RFiT
SOLUTIONS CONNECTÉES POUR L'INDUSTRIE

TOOLTRACK
GESTION ET TRAÇABILITÉ DE MATÉRIEL ET D'OUTILLAGE

Deploiement de TINY MDM

Notre solution dédiée :

TOOLTRACK®

Destinataire : Mr Prénom Nom - Numéro de téléphone			
Rév.	**Auteur**	**Date**	**Commentaires**
1	rcoblentz	18/12/2019	Création

PREAMBULE

RFIT TECHNOLOGIES détient des Droits de Propriété Intellectuelle sur le contenu du présent document, ainsi que sur le savoir-faire qui y est présenté.

RFIT TECHNOLOGIES entend conditionner l'accès et la communication du présent document à l'engagement préalable du destinataire de respecter ces droits de propriété intellectuelle et de conserver, dans les conditions les plus strictes de confidentialité et à ne pas divulguer ou exploiter toutes les informations qu'il aura acquises ou qui ont été portées à son attention, avant, pendant ou après l'exécution du présent document.

Le détournement, l'utilisation non autorisée ou la divulgation de ces informations sont susceptibles de causer un préjudice extrêmement important à **RFIT TECHNOLOGIES**.

Aucune licence sur les droits de propriété intellectuelle n'est conférée au destinataire de ce document.

Par conséquent, toute utilisation, reproduction, ou représentation non autorisée par la société **RFIT TECHNOLOGIES** du contenu de ce document est strictement interdite sans l'autorisation préalable de la société **RFIT TECHNOLOGIES**.

Le destinataire reconnaît avoir reçu le document et accepte les termes de son préambule.

CONTEXTE

Comment pouvoir gerer le deploiement d'apk sur un parc ? Pouvoir limite l'usage des appareils a un but purement professionnel et limiter les bug resultant de mauvaise manipulations des utilisateur, le tout sans aucun deplacement ?

Tiny MDM parametttré par RFIT permet tout cela et bien plus encore.

Dans cet situation nous verrons la procedure pour bloquer un terminal sur une seul application sur laquel nous aurons la mains mise sur son deploiement, ses maj, ainsi que la securité du terminal.

support@rfit-tech.com

N'hésitez pas à zoomer sur les images pour mieux voir la manière dont les menus sont organisés.

1 PREMBULE AU DEPLOIEMENT (DESTINE AU DEV)

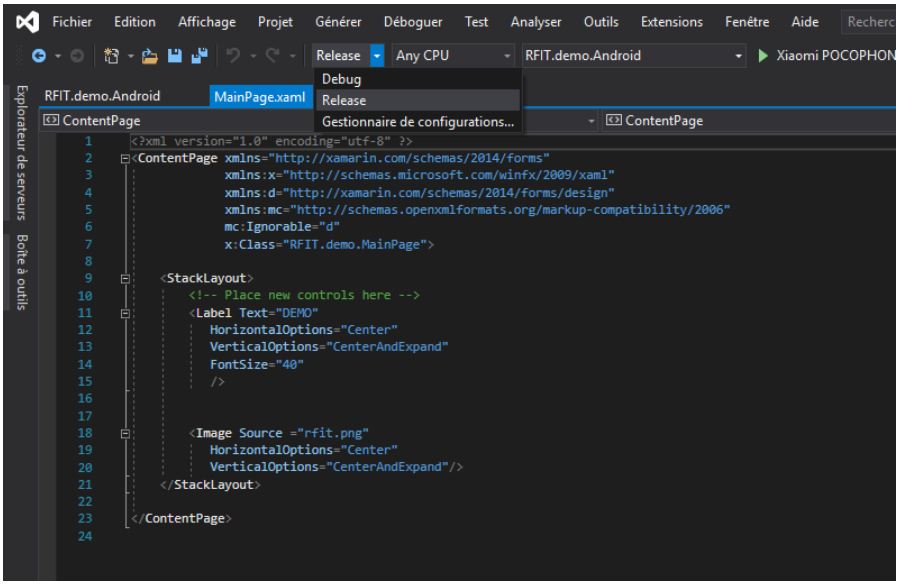
Avant de continuer, nous allons faire un point sur les condition necessaires a la publication d'une apk (car c'est ici bien le but). Cette partie est exclusivement reserver au dev, en effet tinyMDM utilise l'acces au playstore pour crer un store privé afin de deployer les apk. Hors ces apk demandent certaines conditions afin de pouvoir etre publiées sur le store. Nous allons voir les conditions necessaires.

Acceder depuis vos dossier a Y:\02 - Techniques\10 - Publication ANDROID (certificat)

Copier l'integralié des fichiers/dossiers et coller les dans :
C:\Users\[MyUser]\AppData\Local\Xamarin\Mono for Android

Une fois cela fait redemarrer visual studio.

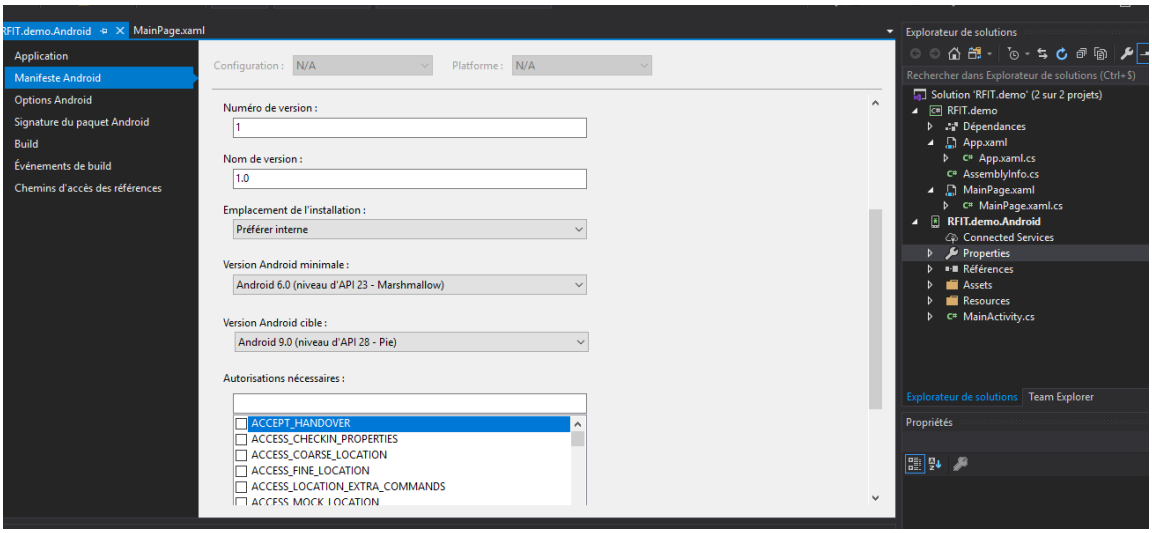
Il faut avant de compiler notre apk passer en release en haut.



