervalles de temps l'appareil envoie des mises à jour de localisation à AppTec
Utilisez la précision de localisation de Google pour la mise à jour de l'emplacement	Si cette option est activée, la précision de localisation de Google (anciennement connue sous le nom de localisation réseau) sera utilisée pour les mises à jour de localisation (si cette option a été désactivée sous "Restrictions", ce paramètre n'aura aucune incidence).
Utiliser la localisation GPS pour la mise à jour de l'emplacement	Si cette option est activée, le GPS sera utilisé pour les mises à jour de la position.

Autoriser les faux emplacements	Permet de falsifier les informations de localisation via des applications tierces
Action en cas de perte de connexion	Vous permet de définir une action qui sera exécutée après un certain nombre d'échecs de battements de cœur.
Mode d'application de la politique	Définit l'agressivité avec laquelle le client AppTec360 demande à l'utilisateur d'effectuer certaines actions qui requièrent une saisie de sa part. Intervalle (par défaut) = demande par intervalles, de sorte que l'utilisateur puisse laisser le programme en arrière-plan pendant un certain temps. Pas d'alerte = pas de popup pour une interaction requise. Vous devez ouvrir le Client AppTec360 manuellement pour vérifier s'il y a une action requise. Alerte constante = L'utilisateur ne peut effectuer que l'action requise. Le client AppTec360 s'imposera au premier plan si l'utilisateur tente de l'éviter.
Verrouillage de la version d'AppTec360	Vous permet de définir une version du client AppTec360 qui est la version maximale vers laquelle le client se met à jour.

Papier peint

Vous pouvez ici définir un papier peint personnalisé.

L'option "Spécifier une couleur" vous permet de définir une couleur au format hexadécimal (par exemple #000000). Seules les valeurs hexagonales sont autorisées.

L'option "Définir une image comme fond d'écran" vous permet de télécharger une image. Veuillez noter que les appareils fonctionnant avec des lanceurs et des versions de système d'exploitation différents ne fonctionnent pas tous de la même manière. Il n'y a pas de ligne directrice générale pour la taille et le ratio, car cela dépend de l'appareil.

Utilisez JPG (ou JPEG) ou PNG pour le format de fichier.

Gestion des actifs (uniquement au niveau de l’appareil)

Gestion des actifs

Informations sur l’appareil

Modèle	**Désignation du modèle de l'appareil**
Système d'exploitation	OS
Version OS	Version du système d'exploitation
Soutien à l'AE	Prise en charge d'Android Enterprise (conteneur et gestion complète)
Numéro de série	Numéro de série
Nom de l'appareil	Nom de l'appareil
État de la batterie	État de la batterie
Mémoire libre / totale	Mémoire libre / totale
Samsung KNOX	Niveau API KNOX de Samsung
Carte SD disponible	Carte SD disponible
Carte SD émulée	Carte SD émulée
Carte SD amovible	Carte SD amovible
SD Mémoire libre / totale	SD Libre / Mémoire totale de la carte SD

Wi-Fi

Adresse IP	Adresse IP de l'appareil
WiFi MAC	Adresse MAC du WiFi

Cellulaire

Statut	État (carte SIM installée)
Numéro de téléphone	Numéro de téléphone
Itinérance (voix/données)	Itinérance pour la voix et les données
État de l'itinérance	État actuel de l'itinérance
Adresse IP	Adresse IP
Opérateur/transporteur	Opérateur/transporteur
Technologie cellulaire	Technologie cellulaire
IMEI	Numéro IMEI
ICCID	Il s'agit de l'identifiant de la carte SIM, qui est souvent aussi une carte à puce ou une carte à circuit intégré (ICC).
IMSI	L'International Mobile Subscriber Identity (IMSI) permet, dans les réseaux mobiles GSM et UMTS, une identification précise des utilisateurs du réseau. L'IMSI est composé d'un maximum de 15 chiffres et est configuré de la manière suivante : • Indicatif de pays du mobile (MCC), 3 chiffres • Code de réseau mobile (MNC), 2 ou 3 chiffres • Numéro d'identification de l'abonné mobile (MSIN), 1 à 10 chiffres
Actuel MCC/MNC	Voir "SIM MCC/MNC"
SIM MCC/MNC	L'indicatif de pays du mobile est un identificateur de pays établi par l'UIT selon la norme E.212. Il est associé au code de réseau mobile (MNC) pour l'identification du réseau mobile. Signifie le code de pays/réseau mobile de la carte SIM. Si vous vous rendez sur un autre réseau mobile, il est logique que le "MCC/MNC actuel" et le "MCC/MNC SIM" soient différents.

Bluetooth

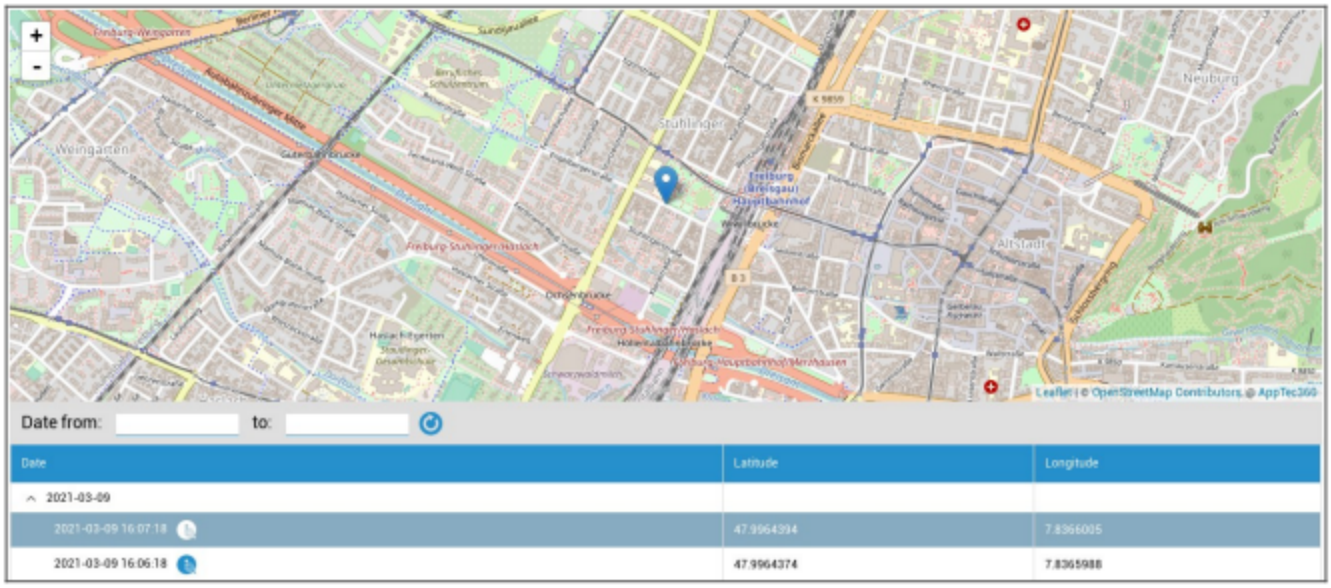
Bluetooth MAC	Adresse MAC Bluetooth

Gestion de la sécurité

Antivol (uniquement au niveau de l’appareil)

Informations GPS (uniquement au niveau de l’appareil)

Vous pouvez ici déterminer l'emplacement actuel/dernier emplacement de l'appareil. La localisation peut être protégée par un ou deux mots de passe - Voir : Paramètres généraux - Confidentialité - Accès GPS



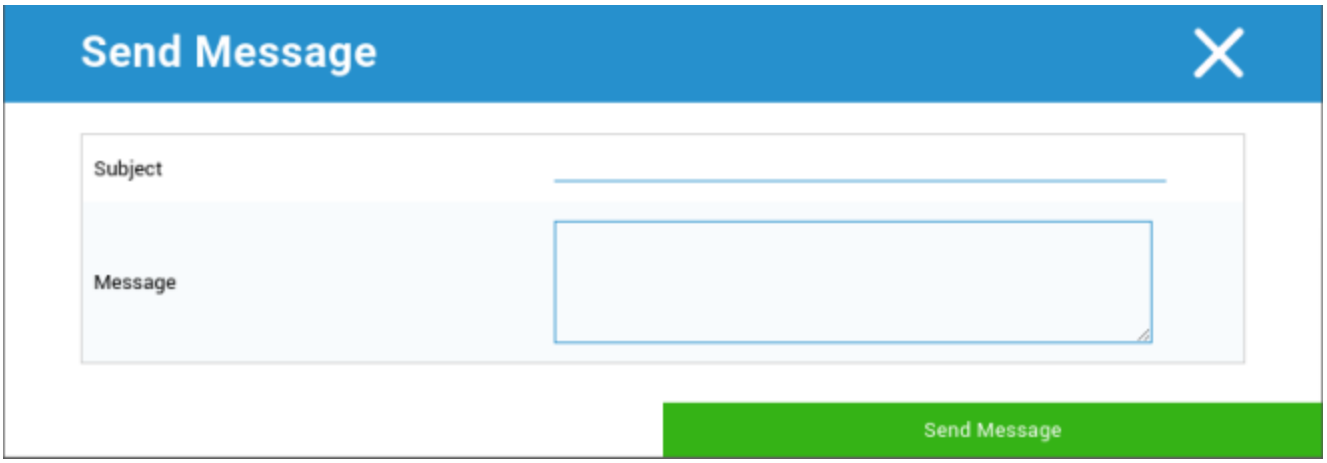
Effacement et verrouillage (uniquement au niveau de l’appareil)

Sous "Effacer et verrouiller", vous pouvez effectuer les trois actions suivantes :

Essuyage complet	L'appareil est restauré à ses paramètres d'usine (les données de l'entreprise et les données personnelles sont supprimées).
Nettoyage de l'entreprise	Seules les données de l'entreprise sont supprimées de l'appareil de l'utilisateur final (toutes les applications, données, etc. qui ont été fournies par AppTec360).
Écran de verrouillage	Le verrouillage de l'écran est activé, il suffit de déverrouiller l'appareil avec le mot de passe/NIP de l'appareil.

Message (uniquement au niveau de l’appareil)

Vous pouvez remplir l'objet et un message et l'envoyer à un appareil d'utilisateur final. Ce message sera affiché dans le client AppTec360.



Configuration de la sécurité

Code d’accès

Sous "Passcode", vous pouvez mandater un mot de passe pour l'appareil, les options de réglage suivantes sont disponibles

Longueur minimale du mot de passe	Fixe le nombre minimum de symboles que doit comporter un mot de passe
Qualité du mot de passe	Force du mot de passe Non spécifié = non spécifié Tous les mots de passe sont acceptables = tous les mots de passe sont acceptables au moins des caractères numériques = doit contenir au moins des caractères numériques au moins des caractères complexes = doit contenir au moins des caractères spéciaux au moins des caractères alphanumériques = doit contenir au moins des caractères alphanumériques au moins des caractères alphabétiques = doit contenir au moins des caractères alphabétiques
Verrouillage du temps d'inactivité maximum	Délai maximum d'affichage de l'écran. Ceci configure uniquement la valeur maximale qui peut être sélectionnée par l'utilisateur.
Minimum de lettres minuscules requis dans le mot de passe	Minimum de lettres minuscules requis dans le mot de passe
Minimum de lettres majuscules requis dans le mot de passe	Minimum de lettres majuscules requis dans le mot de passe
Nombre minimum de caractères non alphabétiques requis dans le mot de passe	Nombre minimum de caractères non alphabétiques requis dans le mot de passe
Nombre minimum de chiffres requis pour le mot de passe	Nombre minimum de chiffres requis pour le mot de passe
Symboles minimums requis dans le mot de passe	Symboles minimums requis dans le mot de passe
Délai d'expiration du mot de passe	Établit, après quoi le mot de passe expire et un nouveau mot de passe doit être délivré.
Restriction de l'historique des mots de passe	Nombre de mots de passe précédemment utilisés qui ne sont pas autorisés
Nombre maximal d'échecs de tentatives de saisie du mot de passe	Détermine le nombre de fois qu'un mot de passe peut être saisi de manière incorrecte avant qu'un effacement complet de l'appareil ne soit effectué.

Cryptage

À ce stade, vous pouvez crypter la mémoire interne de l'appareil, ainsi que la mémoire de la carte SD.

Exiger le chiffrement du stockage	Si ce paramètre est activé, la mémoire de l'appareil sera cryptée, à condition que l'appareil prenne en charge cette fonctionnalité. Une fois que la mémoire de l'appareil a été cryptée pour la première fois, il n'est plus possible de la décrypter. De même, la politique en matière de mot de passe sera automatiquement remplacée par 6 symboles alphanumériques.
Exiger le cryptage de la carte SD	Ce paramètre ne s'applique qu'aux appareils Samsung ! Si ce paramètre est activé, la carte SD externe peut être cryptée et ne peut être décryptée que manuellement sur l'appareil de l'utilisateur final. De même, la politique en matière de mot de passe sera automatiquement remplacée par 6 symboles alphanumériques.

AntiVirus

L'activation de l'antivirus installera Ikarus sur les appareils. Sachez que cela nécessite une licence distincte qui peut être saisie dans Paramètres généraux → Gestion des applications → Apps tierces.

Scan automatique	Définit si Ikarus effectue ou non un balayage automatique et à quelle fréquence il l'effectue. L'activation de l'option "Analyse automatique complète" permet d'effectuer une analyse complète. Dans le cas contraire, une analyse rapide sera effectuée
Mises à jour automatiques	Active les mises à jour automatiques de la base de données des virus et définit la fréquence de ces mises à jour.
Protection des applications	Permet d'analyser les applications en plus de l'analyse normale qui n'analyse que les fichiers.
Protection de la carte SD	Active la protection de la carte SD. Si ce n'est pas le cas, l'analyse est limitée au stockage local.
Mise à jour Wi-Fi uniquement	Limite la mise à jour au Wi-Fi

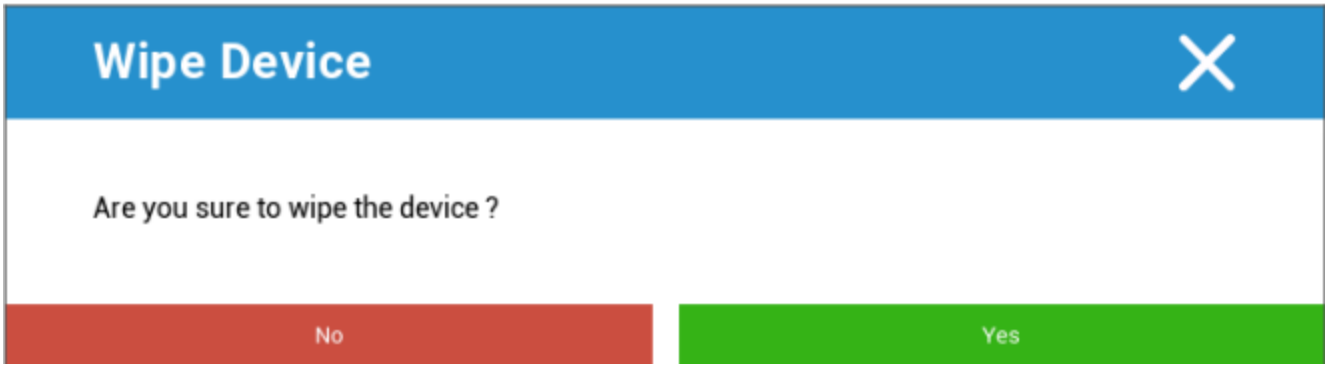
Fin de vie (uniquement au niveau de l’appareil)

Effacer (uniquement au niveau de l’appareil)

Sous "Effacer", vous pouvez rétablir les paramètres d'usine de l'appareil. Dans ce cas, les données de l'entreprise et les données privées sont supprimées sur l'appareil de l'utilisateur final.

En cliquant sur le "symbole moins", vous devriez recevoir le message suivant

Effacer aussi la carte SD ?	La mémoire de la carte SD sera également effacée



Si vous répondez "Oui", vous pouvez procéder à l'effacement.

Sous "Rapport d'effacement", les éléments suivants peuvent être affichés

Effacé par	Historique de la personne qui a effectué l'essuyage
Date	Date
Statut	État (par exemple, si le nettoyage a été effectué avec succès)

Paramètres de restriction

Restrictions

Ici, il est possible de restreindre et de bloquer toute une série de choses.

Activer la caméra	Permettre l'utilisation de l'appareil photo
Forcer la synchronisation automatique	Concerne l'interface "Sync On = la synchronisation est activée en permanence Éteint = la synchronisation est désactivée en permanence Choix de l'utilisateur = sélectionné par l'utilisateur
Force Bluetooth	On = Bluetooth est activé en permanence Off = Bluetooth est désactivé en permanence Choix de l'utilisateur = sélectionné par l'utilisateur
Force GPS	On = le GPS est activé en permanence Éteint = le GPS est désactivé en permanence Choix de l'utilisateur = sélectionné par l'utilisateur
Forcer la précision de la géolocalisation de Google	Activé = localisation permanente sur l'internet Désactivé = Désactivation permanente de la localisation sur internet Choix de l'utilisateur = sélectionné par l'utilisateur

Pour les appareils Samsung dotés de l'interface KNOX 1.0 ou supérieure, les options de réglage suivantes sont disponibles.

Autoriser la carte SD	Autoriser la carte SD
Autoriser l'écriture sur la carte SD	Autoriser l'écriture sur la carte SD
Autoriser la capture d'écran	Permettre la capture d'écran
Autoriser le presse-papiers	Autoriser le presse-papiers
Sauvegarde des paramètres et des données de l'application dans Google Cloud	Désactivé = désactiver Google Backup Activé = activer Google Backup Choix de l'utilisateur = sélectionné par l'utilisateur
Autoriser le débogage USB	Autoriser le débogage USB (utilisé, par exemple, pour la création de journaux de périphériques (ADB))
Autoriser le rapport d'accident de Google	Autoriser l'envoi de Google Crash Report depuis les applications
Autoriser la réinitialisation d'usine	Permet à l'utilisateur de rétablir les paramètres d'usine de l'appareil.
Autoriser la mise à jour OTA	Autoriser les mises à jour "en direct".
Autoriser le stockage hôte USB	Si elle est activée, la mémoire USB, sous la forme d'un disque dur ou d'un lecteur de carte SD, peut être connectée.
Autoriser le lecteur multimédia USB (MTP, PTP)	Autoriser le lecteur multimédia USB (MTP, PTP)
Autoriser le microphone	Activé = autoriser le microphone pour les applications tierces Désactivé = bloquer le microphone pour les applications tierces Choix de l'utilisateur = les utilisateurs peuvent choisir, si l'application tierce a accès au microphone
Autoriser la NFC (Near Field Communication)	Autoriser le NFC
Autoriser les sources inconnues (APK Sideloading)	Si cette option est activée, le chargement latéral d'applications (fichiers APK) est autorisé. Une fois ce paramètre désactivé, l'utilisateur doit l'activer manuellement lorsque vous autorisez à nouveau l'installation d'APK provenant de sources inconnues.
Autoriser la création d'un utilisateur	Permet la création de plusieurs utilisateurs

Propriétaire de l’appareil AE

(L'appareil doit être en mode propriétaire d'appareil d'entreprise Android) Il est recommandé de créer les appareils en tant qu'appareils "Android Enterprise" et non en tant qu'appareils "Android".

Sécurité	
Interdire l'emplacement du partage	Indique si un utilisateur n'est pas autorisé à activer le partage de la localisation.
Interdire le démarrage sécurisé	Indique si l'utilisateur n'est pas autorisé à redémarrer l'appareil en mode de démarrage sécurisé.
Interdire la réinitialisation du réseau	Indique si un utilisateur n'est pas autorisé à réinitialiser les paramètres du réseau à partir des paramètres.
Interdire la réinitialisation d'usine	Indique si un utilisateur n'est pas autorisé à réinitialiser l'appareil.
Activer ADB	Permet la connexion à un PC via ADB
Désactiver le Keyguard	Désactive le Keyguard
Propriétaire de l'appareil Informations sur l'écran de verrouillage	Définit les informations relatives au propriétaire de l'appareil à afficher sur l'écran de verrouillage.
Contrôle de la conformité	Mode Inviter l'utilisateur - L'utilisateur sera invité à effectuer les actions nécessaires. Mode Lock-Down Container - Masquer toutes les applications jusqu'à ce que toutes les conditions soient remplies

Gestion des applications	
Autoriser l'établissement de liens entre les applications d'un même profil	Permet aux applications du profil parent de gérer les liens web du profil géré.
Interdire le contrôle des applications	Indique si un utilisateur n'est pas autorisé à modifier les applications dans les paramètres ou les lanceurs.
Interdire l'installation d'une application	Indique si un utilisateur n'est pas autorisé à installer des applications.
Désactiver les applications de désinstallation	Indique si un utilisateur n'est pas autorisé à désinstaller des applications.
Politique d'autorisation d'exécution	Indique comment les nouvelles demandes d'autorisation des applications seront traitées.

Autoriser les sources inconnues	Si cette option est activée, les utilisateurs peuvent charger des applications de manière latérale en installant un fichier .apk.

Connectivité	
Désactiver la configuration du réseau mobile	Indique si un utilisateur n'est pas autorisé à configurer des réseaux mobiles.
Disallow Tethering Config	Indique si un utilisateur n'est pas autorisé à configurer le Tethering et les points d'accès portables.
Interdire la configuration du VPN	Indique si un utilisateur n'est pas autorisé à configurer un VPN.
Désactiver la configuration Wifi	Indique si un utilisateur n'est pas autorisé à modifier les points d'accès WiFi.
Interdire les faisceaux NFC sortants	Indique si l'utilisateur n'est pas autorisé à utiliser la technologie NFC pour transmettre des données à partir d'applications.
Verrouiller la configuration WiFi	Ce paramètre détermine si les configurations WiFi créées par une application du propriétaire de l'appareil doivent être verrouillées (c'est-à-dire qu'elles ne peuvent être modifiées ou supprimées que par l'application du propriétaire de l'appareil, même pas par l'application Paramètres).
Activer l'itinérance des données	Active l'itinérance des données

Bluetooth	
Désactiver le Bluetooth	Indique si le Bluetooth est interdit sur l'appareil. Nécessite Android 8.0
Désactiver le partage Bluetooth	Spécifie si le partage Bluetooth sortant est interdit sur l'appareil. Nécessite Android 8.0
Désactiver la configuration Bluetooth	Indique si un utilisateur n'est pas autorisé à configurer Bluetooth.

