Configuration du téléphone ANDROID zéro en ANDROID entreprise

Objectifs du document

Le document a pour objectif de présenter les différentes étapes d'enrôlement des téléphone Android en Android Enterprise en mode Corporate-Owned Work Profile..
Ce mode permet de fournir un espace personnel et un espace professionnel. L'objectif est double :

- Fournir un catalogue d'applications « whitelistées » par l'entreprise via un PlayStore privé et laisser l'utilisateur installer des applications par le biais du PlayStore public via leur compte google personnel.
- Être dans un mode supporté par Android.

Les différentes étapes

Configuration de Android Zero Touch sur le smartphone

Lors de l'achat de téléphones Android, les revendeurs agréés par notre entreprise inscrivent les téléphones dans Android Zero Touch afin qu'ils soient gérés par notre entreprise

Au premier démarrage d'un Téléphone Androiud, Deux possibilités :

- Si le téléphone est un Samsung, le téléphone contacte le service Knox Mobile Enrollment (KME) puis le service Android Zero Touch (AZT)
- Pour tous les autres téléphones, le téléphone contacte uniquement le service Android Zero Touch (AZT)

Les services KME et AZT ont les mêmes fonctions. C'est un service sans inscription qui permet aux téléphones de savoir que c'est un téléphone géré par AG2R La Mondiale et qui indique quel MDM sera utilisé

Les téléphones doivent être à minima en version **Android 9.0** pour supporter à la fois le mode Android Entreprise et les protections MAM Intune

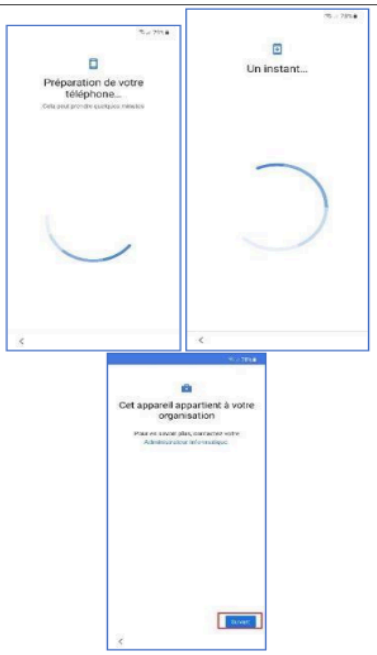
Procédure

Ci-après, la procédure d'enrôlement des téléphones Android à suivre étape par étape (les imprimes écrans proviennent d'un téléphone en version 12.0. Les écrans peuvent ainsi différer d'un téléphone à un autre

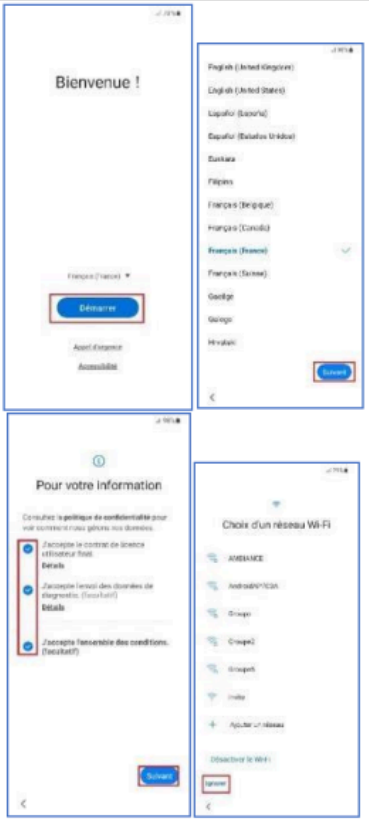
L'enrôlement Microsoft Intune est un enrôlement orienté utilisateurs. Il n'y aura donc pas de code d'enrôlement à générer de la part du technicien via le portail. L'enrôlement se fera via le compte et le mot de passe de l'utilisateur

➢ Insérer la carte SIM dans le téléphone. Une connexion Mobile ou Invité (accès Internet) est nécessaire pour effectuer les opératios ➢ Démarrer le téléphone	