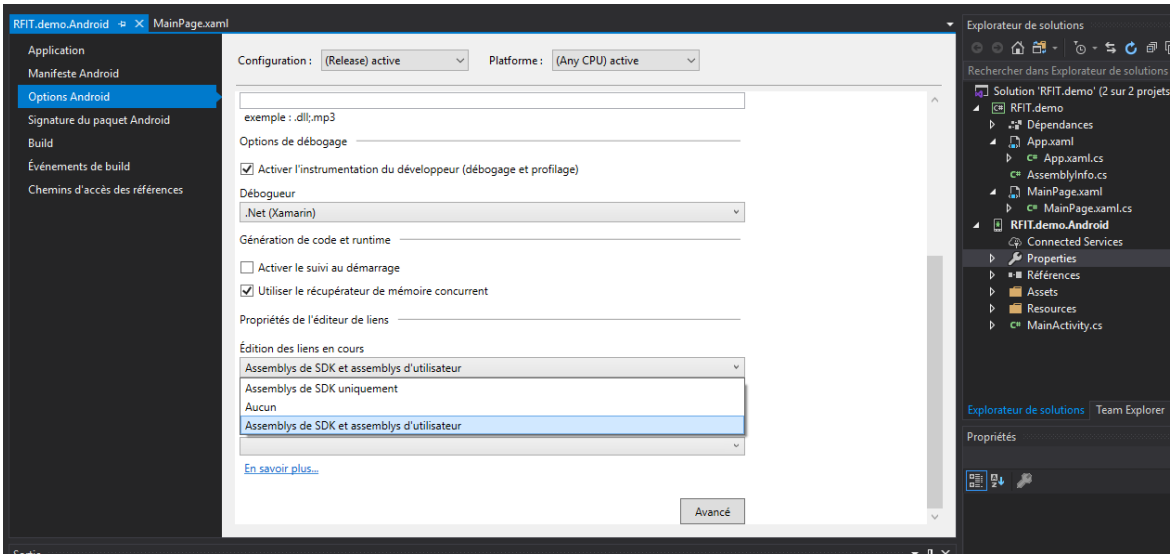
En suite, accedons au propriétés du projet android (double clique sur propriété).

Sous application : lui donner un nom.

Sous manifest Android : pensez à bien sur mettre à jour a chaque maj le numero de version, et le nom de version. La version minimal d'android doit etre obligatoirement la version 6.0 api23 et la maximale la plus haute disponible (ici 9.0 api28). Les versions precedantes peuvent poser probleme car les chemin d'acces interne a l'apk sons gerer differament par le playsotre.

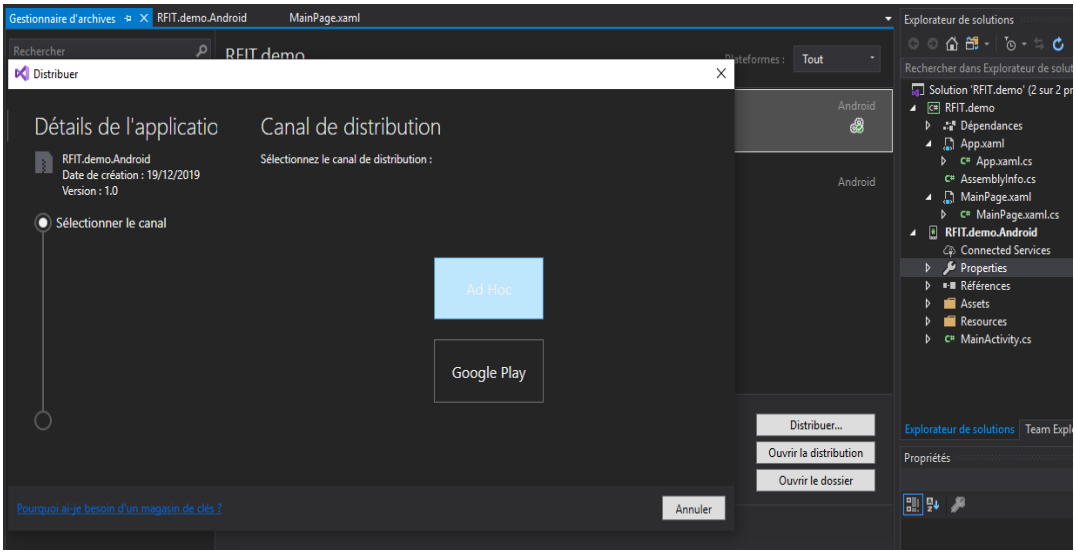


Sous options Android : passer la configuration en release aussi en haut et en bas l'édition des liens en cours doit etre mise sur « Assemblys de SDK et Assemblys d'utilisateur ».

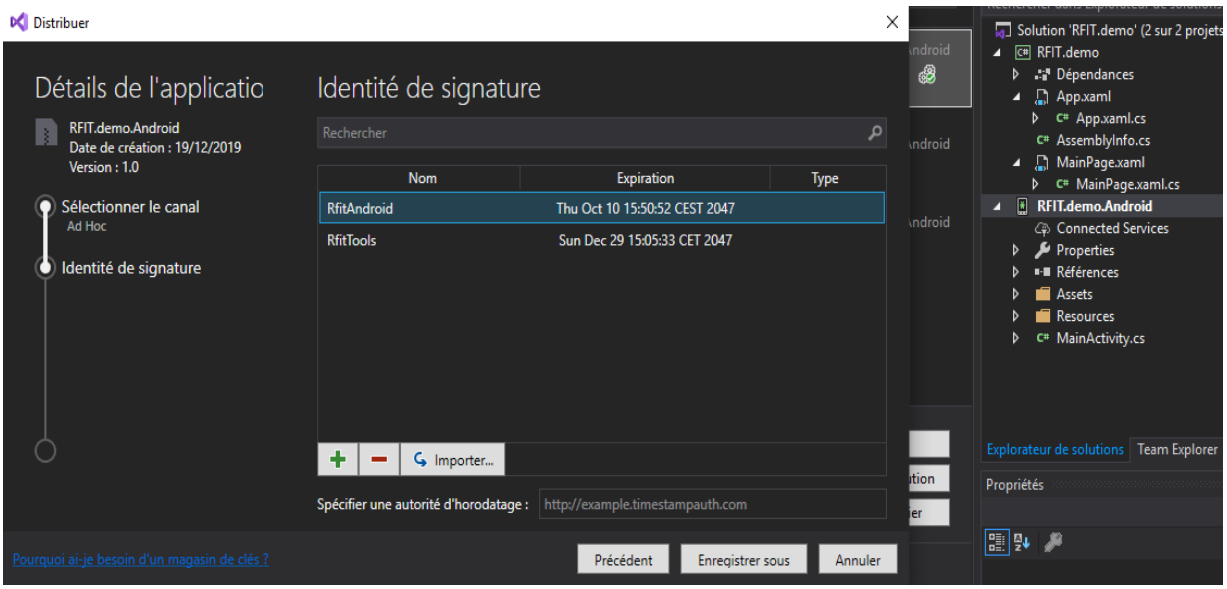


Je vous conseille de regénérer la solution histoire de verifier que cela n'est pas crée de bug. Une fois fait, cliquez sur generez, puis Archiver. Cela peut durer un certain temps.

Une fois fait, un menu apparait en bas : Cliquez sur distribuer, puis sur AD-HOC.



Selectionnez RfitAndroid, le mdp est Rfit/26, puis enregistrer sous. Voila, votre apk est prete a etre publié.



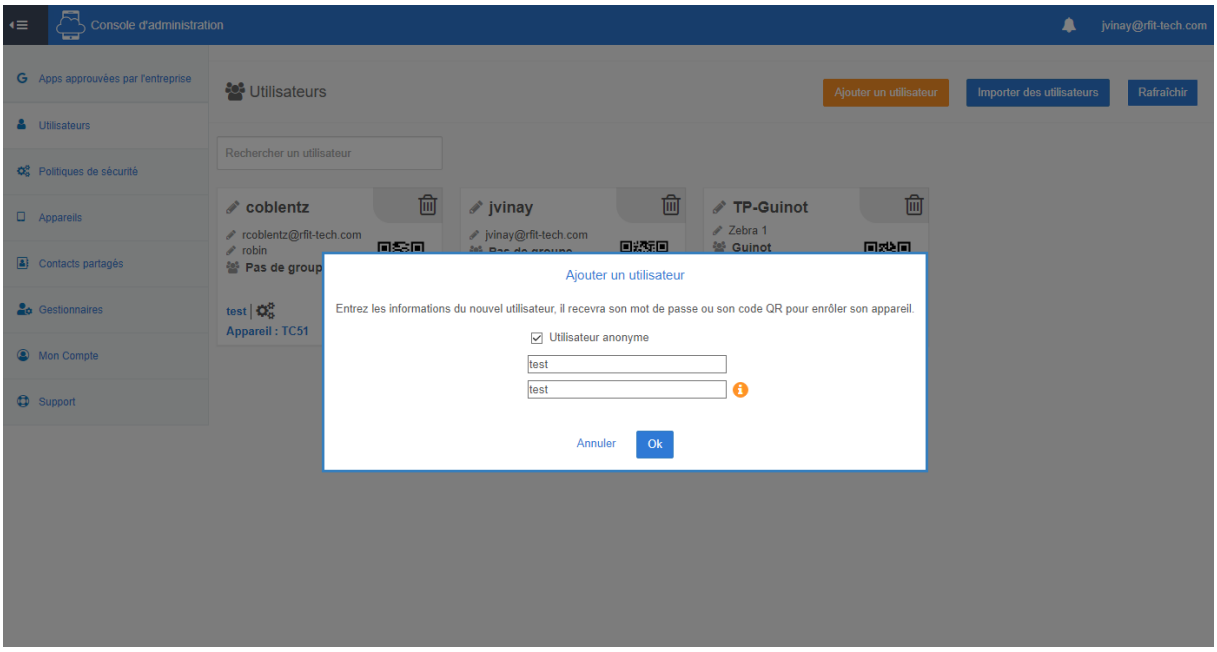
N'oubliez pas a chaque version d'augmenter le numero de version de l'application ainsi que sont numero de build, sans quoi une MAJ d'APK n'est pas possible par la suite dans le store si les versions sont identiques ou inferieurs.