Gestion des comptes	
Interdire l'ajout d'un profil géré	Spécifie si un utilisateur n'est pas autorisé à ajouter des profils gérés. Nécessite Android 8.0
Interdire l'ajout d'utilisateurs	Indique si un utilisateur n'est pas autorisé à ajouter de nouveaux utilisateurs.
Désactiver Supprimer le profil géré	Spécifie si les profils gérés de cet utilisateur peuvent être supprimés, sauf par le propriétaire du profil. Nécessite Android 8.0
Interdire la modification du compte	Indique si un utilisateur n'a pas le droit d'ajouter ou de supprimer des comptes, à moins qu'ils ne soient ajoutés par programme par Authenticator.

Téléphonie	
Interdire les appels sortants	Spécifie que l'utilisateur n'est pas autorisé à passer des appels téléphoniques sortants.
Interdire les SMS	Spécifie que l'utilisateur n'est pas autorisé à envoyer ou à recevoir des messages SMS.

Système	
Interdire la création de fenêtres	Spécifie que les fenêtres autres que les fenêtres d'application ne doivent pas être créées.
Désactiver l'icône de l'utilisateur	Indique si un utilisateur n'est pas autorisé à modifier son icône.
Disallow Set Wallpaper	Restriction de l'utilisateur pour interdire la définition d'un fond d'écran.
Désactiver la barre d'état	La désactivation de la barre d'état bloque les notifications, les réglages rapides et autres superpositions d'écran qui permettent de s'échapper d'un appareil à usage unique.
Activer l'heure automatique	Règle l'heure automatiquement.
Activer le fuseau horaire automatique	Définit automatiquement le fuseau horaire.
Reste allumé lorsqu'il est branché	L'appareil reste actif lorsqu'il est connecté à une source d'alimentation.

Stockage	
Désactiver la vérification des applications	Indique si un utilisateur n'est pas autorisé à désactiver la vérification des applications.
Interdire le montage de supports physiques	Indique si un utilisateur n'est pas autorisé à monter des supports physiques externes.
Activer le service de sauvegarde	Le service de sauvegarde gère tous les mécanismes de sauvegarde et de restauration sur l'appareil. Si vous réglez ce paramètre sur faux, les données ne pourront pas être sauvegardées ou restaurées. Le service de sauvegarde est désactivé par défaut. Nécessite Android 8.0
Activer la mémoire de masse USB	Active l'utilisation de la mémoire de masse USB.

Clavier	
Interdire le remplissage automatique	Spécifie si un utilisateur n'est pas autorisé à utiliser les services de remplissage automatique. Nécessite Android 8.0
Interdire le copier-coller entre profils	Spécifie si ce qui est copié dans le presse-papiers de ce profil peut être collé dans des profils connexes.

Son	
Refuser l'ajustement des volumes	Indique si un utilisateur n'est pas autorisé à régler le volume principal.
Désactiver Désactiver le microphone	Indique si un utilisateur n'est pas autorisé à régler le volume du microphone.
Dispositif de mise en sourdine	Dispositif de mise en sourdine.

Politique de mise à jour du système	
Contrôlez les mises à jour du système d'exploitation	Activez cette option pour définir le comportement de la mise à jour : automatique, fenêtré ou différé.

Conteneur BYOD

Android Enterprise

Android Enterprise

Activer Android Enterprise	Activez Android Enterprise (AE). AE est pris en charge à partir de la version 5.1 d'Android.
Contrôle de la conformité	Mode Inviter l'utilisateur - L'utilisateur sera invité à effectuer les actions nécessaires. Mode Lock-Down Container - Masquer toutes les applications jusqu'à ce que toutes les conditions soient remplies
Politique d'autorisation d'exécution	Inviter l'utilisateur à demander de nouvelles autorisations Accordez toujours les nouvelles demandes d'autorisation Refusez toujours les nouvelles demandes d'autorisation Attention : Certaines applications ont des difficultés à reconnaître les autorisations si celles-ci sont définies automatiquement. Si vous accordez toujours les autorisations et que vous rencontrez des problèmes avec des applications qui disent que les autorisations sont manquantes, réglez ce paramètre sur "demander à l'utilisateur" et réinstallez l'application.
Autoriser le presse-papiers sortant	Permet de faire des copier-coller de l'intérieur du conteneur vers l'extérieur.
Autoriser la résolution de l'identification de l'appelant	Affiche le nom d'un appel entrant en fonction des contacts présents dans le conteneur.
Autoriser la résolution de la recherche de contacts	Permet de rechercher des noms dans les contacts du conteneur lors des appels.
Autoriser le partage des contacts par Bluetooth	Permet d'accéder au contact des conteneurs dans une voiture
Interdire les faisceaux NFC sortants	Désactive le NFC pour le conteneur

Autoriser les sources inconnues	Si cette option est activée, les utilisateurs peuvent charger des applications de manière latérale en installant un fichier .apk.
Autoriser le débogage USB	Si cette option est activée, les utilisateurs peuvent activer le débogage USB.
Interdire la modification du compte	Interdit la création, la suppression et la modification des comptes dans le conteneur. N'oubliez pas que certaines applications ont besoin de créer ou de modifier des comptes pour fonctionner correctement.

Gmail Exchange

Permet de configurer Gmail dans le conteneur. Veuillez noter que l'activation de cette configuration n'entraîne pas l'installation automatique de l'application. Vous devez toujours ajouter cette application comme application obligatoire.

Adresse électronique	Adresse électronique
Nom d'hôte du serveur	Nom d'hôte du serveur
Nom de connexion	Nom de connexion
Signature	Signature
Nombre de jours précédents à synchroniser	Nombre de jours précédents à synchroniser.
Identifiant de l'appareil	Identifiant EAS. Laissez ce champ vide si votre environnement ne l'exige pas.
Utilisez le protocole SSL (Secure Sockets Layer)	Active l'utilisation de SSL. La désactivation de cette option peut réduire la sécurité
Accepter tous les certificats	Accepte tous les certificats. L'activation de cette option peut réduire la sécurité
Autoriser les comptes non gérés	Permet à l'utilisateur d'ajouter des comptes supplémentaires
Certificat de client	Télécharger le certificat client si votre serveur Exchange l'exige

Applications du système AE

Ici, vous pouvez activer les applications système pour le conteneur d'entreprise Android. N'oubliez pas que l'application spécifiée doit se trouver dans la mémoire du système, sinon rien ne se passe.

Code d’accès au conteneur

Uniquement pour Android 7.0 ou supérieur

Permet de définir un mot de passe spécifique pour le conteneur.

Longueur minimale du mot de passe	Fixe le nombre minimum de symboles que doit comporter un mot de passe
Qualité du mot de passe	Force du mot de passe Non spécifié = non spécifié Tous les mots de passe sont acceptables = tous les mots de passe sont acceptables au moins des caractères numériques = doit contenir au moins des caractères numériques au moins des caractères complexes = doit contenir au moins des caractères spéciaux au moins des caractères alphanumériques = doit contenir au moins des caractères alphanumériques au moins des caractères alphabétiques = doit contenir au moins des caractères alphabétiques
Verrouillage du temps d'inactivité maximum	Temps maximum avant que le conteneur ne soit verrouillé. Ceci configure uniquement la valeur maximale qui peut être sélectionnée par l'utilisateur.
Minimum de lettres minuscules requis dans le mot de passe	Minimum de lettres minuscules requis dans le mot de passe
Minimum de lettres majuscules requis dans le mot de passe	Minimum de lettres majuscules requis dans le mot de passe
Nombre minimum de caractères non alphabétiques requis dans le mot de passe	Nombre minimum de caractères non alphabétiques requis dans le mot de passe
Nombre minimum de chiffres requis pour le mot de passe	Nombre minimum de chiffres requis pour le mot de passe
Symboles minimums requis dans le mot de passe	Symboles minimums requis dans le mot de passe
Délai d'expiration du mot de passe	Établit, après quoi le mot de passe expire et un nouveau mot de passe doit être délivré.
Restriction de l'historique des mots de passe	Nombre de mots de passe précédemment utilisés qui ne sont pas autorisés
Nombre maximal d'échecs de tentatives de saisie du mot de passe	Détermine le nombre de fois qu'un mot de passe peut être saisi de manière incorrecte avant que le conteneur ne soit supprimé.

Samsung KNOX

Activation

Vous pouvez ici activer le conteneur Samsung KNOX. Sachez que cette fonction n'est plus prise en charge par Samsung sur Android 10 ou une version ultérieure. Utiliser Android Enterprise Container sur Android 10 ou supérieur

Code d’accès Knox

Établir les lignes directrices relatives aux paramètres du mot de passe de l'appareil

Longueur minimale du mot de passe	Détermine le nombre de symboles que le mot de passe doit comporter.
Qualité du mot de passe	Force du mot de passe Tous les mots de passe sont corrects = Tous les mots de passe sont corrects Au moins des caractères numériques = Un minimum de caractères numériques doit être présent Au moins des caractères complexes = Un minimum de caractères spéciaux doit être présent Au moins des caractères alphanumériques = Au moins des caractères alphanumériques doivent être présents Au moins des caractères alphabétiques = Au moins des caractères alphabétiques doivent être présents
Caractères complexes minimum requis	Un minimum de caractères complexes doit être présent
Délai maximum d'inactivité	Délai maximum d'inactivité de l'utilisateur, avant le verrouillage du clavier
Autoriser l'authentification par empreinte digitale	Autoriser l'authentification par empreinte digitale
Autoriser l'authentification par iris	Autoriser l'authentification par reconnaissance de l'iris
Âge maximum du mot de passe	Fixe le délai au terme duquel le mot de passe expire et un nouveau mot de passe doit être délivré.
Historique des mots de passe enregistrés	Nombre d'anciens mots de passe non autorisés
Nombre maximal d'échecs de tentatives de saisie du mot de	Détermine le nombre de fois où le mot de passe peut être soumis de manière incorrecte avant qu'un effacement complet

passe	de l'appareil n'ait lieu.

Knox Security

Limiter les fonctionnalités spécifiques des appareils

Activer la caméra	Permettre l'utilisation de l'appareil photo
Autoriser le Samsung KNOX App Store	Permettre l'utilisation du Samsung KNOX App Store
Autoriser les services Google Play	Autoriser les services Google Play
Autoriser le navigateur	Permettre l'utilisation du navigateur natif
Autoriser les captures d'écran	Permettre la création de captures d'écran
Autoriser l'importation de contacts	Si cette option est activée, l'accès aux contacts de l'appareil à partir du conteneur KNOX est autorisé.
Autoriser l'exportation de contacts	Si cette option est activée, l'accès aux contacts KNOX à partir de l'appareil est autorisé.
Autoriser l'importation de calendriers	Si l'option est activée, l'accès au calendrier de l'appareil à partir du conteneur KNOX est autorisé.
Autoriser l'exportation du calendrier	Si l'option est activée, l'accès au calendrier KNOX à partir de l'appareil est autorisé.
Autoriser un clavier non sécurisé	Autoriser l'utilisation d'un clavier non sécurisé
Activer l'importation de fichiers	Activer l'importation de fichiers dans le conteneur KNOX
Activer l'exportation de fichiers	Activer l'exportation de fichiers à partir du conteneur KNOX

Échange Knox

Vous pouvez ici configurer le profil d'échange pour le conteneur KNOX.

Adresse électronique	L'adresse électronique de l'utilisateur fourni Veuillez noter les "Placeholders", que vous pouvez utiliser pour travailler avec les informations d'identification et que vous ne devez pas modifier manuellement sur chaque appareil. En cliquant sur **Afficher les espaces réservés**, vous pouvez les afficher vous-même.
Nom d'hôte du serveur	Adresse de votre serveur Exchange
Nom de connexion	Le nom de connexion pour l'appareil de l'utilisateur final respectif, veuillez également noter les "Placeholders" ici.
Domaine	Adresse du domaine
Mot de passe (uniquement au niveau de l'appareil)	En option, il est possible de fournir un mot de passe à un appareil individuel. Si ce mot de passe reste vide, l'utilisateur sera invité à saisir son mot de passe Exchange.
Nombre de jours précédents à synchroniser	Nombre de jours déterminant le moment où les courriels sont synchronisés à nouveau
Signature	Une signature peut être jointe
Compte par défaut	Établit que ce compte de courrier électronique est le compte standard.
Utilisez le protocole SSL (Secure Sockets Layer)	Utiliser une connexion SSL
Utiliser la sécurité de la couche transport (TLS)	Utiliser une connexion TLS
Accepter tous les certificats	Tous les certificats sont acceptés. Veuillez sélectionner cette option si votre serveur Exchange utilise un certificat auto-signé.

Knox eMail

Adresse électronique	L'adresse électronique de l'utilisateur fourni Veuillez noter les "Placeholders", que vous pouvez utiliser pour travailler avec les informations d'identification et que vous ne devez pas modifier manuellement sur chaque appareil. En cliquant sur **Afficher les espaces réservés**, vous pouvez les afficher vous-même.
Protocole du serveur entrant	Protocole du serveur entrant IMAP ou POP
Adresse du serveur entrant	Adresse du serveur entrant
Port du serveur entrant	Port du serveur entrant
Nom d'utilisateur du serveur entrant	Nom d'utilisateur du serveur entrant
Mot de passe du serveur entrant	Mot de passe du serveur entrant
Le serveur entrant utilise SSL	Le serveur entrant utilise SSL
Le serveur entrant utilise TLS	Le serveur entrant utilise TLS
Le serveur entrant accepte tous les certificats	Le serveur entrant accepte tous les types de certificats
Protocole du serveur sortant	Protocole du serveur sortant SMTP
Port du serveur sortant	Port du serveur sortant
Le serveur sortant utilise des informations d'identification supplémentaires	Informations d'identification supplémentaires pour le serveur sortant. Si ce paramètre est désactivé, les paramètres du serveur entrant seront utilisés.
Nom d'utilisateur du serveur sortant	Nom d'utilisateur du serveur sortant
Mot de passe du serveur sortant	Mot de passe du serveur sortant
Le serveur sortant utilise SSL	Le serveur sortant utilise SSL
Le serveur sortant utilise TLS	Le serveur sortant utilise TLS
Le serveur sortant accepte tous les certificats	Le serveur sortant accepte tous les types de certificats
Signature	Une signature peut être apposée ici
Notifier l'utilisateur lors de la réception d'un nouvel e-mail	Notifier l'utilisateur lors de la réception d'un nouvel e-mail

Knox Apps

Établissez ici les applications que vous souhaitez distribuer aux appareils des utilisateurs finaux. Ceux-ci seront alors disponibles dans le conteneur KNOX. Pour ajouter une application, procédez comme vous le feriez dans le menu Applications obligatoires.

Nom de l'application	Nom de l'application
Obligatoire depuis	Moment où l'application a été ajoutée
Source	Source de l'application (Play Store | In-House)

En cliquant sur le symbole, l'application concernée peut être à nouveau supprimée.

Gestion des connexions

Wifi

Pour ce paramètre, effectuer la préconfiguration des dispositifs de l'utilisateur final, pour l'accès aux points d'accès internes.

Identificateur d'ensemble de services (SSID)	SSID du réseau à connecter
Réseau caché	Activer, dans le cas où le point d'accès ne diffuse pas le SSID.
Type de sécurité	Établir le type de sécurité de l'AP

Type de sécurité

WEP

Mot de passe	Mot de passe pour l'AP

WPA/WPA2

Mot de passe	Mot de passe pour l'AP

802.1x EAP

Méthode EAP	

PWD	Identité	Identité
	Mot de passe	Mot de passe

PEAP	Protocole d'authentification de phase 2	aucun	Pas de protocole supplémentaire
		MSCHAPV2	Protocole MSCHAPV2
		CTG	Protocole GTC
	Certificat CA	Certificat CA	
	Identité	Identité	
	Identité anonyme	Identité anonyme	
	Mot de passe	Mot de passe	

Méthode EAP	

TTLS	Protocole d'authentification de phase 2	aucun	Pas de protocole supplémentaire
		PAP	Protocole PAP
		MSCHAP	Protocole MSCHAP
		MSCHAPV2	Protocole MSCHAPV2
		CTG	Protocole GTC
	Certificat CA	Certificat CA	
	Identité	Identité	
	Identité anonyme	Identité anonyme	
	Mot de passe	Mot de passe	

TLS	Certificat CA	Certificat CA
	Identité	Identité
	Mot de passe	Mot de passe

VPN

Type de connexion	**Établir le type de connexion VPN**

Si vous sélectionnez "VPN par application" comme type de VPN, les clients VPN disponibles changeront. Le VPN par application limite le VPN à certaines applications et démarre la connexion VPN automatiquement si une application spécifique est lancée.

Client VPN AppTec360	Utilise le client VPN AppTec360 en combinaison avec la passerelle universelle.
Nom de la connexion	Nom de la connexion VPN
Configuration de la passerelle	Sélectionnez la configuration VPN de la passerelle universelle.
VPN toujours actif	Force le VPN à être toujours actif, de sorte que l'ensemble du trafic passe par le VPN.
Activer le verrouillage natif	Bloque toute mise en réseau lorsque l'appareil n'est pas connecté au VPN. Utilisez cette option avec précaution, car elle peut entraîner une perte totale de connexion si elle n'est pas configurée correctement. Uniquement pour Android Enterprise sur Android 7 ou supérieur
Activer le verrouillage d'AppTec360	Bloque l'utilisation de toutes les applications jusqu'à ce que la connexion VPN soit lancée.

Cisco AnyConnect	
Nom de la connexion	Nom de la connexion VPN
Serveur	Adresse du serveur
Mode certificat	Désactivé = désactivé Automatique = automatique

L2TP (KNOX uniquement)	Uniquement disponible sur les appareils Samsung
Nom de la connexion	Nom de la connexion
Serveur	Adresse du serveur
Activer le secret L2TP	
Domaines de recherche DNS	Domaines de recherche DNS

Type de connexion	**Établir le type de connexion VPN**

PPTP (KNOX uniquement)	Uniquement disponible sur les appareils Samsung
Nom de la connexion	Nom de la connexion VPN
Serveur	Adresse du serveur
Activer le cryptage	Activer le cryptage
Domaines de recherche DNS	Domaines de recherche DNS

L2TP / IPSec PSK (KNOX uniquement)	Uniquement disponible sur les appareils Samsung
Nom de la connexion	Nom de la connexion VPN
Serveur	Adresse du serveur
Clé pré-partagée IPSec	Clé pré-partagée pour l'authentification
Activer le secret L2TP	
L2TP Secret	
Domaines de recherche DNS	Domaines de recherche DNS

IPSec XAuth PSK (KNOX uniquement)	Uniquement disponible sur les appareils Samsung
Nom de la connexion	Nom de la connexion VPN
Serveur	Adresse du serveur
Identifiant IPSec	Nom d'utilisateur pour la connexion
Clé pré-partagée IPSec	Mot de passe pour la connexion
Domaines de recherche DNS	Domaines de recherche DNS

OpenVPN	

Nom de la connexion	Nom de la connexion
Profil OpenVPN	Voici où le contenu du fichier .ovpn sera copié
Application OpenVPN	Il existe deux applications différentes pour l'utilisation d'OpenVPN Nous recommandons l'application "OpenVPN for Android". Mais vous pouvez également utiliser l'application "OpenVPN Connect".

Restrictions

Vous pouvez ici définir les restrictions relatives à la gestion des connexions.

Autoriser l'itinérance des données	Autoriser les données mobiles en itinérance
Forcer l'itinérance des données	Si elle est activée, l'itinérance pour les données mobiles est activée en permanence (non recommandé !). Ce paramètre écrase le paramètre "Allow Data Roaming" (autoriser l'itinérance des données) !
Les paramètres suivants ne sont disponibles que sur Samsung KNOX 2.0 ou supérieur	
Autoriser les appels d'urgence uniquement	Autoriser les appels d'urgence uniquement
Autoriser le WiFi	Autoriser le WiFi
Niveau de sécurité minimum du réseau WiFi	Niveau de sécurité minimum du réseau WiFi Ouvert = tous les types de WiFi sont autorisés
Interdire à l'utilisateur d'ajouter des réseaux WiFi	L'utilisateur ne peut pas ajouter lui-même un réseau WiFi Ce réglage n'est possible que si un profil WiFi a été défini sous "Gestion des connexions"
Autoriser les SMS et MMS	Tous = Tout le trafic SMS et MMS est autorisé SMS entrants uniquement = Seuls les SMS entrants sont autorisés. SMS sortants uniquement = Seuls les SMS sortants sont autorisés. Aucun = Aucun trafic SMS / MMS n'est autorisé
Autoriser la synchronisation en itinérance	Autoriser la synchronisation en itinérance Allumé = activé Désactivé = désactivé Choix de l'utilisateur = choix de l'utilisateur
Autoriser l'itinérance vocale	Autoriser l'itinérance vocale Allumé = activé Désactivé = désactivé Choix de l'utilisateur = choix de l'utilisateur
Utiliser le serveur proxy http du système	L'utilisation d'un serveur proxy HTTP, qui est fourni par les paramètres du système dans les réglages, dépend du réseau connecté (WiFi ou APN).

APN

Les paramètres suivants ne sont disponibles que sur Samsung SAFE 2.0 ou une version plus récente !