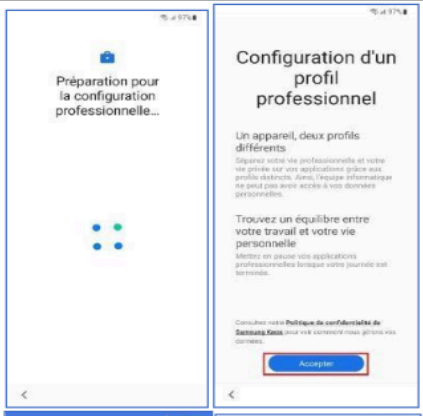
- Patienter un instant
- Le téléphone va contacter le service Android Zero Touch et va détecter que ce téléphone est géré par notre organisation. Cliquer sur « Suivant » (Photo 3)

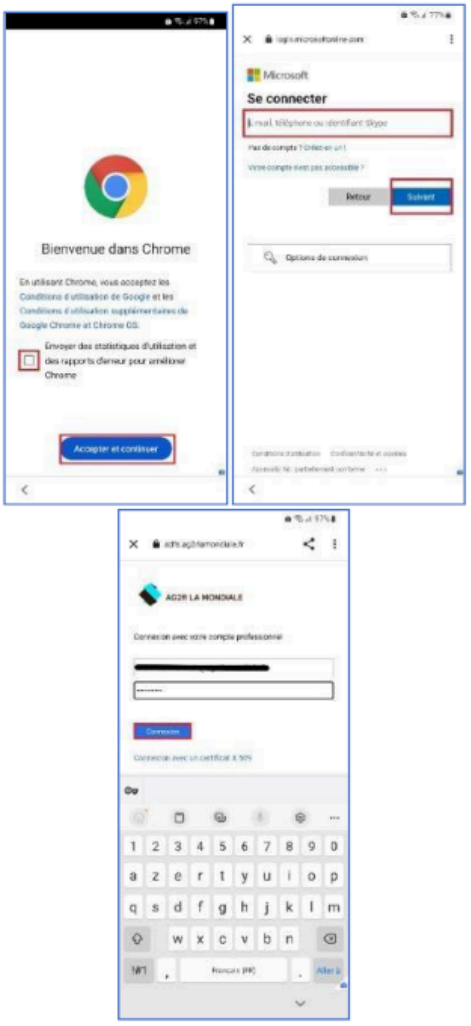
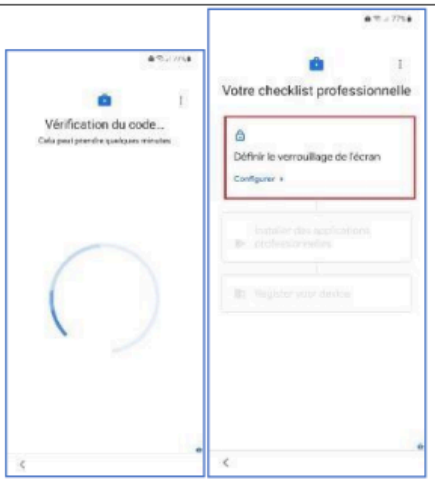


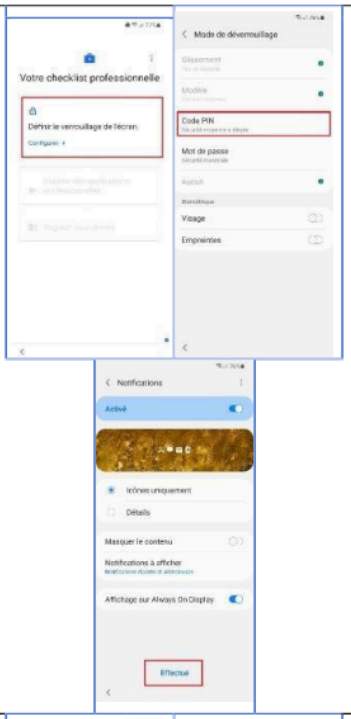
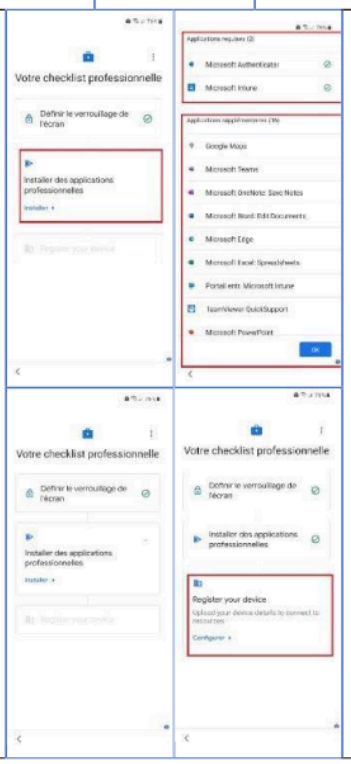
- Au premier démarrage du téléphone, vous serez inviter à passer les écrans de bienvenue et à configurer un réseau Wifi :
  - Cliquer sur « Démarrer » (Photo 1)
  - Sélection la Langue (Français) puis cliquer sur « Suivant » (Photo 2)
  - Accepter l'ensemble des conditions puis cliquer sur « Suivant » (Photo 3)
  - Cliquer sur « Ignorer » pour utiliser le réseau mobile 4G ou utiliser la Wifi Invité (Photo 4). En effet, un accès réseau est indispensable pour enrôler le téléphone