2 CONNECTION A TINY MDM

Rdv sur www.tinymdm.fr puis s'identifier, les identifiants sont dispo vous savez ou.

3 CREATION D'UN NOUVEL UTILISATEUR

Cliquez sur ajouter un utilisiteur (en haut a droite), cochez utilisateur anonyme, entrez un nom correspondant puis un pseudo pour cet USER (ici test / test).



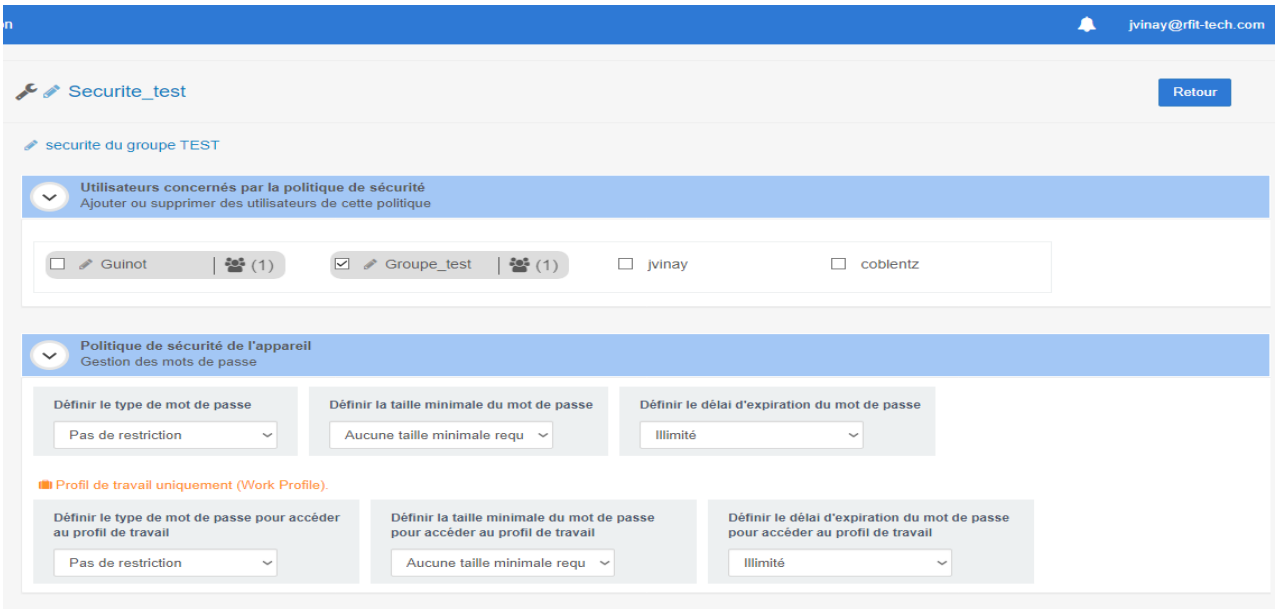
4 CONFIGURATION DE GROUPE

On peut l'ajouter à un groupe, si plusieurs appareils sont concernés par la commande, ici groupe_test.

Il n'y aura qu'a taper le meme groupe name a un autre user pour l'ajouter au groupe, à noter que nous pourrons grace a cela faire des modification sur l'integralité des user d'un meme groupe.

5 POLITIQUES DE SECURITE

Attaquons nous à la partie securité. On commence par crer une nouvelle politique de sécurité . Pour cela cliquz sur politique de securité (en haut a gauche) puis sur créer une politique de sécurité. On lui donne un nom(ici securite_test) ainsi qu'une description. On coche egalement le groupe d'user auxquels on veut appliquer cette politique (ici Groupe_test).

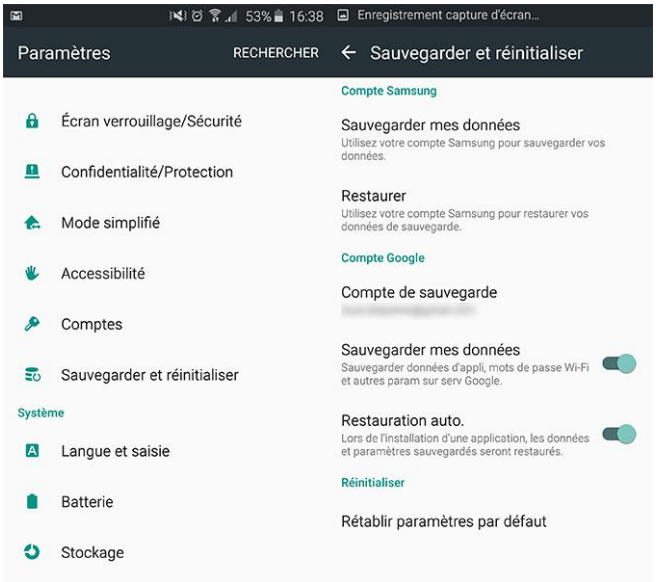


Nous parametterons tous cela plus tard, car pour la suite nous aurons besoins de voir si tout ce passe bien, nous allons donc lier notre terminal a tiny MDM.

6 INSTALLATION DE TINY MDM

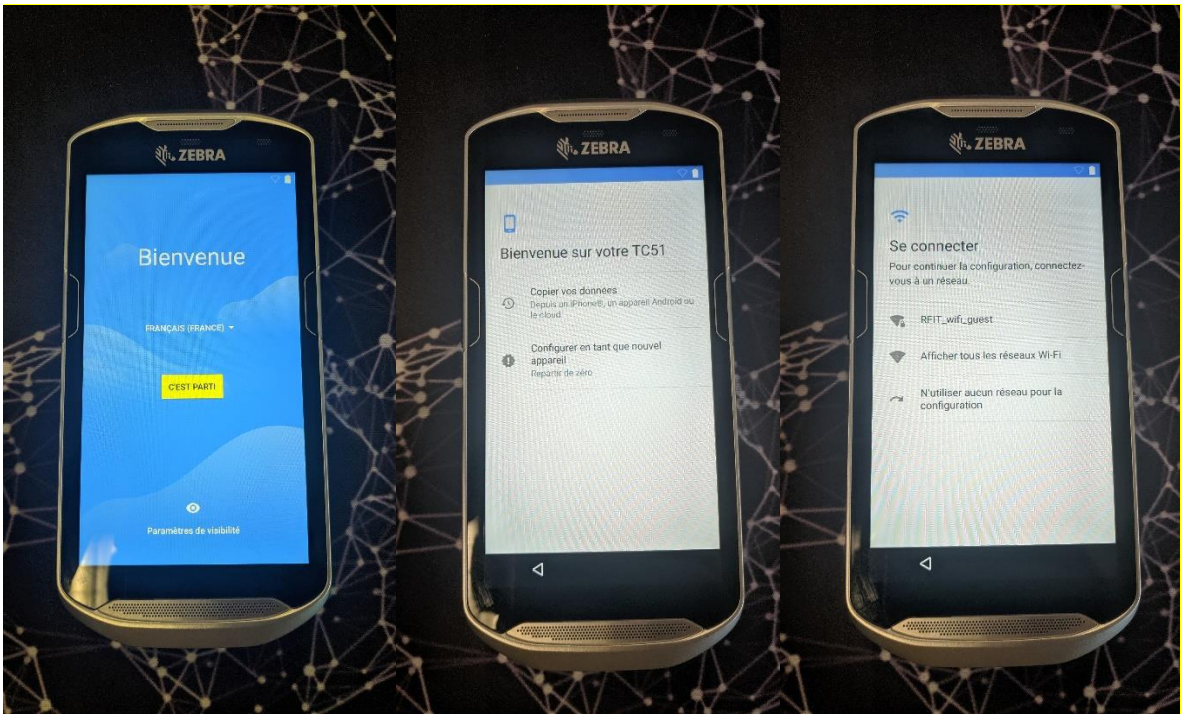
Pour installer tiny mdm sur un appareil, il faut que se soit ou la 1ere utilisation de cet apppareil ou alors le remettre a l'etat d'usine de manière a nous retrouver sur la page de 1ere configuration.