Nom d'affichage de l'APN	Nom d'affichage de l'APN	
Nom du point d'accès	Nom de l'APN	
Protocole du serveur sortant	Non défini	
	Aucun	
	PAP	Protocole PAP
	CHAP	Protocole CHAP
	PAP ou CHAP	Protocole PAP ou CHAP
MCC - Indicatif de pays de téléphonie mobile	Le MCC est saisi ici. Laissez ce champ vide si le MCC de la carte SIM insérée doit être utilisé.	
MNC - Code de réseau mobile	Le MNC est saisi ici. Laissez ce champ vide si le MCC de la carte SIM insérée doit être utilisé.	
Adresse du serveur	Adresse du serveur	
Numéro de port du serveur	Numéro de port du serveur	
Adresse proxy du serveur	Adresse proxy du serveur	
Adresse du serveur MMS	Adresse du serveur MMS, pour Standard veuillez laisser vide	
Numéro de port MMS	Numéro de port MMS	
Adresse proxy MMS	Adresse proxy MMS	
Nom de l'utilisateur	Nom de l'utilisateur	
Mot de passe	Mot de passe	
Type de point d'accès	Les types autorisés sont : "default", "mms", "supl" Si ce champ n'est pas renseigné, le type "default,supl,mms" sera utilisé.	
APN préféré	APN de préférence	

Bluetooth

Ici, il est possible d'effectuer divers réglages Bluetooth.

Les paramètres suivants ne sont disponibles que sur Samsung KNOX 1.0 ou supérieur !

Autoriser la découverte de l'appareil via Bluetooth	Permettre la découverte d'appareils via Bluetooth
Autoriser l'appairage Bluetooth	Autoriser l'appairage Bluetooth
Autoriser les oreillettes Bluetooth	Autoriser les oreillettes Bluetooth
Autoriser les dispositifs mains libres Bluetooth	Autoriser les dispositifs mains libres Bluetooth
Autoriser les périphériques Bluetooth A2DP	Autoriser la diffusion audio Bluetooth A2DP entre les appareils
Autoriser les appels sortants	Autoriser les appels sortants viaBT
Autoriser le transfert de données via Bluetooth	Permettre le transfert de données via Bluetooth
Autoriser le Bluetooth Tethering	Permet d'utiliser l'appareil comme modem (connexion internet Bluetooth)
Autoriser la connexion à l'ordinateur via Bluetooth	Autoriser la connexion à l'ordinateur via Bluetooth

Gestion du PIM

Échange

Uniquement disponible pour Samsung KNOX 1.0 ou plus !

Adresse électronique	L'adresse électronique de l'utilisateur fourni Veuillez noter les "Placeholders", que vous pouvez utiliser pour travailler avec les informations d'identification et que vous ne devez pas modifier manuellement sur chaque appareil. En cliquant sur **Afficher les espaces réservés**, vous pouvez les afficher vous-même.
Nom d'hôte du serveur	Adresse de votre serveur Exchange
Nom de connexion	Le nom de connexion pour l'appareil de l'utilisateur final respectif, veuillez également noter les "Placeholders here".
Domaine	Adresse du domaine
Mot de passe (uniquement au niveau de l'appareil)	En option, un mot de passe peut être attribué à un appareil individuel. Si ce mot de passe reste vide, l'utilisateur sera invité à saisir son mot de passe Exchange.
Nombre de jours précédents à synchroniser	Nombre de jours déterminant le moment où les courriels sont synchronisés à nouveau
Signature	Une signature peut être jointe (Remarque : certains appareils exigent un formatage HTML pour la signature).
Compte par défaut	Établit que ce compte de messagerie est le compte standard.
Utilisez le protocole SSL (Secure Sockets Layer)	Utiliser une connexion SSL
Utiliser la sécurité de la couche transport (TLS)	Utiliser une connexion TLS
Accepter tous les certificats	Tous les certificats sont acceptés. Veuillez sélectionner cette option si votre serveur Exchange utilise un certificat auto-signé.

eMail

Ici, vous pouvez distribuer des comptes IMAP et POP aux appareils respectifs des utilisateurs finaux.

Les paramètres suivants ne sont disponibles que sur Samsung KNOX 1.0 ou supérieur !		
Adresse électronique	L'adresse électronique de l'utilisateur fourni Veuillez noter les "Placeholders", que vous pouvez utiliser pour travailler avec les informations d'identification et que vous ne devez pas modifier manuellement sur chaque appareil. En cliquant sur **Afficher les espaces réservés**, vous pouvez les afficher vous-même.	
Protocole du serveur entrant	Protocole du serveur entrant	IMAP ou POP
Adresse du serveur entrant	Adresse du serveur entrant	
Port du serveur entrant	Port du serveur entrant	
Nom d'utilisateur du serveur entrant	Nom d'utilisateur du serveur entrant	
Mot de passe du serveur entrant (uniquement au niveau de l'appareil)	Mot de passe du serveur entrant (uniquement au niveau de l'appareil)	
Le serveur entrant utilise SSL	Le serveur entrant utilise SSL	
Le serveur entrant utilise TLS	Le serveur entrant utilise TLS	
Le serveur entrant accepte tous les certificats	Le serveur entrant accepte tous les types de certificats	
Protocole du serveur sortant	Protocole du serveur sortant	SMTP
Port du serveur sortant	Port du serveur sortant	
Le serveur sortant utilise des informations d'identification supplémentaires	Informations d'identification supplémentaires pour le serveur sortant. Si ce paramètre est réglé sur "off", les paramètres du serveur entrant seront utilisés.	
Nom d'utilisateur du serveur sortant	Nom d'utilisateur du serveur sortant	
Mot de passe du serveur sortant (uniquement au niveau de l'appareil)	Mot de passe du serveur sortant	
Le serveur sortant utilise SSL	Le serveur sortant utilise SSL	
Le serveur sortant utilise TLS	Le serveur sortant utilise TLS	

Le serveur sortant accepte tous les certificats	Le serveur sortant accepte tous les types de certificats
Signature	Une signature peut être jointe ici (Conseil : certains appareils exigent un formatage HTML pour la signature).
Notifier l'utilisateur lors de la réception d'un nouvel e-mail	Notification à l'utilisateur de la réception d'un nouveau courrier électronique

AE Gmail Exchange

Info : Cette configuration sera appliquée à l'application Gmail. Vous devez donc approuver et installer Gmail.

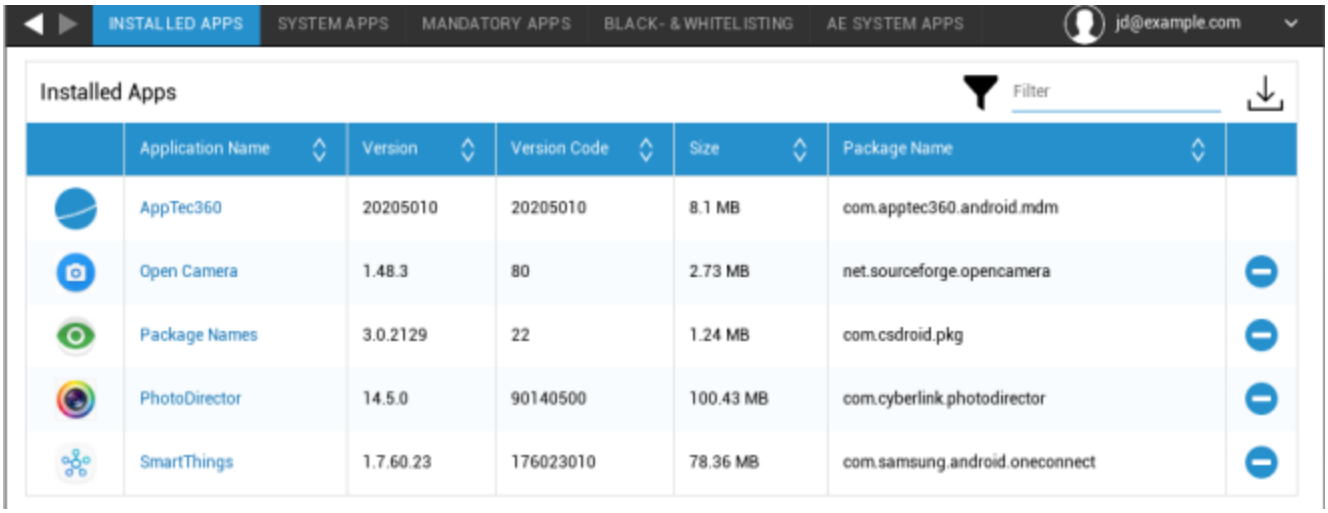
Adresse électronique	L'adresse électronique de l'utilisateur fourni Veuillez noter les "Placeholders", que vous pouvez utiliser pour travailler avec les informations d'identification et que vous ne devez pas modifier manuellement sur chaque appareil. En cliquant sur Afficher les espaces réservés, vous pouvez les afficher vous-même.
Nom d'hôte du serveur	Adresse de votre serveur Exchange
Nom de connexion	Le nom de connexion pour l'appareil de l'utilisateur final respectif, veuillez également noter les "Placeholders here".
Signature	Une signature peut être jointe (Remarque : certains appareils exigent un formatage HTML pour la signature).
Nombre de jours précédents à synchroniser	Nombre de jours déterminant le moment où les courriels sont synchronisés à nouveau
Identifiant de l'appareil	Identifiant EAS. Laissez ce champ vide si votre environnement ne l'exige pas.
Utilisez le protocole SSL (Secure Sockets Layer)	Utiliser une connexion SSL
Accepter tous les certificats	Tous les certificats sont acceptés. Veuillez sélectionner cette option si votre serveur Exchange utilise un certificat auto-signé.
Autoriser les comptes non gérés	Permet à l'utilisateur d'ajouter des comptes supplémentaires
Certificat de client	Télécharger le certificat client si votre serveur Exchange l'exige

Gestion des applications

Gestionnaire d’applications d’entreprise

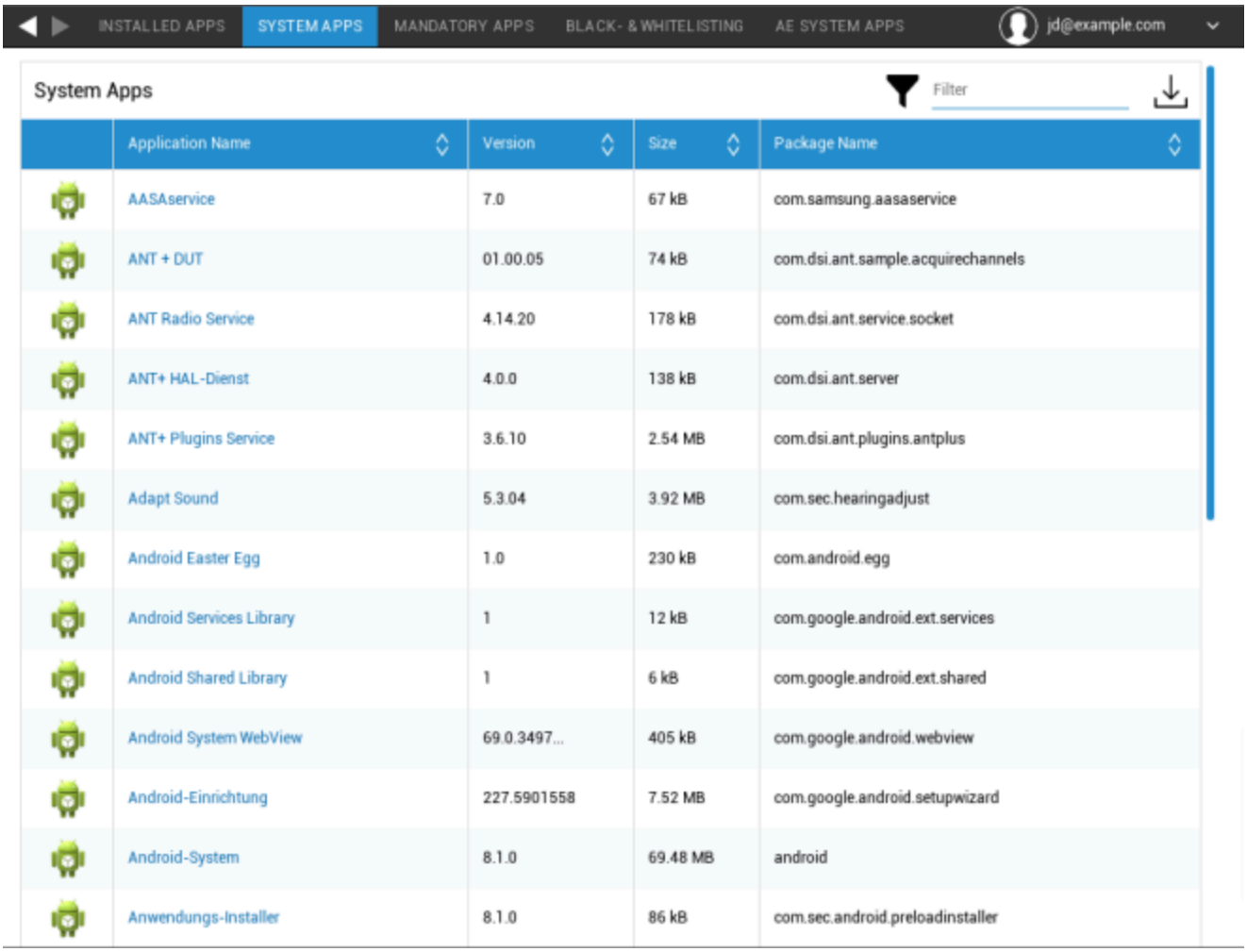
Applications installées (uniquement au niveau de l’appareil)

Toutes les applications actuellement installées sur l'appareil de l'utilisateur final s'affichent ici.


INSTALLED APPS
SYSTEM APPS
MANDATORY APPS
BLACK- & WHITELISTING
AE SYSTEM APPS
jd@example.com
Installed Apps
Filter
Application Name
Version
Version Code
Size
Package Name
AppTec360
20205010
20205010
8.1 MB
com.apptec360.android.mdm
Open Camera
1.48.3
80
2.73 MB
net.sourceforge.opencamera
Package Names
3.0.2129
22
1.24 MB
com.csdroid.pkg
PhotoDirector
14.5.0
90140500
100.43 MB
com.cyberlink.photodirector
SmartThings
1.7.60.23
176023010
78.36 MB
com.samsung.android.oneconnect

Apps système (uniquement au niveau de l’appareil)

Sous "System Apps", tous les systèmes préinstallés sont répertoriés avec leur nom et leur version.



Application Name	Version	Size	Package Name
AASAservice	7.0	67 kB	com.samsung.aasaservice
ANT + DUT	01.00.05	74 kB	com.dsi.ant.sample.acquirechannels
ANT Radio Service	4.14.20	178 kB	com.dsi.ant.service.socket
ANT+ HAL-Dienst	4.0.0	138 kB	com.dsi.ant.server
ANT+ Plugins Service	3.6.10	2.54 MB	com.dsi.ant.plugins.antplus
Adapt Sound	5.3.04	3.92 MB	com.sec.hearingadjust
Android Easter Egg	1.0	230 kB	com.android.egg
Android Services Library	1	12 kB	com.google.android.ext.services
Android Shared Library	1	6 kB	com.google.android.ext.shared
Android System WebView	69.0.3497...	405 kB	com.google.android.webview
Android-Einrichtung	227.5901558	7.52 MB	com.google.android.setupwizard
Android-System	8.1.0	69.48 MB	android
Anwendungs-Installer	8.1.0	86 kB	com.sec.android.preloadinstaller

Applications obligatoires

Dans la rubrique Applications obligatoires, vous pouvez définir les applications qui doivent être installées sur l'appareil. En fonction de votre configuration et de votre appareil, l'application sera installée automatiquement ou l'utilisateur sera invité à l'installer.

Sachez qu'il est recommandé d'utiliser Android Enterprise pour faciliter la gestion des applications.

Les scénarios sont énumérés ci-dessous :

Normal Play Store Apps

Les installations d'applications sur le Playstore nécessitent toujours une interaction avec l'utilisateur. En outre, un compte Google doit être configuré sur l'appareil.

Installation de l'application en interne

Sur les appareils Samsung, ces applications seront installées silencieusement. La seule exception est le conteneur, où l'utilisateur doit confirmer l'installation.

Dans tous les autres cas, l'utilisateur doit confirmer l'installation de l'application.

Android Enterprise Play Store Apps

Ces applications seront toujours installées silencieusement, sans interaction de la part de l'utilisateur.

Pour ajouter une application obligatoire, cliquez sur le "+" et sélectionnez l'application souhaitée dans la liste. Sachez que vous ne pouvez pas installer d'applications à partir de l'onglet "Google Play Store" si l'appareil est configuré avec Android Enterprise en tant que système entièrement géré ou en tant que conteneur.

Si vous utilisez Android Enterprise, sélectionnez les applications dans la section "AE Play Store". Pour rendre les applications disponibles ici, confirmez-les dans la boutique Google Enterprise Play en allant dans Paramètres généraux → AE Play Store → Play Store Apps.

Lorsqu'une application obligatoire est supprimée, elle est également désinstallée de l'appareil.

Vous pouvez cliquer sur le nom d'une application dans la liste des applications obligatoires et aller dans l'onglet "configuration" pour configurer une application. Cela nécessite l'utilisation d'Android Enterprise et l'application doit le prendre en charge. Les options disponibles dépendent donc de l'application sélectionnée.

Applications du système AE

Ici, vous pouvez activer les applications système pour les appareils Android Enterprise. N'oubliez pas que l'application spécifiée doit se trouver dans la mémoire du système, sinon rien ne se passe. 296

Restrictions et paramètres

Liste noire et liste blanche

Vous pouvez ici définir une liste noire ou une liste blanche. Toutes les applications figurant sur la liste noire seront bloquées. Toutes les applications qui ne figurent pas dans la liste blanche seront bloquées. Une liste noire vide ne bloque rien, tandis qu'une liste blanche vide bloque tout*

**Toutes les applications obligatoires et les applications de l'App Store d'entreprise seront automatiquement inscrites sur la liste blanche. Il n'est pas nécessaire de les ajouter manuellement*

En cliquant sur le "+", vous pouvez soit rechercher une application que vous souhaitez ajouter à votre liste noire ou blanche, soit saisir manuellement le nom d'un paquet.

Restrictions des applications système

Sous "Sys App Restrictions", vous pouvez, entre autres, bloquer les applications et services préinstallés.

Désactiver le navigateur	Désactiver le navigateur standard
Désactiver le calendrier	Désactiver le calendrier natif
Désactiver la calculatrice	Désactiver la calculatrice
Désactiver le navigateur Chrome	Désactiver le navigateur Chrome
Désactiver l'horloge	Désactiver l'horloge
Désactiver les contacts	Désactiver les contacts
Désactiver le numéroteur	Désactiver le numéroteur natif
Désactiver l'eMail	Désactiver le courrier électronique
Désactiver Exchange	Désactiver les comptes Exchange
Désactiver Facebook	Désactiver l'application Facebook
Désactiver la galerie	Désactiver l'application native de la galerie
Désactiver Gmail	Désactiver Gmail
Désactiver Google Livres	Désactiver Google Livres
Désactiver le kiosque Google Play	Désactiver le kiosque Google Play
Désactiver Google Maps	Désactiver Google Maps
Désactiver Google Music	Désactiver Google Music
Désactiver les films Google	Désactiver les films Google
Désactiver Google Play Store	Désactiver Google Play Store (App Store public)
Désactiver Google Plus	Désactiver Google Plus
Désactiver la recherche Google	Désactiver la recherche Google
Désactiver Google Talk / Google Hangouts	Désactiver Google Talk / Google Hangouts
Désactiver le lecteur de musique	Désactiver l'application native du lecteur de musique
Désactiver les paramètres	Désactiver les paramètres de l'appareil
Désactiver Sim Toolkit	Désactiver les services de Sim Toolkit
Désactiver les SMS / MMS	Désactiver les SMS / MMS
Désactiver Street View	Désactiver les services Street View
Désactiver Youtube	Désactiver Youtube

Applications Samsung

Sous "Samsung Apps", vous pouvez définir des paramètres et/ou des restrictions supplémentaires pour les appareils Samsung.

Désactiver AllShare Play / Samsung Link	Désactiver AllShare Play / Samsung Link
Désactiver ChatON	Désactiver ChatON
Désactiver le Game Hub	Désactiver le Game Hub
Désactiver le jeu en groupe	Désactiver le jeu en groupe
Désactiver l'aide	Désactiver l'aide de Samsung
Désactiver le KNOX	Désactiver le conteneur Samsung KNOX
Désactiver le mémo	Désactiver le mémo vocal
Désactiver mes fichiers	Désactiver mes fichiers
Désactiver le lecteur optique	Désactiver le lecteur optique
Désactiver Polaris Office	Désactiver Polaris Office
Désactiver le hub de lecture / Samsung Books	Désactiver le hub de lecture / Samsung Books
Désactiver le S Memo	Désactiver l'application Samsung Memo
Désactiver le traducteur S	Désactiver l'application Samsung Translator
Désactiver la voix S	Désactiver l'assistant vocal
Désactiver les applications Samsung	Désactiver le Samsung App Store
Désactiver le Samsung Hub	Désactiver les magasins de divertissement Samsung
Désactiver le lecteur vidéo	Désactiver le lecteur vidéo
Désactiver l'enregistreur vocal	Désactiver l'enregistreur vocal
Désactiver WatchON	Désactiver WatchON (simule une télécommande)

Applications Huawei

Sous "Huawei Apps", vous pouvez définir des paramètres et/ou des restrictions supplémentaires sur l'appareil Huawei.

Désactiver DLNA	Désactiver DLNA
Désactiver l'installateur d'applications	Désactiver l'installateur d'applications
Désactiver le gestionnaire de fichiers	Désactiver le gestionnaire de fichiers
Désactiver le gestionnaire de sauvegarde	Désactiver le gestionnaire de sauvegarde
Désactiver la mise à jour du système	Désactiver la mise à jour du système
Désactiver la boîte à outils	Désactiver la boîte à outils
Désactiver la météo	Désactiver la météo
Désactiver la radio FM	Désactiver la radio FM

Paramètres de gestion des applications

Vous pouvez définir ici le comportement de mise à jour de InHouse Apps.

La fréquence de vérification des mises à jour définit la fréquence à laquelle l'application AppTec360 recherche des mises à jour pour les applications InHouse. Dès qu'une nouvelle version est détectée, elle est téléchargée et installée.