- La préparation du téléphone va commencer
- Cliquer sur « Accepter » (Photo 2)
- La création du profil professionnel va commencer. Patienter un instant

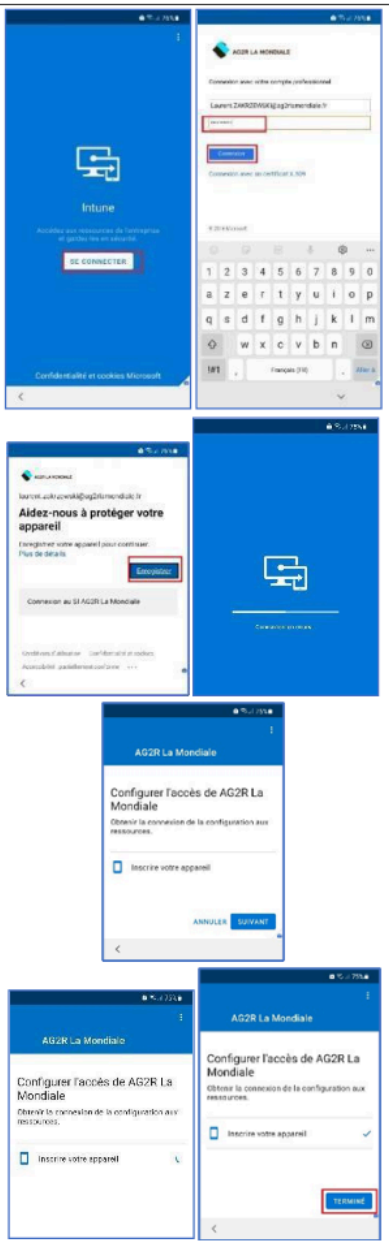


➢ Chrome va s'ouvrir. Décocher la coche et cliquer sur « Accepter et Continuer » (Photo 1) ➢ Saisir le nom de l'utilisateur concerné sous forme xxx@ag2rlamondiale.fr correspondant donc à l'adresse email de l'utilisateur (Photo 2) ➢ Saisir le mot de passe Windows de l'utilisateur puis Cliquer sur « Connexion » (Photo 3)	
➢ Patienter un moment (Photo 1) ➢ Intune vous listera les actions à effectuer (Photo 2)	

➢ Cliquer sur « Configurer » pour la partie « Définir le code de déverouillage » (Photo 1) ➢ Cliquer sur Code PIN et définir un code PIN (minimum 6 chiffres) (Photo 2) ➢ Cliquer sur « Effectué » (Photo 3)	
➢ Une fois le code PIN configuré, passer aux applications professionnelles (Photo 1) ➢ Les applications requises et supplémentaires sont listées. Par défaut, Microsoft Intune et Authenticator seront installées de suite et les applications supplémentaires seront installées via le Managed Google Play (Photo 2) ➢ Patienter (Photo 3) ➢ Une fois l'étape 2 terminée, on vous propose d'enregistrer votre appareil (Photo 4)	