Pour cela acceder au paramette, sauvegarde et reinitialisation puis reinitialiser aux parametres d'usine.

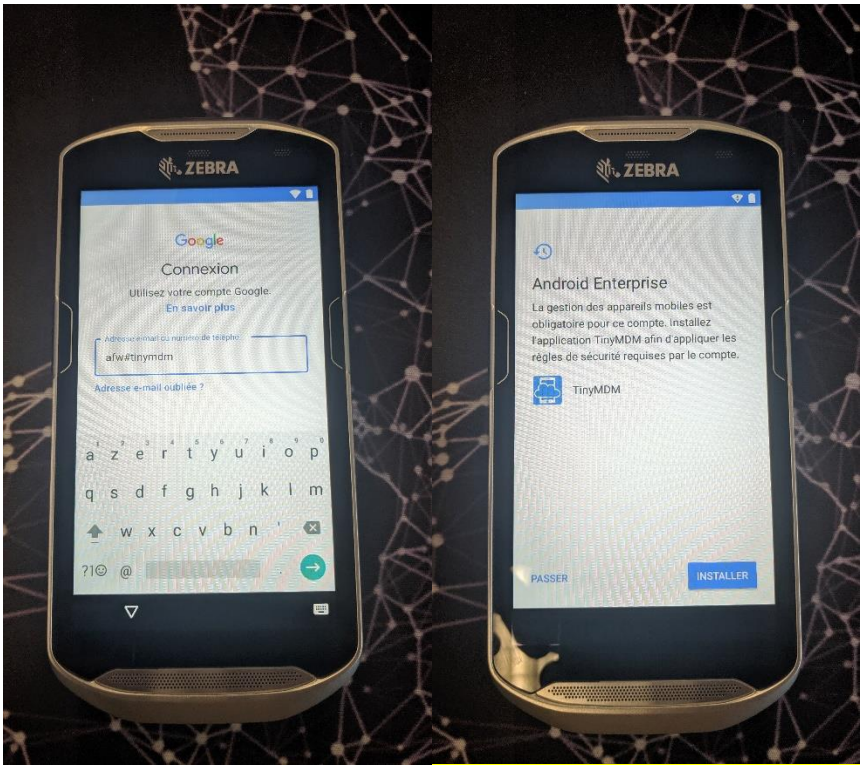


Une fois sur la premiere page de parametrage, selectionner la langue (ici francais), puis cliquer sur suivant

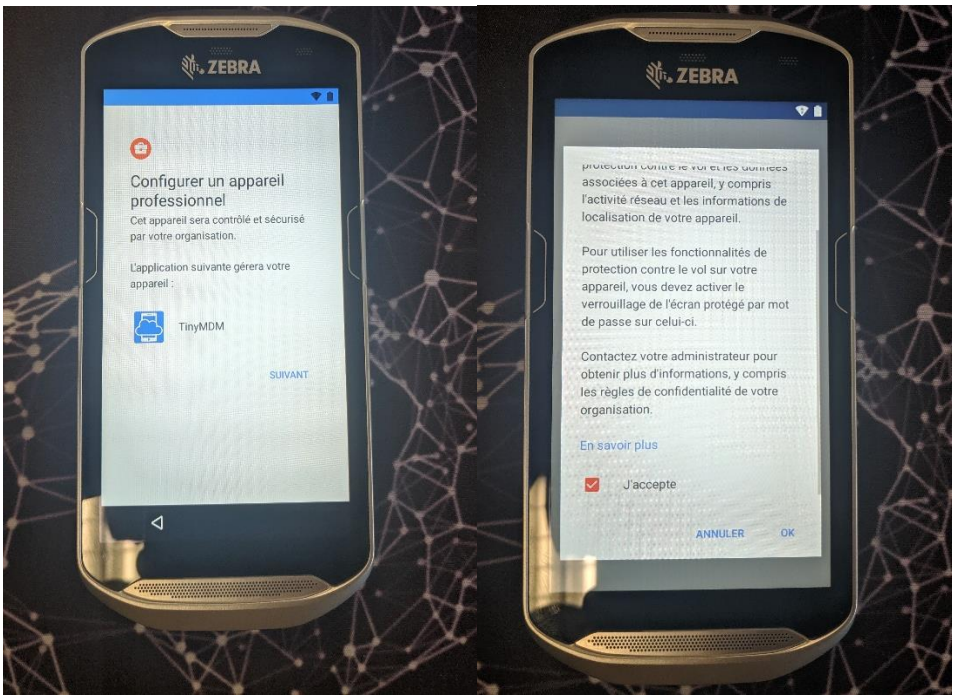
Configurer le en tant que nouvel appareil, connecter le wifi, patientez pendant la recherche de MAJ.



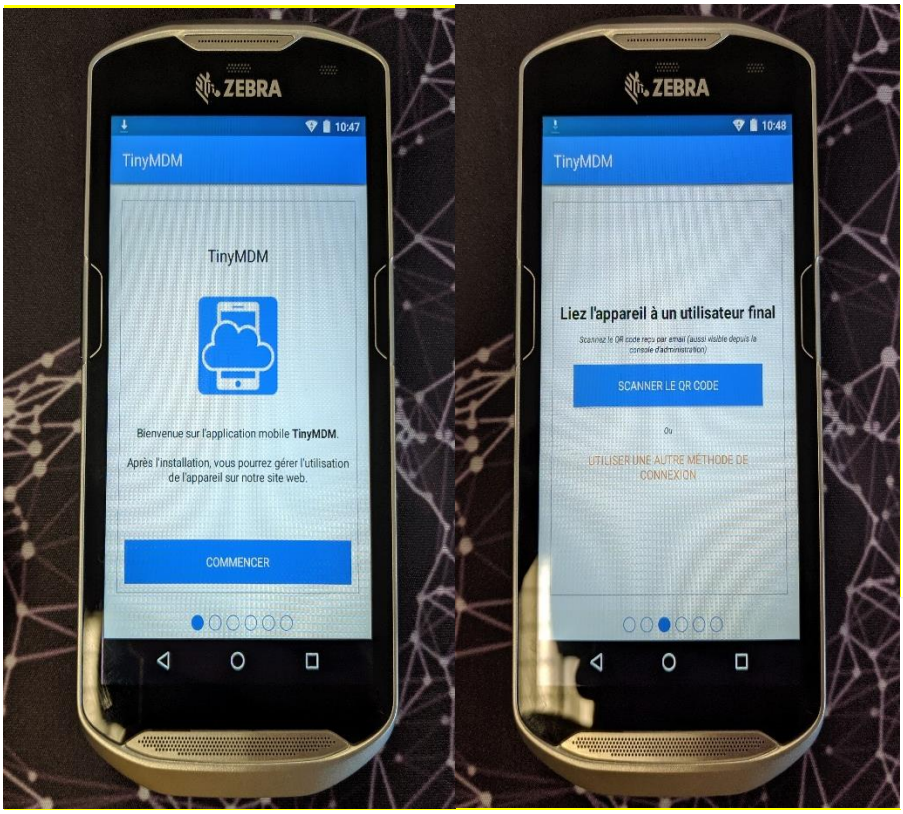
Entrez ***afw#tinymdm*** a la place du compte google puis cliquez sur suivant. On vous proposera par la suite d'installer TinyMDM. Installer-le.