Seuil Wi-Fi définit si le téléchargement doit être limité aux connexions Wi-Fi si l'application est plus grande que le seuil configuré. Si le est plus petit ou si vous ne définissez pas de seuil, l'application sera téléchargée en Wi-Fi et dans un réseau cellulaire.

App Store d’entreprise

Veuillez noter que les applications ajoutées ici (Enterprise App Store) ne seront PAS installées automatiquement sur le(s) appareil(s). L'utilisateur doit ouvrir l'Enterprise App Store sur l'appareil et installer l'application manuellement.

Si vous souhaitez installer automatiquement des applications sur l'appareil, allez dans "Gestion des applications" → "Gestion des applications d'entreprise" → "Apps obligatoires" et ajoutez les applications souhaitées.

À ce stade, vous pouvez distribuer des applications facultatives à vos utilisateurs.

Playstore

Cliquez sur le "+" pour ajouter une application Play Store à la boutique. Si vous utilisez Android Enterprise, allez dans "App Management Enterprise Play Store". Sachez également qu'un compte Google doit être configuré sur → l'appareil pour installer les applications définies ici.

En interne

Sous le point "In-House", vous pouvez télécharger et distribuer des applications développées en interne.

Cliquez sur le "+" pour ajouter une application InHouse à la boutique d'applications de l'entreprise, qui pourra ensuite être installée par l'utilisateur. Dans ce dialogue, vous pouvez également télécharger une nouvelle application InHouse.

Entreprise Play Store

Veuillez noter que les applications ajoutées ici (Enterprise Play Store) ne seront PAS installées automatiquement sur le(s) appareil(s). L'utilisateur doit ouvrir le Play Store sur son appareil et installer l'application manuellement.

Si vous souhaitez installer automatiquement des applications sur l'appareil, allez dans "Gestion des applications" → "Gestion des applications d'entreprise" → "Apps obligatoires" et ajoutez les applications souhaitées.

À ce stade, vous pouvez distribuer des applications facultatives à vos utilisateurs.

Ici, vous pouvez ajouter des applications à la boutique Android Enterprise Playstore. Veuillez noter que vous devez approuver les applications dans Paramètres généraux → AE Play Store → Play Store Apps. Ces applications seront ajoutées au Google Play Store normal.

Sachez également que vous devez d'abord définir une disposition avec les applications dans Paramètres généraux → Gestion des applications → AE Play Store → Disposition du magasin.

Les applications doivent se trouver dans une présentation avant que vous puissiez les ajouter à la boutique.

Mode kiosque et lanceur

Mode kiosque

Le mode kiosque vous permet de prédéfinir une application ou une URL. Il sera alors exclusivement possible d'exécuter/de visiter cette application et/ou cette URL.

De même, divers boutons matériels peuvent être désactivés dans le mode kiosque.

Démarrage automatique	Lance automatiquement le mode kiosque dès que le profil atteint l'appareil de l'utilisateur final.
Mode kiosque programmé ?	Vous pouvez planifier une durée pour le mode kiosque, qui commencera et s'achèvera automatiquement à l'heure que vous aurez fixée.
Heure de début	Heure de début
Temps en minutes	Temps en minutes après lequel le mode kiosque doit se terminer à nouveau

Type d'application

Application unique	Si vous souhaitez démarrer l'application en mode kiosque, sélectionnez "Package" sous "Type d'application"
Application kiosque	Cliquez ici pour sélectionner une application qui doit être lancée en mode kiosque. Vous trouverez l'aperçu habituel de la gestion des applications Vous pouvez choisir entre "Google Play Store", "Android In-House Apps" et "Packagename"

Type d'application	

URL		Si vous souhaitez lancer une URL en mode kiosque, sélectionnez "URL" sous "Type d'application" Définissez ensuite l'adresse URL souhaitée
	Effacer le navigateur après l'inactivité	Vous pouvez définir ici un intervalle de temps en minutes, après lequel le mode kiosque doit être relancé.
	Effacer le cache et les cookies	Si vous activez cette fonction, après un redémarrage du mode kiosque, le cache Web (cookies et images en cache) sera effacé.
	Politique de la même origine	Si cette fonction est activée, l'utilisateur ne peut naviguer que sur les sous-pages d'un URL défini. Par exemple, vous avez défini l'URL suivante: www.mypage.com Ensuite, l'utilisateur peut surfer sur : www.mypage.com/subpage
	URL sur liste blanche	Ici, vous pouvez maintenir une liste blanche, tous ces URL sont autorisés. Maximum 1 URL par ligne Un URL doit commencer par http:/ ou https://.
	URL sur liste noire	Ici, vous pouvez maintenir une liste noire, tous ces URL ne sont pas autorisés. Maximum 1 URL par ligne Un URL doit commencer par http:/ ou https://
	Orientation de l'écran	Ce paramètre concerne les réglages de l'écran Automatique = automatique Portrait = format vertical Paysage = mode paysage

Multi App		Si vous sélectionnez le mode kiosque "Multi App", l'utilisation du lanceur AppTec360 sera obligatoire.
	Applications	Application : Sélectionnez une application Playstore ou une application interne comme application kiosque. Il est également possible de saisir un nom de pack. L'application kiosque sélectionnée doit être installée sur l'appareil. N'oubliez pas de rendre l'application kiosque obligatoire. Raccourci sur l'écran d'accueil : Si ce paramètre est réglé sur "On", un raccourci sera créé sur l'écran d'accueil. S'il est réglé sur "Off", l'application s'affichera toujours dans la liste des applications.

Mot de passe de sortie activé	Si vous activez cette fonction, l'utilisateur peut quitter le mode kiosque avec un mot de passe que vous avez prédéfini.
Quitter le mot de passe	Il s'agit du mot de passe que vous avez prédéfini.
Réduction automatique de la barre d'état	Si cette option est activée, la barre d'état sera automatiquement mise en surbrillance. Avec cette option, les utilisateurs peuvent voir les informations de la barre d'état, mais ne peuvent pas accéder à ses fonctions.
Désactiver la barre d'état	La barre d'état contient des notifications, des raccourcis et des informations. Disponible uniquement pour les appareils Samsung équipés de KNOX 1.0 ou supérieur.
Désactiver les touches de volume	Désactiver les touches de volume (disponible uniquement sur les appareils Samsung équipés de KNOX 1.0 ou supérieur)
Désactiver l'interrupteur marche/arrêt	Désactiver l'interrupteur marche/arrêt (disponible uniquement sur les appareils Samsung équipés de KNOX 1.0 ou supérieur)
Désactiver le bouton d'accueil	Désactiver le bouton Home. Si cette fonction a été activée, le mode kiosque ne peut être interrompu que dans la console AppTec360. (disponible uniquement sur les appareils Samsung équipés de KNOX 1.0 ou supérieur)
Désactiver la barre de navigation	Cette option vous permet de désactiver la barre de navigation (Retour / Menu). Si cette fonction a été activée, le mode kiosque ne peut être interrompu que dans la console AppTec360. (disponible uniquement sur les appareils Samsung équipés de KNOX 1.0 ou supérieur)

Paramètres de mise à jour de l'application	
Autoriser les mises à jour des applications	Les utilisateurs seront invités à effectuer des mises à jour d'applications même lorsque le mode kiosque est activé. Sur les appareils équipés de Samsung KNOX, les applications seront mises à jour silencieusement.
Fenêtre de mise à jour	Définissez un intervalle dans lequel les utilisateurs seront invités à installer les mises à jour de l'application.

TeamViewer	
Activer l'accès sans surveillance	Si cette option est activée, les administrateurs peuvent contrôler l'appareil à distance sans interaction avec l'utilisateur. L'application TeamViewer Host doit

	être installée sur l'appareil.

AppTec360 Launcher

Activer le lanceur AppTec360	Activé : Active le lanceur AppTec360. L'utilisateur doit le définir comme lanceur par défaut une fois. Note : Si le mode kiosque est activé et que le mode kiosque est réglé sur "Multi App", l'utilisation du lanceur AppTec360 sera imposée.
Grandes icônes	Allumé : Affiche une version plus grande des icônes des applications dans le lanceur.
Cacher l'icône de l'application AppTec360	Activé : Masque complètement l'application AppTec360
Cacher l'icône de la boutique AppTec360	Activé : Masque complètement l'AppStore AppTec360 Enterprise

Paramètres AppTec360

Activer l'application AppTec360 Settings	L'application AppTec360 Settings permet de contrôler les connexions WiFi et Bluetooth.
Activer les paramètres dans les applications multiples Mode kiosque	Si cette option est activée, les utilisateurs peuvent accéder à l'application de paramétrage AppTec360 lorsque le mode kiosque multi-applications est actif.

Télécommande

Splashtop

Affiche l'état actuel de la configuration du Splashtop. Vous verrez ici les étapes à suivre pour accéder à distance à l'appareil via Splashtop. Vous devez également saisir votre code de déploiement que vous pouvez obtenir sur le site Web de Splashtop. Le code de déploiement est nécessaire pour se connecter à l'appareil.

Teamviewer

Affiche l'état actuel de la configuration de Teamviewer. Vous verrez ici les étapes à suivre pour accéder à distance à l'appareil via Teamviewer.

Gestion du contenu

Boîte de contenu

Ici, vous pouvez activer la boîte de contenu pour cet appareil. Une fois activée, l'application Contentbox sera installée sur l'appareil.

Navigateur sécurisé

Vous pouvez ici activer le navigateur sécurisé pour cet appareil. Une fois activée, l'application Secure Browser sera installée sur l'appareil. Ce navigateur peut être configuré pour offrir un navigateur Web sur l'appareil qui est limité à vos besoins.

Demande de mot de passe	Exiger de l'utilisateur qu'il définisse et utilise un mot de passe pour accéder au navigateur.
Restreindre les téléchargements / Ouvrir en	Bloque les téléchargements à partir de sites web
Limiter les téléchargements	Limite les téléchargements à certaines URL. N'indiquez pas d'URL pour bloquer complètement le téléchargement.
Autoriser la copie	Permettre de copier, de couper ou de partager du texte à l'intérieur des pages web.
Autoriser la capture d'écran	Permettre la réalisation de captures d'écran.
Fréquence de nettoyage des données	Sélectionnez la fréquence à laquelle TOUTES les données de l'utilisateur (historique, cache, etc.) doivent être automatiquement supprimées.
Signets d'entreprise	Les signets s'affichent dans le dossier "Signets de l'entreprise" des signets du navigateur. Ils ne sont pas modifiables par l'utilisateur.
Masquer la barre d'adresse	Masque la barre d'adresse afin que l'utilisateur ne voie pas l'URL qu'il visite.
Liste blanche dans le navigateur (sans passerelle universelle)	Permet l'établissement d'une liste blanche d'URL côté client. - Les signets de l'entreprise sont toujours mis sur liste blanche - Prise en charge de 100 URL uniquement - Veuillez utiliser la passerelle universelle pour une mise sur liste noire et blanche illimitée.
Liste noire et liste blanche basées sur la passerelle	Le blacklistage a les exigences suivantes : - Une passerelle universelle AppTec360 opérationnelle ("Paramètres généraux" → "Passerelle universelle") - Une configuration VPN opérationnelle avec un serveur DNS spécifié ("Paramètres généraux" → "Passerelle universelle" → "Paramètres VPN") - Une configuration de liste noire ("Paramètres généraux" →

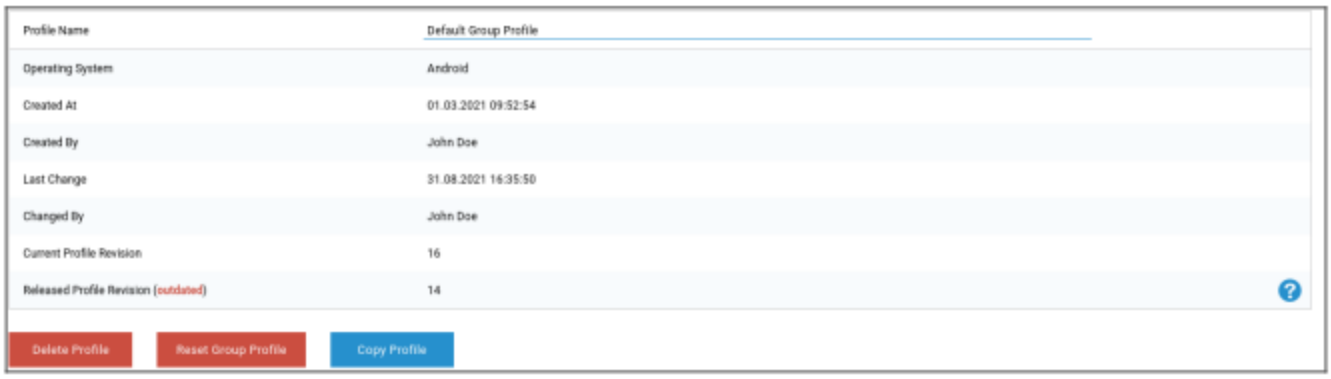
	"Passerelle universelle" → "Liste noire de domaines") - Une connexion VPN valide dans le profil ("Gestion des connexions" → "VPN").

Configuration PC Windows 10

Général

Aperçu du profil du groupe (uniquement au niveau du groupe)

Lorsque vous ouvrez un profil de groupe, vous obtenez un aperçu rapide du profil.



Nom du profil	Nom du profil (peut être modifié ici)
Système d'exploitation	Système d'exploitation pour lequel le profil est établi
Créé à	Moment de la création
Créé par	Le créateur du profil
Dernier changement	Date de la dernière modification du profil
Modifié par	Compte ayant effectué les dernières modifications
Révision du profil actuel	Révision de l'état du profil sauvegardé
Révision du profil validé	Révision du profil attribué ("Attribuer maintenant"). Si l'étiquette affiche "(obsolète)" derrière le texte, cela signifie que vous avez enregistré le profil mais que vous ne l'avez pas encore attribué.

Aperçu de l’appareil (uniquement au niveau de l’appareil)

La vue d'ensemble de l'appareil, qui contient les éléments suivants :

Nom du PC	Nom du PC
Client	Les appareils de type Windows
Dernier lieu connu	La latitude et la longitude de la dernière localisation connue de l'appareil
Apps obligatoires assignées	Nombre d'applications obligatoires attribuées à l'appareil
PC UID	UID du PC
Édition OS	Affiche votre édition Windows
Version OS	Version de Windows actuellement installée
Construction du système d'exploitation	Version actuelle de Windows
Système d'exploitation	Système d'exploitation actuellement installé
Numéro de série	Numéro de série de l'appareil
Propriété des appareils	Le type de propriété configuré
Type d'appareil	Le type d'appareil
Enraciné	Indique si l'appareil est enraciné
Conforme à la loi	Indique si l'appareil est conforme
Dernière visite	Date et heure auxquelles des modifications ont été apportées au profil
Affectation des utilisateurs	Affiche l'utilisateur ou le groupe auquel ce dispositif est actuellement affecté. Vous pouvez déplacer le dispositif en sélectionnant un autre utilisateur ou groupe dans la liste déroulante.

Paramètres

Autoriser la mise à jour automatique	Autoriser ou interdire les mises à jour automatiques du système d'exploitation.

Révision de la configuration (uniquement au niveau de l’appareil)

Vous obtiendrez ici une vue d'ensemble du profil de groupe attribué à l'appareil.

Si vous cliquez sur le profil du groupe, vous accédez directement au profil et vous pouvez effectuer des réglages.

Le symbole vous permet de rétablir les paramètres du profil de groupe pour les applications attribuées.

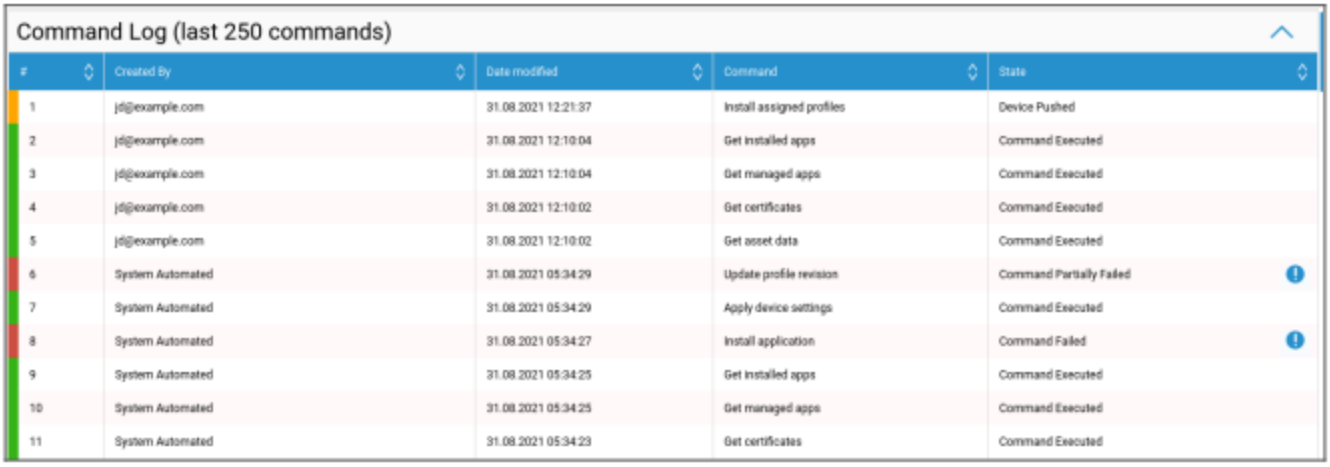
Le symbole permet de réinitialiser le profil de l'appareil pour qu'il ne comporte aucun paramètre.

La mention "Révision plus récente disponible" indique que le profil de groupe a été modifié et enregistré, mais qu'il n'a pas été attribué. Le profil de groupe doit être attribué avec "Attribuer maintenant" au niveau du groupe pour appliquer les changements aux appareils.

Journal de l’appareil (uniquement au niveau de l’appareil)

Journal des commandes

Vous pouvez voir ici quelles commandes ont été émises pour l'appareil et quel est leur état.



Les commandes créées par le "système automatisé" sont automatiquement créées par le système.

États possibles de la commande

Dispositif poussé	Une requête "push" a été envoyée au service "push" (par exemple APNS) pour demander à l'appareil de se reconnecter au serveur EMM.
Commande créée	La commande a été créée dans le système.
Commande envoyée	La commande a été envoyée à l'appareil après qu'il se soit connecté au serveur.
Commande exécutée	La commande a été exécutée avec succès.
Échec de la commande	La commande a échoué. *
Échec partiel de la commande	Selon le système d'exploitation de l'appareil, certaines commandes peuvent être regroupées. Dans ce cas, certaines parties de ce groupe de commande ont échoué. *
Commande exécutée, échec éventuel	La commande a été exécutée, mais peut-être qu'elle ne l'a pas été.
Commandement repoussé	La commande a été repoussée par un utilisateur.
Mise au rebut	La commande a été supprimée. Par exemple, parce qu'elle a été remplacée par une autre commande ou parce que l'appareil a été réenrôlé et que les anciennes commandes ont été supprimées.

*Si le message est accompagné d'un point d'exclamation, vous pouvez obtenir plus d'informations en survolant l'icône avec votre curseur.

Gestion des actifs (uniquement au niveau de l’appareil)

Informations sur l’appareil

Fabricant	Fabricant de l'appareil
Modèle	Modèle d'appareil
Numéro de modèle	Numéro de modèle
Système d'exploitation	Système d'exploitation
Version OS	Version du système d'exploitation
Numéro de série	Numéro de série
ExchangeID	ExchangeID
Total RAM	Total RAM
Résolution de l'écran	Résolution de l'écran
Langue du téléphone	Langue de l'appareil
Version du micrologiciel	Version du micrologiciel
Version du client DM	Version du client de gestion des appareils
Version du matériel	Version du matériel de l'appareil
Architecture de l'unité centrale	Architecture du CPU (type de processeur)

Cellulaire

Réseau de l'opérateur SIM	Réseau de transporteurs
Numéro de téléphone	Numéro de téléphone
État de l'itinérance	État de l'itinérance
IMEI	IMEI
IMSI	IMSI
Firmware du modem	Firmware du modem

Informations sur la synchronisation

Connexion instantanée au DM	L'appareil doit immédiatement établir une connexion avec AppTec.
Délai de réessai initial	Délai de réessai initial pour cette première connexion
Tentatives de connexion	Nombre de tentatives de nouvelles connexions, après une déconnexion du gestionnaire de connexions ou une erreur au niveau de WinInet.
Durée maximale de sommeil	Temps de sommeil maximum après une erreur d'envoi de paquet
Premiers essais de synchronisation	Délai pour la première étape après l'inscription
Premier intervalle de réessai	Délai pour la première étape après l'inscription
Secondes tentatives de synchronisation	Délai pour la deuxième étape après l'enrôlement
Intervalle de réessai de deux secondes	Délai pour la deuxième étape après l'enrôlement
Tentatives de synchronisation régulières	Délai pour les étapes supplémentaires après l'inscription
Intervalle de réessai régulier	Délai pour les étapes supplémentaires après l'inscription

Gestion de la sécurité

Antivol (uniquement au niveau de l’appareil)

Informations GPS (uniquement au niveau de l’appareil)

Vous pouvez ici déterminer l'emplacement actuel/dernier emplacement de l'appareil. La localisation peut être protégée par un ou même deux mots de passe - Voir : "Réglages généraux" > "Confidentialité" > "Accès GPS"

Paramètres GPS

Activer le suivi GPS	Permet une synchronisation régulière des informations GPS.
Intervalle de suivi	Définissez l'intervalle de synchronisation des informations GPS.