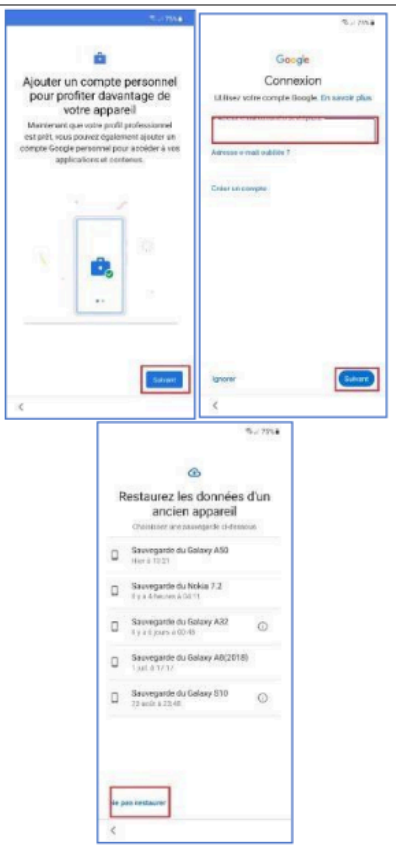
- L'application Microsoft Intune s'ouvre. Cliquer sur « Connecter » (Photo 1)
- Saisir le mot de passe Windows de l'utilisateur puis Cliquer sur « Connexion »
- Enregistrer l'appareil dans Azure AD. Cet appareil fera partie de la liste des appareills pour l'utilisateur concerné (Photo 3)
- Patienter (Photo 4)
- Inscrire l'apprail. Cliquer sur « Suivant » (Photo 5)
- Patienter (Photo 6)
- L'inscription est terminée. Cliquer sur « Terminer » (Photo 7)

Ses étapes permettent d'inscrire l'appareil dans Azure AD et de faire le lien entre l'appareil dans Intune et l'appareil dans AzureAD.
Les informations de conformité seront donc remontées dans AzureAD et est donc un critère pour appliquer des Accès Conditionnels. (Exemple : interdiction d'accèder aux données d'entreprise si le téléphone n'est pas conforme)

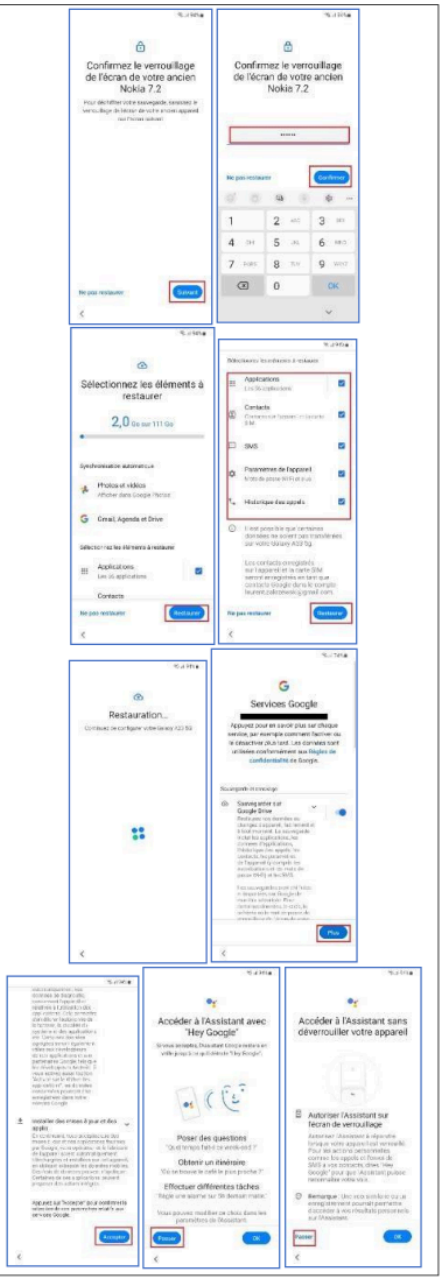


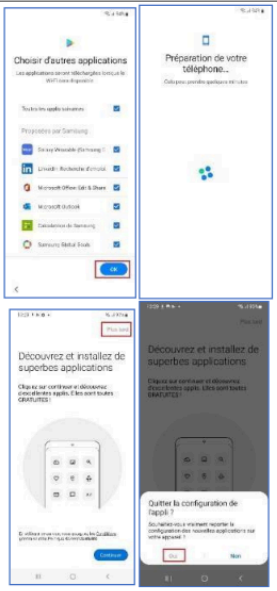
La configuration Professionnelle est maintenant terminée. Passons à la configuration personnelle des Services Google. Il est conseillé de configurer un compte personnel Google afin d'offrir la possibilité à l'utilisateur d'installer des applications personnelles.