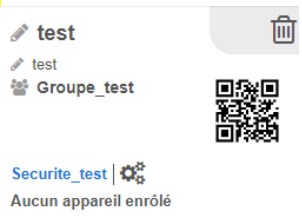


Ensuite il vous sera proposé de le configurer comme un appareil professionnel : cliquez sur suivant, scrollez en bas pour accepeter les conditions.



Cliquez sur commencer et acceptez. Vous allez vous retrouver sur la page pour lier un appareil a un user. Il vous suffit depuis le site tinymdm d'acceder a utilisateur sur la console d'administrateur (la ou l'on a crer l'user « test »), et de scanner son QR-CODE. L'appareil se met a jour, puis cliquez sur commencer. Voila l'appareil est lié.

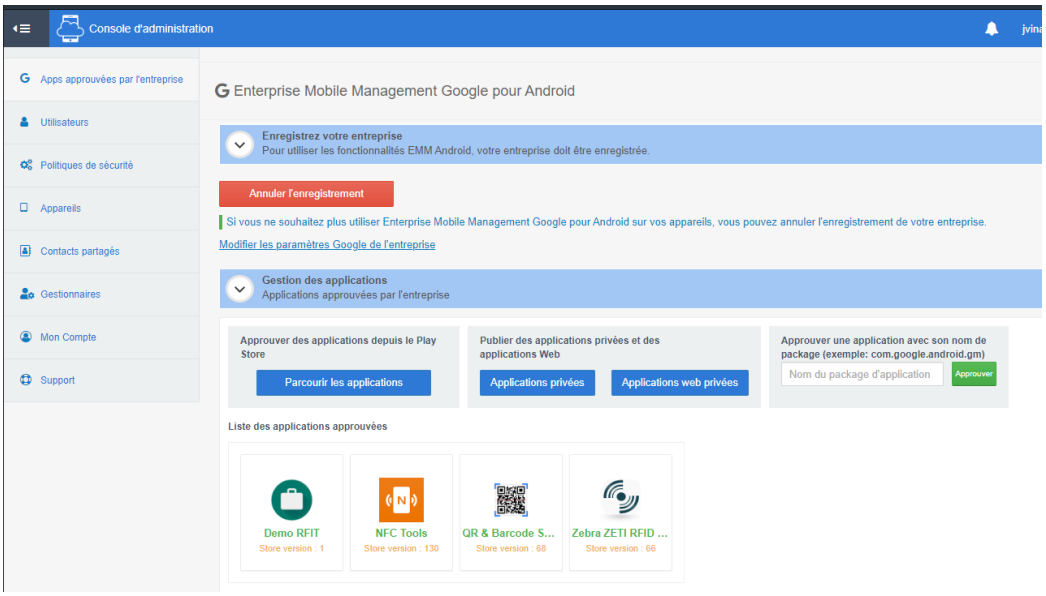




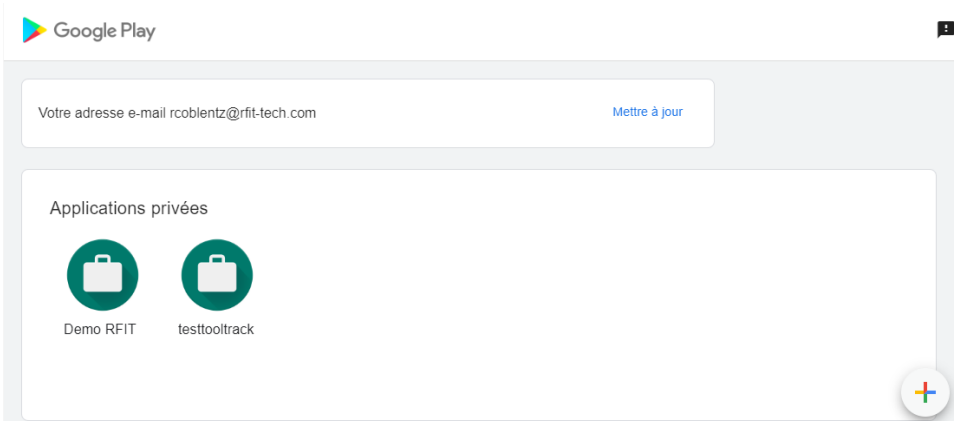
7 DEPLOIEMENT SUR PLAYSTORE

Rendez-vous sur la console tinyMDM, section Apps approuvées par l'entreprise.

7.1 APK DEVELOPPE EN INTERNE



Cliquez sur application privées, puis sur le plus en bas a droite afin d'ajouter une application.



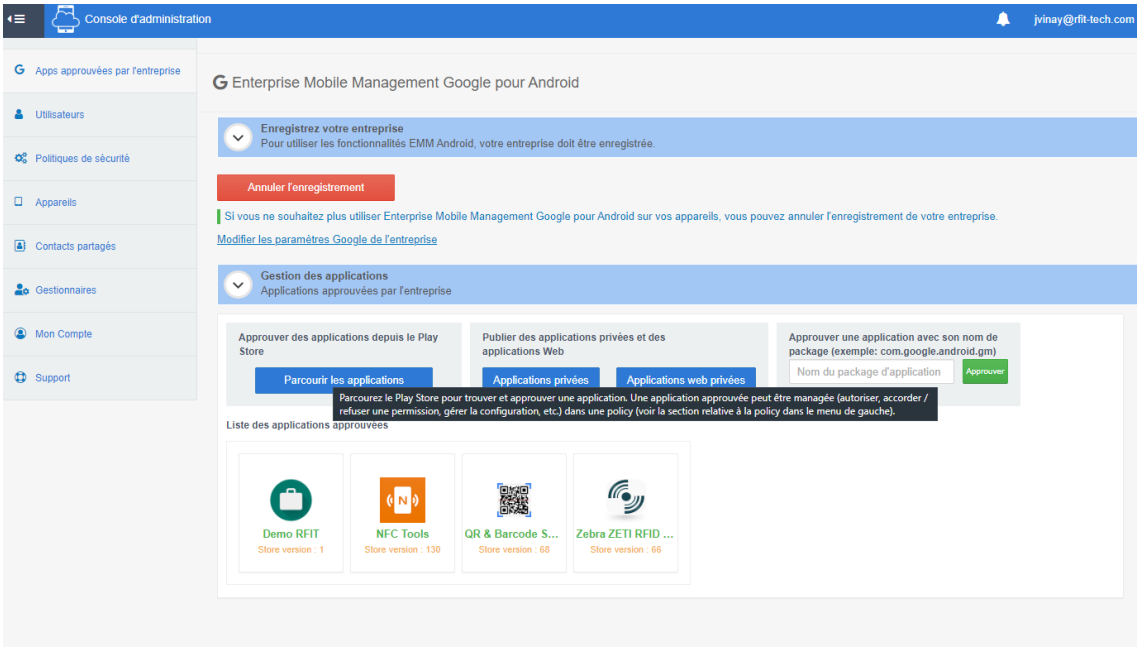
Il ne vous reste plus qu'a trouver un titre et upload votre apk.

Pour mettre a jour l'apk, penser bien a augmenter le numero de version et ne nom de version (les 2 doivent etre upgrade dans visual studio).