Configuration de la sécurité

Code d’accès

Longueur minimale du mot de passe	Longueur minimale du mot de passe	
Composition du mot de passe	Spécifie le nombre de caractères spécifiques que le mot de passe doit contenir Ils sont composés de lettres majuscules, de lettres minuscules, de chiffres et de symboles spéciaux.	
Qualité du mot de passe	Vous pouvez ici définir la qualité du mot de passe	
	Alphanumérique	Uniquement des chiffres et des lettres
	Numérique	Seulement des chiffres
	Numérique ou alphanumérique	Chiffres ou chiffres et lettres
Verrouillage du temps d'inactivité maximum	Nombre de minutes d'inactivité de l'utilisateur sur l'appareil, après quoi l'appareil sera verrouillé. L'utilisateur doit déverrouiller l'appareil après ce délai en saisissant le mot de passe de l'appareil.	
Expiration du mot de passe	Définissez le délai dans lequel un nouveau mot de passe doit être défini.	
Restriction de l'historique des mots de passe	Nombre de mots de passe utilisés précédemment, qui ne sont pas autorisés	
Nombre maximal de tentatives d'échec du mot de passe	Nombre de fois où le mot de passe peut être saisi de manière incorrecte, avant qu'un effacement complet de l'appareil ne soit effectué.	

Antivirus

Paramètres antivirus - Configuration de l'analyse	
Type d'analyse	Permet de choisir entre une analyse rapide et une analyse complète.
Définir le début du balayage	Sélectionne l'heure de la journée à laquelle Windows Defender commencera l'analyse.
Fréquence de balayage	Sélectionne le jour où l'analyse de Windows Defender doit être exécutée
Fréquence de mise à jour de la signature	Spécifie l'intervalle en heures qui sera utilisé pour vérifier les signatures.

Configurer le type de fichiers à scanner	
Permettre l'analyse des fichiers d'archives	Autoriser ou non l'analyse des archives (telles que .zip) lors de l'accès.
Autoriser l'analyse des scripts	Permet ou désactive la fonctionnalité d'analyse des scripts de Windows Defender.
Permettre l'analyse des courriels	Autoriser ou interdire l'analyse des courriels.
Autoriser l'analyse des fichiers du réseau	Autoriser ou interdire l'analyse des fichiers du réseau.
Permettre l'analyse complète des lecteurs réseau mappés	Autoriser ou interdire l'analyse des lecteurs réseau mappés (activé uniquement lorsque l'analyse complète est activée).
Contrôle du balayage bidirectionnel	Contrôle les ensembles de fichiers à surveiller.
Permettre l'analyse complète des disques amovibles	Autoriser ou interdire l'analyse complète des lecteurs amovibles. Uniquement lorsque l'analyse complète est lancée.

Type de fichiers à exclure de l'analyse	
Ignorer les types de fichiers à numériser	Définissez un ensemble de types d'extensions de fichiers. Chaque extension de fichier pour chaque champ.
Ignorer les chemins d'accès aux répertoires	Définissez un ensemble de chemins d'accès aux répertoires afin de ne pas les analyser. Un chemin par champ. Exemples : "C:\NExemple", "C:\NWindows" ou "C:\NUsers".
Exclure les processus de l'analyse	Excluez des analyses antivirus de Microsoft Defender les fichiers qui ont été ouverts par des processus spécifiques. . Un chemin par champ. Exemples : "C:\NmyFile.exe", "C:\NWindows\NmyProcess.exe", "C:\NmyScript.bat", "C:\NMyFile.exe", "C:\NWindows\NProcess.exe".

Paramètres supplémentaires	
Permettre un contrôle en temps réel	Autoriser ou interdire la fonctionnalité de surveillance en temps réel de Windows Defender
Permettre le suivi des comportements	Autoriser ou interdire la fonctionnalité de surveillance du comportement de Windows
Permettre la protection du nuage	Autorisez ou non Windows Defender à envoyer des informations à Microsoft sur les problèmes qu'il détecte. Microsoft analysera ces informations, en apprendra davantage sur le problème affectant l'appareil et proposera des solutions améliorées.
	Comportement lors de l'envoi d'échantillons
Autoriser la protection IOAV de Windows Defender	Autoriser ou refuser la protection IOAV de Windows Defender
Autoriser l'accès à l'interface utilisateur de Defenders "Protection de l'accès".	
Facteur de charge moyen de l'unité centrale	Représente le facteur de charge moyen du processeur pour l'analyse de Windows Defender (en pourcentage).

Traitement des logiciels malveillants	
Faible gravité	Vous pouvez définir, pour chaque niveau de gravité, la manière dont l'appareil traite les logiciels malveillants. Les options disponibles sont les suivantes : • Nettoyer • Quarantaine • Enlever • Permettre • Défini par l'utilisateur • Bloc
Gravité modérée	
Gravité élevée	
Gravité sévère	
Jours de conservation des logiciels malveillants nettoyés	Période de temps en jours pendant laquelle les fichiers/éléments en quarantaine seront stockés sur le système. La valeur par défaut est 0, ce qui permet de conserver les éléments en quarantaine et de ne pas les supprimer automatiquement. La valeur maximale est de 90.

Centre de sécurité

Centre de sécurité Windows - Paramètres de sécurité Windows	
Désactiver l'interface utilisateur de protection contre les virus et les menaces	
Hide Ransomware Data Recovery UI (en anglais)	
Désactiver l'interface utilisateur de protection des comptes	
Désactiver le pare-feu et la protection du réseau	
Désactiver l'interface de contrôle des applications et du navigateur	
Interdire les modifications de la protection contre les exploits	Interdire à l'utilisateur de modifier les paramètres de protection contre les exploits
Désactiver l'interface utilisateur de sécurité des appareils	
Masquer le dépannage du TPM	Masquer les paramètres de dépannage du TPM
Désactiver le bouton Clear TPM	
Désactiver l'interface utilisateur relative aux performances et à l'état de santé de l'appareil	
Désactiver l'interface utilisateur des options familiales	

Personnalisez les toasts	
Activer les informations d'assistance personnalisées	Permet d'afficher les coordonnées de l'assistance personnalisée de votre entreprise en bas à droite de l'application du centre de sécurité.
Adresse électronique	Définir l'adresse électronique de l'entreprise
Nom de l'entreprise	Définir le nom de l'entreprise
Téléphone de l'entreprise	Définir le téléphone de l'entreprise
URL d'aide	Définir l'URL d'aide de l'entreprise

Paramètres supplémentaires	
Désactiver les notifications	Désactivez l'affichage des notifications du Centre de sécurité Windows Defender.
Cacher les recommandations de mise à jour du micrologiciel du TPM	Masquer la recommandation de mettre à jour le microprogramme TPM lorsqu'un microprogramme vulnérable est détecté.
Afficher le nom de l'entreprise et les options de contact	Affichez le nom de votre entreprise et les options de contact dans une carte de contact affichée dans le Centre de sécurité Windows Defender.
Masquer Secure Boot	Masquer la zone d'amorçage de sécurité.
Masquer le contrôle de la zone de notification de sécurité	Masquer le contrôle de la zone de notification de Windows Security.

Configuration du pare-feu

Configuration du pare-feu - Paramètres généraux	
Ignorer l'authentification définie	Ignorer l'ensemble du jeu d'authentification s'il ne prend pas en charge toutes les suites d'authentification spécifiées dans le jeu.
Type de mise en file d'attente des paquets	Spécifie comment la mise à l'échelle du logiciel côté réception est activée à la fois pour la réception cryptée et l'effacement du chemin d'acheminement pour le scénario de passerelle de tunnel IPsec.
Désactiver le filtrage FTP avec état	S'il est désactivé, il n'effectuera pas de filtrage du protocole de transfert de fichiers (FTP) avec état pour autoriser les connexions secondaires.
Temps d'inactivité de l'association de sécurité	Ce champ configure le temps d'inactivité de l'association de sécurité, en secondes. Les associations de sécurité sont supprimées après l'absence de trafic réseau pendant la période spécifiée.
Encodage de la clé prépartagée	Définir l'encodage de la clé prépartagée
Exceptions IPSec	Configurer les exceptions au protocole Internet
Vérification de la liste de révocation des certificats	

Profils de pare-feu (profil de domaine / profil privé / profil public)	
Activer le pare-feu pour ce profil	
Désactiver les notifications	Désactiver l'affichage d'une notification à l'utilisateur lorsqu'une application est bloquée à l'écoute sur un port.
Bloquer les réponses unicast aux broadcasts multicast	
Appliquer les règles de pare-feu des applications autorisées	Si elle n'est pas appliquée, les règles de pare-feu des applications autorisées dans le magasin local sont ignorées et ne sont pas appliquées.
Appliquer les règles globales de pare-feu des ports	S'il n'est pas appliqué, les règles de pare-feu des ports globaux dans la base de données locale sont ignorées et ne sont pas appliquées. Le paramètre n'a de sens que s'il est défini ou énuméré dans le magasin de stratégies de groupe ou s'il est énuméré à partir du magasin GroupPolicyRSoPStore.
Appliquer les règles du pare-feu	Si elle n'est pas appliquée, les règles de pare-feu du magasin local sont ignorées et ne sont pas appliquées.
Appliquer les règles de sécurité des connexions	S'il n'est pas appliqué, les règles de sécurité des connexions du magasin local sont ignorées et ne sont pas appliquées.
Action de sortie par défaut	L'action que le pare-feu effectue par défaut sur les connexions sortantes.
Action de réception par défaut	L'action que le pare-feu effectue par défaut sur les connexions entrantes.
Désactiver le mode furtif	Le mode furtif est un mécanisme du pare-feu Windows qui permet d'empêcher les utilisateurs malveillants de découvrir des informations sur les ordinateurs du réseau et les services qu'ils exécutent.
Désactiver l'empêchement de répondre au trafic non sollicité	Si elles sont désactivées, les règles du mode furtif du pare-feu ne doivent pas empêcher l'ordinateur hôte de répondre au trafic réseau non sollicité si ce trafic est sécurisé par IPsec.

Règles de pare-feu

Règles de pare-feu	
Nom	Nom de la règle
Description	Description de la règle
Action	Indiquez si cette règle bloque le trafic ou l'autorise. Veuillez noter que l'option Bloquer peut également bloquer le trafic (en fonction du reste de la configuration) entre le serveur MDM et l'appareil.
Direction	
Activer la traversée des frontières (disponible uniquement lorsque la **direction** est définie sur le **trafic entrant)**	Indique que le trafic entrant spécifique est autorisé à traverser les NAT et d'autres périphériques à l'aide de la technologie de tunneling Teredo.

Programmes et services	
Définir les applications, toutes les autres	Si cette option n'est pas activée, toutes les demandes seront prises en compte.
Nom de la famille du paquet	Nom de la famille de paquets à laquelle la règle s'appliquera.
Chemin d'accès au fichier de l'application	L'application complète telle que C:\NWindows\NSystem\NNNotepad.exe à laquelle la règle s'appliquera.
Nom binaire entièrement qualifié	Le nom binaire entièrement qualifié auquel la règle s'appliquera. Un FQBN est une chaîne de caractères de la forme suivante : {Publisher\Product\Filename,Version}
Nom du service	Saisissez le nom d'un service (par exemple "EventLog"). Vous pouvez obtenir une liste de noms de services avec Powershell en exécutant la commande "Get-Service".

Protocoles et ports				
Protocole	Le protocole utilisé par la règle.			
	Valeurs disponibles : - Tous - Sur mesure - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - IPv6-Route - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - IPv6-Opts - VRRP - PGM - L2TP	Lorsqu'il est réglé sur Personnalisé	Insérez un numéro de protocole entre 0 et 255	Le numéro de protocole
		Lorsqu'il s'agit de TCP ou d'UDP	Spécifiez les ports locaux, tous seront utilisés dans le cas contraire.	Ports locaux que la règle utilisera, les ports de plage sont également autorisés.
			Port local	Un seul port ou une série de ports. Par exemple, 100-120, 200, 300-320.
			Spécifiez les ports distants, tous seront utilisés dans le cas contraire.	Ports distants que la règle utilisera, les ports de la plage sont également autorisés.
			Port à distance	Un seul port ou une série de ports. Par exemple, 100-120, 200, 300-320.

Champ d'application	
Spécifiez les adresses IP locales, sinon n'importe quelle adresse IP	Ensemble d'adresses IP locales, il peut également s'agir d'une série d'adresses IP séparées par des -.
Adresse IP locale	Ensemble d'adresses IP individuelles ou série d'adresses IP séparées par des -.
Spécifiez les adresses IP distantes, sinon n'importe quelle adresse IP distante.	Spécifiez un ensemble d'adresses IP distantes ; il peut également s'agir d'une série d'adresses IP séparées par des "-".
Adresse IP distante	Spécifiez des adresses IP uniques ou une série d'adresses IP.
Jetons	Les jetons qui peuvent être définis avec les adresses distantes. Les tokens Intranet, RmtIntranet et Ply2Renders sont pris en charge dans Windows 10, version 1809 et ultérieure.

Paramètres avancés	
Spécifiez les profils, sinon tous seront utilisés	Si cette option est désactivée, tous les profils seront utilisés.
Domaine	Profil du domaine
Privé	Profil privé
Public	Profil public
Spécifiez les interfaces, toutes seront utilisées dans le cas contraire	Si elle est désactivée, toutes les interfaces seront utilisées.
Réseau local	Interface de réseau local
Accès à distance	Interface d'accès à distance
Sans fil	Interface sans fil

Directeurs d'école locaux	
Ajouter des utilisateurs locaux autorisés	Permettre d'ajouter une liste d'utilisateurs locaux qui utiliseront cette règle
Utilisateurs autorisés	Liste des utilisateurs locaux autorisés pour cette règle. L'utilisateur doit être au format SDDL (Security Description Definition Language), par exemple PC_NAME\USERNAME. Ce champ ne doit pas être rempli si un nom de service est défini pour utiliser cette règle.

Paramètres de restriction

Fonctionnalité de l’appareil

Autoriser la carte SD	Permettre l'utilisation d'une carte SD
Autoriser la caméra	Permettre l'utilisation de l'appareil photo
Autoriser le service de localisation	Autoriser le service de localisation de l'appareil
Autoriser le Sideloading d'applications	Autoriser l'installation d'applications à partir de sources inconnues
Autoriser le mode développeur	Permet le mode développeur
Autoriser l'itinérance des données cellulaires	Autoriser l'itinérance des données cellulaires
Autoriser Cortana	Autoriser l'assistant vocal Cortana
Permettre à la recherche d'utiliser la localisation	Permettre à la recherche d'utiliser la localisation
Autoriser l'ajout d'un compte de messagerie non Microsoft	Indiquez si l'utilisateur est autorisé à ajouter des comptes de messagerie non MSA.
Autoriser la connexion au compte Microsoft	Indiquez si vous autorisez l'utilisation du compte MSA pour l'authentification et les services de connexion non liés au courrier électronique.
Autoriser la synchronisation de mes paramètres	Permet de synchroniser les paramètres sur l'ensemble de l'appareil
Noms de domaine protégés par l'entreprise	Spécifie les noms de domaine de l'entreprise séparés par des " ;".
Autoriser l'utilisateur à désactiver la	Permet à l'utilisateur de désactiver la restauration du système. **ATTENTION !**

restauration du système	Cette fonction ne doit être utilisée que sur des appareils appartenant à l'entreprise ou à l'organisation ou fournis par elle, ou sur un appareil appartenant à l'utilisateur, lorsque ce dernier accepte que l'appareil soit entièrement géré par l'entreprise. Si vous désactivez ce paramètre de stratégie, la restauration du système est désactivée et l'assistant de restauration du système n'est pas accessible. L'option permettant de configurer la restauration du système ou de créer un point de restauration via la protection du système est également désactivée.
Autoriser la désinscription d'un utilisateur	Permet à l'utilisateur de retirer la partie entreprise de l'appareil et donc de se déconnecter des serveurs AppTec360. Dans ce cas, il ne sera plus possible de gérer l'appareil. **ATTENTION !** Cette fonction ne doit être utilisée que sur des appareils appartenant à l'entreprise ou à l'organisation ou fournis par elle, ou sur un appareil appartenant à l'utilisateur, lorsque ce dernier accepte que l'appareil soit entièrement géré par l'entreprise. Si vous désactivez ce paramètre de stratégie, les utilisateurs ne pourront pas supprimer les inscriptions MDM. Indiquez si l'utilisateur est autorisé à supprimer le compte du poste de travail via le panneau de contrôle du poste de travail. Le serveur MDM peut toujours supprimer le compte à distance.

BitLocker

Configuration de BitLocker

Paramètres généraux	
Exiger le cryptage des appareils	Selon l'édition de Windows et la configuration du système, les utilisateurs peuvent être invités à activer le cryptage de l'appareil : - Pour confirmer que le cryptage d'un autre fournisseur n'est pas activé. - Pour désactiver BitLocker Drive Encryption et le réactiver.
Méthodes de cryptage	
Méthode de cryptage pour les lecteurs du système d'exploitation	
Méthode de cryptage pour les lecteurs de données fixes	
Méthode de cryptage pour les lecteurs de données amovibles	
Désactiver l'avertissement concernant le chiffrement des disques par des tiers	Désactivez l'avertissement concernant l'utilisation d'un service de cryptage de disque tiers sur l'appareil. À partir de Windows 10, version 1803, ce paramètre n'est pris en charge que pour les appareils reliés à Azure Active Directory.
Autoriser l'exécution du chiffrement lorsque l'utilisateur non administrateur est connecté	Uniquement pour les appareils reliés à Azure Active Directory

Extensions AppTec360	
Cryptage silencieux	Si cette option est sélectionnée en même temps que "Require device encryption", le service de gestion AppTec360 exécutera un chiffrement silencieux automatique des lecteurs de l'appareil.
Générer automatiquement les informations d'identification de l'utilisateur	Le disque d'exploitation crypté sera protégé par des informations d'identification générées automatiquement. Soit un code PIN TPM, lorsqu'un TPM est disponible, soit un mot de passe textuel à 6 chiffres. Les informations d'identification générées sont envoyées à l'adresse électronique enregistrée pour l'appareil en question. Si cette option est désactivée, la seule protection possible pour le chiffrement silencieux est l'utilisation du TPM. Dans ce cas, pour les appareils sans TPM, le chiffrement silencieux échouera.
Cryptage des disques fixes	Tous les lecteurs de données fixes disponibles seront également cryptés et protégés par un "déverrouillage automatique" à l'aide d'une clé stockée sur le lecteur du système d'exploitation.

Paramètres du disque du système d'exploitation

Exiger une authentification supplémentaire au démarrage	Ce paramètre vous permet de configurer si BitLocker requiert une authentification à chaque démarrage de l'ordinateur. Ce paramètre est appliqué lors de la configuration de BitLocker. Si vous activez ce paramètre, les utilisateurs peuvent configurer des options de démarrage avancées dans l'assistant de configuration de BitLocker.
Bloquer BitLocker sans TPM compatible	
TPM uniquement	
TPM et PIN	
TPM et clé	
TPM, clé et code PIN	Si vous souhaitez exiger l'utilisation d'un code PIN et d'une clé USB, l'utilisateur doit configurer BitLocker à l'aide de l'outil de ligne de commande "manage-bde" au lieu de l'assistant de configuration de BitLocker Drive Encryption.

Exiger la longueur minimale du code PIN

	Caractères minimums

Configurer le message et l'URL de récupération avant démarrage	Configurez l'intégralité du message de récupération ou remplacez l'URL existante qui s'affiche sur l'écran de récupération de la clé de pré-amorçage lorsque le lecteur de système d'exploitation est verrouillé. Remarque : tous les caractères et toutes les langues ne sont pas pris en charge par le système de pré-amorçage. Il est fortement recommandé de vérifier que les caractères que vous utilisez s'affichent correctement sur l'écran de récupération avant le démarrage.
	Option de message de récupération avant le démarrage
	Message de récupération personnalisé
	URL de récupération personnalisée

Options de récupération du disque du système d'exploitation		Ce paramètre vous permet de contrôler la façon dont les lecteurs du système d'exploitation protégés par BitLocker sont récupérés en l'absence des informations d'identification requises. Ce paramètre est appliqué lors de la configuration de BitLocker. Par défaut, un agent de récupération des données basé sur un certificat est autorisé, les options de récupération peuvent être spécifiées par l'utilisateur, y compris le mot de passe et la clé de récupération, et les informations de récupération ne sont pas sauvegardées sur AD DS.
	Agent de récupération des données basé sur un certificat de bloc	Indiquez si un agent de récupération des données peut être utilisé avec des lecteurs de système d'exploitation protégés par BitLocker. Avant qu'un agent de récupération des données puisse être utilisé, il doit être ajouté à partir de l'élément Stratégies de clés publiques dans la console de gestion des stratégies de groupe ou dans l'éditeur local de stratégies de groupe. Consultez le BitLocker Drive Encryption Deployment Guide sur Microsoft TechNet pour plus d'informations sur l'ajout d'agents de récupération de données.
	Paramètres du mot de passe de récupération BitLocker	
	Paramètres de la clé de récupération BitLocker	
	Sauvegarder les informations de récupération BitLocker dans Active Directory Domain Services	
	Configuration du stockage de récupération BitLocker de l'AD DS	Le stockage du paquet de clés permet de récupérer les données d'un disque physiquement endommagé.
	Exiger le stockage des données de récupération dans AD DS	Empêchez les utilisateurs d'activer BitLocker à moins que l'ordinateur ne soit connecté au domaine et qu'il n'y ait pas d'erreur.

Réglages fixes de l'entraînement	
Options de récupération des disques fixes	Ce paramètre vous permet de contrôler la manière dont les lecteurs fixes protégés par BitLocker sont récupérés en l'absence des informations d'identification requises. Ce paramètre est appliqué lors de la configuration de BitLocker. Par défaut, un agent de récupération des données basé sur un certificat est autorisé, les options de récupération peuvent être spécifiées par l'utilisateur, y compris le mot de passe et la clé de récupération, et les informations de récupération ne sont pas sauvegardées sur AD DS.
Agent de récupération des données basé sur un certificat de bloc	
Paramètres du mot de passe de récupération BitLocker	
Paramètres de la clé de récupération BitLocker	
Sauvegarder les informations de récupération BitLocker dans Active Directory Domain Services	
Configuration du stockage de récupération BitLocker de l'AD DS	Le stockage du paquet de clés permet de récupérer les données d'un disque physiquement endommagé.
Exiger le stockage des données de récupération dans AD DS	Empêchez les utilisateurs d'activer BitLocker à moins que l'ordinateur ne soit connecté au domaine et que la sauvegarde des informations de récupération BitLocker dans AD DS ne réussisse. Note : Le mot de passe de récupération est généré automatiquement.
Interdire l'accès en écriture aux lecteurs fixes non protégés	

Paramètres du lecteur amovible	
Interdire l'accès en écriture aux lecteurs amovibles non protégés	Interdire l'accès en écriture aux lecteurs de données amovibles qui ne sont pas protégés par Bitlocker. Remarque : si l'option "Disques amovibles : Refuser l'accès en écriture" est activé dans la stratégie de groupe, ce paramètre de stratégie sera ignoré.
Interdire 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 bénéficieront d'un accès en écriture. Ces champs sont définis par le paramètre de stratégie de groupe "Fournir les identifiants uniques de votre organisation".