- Cliquer sur « Suivant » (Photo 1)
- Saisir l'adresse mail personnelle de l'utilisateur puis Cliquer sur « Suivant »
- Par défaut, une sauvegarde peut être stockée dans le Cloud Google. Cliquer sur « Ne pas restaurer » ou sélectionner l'appareil à restaurer (Photo 3)



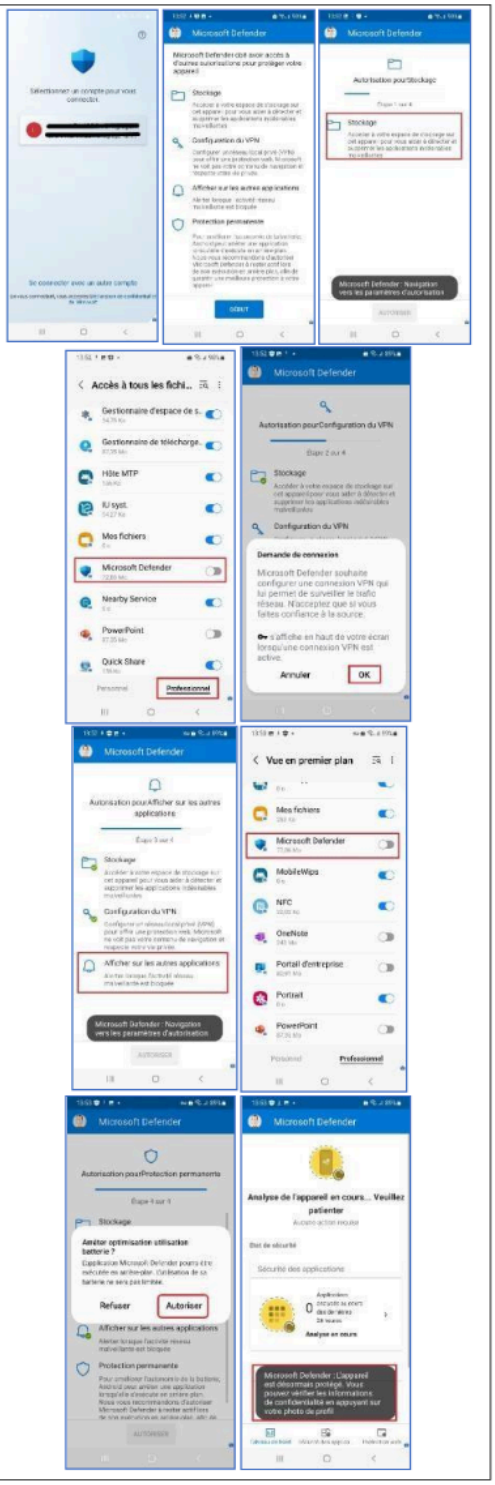
- Une fois l'appareil sélectionné, Cliquer sur « Suivant » (Photo 1)
- Saisir le code de déverouillage de votre ancien téléphone puis Cliquer sur « Confirmer »
- Sélectionner les éléments à restaurer puis cliquer sur « Restaurer » (Photos 3 et 4)
- La restauration est en cours (Photo 5)
- Activer les services Google pour votre compte personnel (Les données seront enregistrées dans le Cloud Google). Cliquer sur « Plus » (Photo 6)
- Cliquer sur « Accepter » (Photo 7)
- Cliquer sur « Passer » pour les assistants (Photos 8 et 9)



➢ Sélectionner tout ou en partie les applications à installer par défaut dans la partie personnelle de votre téléphone puis Cliquer sur « OK » (Photo 1) ➢ Le téléphone est en cours de préparation (Photo 2) ➢ Cliquer sur « Continuer » (Photo 3) ➢ Quitter la configurer en cliquant sur « Oui » (Photo 4)	
➢ Le téléphone est maintenant opérationnel. On distingue bien les deux espaces personnels et professionnels (Photo 1) ➢ Les applications professionnelles obligatoires s'installeront automatiquement par le réseau Mobile ou via une connexion Wifi. ➢ A noter que les applications professionnelles sont différenciées par un badge	

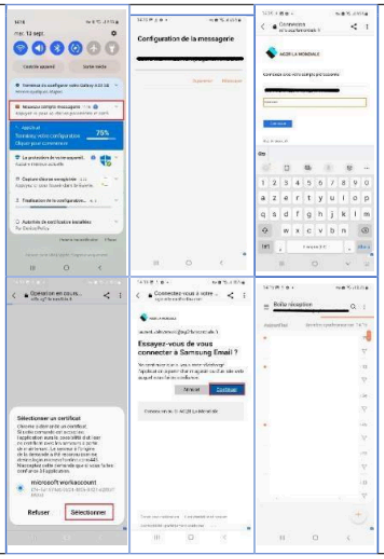
- Afin d'accéder aux applications professionnelles, il est indispensable de se mettre en conformité et de configurer l'Antivirus Microsoft Defender et de l'activer
- Une fois l'application Defender installée dans la partie professionnelle, Ouvrir l'application