Cliquez sur votre application sans vos applications privé sur la console tiny MDM, vous pourrez alors modifiez le nom et upload une apk de version superieur.

7.2 APK DISPO SUR PLAYSTORE

Pour deployer des applications disponibles sur le playstore, rien de plus simple : cliquez sur « Apps approuvées par l'entreprise » puis sur « parcourir des applications depuis le playstore ».



Cherchez sur le playstore l'application que vous voulez deployer (ici speedtest) et cliquez sur approuver. Cliquez sur « reste approuvée… ».

Voila l'appli est autorisé sur votre store privé.

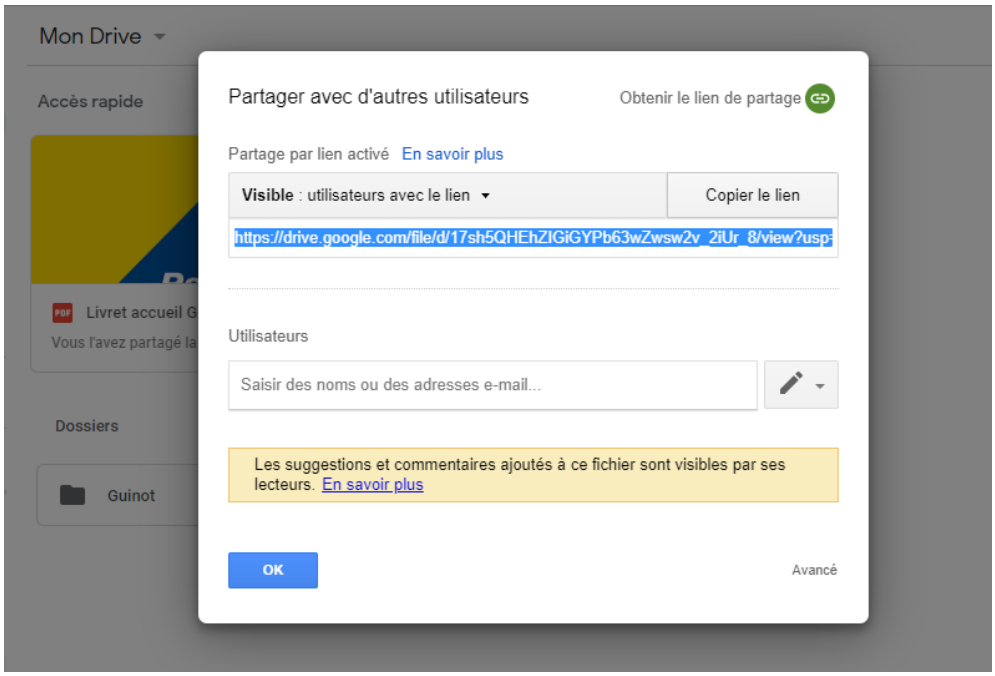
7.3 DEPLOIEMENT DE PDF OU FICHIER

Pour deployer des fichier pdf par exemple on peut les transformer en application via tiny mdm.

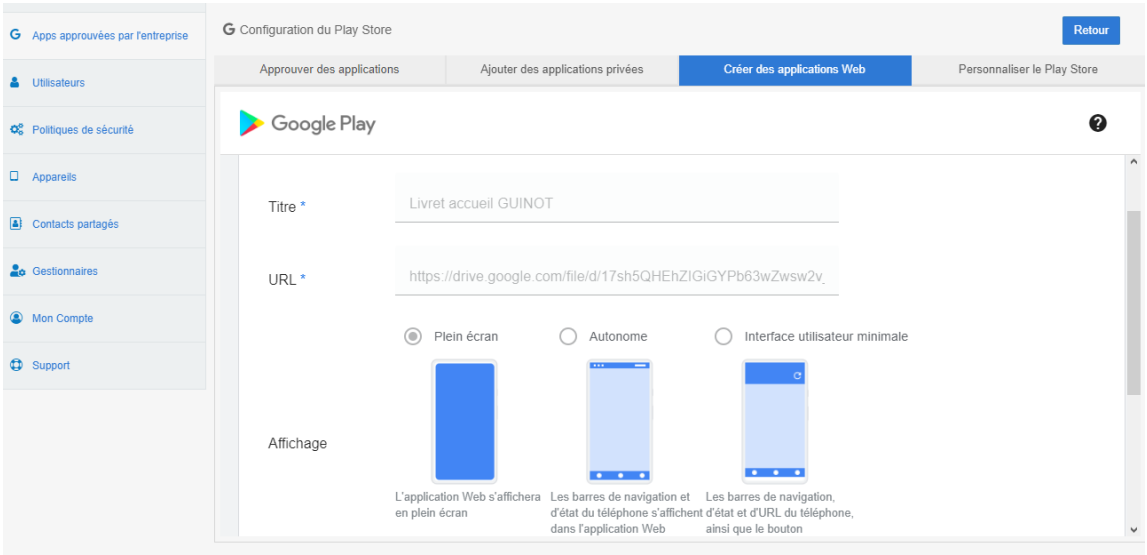
Pour cela il faudra déjà heberger le pdf sur un google drive (j'utilise le google drive de nas.rfit@gmail.com , ce compte sert a la gestion des mail du nas, et pour les infos de transfert de donnée entre azure notre NAS, toutes les infos de connexions sont sur le wiki).

Ensuite créez un dossier pour le client et glisser y le pdf afin de l'upload . Une fois l'upload fini, faite clique droit dessus, partagez.

Un onglet s'ouvre, cliquez sur le liens en haut a droite de celui-ci « obtenir le liens de partage ». Gardez le lien qui apparait il nous sera utile.

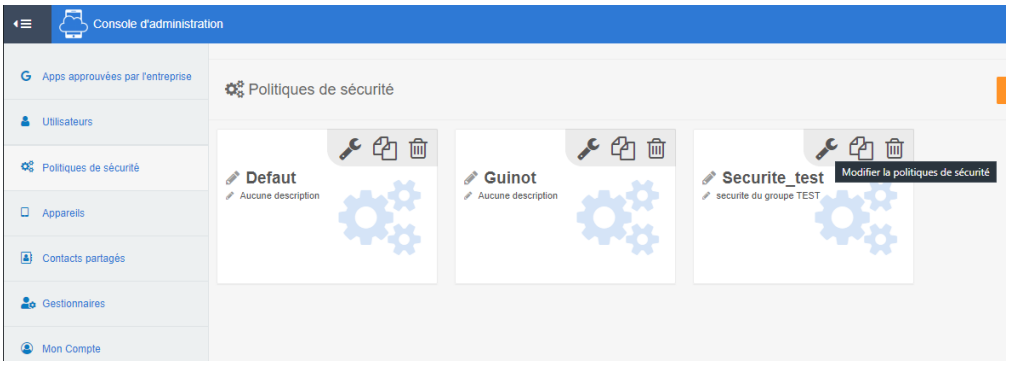


Rdv dans TinyMDM, dans la section «Apps approuvé par l'entreprise ». Puis application Web privé, puis sur le « + » en bas a droite, coller le liens dans la partie URL, donné un titre. L'enregistrement se fait en bas a droite.



8 PARAMETRAGE DE VOS APPAREILS

Tout est en place pour procéder au parametrage de vos terminaux. Retournons sur Politiques de sécurité, puis sur la clée a molette de Sécurite_test. Toutes les modifications faites sont appliquées de manière instantanées (max 5 secondes de décallages ce qui permet de verifier que le resultat obtenu est celui souhaité.