État de BitLocker

Vous pouvez voir ici l'état actuel des disques cryptés par BitLocker.

C [OS Drive]
État du chiffrement
Chiffré (%)
Statut de protection
Méthode de cryptage
Protecteurs de clés
Récupération du mot de passe

En cliquant sur le bouton "Rotation du mot de passe de récupération", vous pouvez faire pivoter le mot de passe de récupération BitLocker.

Gestion des certificats

Liste des certificats

Voici une liste des certificats installés sur l'appareil affiché.

Configuration du certificat

Vous pouvez ici configurer les certificats et la manière dont ils seront installés sur l'appareil.

Certificat de confiance	
Description	Description du certificat
Champ d'application	Portée du déploiement du certificat : Utilisateur actuel et appareil
Magasin de certificats	"Certificats non fiables" n'est disponible qu'à partir de Windows 10, version 1803.
Dossier de certificat	Télécharger un fichier PKCS#1

Certificat d'identité			
Description	Description du certificat		
Champ d'application	Portée du déploiement du certificat : Utilisateur actuel et appareil		
Emplacement clé	Le fournisseur de stockage de clés sur lequel installer la clé privée.		
		TPM. Échec en l'absence de TPM	
	TPM. En l'absence de TPM, le logiciel KSP est utilisé comme solution de repli.		
	Fournisseur de clé logicielle de stockage		Marquer la clé privée comme exportable
	Windows Hello pour les entreprises	Nom du conteneur	Spécifie le nom du conteneur Windows Hello for Business (anciennement Microsoft Passport for Work).
		Texte de l'invite PIN	Spécifie le texte personnalisé à afficher à l'invite du code PIN de Windows Hello for Business lors de l'inscription au certificat.
Titre de compétence	Télécharger un fichier PKCS#12		

SCEP

Description	Description du serveur SCEP		
Champ d'application du déploiement	Portée du déploiement du certificat : Appareil actuel et utilisateur		
URL du serveur SCEP	Un ou plusieurs serveurs qui émettent des certificats par l'intermédiaire de SCEP		
Sujet	Représentation d'un nom X.500. Par exemple : "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar".		
Noms alternatifs du sujet	Type	Adresse électronique	
		DNS	
		URI	
		Nom principal de l'utilisateur (UPN)	
Empreinte digitale CA	L'empreinte SHA1 du certificat de l'autorité de certification. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Période de validité unités	Jours, mois ou années		
Période de validité			
Défi	Utilisé comme secret pré-partagé pour l'inscription automatique		
Tentatives	Nombre de tentatives de l'appareil si le serveur envoie une réponse PENDING. La valeur par défaut est 5 et la valeur maximale est 30.		
Délai de réessai	Nombre de minutes à attendre avant de réessayer. La valeur par défaut est 5 et la valeur minimale est 1.		
Taille de la clé	Taille de la clé en bits		
Algorithme de hachage	Famille d'algorithmes de hachage		
Utilisation des clés	L'extension de l'utilisation de la clé définit l'objectif (par exemple, déchiffrement, signature) de la clé contenue dans le certificat. Au moins l'une des options "Digital signature" ou "Key encipherment" doit être sélectionnée.		
Utilisation étendue des clés	Spécifie l'utilisation des clés étendues, sous réserve de la configuration du serveur SCEP. Spécifiez la liste des OID correspondants, par exemple 1.3.6.1.5.5.7.3.2 (authentification du client).		

Emplacement clé	Le fournisseur de stockage de clés sur lequel installer la clé privée.		
		TPM. Échec en l'absence de TPM	
	TPM. En l'absence de TPM, le logiciel KSP est utilisé comme solution de repli.		
	Fournisseur de clé logicielle de stockage		
	Windows Hello pour les entreprises	Nom du conteneur	Spécifie le nom du conteneur Windows Hello for Business (anciennement Microsoft Passport for Work).
		Texte de l'invite PIN	Spécifie le texte personnalisé à afficher à l'invite du code PIN de Windows Hello for Business lors de l'inscription au certificat.

Gestion des connexions

Wifi

Ce paramètre permet d'effectuer la préconfiguration des dispositifs de l'utilisateur final pour l'accès aux points d'accès internes.

Identificateur d'ensemble de services (SSID)	SSID du réseau avec lequel la connexion sera établie
Jointure automatique	Activer la connexion automatique au réseau
Réseau caché	Activer, dans le cas où le point d'accès ne diffuse pas le SSID.

Type de sécurité

Établir le type de sécurité de l'AP

Système ouvert WEP	
Mot de passe	Mot de passe pour l'AP

WPA PSK	
Mot de passe	Mot de passe pour l'AP

WPA EAP	
Type d'authentification	Type d'authentification, uniquement possible avec "PEAP-MSCAHPv2".
Reconnexion rapide	Les appareils peuvent passer d'un point d'accès à l'autre sans avoir à s'authentifier à nouveau.
Accès des invités	L'utilisateur n'a pas de compte et doit donc s'inscrire en tant qu'invité.
Contrôles de quarantaine	Le client doit effectuer des contrôles NAP (Network Access Protection) et partager les résultats avec le système, qui décide alors si le client peut se connecter.
Exiger le Crypto Binding	L'authentification n'est possible que par Crypto Binding.
Validation du serveur	Le client vérifie si le certificat du serveur est valide. Si c'est le cas, une connexion sera établie.
Demande de certificats	Permet à l'utilisateur d'accepter des certificats non fiables
Noms des serveurs	Offre la possibilité d'afficher le nom du serveur RADIUS qui assure l'authentification et l'autorisation du réseau.

WPA2-PSK	
Mot de passe	Mot de passe AP

WPA2 EAP	
Type d'authentification	Type d'authentification, uniquement possible avec "PEAP-MSCAHPv2".
Reconnexion rapide	
Accès des invités	
Contrôles de quarantaine	Active la protection de l'accès au réseau NAP
Exiger le Crypto Binding	L'authentification n'est possible que par Crypto Binding.
Validation du serveur	
Demande de certificats	Demande d'un certificat de serveur validé, d'un nom ou d'un certificat d'authentification racine (CA).
Noms des serveurs	Liste des serveurs auxquels les appareils doivent faire confiance
Aucun	Pas de sécurité établie
Utiliser un serveur proxy	Utilisation d'un serveur proxy
Adresse du serveur	Adresse du serveur proxy
Port du serveur	Port du serveur proxy

Utiliser un serveur proxy

Activer l'utilisation du serveur proxy.

Adresse du serveur	Adresse du serveur proxy utilisé par ce réseau.
Port du serveur	Port du serveur proxy utilisé par ce réseau.

Restrictions concernant le Wifi

Ici, vous pouvez définir diverses restrictions Wifi.

Autoriser le WiFi	Autoriser/refuser le WiFi
Autoriser le partage d'Internet	Autoriser l'utilisation d'un Hotspot
Autoriser la connexion automatique aux points chauds WiFi Sense	Autoriser la connexion automatique aux points chauds WiFi Sense
Autoriser la configuration manuelle du WiFi	Permettre à l'utilisateur de se connecter à des réseaux WiFi qui n'ont pas été définis par AppTec
Fréquence de balayage WLAN	Définit l'intervalle de balayage du réseau local sans fil. Une valeur plus élevée augmente la capacité à reconnaître les réseaux WIFI.

VPN

Effectuez les réglages appropriés ici, afin de configurer les connexions VPN.

Nom de la connexion	Nom de la connexion indiqué		
Type de VPN	Une connexion VPN par application est utilisée pour sécuriser le trafic de certaines applications.		
	VPN	Toujours activé	Cela connectera automatiquement le VPN lors de la connexion et restera connecté jusqu'à ce que l'utilisateur se déconnecte manuellement.
	VPN par application	Applications VPN	Définir les applications qui utilisent cette connexion VPN
		Verrouillage par application	Le verrouillage par application permet aux applications sélectionnées de n'avoir accès qu'à cette connexion VPN. Cette fonction dépend du pare-feu Windows Defender.
	Profil WIP	Domaine WIP pour cette connexion	l'identifiant d'entreprise, qui est nécessaire pour connecter ce profil VPN à une politique de protection des informations Windows (WIP).

Type de connexion

AppTec360 VPN	
Pour "AppTec360 VPN", il est nécessaire que le chargement latéral d'applications soit autorisé. Veuillez activer "Allow App Sideloading" dans "Security Management" → "Restriction Settings" → "Device Functionality".	
Configuration de la passerelle	Pour configurer une connexion VPN avec liste noire, veuillez sélectionner une configuration VPN avec un serveur DNS spécifié. Vous pouvez définir une configuration VPN dans "Paramètres généraux" → "Passerelle universelle" → "Paramètres VPN".

IKEv2		
Serveurs	Liste des serveurs VPN	
Tunnel de l'appareil	Activer la connexion avant l'ouverture de la session de l'utilisateur.	
Méthode d'authentification	PAE	EAP XML
	Certificats de machine	
Algorithme de cryptage		
Algorithme de contrôle d'intégrité		
Groupe Diffie-Hellman		
Algorithme de transformation du chiffrement		
Algorithme de transformation d'authentification		
Groupe "Perfect Forward secrecy" (PFS)		

PPTP		
Serveurs	Liste des serveurs VPN	
Méthode d'authentification	PAE	EAP XML

L2TP		
Serveurs	Liste des serveurs VPN	
Méthode d'authentification	PAE	EAP XML
Algorithme de cryptage		
Algorithme de contrôle d'intégrité		
Groupe Diffie-Hellman		
Algorithme de transformation du chiffrement		
Algorithme de transformation d'authentification		
Groupe "Perfect Forward secrecy" (PFS)		

Automatique		
Serveurs	Liste des serveurs VPN	
Méthode d'authentification	PAE	EAP XML

Configurations VPN génériques

Mémoriser les informations d'identification à chaque connexion	
Enregistrer les adresses IP avec le DNS interne	
Règles de filtrage du trafic réseau	Limiter la connexion VPN à l'ensemble des règles définies.
Liste de recherche de suffixes DNS	Suffixes DNS à ajouter à la liste de recherche DNS pour l'acheminement des noms courts.
Règles de la table de politique de résolution des noms (NRPT)	Les règles de la table de politique de résolution des noms (NRPT) définissent la manière dont le DNS résout les noms lorsqu'il est connecté au VPN.
Détection des réseaux de confiance	Liste des suffixes DNS permettant d'identifier le réseau de confiance.
Tunnel divisé	Le tunnelage fractionné signifie que le trafic peut passer par n'importe quelle interface déterminée par la pile de réseau.
Fractionnement des itinéraires de tunnelage	Liste des routes à ajouter à la table de routage pour l'interface VPN.
Configuration du proxy	Configure le proxy utilisé avec ce réseau
Adresse du mandataire	Adresse du serveur proxy sous la forme d'un nom d'hôte complet ou d'une adresse IP.
Port	Port du serveur proxy.
URL de configuration automatique du proxy	pour récupérer automatiquement les paramètres du proxy.

Restrictions VPN

Vous pouvez définir ici diverses restrictions VPN.

Autoriser les paramètres VPN	Cette ligne directrice permet/interdit à l'utilisateur de désactiver et de modifier les paramètres du VPN.
Autoriser le VPN sur réseau cellulaire	Autorise/interdit à l'appareil d'établir une connexion VPN, si l'appareil utilise des données mobiles.
Autoriser l'itinérance VPN sur réseau cellulaire	Autorise/interdit à l'appareil d'établir une connexion VPN, si l'appareil est en itinérance.

Bluetooth

Ici, vous pouvez déterminer si le Bluetooth doit être autorisé/interdit.

Autoriser Bluetooth	Activer/désactiver Bluetooth

Gestion du PIM

Exchange Active Sync

Configuration du compte ActiveSync sur l'appareil de l'utilisateur final

Nom du compte	Nom du compte de messagerie
Nom d'hôte du serveur	Adresse du serveur/FQDN
Nom de domaine	Domaine du serveur
Adresse électronique	Adresse électronique
Nom de l'utilisateur	Nom de l'utilisateur
Mot de passe de l'utilisateur	En option, vous pouvez déjà attacher un mot de passe à l'utilisateur ici
Utiliser SSL	Utiliser une connexion SSL
Intervalle de synchronisation	L'intervalle de synchronisation peut être défini ici Synchronisation manuelle = L'utilisateur doit télécharger ses courriels et effectuer une synchronisation manuelle.
Filtre d'âge du courrier	Délai avant la synchronisation des courriels Pas de filtre = illimité
Niveau d'enregistrement	Établissement des niveaux de journalisation pour le trafic ActiveSync
Sync Email	Activé = les courriels sont synchronisés
Synchroniser les contacts	Activé = les contacts sont synchronisés
Synchroniser le calendrier	Activé = le calendrier est synchronisé
Synchronisation des tâches	Activé = les tâches sont synchronisées

eMail

Création de comptes POP3/IMAP4 sur l'appareil de l'utilisateur final.

Description du compte	Nom du compte de messagerie
Nom de l'expéditeur	Nom de l'expéditeur affiché
Nom de domaine	Nom de domaine du compte de messagerie
Adresse électronique	Adresse électronique de l'utilisateur
Nom de l'utilisateur	Nom de l'utilisateur
Mot de passe de l'utilisateur	En option, vous pouvez déjà attacher un mot de passe à l'utilisateur ici
Autres informations d'identification du serveur sortant	Vous pouvez définir ici si d'autres informations d'identification sont requises pour le serveur sortant.
Nom de domaine sortant	Nom de domaine sortant
Nom d'utilisateur du serveur sortant	Nom d'utilisateur du serveur sortant
Mot de passe du serveur sortant	Mot de passe du serveur sortant
Protocole de courrier électronique	POP3 ou IMAP4, peut être utilisé comme protocole
Nom d'hôte du serveur de courrier entrant	Nom d'hôte du serveur de courrier entrant
Utiliser SSL pour les courriers entrants	Utilisez le protocole SSL pour les courriels entrants
Nom d'hôte du serveur de courrier sortant	Nom d'hôte du serveur de courrier sortant
Utiliser SSL pour les courriers sortants	Utilisez le protocole SSL pour les courriels sortants
Authentification du serveur sortant	Une authentification du serveur sortant est nécessaire
Intervalle de synchronisation	L'intervalle de synchronisation peut être défini ici Synchronisation manuelle = L'utilisateur doit télécharger ses courriels et effectuer une synchronisation manuelle.
Filtre d'âge du courrier	Délai avant la synchronisation des courriels Pas de filtre = illimité

Gestion des applications

Gestionnaire d’applications d’entreprise

Applications installées

Voici une liste des applications actuellement installées sur l'appareil affiché.

Applications obligatoires

Vous pouvez ici configurer une liste d'applications obligatoires sur l'appareil.

Cette liste sera vérifiée à chaque fois que l'appareil se connectera au MDM et installera toutes les applications de cette liste qui ne sont pas installées sur l'appareil, que l'application ait été désinstallée ou qu'elle n'ait jamais été installée auparavant.

Vous pouvez télécharger des applications Windows 10 In-House Apps puis les ajouter à cette liste ou vous pouvez ajouter des configurations Microsoft Office qui doivent être configurées au préalable dans "General Settings" > "App Management" > "Microsoft Office".

Restrictions des applications système

Applications de la boîte de réception
Autoriser les alarmes et l'horloge
Calculateur d'allocations
Autoriser la caméra
Autoriser le support de contact
Autoriser Cortana
Autoriser l'explorateur de fichiers
Permettre de démarrer
Allow Groove Music
Autoriser les cartes
Autoriser la messagerie
Autoriser Microsoft Edge
Autoriser les films et la télévision
Allocation d'argent
Autoriser les nouvelles
Autoriser OneDrive
Autoriser OneNote
Autoriser le calendrier et le courrier Outlook
Autoriser les personnes
Autoriser le téléphone
Autoriser les photos
Autoriser Powerpoint
Autoriser les paramètres
Autoriser Skype
Autoriser les sports
Autoriser le magasin
Autoriser l'enregistreur vocal
Autoriser le portefeuille
Autoriser le temps

Autoriser le Windows Feedback Hub
Autoriser le mot
Autoriser la Xbox

Pages de réglage
Autoriser les comptes Lieu de travail
Autoriser les informations avancées
Autoriser le coin des applications
Autoriser le blocage et le filtrage
Autoriser le profil de couleur
Autoriser le mode de conduite
Autoriser le courrier électronique et les comptes
Autoriser l'égaliseur
Autoriser le clavier
Autoriser la barre de navigation
Autoriser le mode avion du réseau
Autoriser le partage de l'Internet en réseau
Autoriser les services de réseau
Autoriser le réseau Wi-Fi
Autoriser le système PC Bluetooth
Autoriser l'évaluation de votre appareil
Autoriser la restauration de la mise à jour
Autoriser le partage
Autoriser le démarrage
Temps alloué Langue
Temps alloué Région
Autoriser l'écran de verrouillage par défaut de Windows
Autoriser le compte du travail ou de l'école

Liste noire et liste blanche

Sous "Liste noire et liste blanche", vous pouvez choisir entre le mode "Liste blanche" et le mode "Liste noire".

Liste blanche	Seuls les applications et services ajoutés à la liste peuvent être installés sur l'appareil de l'utilisateur final. S'ils sont déjà préinstallés sur l'appareil de l'utilisateur final, ils seront activés et configurés pour que l'utilisateur puisse les exécuter.
	Toutes les autres applications qui ne sont pas ajoutées à la liste ne peuvent pas être installées sur l'appareil de l'utilisateur final. Si elles sont déjà préinstallées sur l'appareil de l'utilisateur final, elles seront désactivées et paramétrées de sorte que l'utilisateur ne puisse pas les exécuter.
Liste noire	Les applications et services ajoutés à la liste ne peuvent pas être installés sur l'appareil de l'utilisateur final. S'ils sont déjà préinstallés sur l'appareil de l'utilisateur final, ils seront désactivés et configurés de manière à ce que l'utilisateur ne puisse pas les exécuter.
	Toutes les autres applications qui ne sont pas ajoutées à la liste peuvent être installées sur l'appareil de l'utilisateur final. Si elles sont déjà préinstallées sur l'appareil de l'utilisateur final, elles seront activées et paramétrées pour que l'utilisateur puisse les exécuter.

La touche , vous permet d'ajouter des applications ou des services supplémentaires à la liste des applications utilisées.

La touche , vous permet d'ajouter des applications ou des services à la liste des applications inactives.

Vous pouvez ajouter une application à partir du "Windows App Store" ou saisir directement un "identifiant d'application" pour l'ajouter à la liste noire ou blanche.

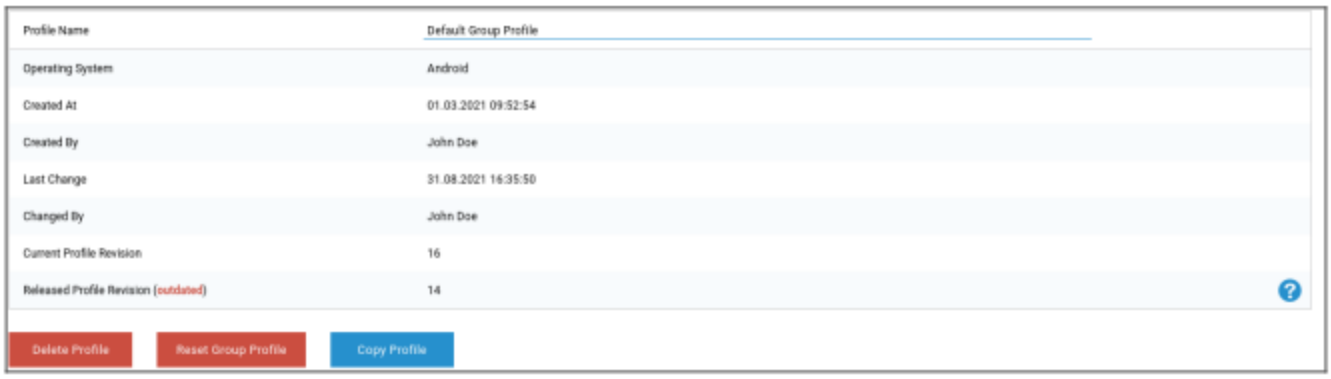
Configuration de MacOS

Selon que vous avez sélectionné un profil ou un appareil, l'affichage et ses sous-points sont différents.

Général

Aperçu du profil du groupe (uniquement au niveau du groupe)

Lorsque vous ouvrez un profil de groupe, vous obtenez un aperçu rapide du profil.



Nom du profil	Nom du profil (peut être modifié ici)
Système d'exploitation	Système d'exploitation pour lequel le profil est établi
Créé à	Moment de la création
Créé par	Le créateur du profil
Dernier changement	Date de la dernière modification du profil
Modifié par	Compte ayant effectué les dernières modifications
Révision du profil actuel	Révision de l'état du profil sauvegardé
Révision du profil validé	Révision du profil attribué ("Attribuer maintenant"). Si l'étiquette affiche "(obsolète)" derrière le texte, cela signifie que vous avez enregistré le profil mais que vous ne l'avez pas encore attribué.

Aperçu de l’appareil (uniquement au niveau de l’appareil)

Vue d'ensemble de l'appareil.