- Sélectionner votre compte (il sera pré renseigné) (Photo 1)
- Cliquer sur « Début » (Photo 2)
- Cliquer sur « Stockage » (Photo 3)
- Autoriser l'appli à accéder aux fichiers (Photo 4)
- Une demande de connexion vous sera demandé. Cliquer sur « OK » (Photo 5)
- Cliquer sur « Afficher sur les autres applications » (Photo 6)
- Autoriser Microsoft Defender à être en premier plan (Photo 7)
- Cliquer sur « Autoriser » (Photo 8)
- Microsoft Defender est maintenant activé et commence à scanner les applications installées (Photo 9)



Vous pouvez maintenant configurer la messagerie

- Dans la barre de notification, Cliquer sur « Nouveau compte de messagerie » ou ouvrez directement l'application Email dans la partie Professionnelle (Photo 1)
- Votre compte est pré renseigné (Photo 2)
- Saisir votre mot de passe de session Windows (Photo 3)
- Cliquer sur « Sélectionner ». C'est un comportement normal. Le téléphone pré sélectionne le certificat à utiliser (Photo 4)
- Cliquer sur « Continuer » (Photo 5)
- L'accès à la messagerie est maintenant opérationnel (Photo 6)

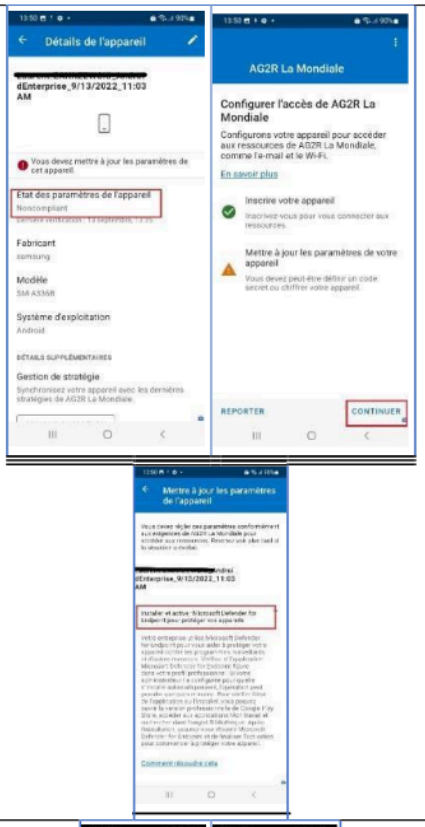


- Facultatif : expliquer à l'utilisateur final comment créer ou connecter un compte Google pour pouvoir accéder au Play Store Personnel et installer des applications.

- Information : Le droit à la déconnexion
- Il est possible durant le week end ou les congés de désactiver son espace professionnel afin de ne pas recevoir les notifications de son espace professionnel (Email par exemple)

Commenté [J1]: Tu aurais une capture d'écran pour comment le désactiver ?

Remarque :

➢ Microsoft Intune permet de vérifier en autre l'état de conformité du téléphone. Ici le téléphone n'est pas conforme ➢ Pour en savoir plus, Cliquer sur « Vous devez mettre à jour des paramètres de l'appareil » (Photo 1) ➢ Cliquer sur « Continuer » (Photo 2) ➢ L'application indique qu'il faut installer et configurer Microsoft Defender pour se mettre en conformité (Photo 3)	
➢ Un autre exemple de blocage potentiel, le MAM Intune utilisé dans les applications Microsoft. ➢ Une information vous est donnée au lancement de l'application pour voir si tout est conforme (Ici « Tout est à jour » présente une anomalie) (Photo 1) ➢ L'accès a été bloqué et vous donne la raison (Version minimale autorisée est la version 12) (Photo 2)	

➢ Si l'utilisateur clique sur « Mettre à jour », le Play Store s'ouvre afin de mettre à jour l'application **PS :** Si une application est mise à jour dans un container, elle sera automatiquement mise à jour dans l'autre container ➢ **Exemple :** La politique entreprise met à jour automatiquement les applications du container professionnel. Si l'application Chrome se met à jour dans le container professionnel, elle sera également mise à jour dans le container personnel si l'application est installée dans le container personnel