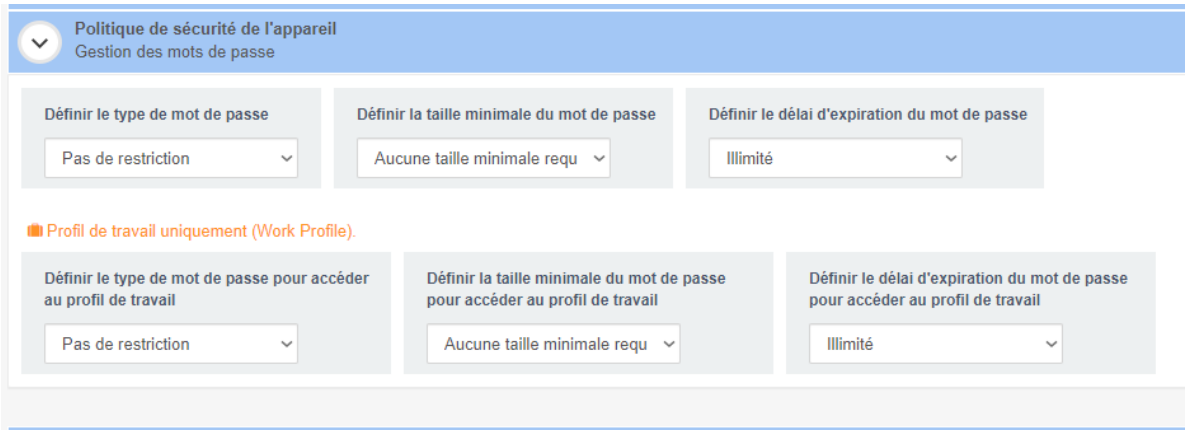
Nous allons voir toutes les options disponibles pour nos terminaux.

8.1 UTILISATEURS CONCERNES PAR LA POLITIQUE DE SECURITE

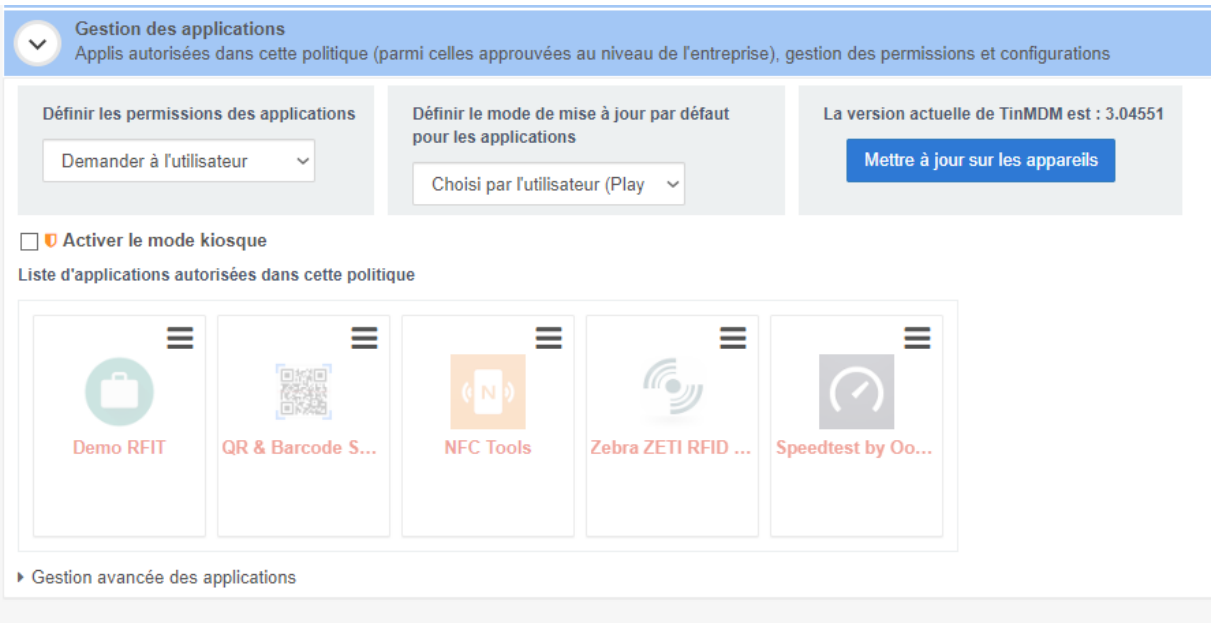
Nous avons déjà vu comment fonctionne les liens entre user/groupes et politiques de securité.

8.2 POLITIQUE DE SECURITE DE L'APPAREIL

On peut grâce à ce paramettre obliger les users à definir des mdp/pin/schema pour sécuriser leurs appareils.



8.3 GESTION DES APPLICATIONS

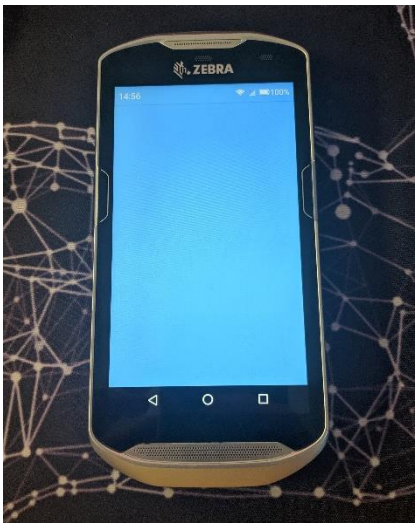


Cet onglet est l'un des plus intérrésant :

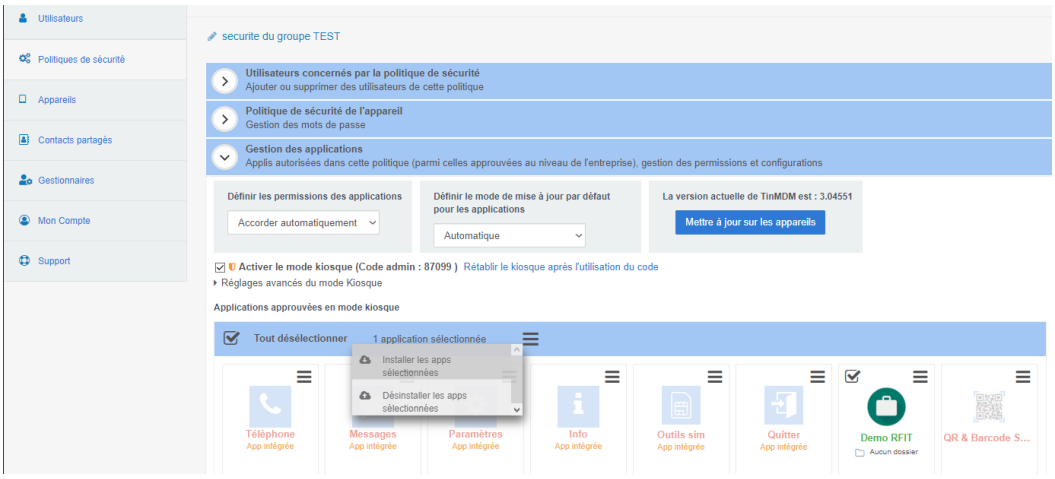
Definir les permissions des applications doit etre switch à « accorder automatiquement » afin d'eviter des refus de permission accidentelle.

Le mode de mise a jour par defaut doit etre mis en « automatique » pour forcer les mise a jour a se faire de manière transparente et instantané.

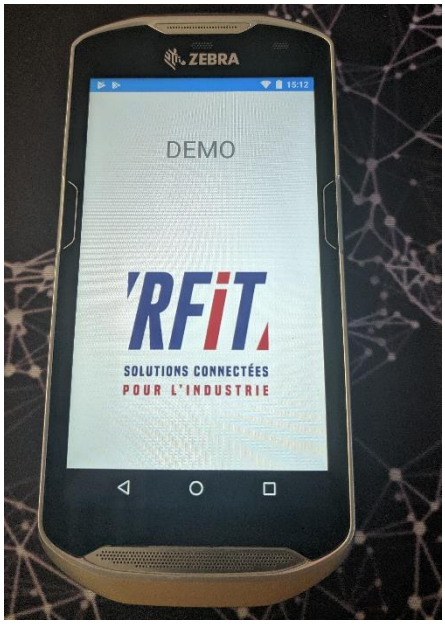
Le gros plus de TinyMDM : Le mode kiosque permet de bloquer l'utilisateur sur une ou plusieurs applications, il ne peut rien faire d'autre qu'utiliser la ou les applis autorisées, n'a plus accès à aucune autres fontionnalités. Activer le et l'appareil se retrouvera bloqué sur un ecran bleu.