Nom de l'appareil	Nom de l'appareil
Modèle	Modèle
Système d'exploitation	Système d'exploitation
Numéro de série	Numéro de série de l'appareil
Propriété des appareils	Le type de propriété configuré
Type d'appareil	Le type d'appareil
Conforme à la loi	Indique si l'appareil est conforme
Adresse IP	L'adresse IP de l'appareil connecté au serveur.
Dernière visite	Heure de la dernière connexion de l'appareil
Dernière poussée	Heure de la dernière impulsion envoyée à l'appareil
Affectation	Ici, vous pouvez déplacer l'appareil vers un autre utilisateur ou groupe.

Révision de la configuration (uniquement au niveau de l’appareil)

Vous obtiendrez ici une vue d'ensemble du profil de groupe attribué à l'appareil.

Si vous cliquez sur le profil du groupe, vous accédez directement au profil et vous pouvez effectuer des réglages.

Le symbole vous permet de rétablir les paramètres du profil de groupe pour les applications attribuées.

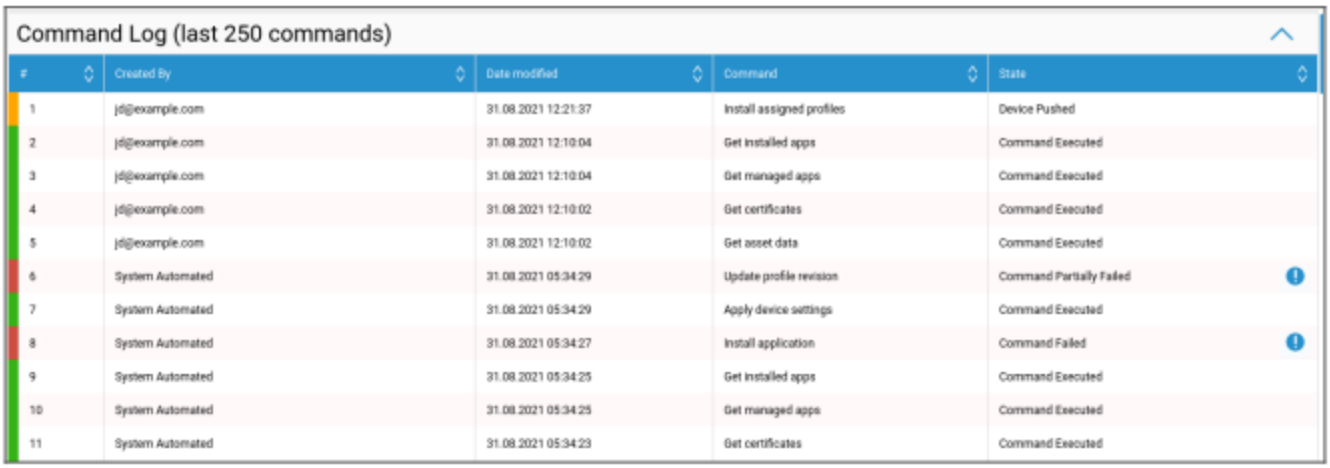
Le symbole permet de réinitialiser le profil de l'appareil pour qu'il ne comporte aucun paramètre.

La mention "Révision plus récente disponible" indique que le profil de groupe a été modifié et enregistré, mais qu'il n'a pas été attribué. Le profil de groupe doit être attribué avec "Attribuer maintenant" au niveau du groupe pour appliquer les changements aux appareils.

Journal de l’appareil (uniquement au niveau de l’appareil)

Journal des commandes

Vous pouvez voir ici quelles commandes ont été émises pour l'appareil et quel est leur état.



Les commandes créées par le "système automatisé" sont automatiquement créées par le système.

États possibles de la commande

Dispositif poussé	Une requête "push" a été envoyée au service "push" (par exemple APNS) pour demander à l'appareil de se reconnecter au serveur EMM.
Commande créée	La commande a été créée dans le système.
Commande envoyée	La commande a été envoyée à l'appareil après qu'il se soit connecté au serveur.
Commande exécutée	La commande a été exécutée avec succès.
Échec de la commande	La commande a échoué. *
Échec partiel de la commande	Selon le système d'exploitation de l'appareil, certaines commandes peuvent être regroupées. Dans ce cas, certaines parties de ce groupe de commande ont échoué. *
Commande exécutée, échec éventuel	La commande a été exécutée, mais peut-être qu'elle ne l'a pas été.
Commandement repoussé	La commande a été repoussée par un utilisateur.
Mise au rebut	La commande a été supprimée. Par exemple, parce qu'elle a été remplacée par une autre commande ou parce que l'appareil a été réenrôlé et que les anciennes commandes ont été supprimées.

*Si le message est accompagné d'un point d'exclamation, vous pouvez obtenir plus d'informations en survolant l'icône avec votre curseur.

Gestion des actifs (uniquement au niveau de l’appareil)

Informations sur l’appareil

Numéro de modèle	Numéro de modèle
Nom d'hôte	Nom d'hôte
Nom d'hôte local	Nom d'hôte local
Système d'exploitation	Système d'exploitation
Version OS	Version du système d'exploitation
UDID	UDID
Mémoire libre / totale	Mémoire libre / totale

WiFi

Adresse IP	Adresse IP
WiFi MAC	WiFi MAC

Cellulaire

Numéro de téléphone	Numéro de téléphone
État de l'itinérance	État de l'itinérance
Itinérance (voix/données)	Itinérance (voix/données)
Adresse IP	Adresse IP
Opérateur/transporteur	Opérateur/transporteur
Réseau de l'opérateur SIM	Réseau de transporteurs
Version transporteur	Version transporteur
ICCID	ICCID
Actuel MCC/MNC	Actuel MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Gestion des mises à jour (uniquement au niveau de l'appareil)

Mise à jour des informations

Cet onglet présente des informations sur les paramètres de mise à jour du système sur l'appareil.

Autocheck activé	Si le système vérifie automatiquement la mise à jour.
Mise à jour automatique des applications activée	Si le système installe automatiquement les mises à jour des applications.
Mise à jour automatique du système d'exploitation activée	Si le système installe automatiquement les mises à jour de l'OS.
Mise à jour automatique de la sécurité activée	Si le système installe automatiquement les mises à jour de sécurité.
Mise à jour de l'application en arrière-plan - téléchargement activé	Si le système télécharge des mises à jour d'applications en arrière-plan.
URL du catalogue	L'URL du catalogue des mises à jour logicielles que le client utilise.
Est le catalogue par défaut	Si "oui", le catalogue est le catalogue par défaut.
Effectuer un contrôle périodique	Si "oui", lancez une nouvelle analyse.
Date de l'examen précédent	Date de la dernière analyse de mise à jour du logiciel.
Résultat de l'examen précédent	Le code de résultat de la dernière analyse de mise à jour du logiciel.

Gestion de la sécurité

Lutte contre le vol

Essuyer et verrouiller

Essuyage complet	Envoyer une commande pour réinitialiser l'appareil
Nettoyage de l'entreprise	Retirez le MDM de l'appareil et supprimez toutes les données du MDM (par exemple, les comptes, les applications).
Écran de verrouillage	Ramener l'appareil à l'écran de verrouillage

Configuration de la sécurité

Code d’accès

Désactivation du code autorisée	Détermine si l'utilisateur est obligé de définir un code PIN. Le simple fait de définir cette valeur (et pas d'autres) oblige l'utilisateur à saisir un code d'accès, sans imposer de longueur ou de qualité.
Autoriser une valeur simple	Permettre à l'utilisateur d'utiliser les mêmes chaînes de numéros, croissants et décroissants (ex. 1234, 1111).
Valeur alphanumérique requise	Les mots de passe doivent contenir au moins une lettre
Longueur minimale du code d'accès	Longueur minimale du mot de passe
Nombre minimum de caractères complexes	Nombre minimal de symboles alphanumériques dans le mot de passe
Âge maximal du code d'accès	Nombre de jours après lesquels le mot de passe doit être modifié
Verrouillage automatique maximal	Durée maximale après laquelle l'appareil est verrouillé
Délai de grâce maximum pour le verrouillage du dispositif	Durée pendant laquelle l'appareil peut être verrouillé sans que le code d'accès ne soit demandé au moment du déverrouillage
Âge maximal du code d'accès (1-730 jours, ou aucun)	Jours après lesquels le code d'accès doit être modifié
Historique des codes d'accès (1 à 50 codes d'accès ou aucun)	Nombre de codes uniques avant réutilisation

Certificat

PKCS#1	
Description	Entrez une description pour le certificat
Titre de compétence	Télécharger un fichier pkcs1

PKCS#12	
Description	Entrez une description pour le certificat
Titre de compétence	Télécharger un fichier pkcs12

Paramètres de restriction

Fonctionnalité de l’appareil

Autoriser la caméra	Permettre l'utilisation de l'appareil photo
Autoriser Game Center	Si la valeur est fausse, le centre de jeux est désactivé et son icône est supprimée de l'écran d'accueil.
Permettre les jeux multijoueurs	Si elle est fausse, elle interdit les jeux multijoueurs.
Permettre l'ajout d'amis Game Center	Si cette option est fausse, elle interdit l'ajout d'amis au Game Center.
Autoriser la photothèque iCloud	Si cette option a la valeur false, elle désactive la photothèque iCloud. Toutes les photos qui n'ont pas été entièrement téléchargées depuis la photothèque iCloud sur l'appareil seront supprimées du stockage local.
Autoriser Touch ID	Si elle est fausse, elle empêche Touch ID de déverrouiller un appareil.

iCloud

Bloquer certaines fonctionnalités lors de l'appairage iCloud

Autoriser la synchronisation des documents	Autoriser la synchronisation des documents
Autoriser la synchronisation du trousseau iCloud	Autoriser la synchronisation du trousseau iCloud
Autoriser les notes iCloud	Si la valeur est fausse, les services iCloud Notes de MacOS ne sont pas autorisés.
Autoriser iCloud BTMM	Si cette option est fausse, elle désactive le service iCloud "Back to My Mac" de MacOS.
Autoriser iCloud FMM	Si la valeur est fausse, le service iCloud Find My Mac de MacOS est désactivé.
Autoriser les signets iCloud	Si la valeur est fausse, la synchronisation des signets iCloud de MacOS n'est pas autorisée.
Autoriser iCloud Mail	Si la valeur est fausse, les services iCloud de MacOS Mail ne sont pas autorisés.

Autoriser le calendrier iCloud	Si cette option est fausse, elle désactive les services iCloud de MacOS Cloud.
Autoriser les rappels iCloud	Si la valeur est fausse, les services de rappel iCloud ne sont pas autorisés.
Autoriser le carnet d'adresses iCloud	Si la valeur est fausse, les services du carnet d'adresses iCloud de MacOS ne sont pas autorisés.

Gestion des médias

Ejecter lors de la déconnexion	Éjecter tous les supports amovibles lors de la déconnexion
Autoriser le réseau	Autoriser l'accès aux médias du réseau
Autoriser le disque interne	Autoriser l'accès au disque interne.
Exiger l'authentification	Exiger l'authentification pour l'utilisation de ce média
Lecture seule	L'utilisateur ne peut que lire les données du support
Autoriser le disque externe	Autoriser l'accès au disque externe.
Exiger l'authentification	Exiger l'authentification pour l'utilisation de ce média
Lecture seule	L'utilisateur ne peut que lire les données du support
Autoriser l'utilisation d'images disque	Autoriser l'accès aux images.
Exiger l'authentification	Exiger l'authentification pour l'utilisation de ce média
Lecture seule	L'utilisateur ne peut que lire les données du support
Permettre l'utilisation de DVD-RAM	Autoriser l'accès au disque DVD-RAM.
Exiger l'authentification	Exiger l'authentification pour l'utilisation de ce média
Lecture seule	L'utilisateur ne peut que lire les données du support
Permettre l'utilisation de DVD	Autoriser l'accès au disque DVD.
Exiger l'authentification	Exiger l'authentification pour l'utilisation de ce média
Permettre l'utilisation de CD	Autoriser l'accès au disque CD.
Exiger l'authentification	Exiger l'authentification pour l'utilisation de ce média

Gestion des connexions

Wi-Fi

Vous pouvez ici ajouter et configurer des connexions Wi-Fi

Identificateur d'ensemble de services (SSID)	SSID du réseau auquel la connexion sera établie
Jointure automatique	Activer la jonction automatique pour le réseau
Réseau caché	Activer, dans le cas où l'AP ne diffuse pas le SSID
Configuration du proxy	Configuration d'un proxy pour chaque point d'accès
Aucun	N'utilisez pas de serveur proxy
Manuel	Établir une procuration manuelle
URL du serveur proxy	Adresse pour accéder aux paramètres du proxy
Port	Établir le port pour le Proxy
Authentification	Nom d'utilisateur pour l'authentification sur le Proxy
Mot de passe	Mot de passe pour l'authentification sur le Proxy
Automatique	Établir automatiquement un proxy
URL du serveur proxy	URL du fichier de configuration du proxy
Type de sécurité	Établir le type de sécurité pour l'AP
WEP	
Mot de passe	Mot de passe pour l'AP
WPA/WPA2	
Mot de passe	Mot de passe pour l'AP
WEP Entreprise - WPA / WPA2 Enterprise / Toute entreprise	Voir le tableau Erreur : La source de référence n'a pas été trouvée ci-dessous
Aucun	Ne pas établir de sécurité
Désactiver la randomisation des adresses MAC	Désactive la randomisation des adresses MAC pour ce réseau Wi-Fi lorsqu'il est associé au réseau. Un avertissement de confidentialité s'affiche également dans les Paramètres, indiquant que le réseau dispose de protections réduites en matière de confidentialité.

Configuration du Wi-Fi d’entreprise

Remarque : Cette option n'est disponible que lorsque le "Type de sécurité" est défini sur un type d'entreprise.

Protocoles	Protocole d'authentification supporté par le réseau cible
TLS	Activer / Désactiver l'utilisation
TTLS	Activer / Désactiver l'utilisation
Authentifications internes	Protocole d'authentification à utiliser : PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Activer / Désactiver l'utilisation
PEAP	Activer / Désactiver l'utilisation
EAP-FAST	Activer / Désactiver l'utilisation
EAP-SIM	Activer / Désactiver l'utilisation
Utiliser le PAC	Utilisation du PAC (contrôle d'accès protégé)
Provision PAC	Configuration du PAC de provision
Provisionner le PAC de manière anonyme	Fourniture anonyme de PAC
Authentification	
Nom d'utilisateur	Nom d'utilisateur pour l'authentification
N'utilisez pas Par connexion Mot de passe	N'utilisez pas de mot de passe par connexion
Mot de passe	Le mot de passe à utiliser
Certificat d'identité	Télécharger/sélectionner le certificat d'authentification
Identité extérieure	Identité visible de l'extérieur
Confiance	
Certificat de confiance 1	Télécharger le premier certificat de confiance
Certificat de confiance 2	Télécharger le deuxième certificat de confiance
Certificat de confiance 3	Télécharger un troisième certificat de confiance
Serveur de confiance Noms des certificats	Les noms des certificats de serveur attendus (dans une liste séparée par des virgules)

VPN

Selon le type de connexion sélectionné, différents champs peuvent être visibles.

Nom de la connexion	Nom du profil VPN
Type de VPN	
VPN	Tout le trafic réseau de l'appareil sera acheminé via une connexion VPN.
Type de connexion	Établir le type de connexion VPN
IPsec (cisco)	Protocole IPsec de Cisco
L2TP	Protocole L2TP
SSL personnalisé	Connexion via SSL personnalisé
IKEv2	Protocole IKEv2
Configuration du proxy	Configuration d'un proxy pour la connexion VPN
Aucun	Ne pas établir de procuration
Manuel	Établir manuellement un proxy
URL du serveur proxy	Adresse pour accéder aux paramètres du proxy
Port	Établir le port pour le Proxy
Authentification	Nom d'utilisateur pour l'authentification au Proxy
Mot de passe	Mot de passe pour l'authentification au Proxy
Automatique	Établir automatiquement un proxy
URL du serveur proxy	URL pour accéder aux paramètres du proxy

Proxy HTTP

Type de mandataire	
Manuel	Établir un proxy manuellement
URL du serveur proxy	Adresse d'accès aux paramètres du proxy
Port	Établir le port du proxy
Authentification	Nom d'utilisateur pour l'authentification au Proxy
Mot de passe	Mot de passe pour l'authentification au Proxy
Automatique	Établir automatiquement un proxy
Proxy PAC URL	Proxy PAC URL
Autoriser la connexion directe si le PAC est inaccessible	Autoriser la connexion directe (sans VPN), si le PAC est inaccessible
Permettre de contourner le proxy pour accéder aux réseaux captifs	Permettre de contourner le proxy pour accéder aux réseaux internes captifs

AirPrint

Adresse IP	Adresse IP de l'imprimante
Chemin d'accès aux ressources	Chemin d'accès défini au périphérique AirPrint

AirPlay

Nom de l'appareil	Nom de l'appareil
Mot de passe	Mot de passe de pairage
Liste blanche	Définissez une liste d'appareils avec lesquels l'appareil peut s'appairer exclusivement.

Gestion du PIM

Exchange Active Sync

Nom du compte	Nom du compte.
Adresse électronique	L'adresse du compte (par exemple max@company.com)
Nom d'hôte du serveur	Nom d'hôte interne
Nom de connexion	Les champs "Domain" et "Login Name" doivent être vides pour que l'appareil demande à l'utilisateur de s'identifier.
Domaine	Les champs "Domain" et "Login Name" doivent être vides pour que l'appareil demande à l'utilisateur de s'identifier. Si une configuration de passerelle ACL est activée et que le champ Domaine n'est pas vide, la passerelle universelle AppTec360 authentifiera l'appareil avec le nom suivant : "Nom de domaine".
Mot de passe	Le mot de passe du compte (par exemple secretUserPassword)
Les jours précédents de Mail to Sync	Le nombre de jours passés de courrier à synchroniser
Utiliser SSL	Utiliser SSL pour l'hôte d'échange interne
Option avancée	Afficher les options avancées
Port du serveur	Port interne
Chemin d'accès au serveur	Chemin interne
Nom d'hôte externe	Hôte externe
Port externe	Port externe
Chemin externe	Chemin externe
Utiliser le protocole SSL pour les applications externes Hôte d'échange	Utiliser SSL pour l'hôte Exchange externe

eMail

Mise en place de comptes POP3 / IMAP sur l'appareil de l'utilisateur final

Description du compte	Nom des comptes e-mail
Type de compte	
IMAP	
Préfixe du chemin	Le préfixe de chemin pour les dossiers spéciaux
POP	
Nom d'affichage de l'utilisateur	Nom d'affichage de l'utilisateur
Adresse électronique	Adresse électronique de l'utilisateur

Courrier entrant	Paramètres du serveur entrant
Adresse du serveur de messagerie	Adresse du serveur de messagerie
Port du serveur de messagerie	Port du serveur de messagerie
Nom de l'utilisateur	Nom d'utilisateur respectif
Type d'authentification	Type d'authentification
Aucun	Pas de type d'authentification
Mot de passe (uniquement au niveau de l'appareil)	Demande de mot de passe
Réponse au défi MDM	
NTLM	NTLM-Authentication
HTTP MD5 Digest	
Utiliser SSL	Utilisez SSL, si nécessaire

Courrier sortant	Paramètres du serveur sortant
Adresse du serveur de messagerie	Adresse du serveur de messagerie
Port du serveur de messagerie	Port du serveur de messagerie
Nom de l'utilisateur	Nom d'utilisateur respectif
Type d'authentification	
Aucun	Pas de méthode d'authentification
Mot de passe (uniquement au niveau de l'appareil)	Demande de mot de passe
Réponse au défi MDM	
NTLM	NTLM-Authentication
HTTP MD5 Digest	
Utiliser SSL	Utilisez SSL, si nécessaire
Mot de passe sortant identique au mot de passe entrant	Mot de passe sortant identique au mot de passe entrant
A utiliser uniquement dans le courrier	Activez cette option si tous les courriels sortants doivent être envoyés par l'intermédiaire de l'application Mail.

CalDav

Configurer la mise en place et la distribution d'un compte CalDav

Description du compte	Nom d'affichage du compte
Nom d'hôte	Nom d'hôte et/ou adresse IP
Port	Port du compte CalDav
URL principal	URL principal du compte
Nom d'utilisateur	Nom d'utilisateur CalDav respectif
Mot de passe (uniquement au niveau de l'appareil)	Mot de passe CalDav respectif
Utiliser SSL	Utilisez SSL, si nécessaire

CardDav

Configurer la mise en place et la distribution d'un compte CardDav

Description du compte	Nom d'affichage du compte
Nom d'hôte	Nom d'hôte et/ou adresse IP
Port	Port du compte CardDav
URL principal	URL principal du compte
Nom d'utilisateur	Nom d'utilisateur respectif de CardDav
Mot de passe (uniquement au niveau de l'appareil)	Mot de passe CardDav respectif
Utiliser SSL	Utilisez SSL, si nécessaire

LDAP

Dans cette zone, établissez une connexion LDAP afin de permettre un échange dynamique de certificats entre l'appareil de l'utilisateur final et l'Active Directory.

Veuillez noter que l'utilisateur sélectionné doit disposer du droit de lecture correspondant.

Description du compte	Description du compte
Nom d'utilisateur du compte	Utilisateur pour l'accès LDAP
Mot de passe du compte	Mot de passe pour l'accès LDAP
Nom d'hôte du compte	Nom d'hôte/adresse IP du serveur LDAP
Utiliser SSL	Utilisez SSL, si nécessaire

Dans la deuxième partie, vous pouvez définir des filtres individuels pour la recherche dans le registre LDAP.

Description	Champ d'application	Base de recherche
Description du filtre	Niveau de recherche dans le registre LDAP	Définir le filtre individuel

Tableau de bord et rapports

Paramètres du tableau de bord

Vous pouvez y voir les tableaux de bord existants, les modifier ou en créer de nouveaux. Chaque tableau de bord dispose de son propre ensemble de données à afficher et de sa propre configuration graphique.

Contrôle des paramètres du tableau de bord

Public	Rend le tableau de bord public, de sorte que d'autres utilisateurs puissent le voir. Bien entendu, les utilisateurs doivent pouvoir se connecter et consulter les tableaux de bord. Si l'option "Public" n'est pas activée, seul le créateur peut voir le tableau de bord.
Défaut	Définit le tableau de bord par défaut de sorte qu'il s'ouvre automatiquement la prochaine fois que vous accédez à la vue du tableau de bord.
	Afficher le tableau de bord et ses graphiques
	Supprimer le tableau de bord
	Modifier le nom et les paramètres du tableau de bord
	Faites une copie du tableau de bord
	Ajouter un tout nouveau tableau de bord

Vue du tableau de bord

Elle affiche les données et les graphiques du tableau de bord sélectionné et vous permet de les modifier.

Contrôle du tableau de bord

	Permet de définir les données à afficher dans le tableau de bord, la quantité de données à afficher et la taille de ces données.
	Vous ramène à l'aperçu du tableau de bord
	Réinitialise le tableau de bord actuellement ouvert à sa valeur par défaut.
	Sauvegarde toutes les modifications que vous avez apportées au tableau de bord actuellement ouvert (par exemple, les données à afficher).
	Changer le type de graphique en graphique à colonnes
	Modifier le type de graphique en diagramme circulaire
	Changer le type de graphique en graphique en forme de beignet
	Modifier le type de carte en carte de zone polaire
	Modifier l'ordre de tri

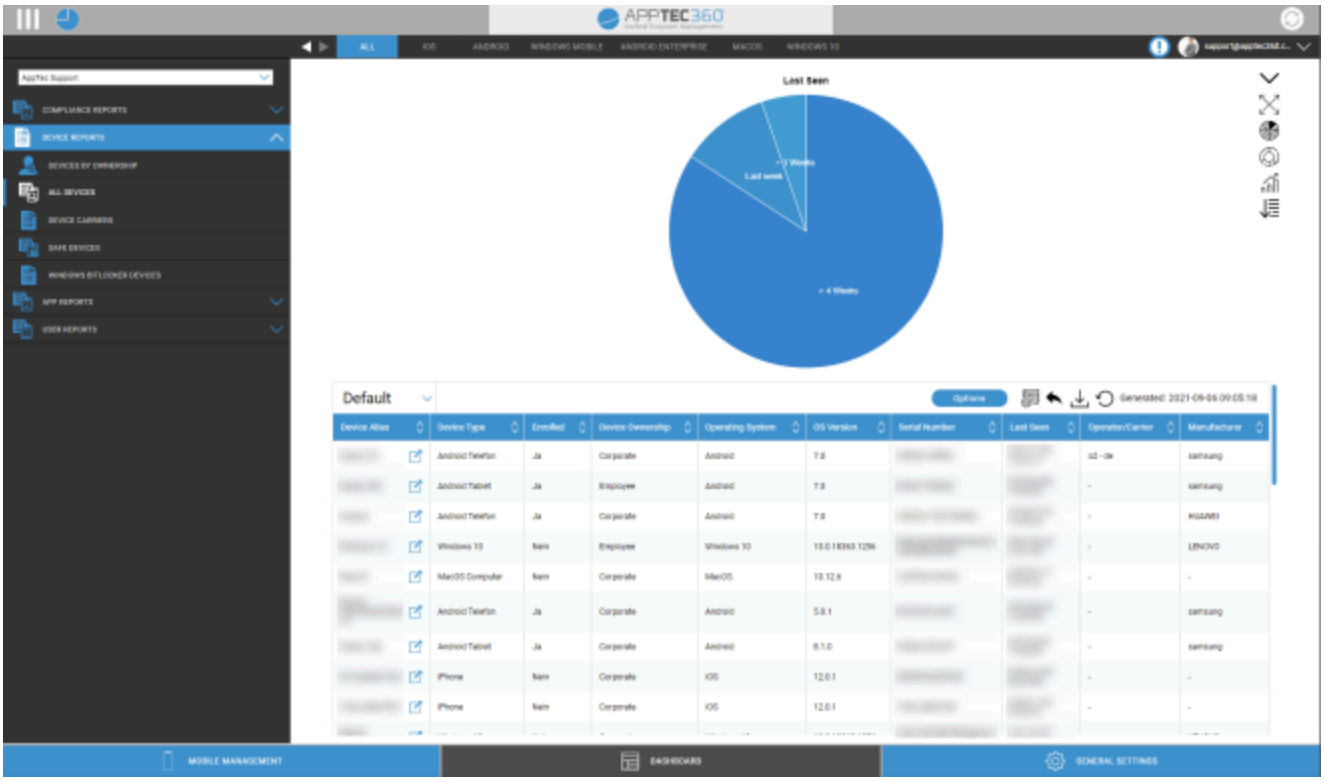
Rapports étendus

Le "rapport étendu" offre des aperçus détaillés et des graphiques sur les informations relatives aux appareils et aux utilisateurs.

Il existe quelques rapports par défaut, mais tous peuvent être modifiés manuellement pour ajouter ou supprimer des données à afficher.

Veuillez noter que vous ne pouvez modifier que manuellement les données affichées. La catégorie de rapport sélectionnée définit les données sur lesquelles elle est basée. Par exemple, vous ne pourrez jamais voir les appareils Android dans le rapport iOS dans Rapports sur les appareils Tous les appareils iOS

En haut à gauche, vous pouvez limiter les données du rapport à un certain groupe (et à tous ses sous-groupes). Par défaut, ce paramètre est défini sur le nœud racine, de sorte qu'il prend en compte TOUS les appareils et utilisateurs.



Contrôle étendu des rapports

Dans chaque synthèse, vous pouvez utiliser les fonctions suivantes pour modifier l'état comme vous le souhaitez :

	Cacher le graphique (si le graphique est affiché)
	Afficher le graphique (si le graphique est caché)
	Développer le graphique (si le graphique est réduit)
	Réduire le graphique (si le graphique est développé)
	Changer le type de graphique en graphique à colonnes
	Modifier le type de graphique en diagramme circulaire
	Changer le type de graphique en graphique en forme de beignet
	Modifier le type de carte en carte de zone polaire
	Modifier l'ordre de tri
	Modifiez les éléments suivants de la vue d'ensemble affichée : • Ajouter/supprimer des colonnes • Spécifiez l'ordre dans lequel les colonnes sont affichées • Afficher/masquer le graphique au-dessus du tableau • Sélectionnez la colonne utilisée pour le graphique • Filtrer les données de votre tableau
	Ouvrez le gestionnaire de configuration pour enregistrer et charger différents rapports.
	Réinitialise le rapport actuellement ouvert à sa valeur par défaut
	Exporter le rapport actuel dans un fichier .csv
	Régénérer les données et recharger le rapport actuel

Vous trouverez une liste de tous les rapports par défaut dans les pages suivantes.

Rapports de conformité

Appareils enracinés

Vue d'ensemble des appareils qui ont été rootés/jailbreakés.

Colonnes par défaut de ce rapport :

Alias du dispositif
Propriétaire de l'appareil
Courrier électronique
Système d'exploitation
Numéro de téléphone
Dernière visite
Fabricant

Dispositifs d’itinérance

Vue d'ensemble de tous les appareils en itinérance

Colonnes par défaut de ce rapport :

Alias du dispositif
Propriétaire de l'appareil
Courrier électronique
Type d'appareil
Système d'exploitation
Numéro de téléphone
Dernière visite

Appareils compatibles avec l’itinérance

Vue d'ensemble de tous les appareils qui ont activé l'itinérance mais qui ne sont pas nécessairement en cours d'itinérance.

Colonnes par défaut de ce rapport :

Alias du dispositif
Propriétaire de l'appareil
Courrier électronique
Type d'appareil
Système d'exploitation
Numéro de téléphone
Dernière visite

Dispositifs supervisés

Vue d'ensemble de tous les appareils supervisés en mode supervisé (iOS uniquement)

Colonnes par défaut de ce rapport :

Alias du dispositif
Propriétaire de l'appareil
Courrier électronique
Type d'appareil
Dernière visite

Dispositifs inactifs

Aperçu de tous les appareils qui ne se sont pas connectés au serveur au cours des 7 derniers jours

Colonnes par défaut de ce rapport :

Alias du dispositif
Propriétaire de l'appareil
Courrier électronique
Type d'appareil
Système d'exploitation
Dernière visite

Rapports sur les appareils

Appareils par propriétaire

Vous pouvez voir ici combien d'appareils ont été déployés en tant qu'appareils d'entreprise (appareils d'entreprise) et d'employés (appareils privés).

Colonnes par défaut de ce rapport :

Alias du dispositif
Propriétaire de l'appareil
Type d'appareil
Propriété des appareils
Système d'exploitation

Tous les appareils

Vous y trouverez une vue d'ensemble de tous les appareils avec les informations les plus importantes.

Colonnes par défaut de ce rapport :

Alias du dispositif
Type d'appareil
Inscrits
Propriété des appareils
Système d'exploitation
Version OS
Numéro de série
Dernière visite
Opérateur/transporteur
Fabricant

Porteurs d’appareils

Vous trouverez ici une vue d'ensemble de l'opérateur (fournisseur de services cellulaires).

Colonnes par défaut de ce rapport :

Alias du dispositif
Propriétaire de l'appareil
Courrier électronique
Système d'exploitation
Version OS
Opérateur/transporteur

Dispositifs SAFE

Vous pouvez voir ici une vue d'ensemble des appareils qui utilisent la version SAFE.

La vue d'ensemble et/ou SAFE n'étant disponible que pour les appareils Samsung, vous ne verrez pas les onglets habituels sous ce point.

Colonnes par défaut de ce rapport :

Alias du dispositif
Propriétaire de l'appareil
Courrier électronique
Type d'appareil
Dernière visite
Version SAFE

Dispositifs Windows BitLocker

Vous trouverez ici une vue d'ensemble des appareils Windows qui utilisent BitLocker.

Colonnes par défaut de ce rapport :

Alias du dispositif
Propriétaire de l'appareil
Courrier électronique

État de BitLocker

Rapports d’application

Vous y trouverez divers aperçus des applications. Dans tous ces rapports, vous pouvez cliquer sur une entrée pour voir quelles versions sont installées sur les appareils et à quelle fréquence. Dans cette vue, vous pouvez cliquer à nouveau sur une version spécifique pour voir quels appareils ont cette version spécifique installée.

Remarque : il peut s'écouler un certain temps avant que le système ne reçoive des informations actualisées de l'appareil. En outre, les rapports ne sont pas mis à jour toutes les minutes. Si vous venez d'attribuer une nouvelle application ou une nouvelle version, vous devrez peut-être faire preuve de patience pour connaître l'état actuel. En rechargeant manuellement le rapport, celui-ci sera forcé d'afficher les données les plus récentes disponibles.

Applications installées

Vous obtenez ici une vue d'ensemble de toutes les applications installées.

Colonnes par défaut de ce rapport :

Nom	Nom de l'application et/ou du service concerné
Identifiant	Identifiant précis de l'application/du service
Nombre total	Combien de fois cette application / ce service a-t-il été installé sur les appareils de l'utilisateur final ?

Applications les plus installées

Vous obtenez ici une vue d'ensemble des applications les plus installées.

Colonnes par défaut de ce rapport :

Nom	Nom de l'application et/ou du service concerné
Identifiant	Identifiant précis de l'application/du service
Nombre total	Combien de fois cette application / ce service a-t-il été installé sur les appareils de l'utilisateur final ?

Applications obligatoires

Vous trouverez ici une vue d'ensemble des applications obligatoires (obligatoires mandatées).

Colonnes par défaut de ce rapport :

Name	Name of the respective app and/or service
Identifier	Definite app/service ID
App Source	Which AppStore is involved: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Operating System

Applis sur liste noire

Vous obtenez ici une vue d'ensemble de toutes les applications définies sur liste noire.

Colonnes par défaut de ce rapport :

Nom	Nom de l'application et/ou du service concerné
Identifiant	Identifiant précis de l'application/du service
Source de l'application	Quel est l'AppStore concerné ? • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Système d'exploitation

Rapports des utilisateurs

Tarif

Vous obtenez ici une vue d'ensemble des tarifs téléphoniques et des cartes SIM de vos utilisateurs.

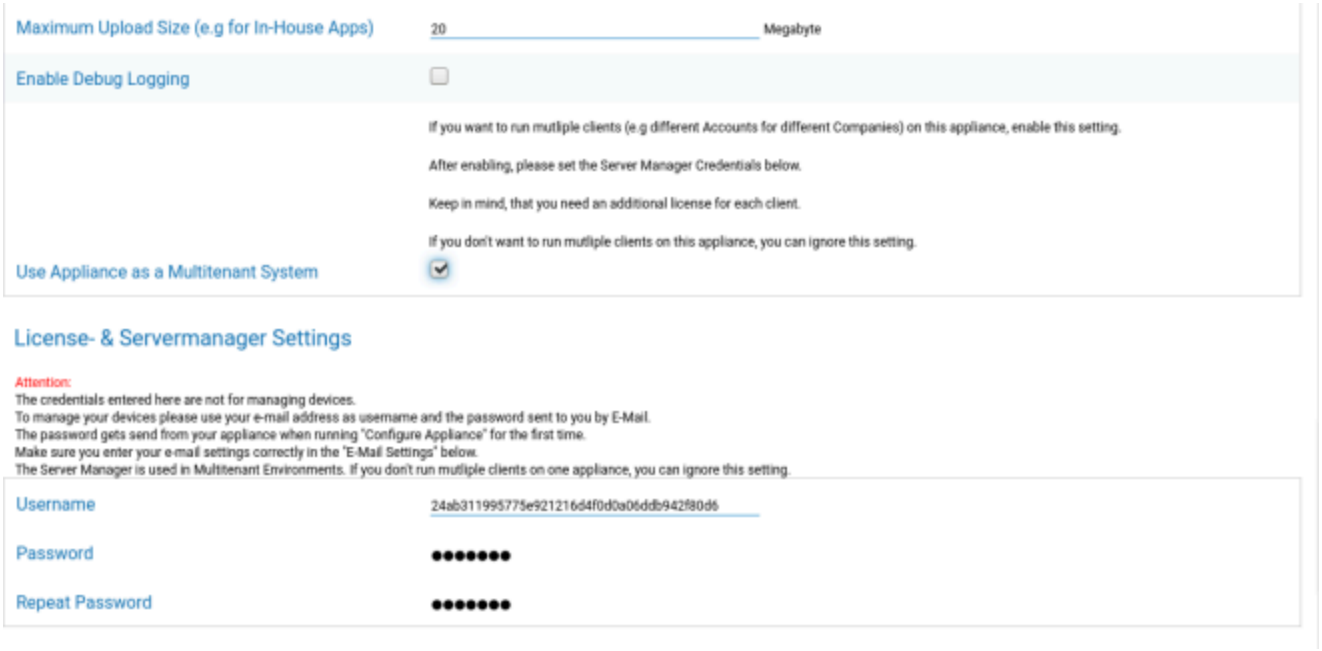
Colonnes par défaut de ce rapport :

Courrier électronique
Nom
Numéro de téléphone
transporteur
tarif
option
prix
Contrat annulé
Début du contrat
pendantTemps
mobileAndData
donnéesVolume
multiSIM
type
simCardSerial1
simCardSerial2
simCardSerial3
broche1
broche2
puk1
puk2
noter

Gestion des locataires multiples

L'EMM AppTec360 est capable d'héberger plusieurs locataires distincts, chacun avec ses propres utilisateurs et groupes, permissions et paramètres globaux.

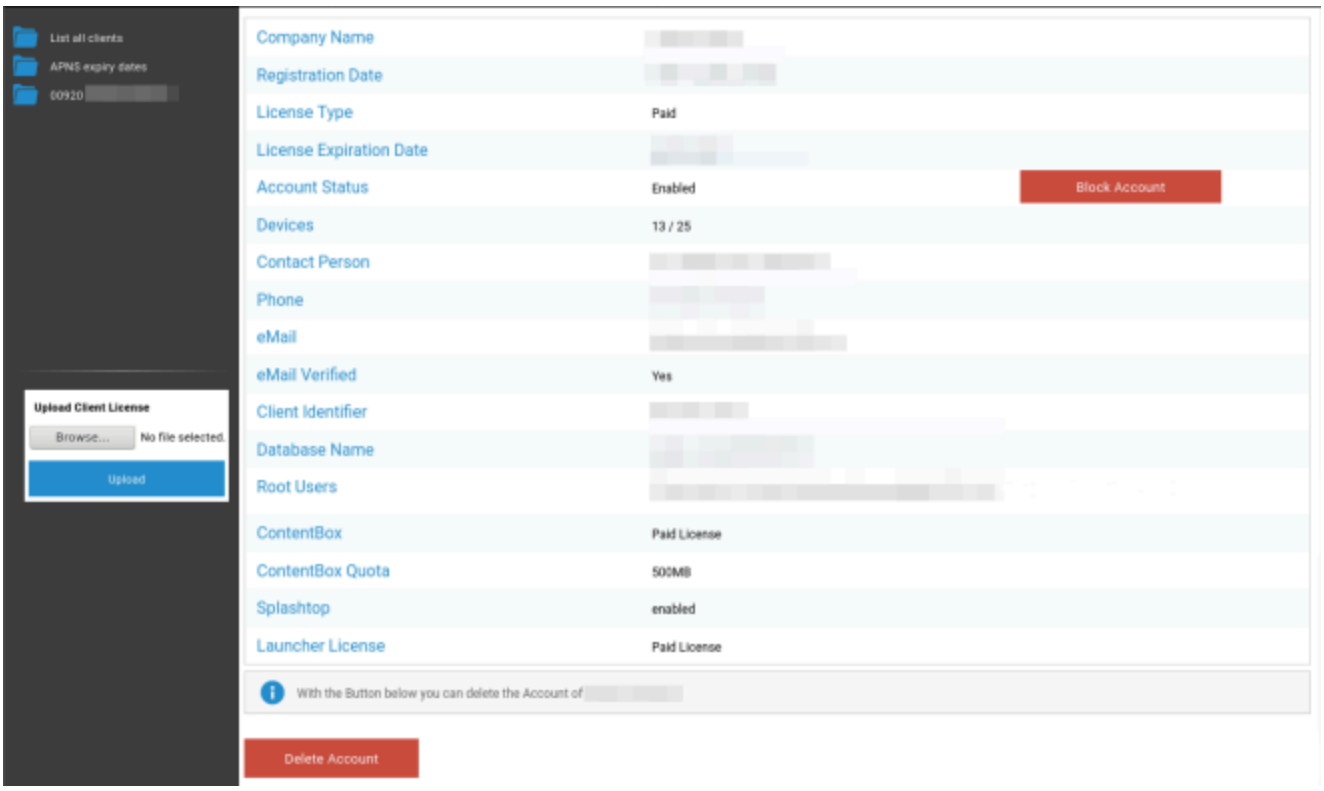
Pour activer les capacités Multitenant, vous devez les activer dans l'interface de configuration de l'Appliance dans "Step Three - Server Settings".



Dans le nouveau menu, définissez un nom d'utilisateur et un mot de passe pour le Gestionnaire de serveur. Enregistrez les paramètres et exécutez "Configure Appliance" dans "Step Five - License Agreement" pour appliquer les paramètres.

Une fois la configuration terminée, vous pouvez vous connecter avec les identifiants définis via l'interface normale de gestion des mobiles.

Après avoir ouvert une session, vous pouvez voir la vue suivante.



Sur la gauche, vous pouvez voir tous les locataires (dans ce cas, un seul avec l'identifiant 920) et sur la droite, les informations sur ce client. Vous avez également la possibilité de bloquer l'accès au compte et de supprimer le client (ATTENTION : cela supprimera toutes les données relatives à ce client).

Sur la gauche, vous pouvez télécharger une nouvelle licence client, qui peut être soit une mise à jour de licence pour un client existant, soit une nouvelle licence qui crée automatiquement un nouveau client. Lorsqu'un nouveau client est créé, un e-mail contenant le mot de passe de connexion est automatiquement envoyé à l'adresse e-mail pour laquelle la licence a été délivrée.

Pour obtenir une nouvelle licence client ou une licence mise à jour (par exemple, si vous avez besoin de plus de licences d'appareils), contactez votre représentant commercial.

Vues supplémentaires

Liste de tous les clients

Affiche une vue d'ensemble de tous les clients du système.

Identifiant du client	Identifiant du client
Identifiant	Identifiant du client
Base de données	Base de données
Nom de l'entreprise	Nom de l'entreprise
eMail	Personne de contact eMail
Vérifié	Si l'e-mail de la personne de contact est vérifié ou non
Pays	Pays
Dispositifs	Nombre de dispositifs enregistrés
Date d'inscription	Moment de l'attribution de la licence
Dernière connexion	Dernière connexion au compte administrateur
Licence	Affichage du type de licence (Gratuit|Payant)
Licence CB	Type de licence ContentBox (Gratuit|Payant)
Statut	Statut actuel du client AppTec
Expiré	Affiche, si la licence a expiré
iOS	Nombre d'appareils iOS
Android	Nombre d'appareils Android
Windows Mobile	Nombre d'appareils Windows Mobile
MacOS	Nombre d'appareils MacOS
Windows 10	Nombre d'appareils Windows 10
Android Enterprise	Nombre d'appareils Android pour entreprises
IOS BYOD (inscription des utilisateurs)	Nombre d'appareils IOS BYOD (inscription des utilisateurs)
IdO	Nombre de dispositifs IdO

Dates d’expiration de l’APNS

Affiche une vue d'ensemble des dates d'expiration des certificats APNS de tous les clients.

Identifiant du client	Identifiant du client
Nom de l'entreprise	Nom de l'entreprise
Date d'expiration	Date d'expiration du certificat Apple APNS
Info	Informations sur l'expiration

Contact

Des questions supplémentaires ? Il suffit de nous contacter à l'adresse suivante

Pour les questions techniques générales

support@apptec360.com

+41 61 511 3210

Pour les questions relatives à l’installation d’une appliance virtuelle

consulting@apptec360.com

+41 61 511 3214

Clause de non-responsabilité

AppTec GmbH