Cliquez sur une applications dans la liste si dessous pour l'autoriser (ici notre appli Demo RFIT). Elle devinent verte : cela signifie qu'elle est desormais autorsé en mode kiosque. Pour l'installer a distance, rien de plus simple : on la selectionne et on clique sur installer.



L'application se telecharge et s'installe de manière transparente puis fini par s'afficher sur le terminal. L'appliaction est désormais bloquée, on ne peut ni la quitter, ni acceder à aucun parametre du telephone, l'utilisateur sera bloqué sur l'application.

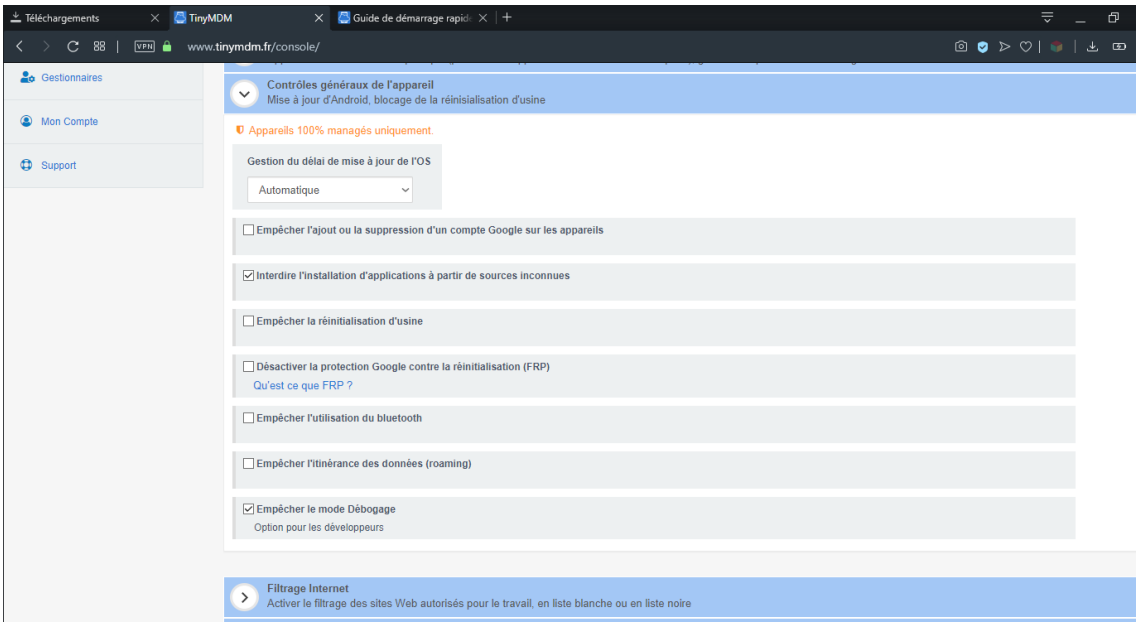


Pour autoriser d'autre applications rien de plus simple : cliquez dessus et installés les de la meme manière .

A noter que lorsque l'on met à jour l'apk sur le store, une option supplementaire au menu installer et desinstaller apparait, celle de mettre a jour afin de forcer la mise a jour de la nouvelle appli sur l'appareil ou le groupe d'appareil concerné par cette politique de sécurité (mise a jour transparente, par contre une fois fais l'appli redemarre donc a utilisé avec précotion. D'ici fevrier 2020 un outils d'envoi de pop-up pour prevenir les utilisateur sera mis en place).

Pour enfin les desactiver, recliquez dessus et elle redeviendront grisé et disparaitrons (on peut par la suite les desinstaller si necessaire) . Enfin on peut desactiver le mode kiosque a sa guise.

8.4 CONTROLES GENERAUX DE L'APPAREIL



Regler « Gestion du delai de mise à jour de l'OS » a « Apres minuit » pour eviter qu'une MAJ android vienne perturber l'employer dans son travail.

Cocher « Empecher l'ajout ou la supression d'un compte Google sur les appareils » pour eviter toutes tentative de fraudes.

Décocher « Interdire l'installation a partir de sources inconnu » seulement si necessaire lors de test par exemple.

Coché « empeché la restoration d'usine » pour eviter tout formatage/vol (on pourra tout de meme le formatter avec le code qui apparaitra lorsque l'option sera cocher.

Laissé decocher « Desactiver la protection Google contre reinitialisation » C'est le FRP (une securité qui empeche l'utilisation d'un appareil volé meme si on arrive a le remettre a l'etat d'usine, un icloud version google safety).

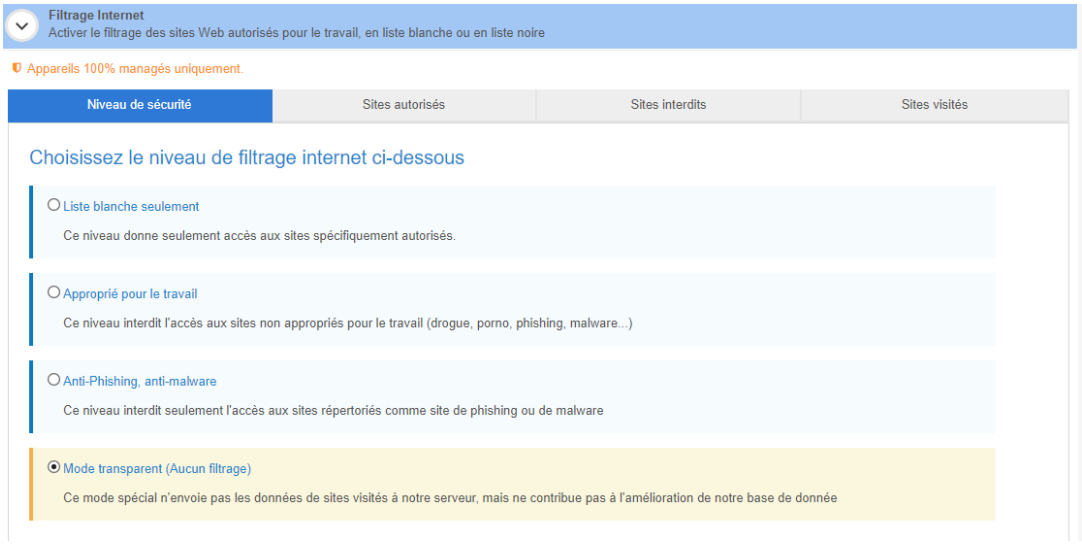
Laissé decocher « Empecher l'utilisation du blutooth » cela pourrait poser probleme dans le cas ou il devrait-y avaoir une connection entre TC et PDA par exemple et les employés n'ont pas acces au blutooth en kiosque de toute manière.

Cocher « empecher l'itinérance des données (roaming) sauf si les appareils seront amener a etre utilisé de manière exeptionnel a l'etranger (options ne concernant que les appareils pouvant utilisé une carte SIM a l'etranger).

Laisser cocher « Empecher le mode Débogage » cela permet d'empecher une personne de communiquer avec l'appareils via usb (ce qui s'avere dangereux en cas de vol ou d'utilisation frauduleuse). Desactiver seulement si reelement necessaire.

8.5 FILTRAGE INTERNET

Bon la, il n'y a rien a expliqué tout est expliqué de manière claire. Cet outils fonctionne tres bien. Il fait office de parefeu en temps reel.



8.6 CONFIGURATION WIFI ET CONTACT PARTAGES

La aussi rien de spécial a ajouter, tout est simple et claire.

Toute l'équipe de **RFiT TECHNOLOGIES** reste à votre dispositon.

Bien cordialement.

Robin COBLENTZ
Technicien
Tel : +33 (0)4 75 75 98 52
Mob : +33 (0)7 80 40 57 22