



# **Deploiement de TINY MDM**

## Notre solution dédiée :

## TOOLTRACK®

Destina	ataire : Mr <mark>P</mark>	rénom Nom - I	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 paramettré 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.





IT damo Android 🕫 🗙 MainPage yam		▼ Evalerateur de selutions
Application		
Manifeste Android	Configuration : N/A V Platforme : N/A V	Rechercher dans Explorateur de solutions (Ctrl+\$)
Manfeste Android Options Android Signature du paquet Android Build Événements de build Chemins d'accès des références	Numéro de version :          1         Nom de version :         1.0         Emplacement de l'installation :         Préférer interne         Version Android minimale :	Rechercher dans Explorateur de solutions (Ctrl+5) Solution 'RFI.demo' (2 sur 2 projets) A BRII.demo B RFI.demo C Apparant C Apparant C Apparant.cs C AssemblyInfo.cs A BRII.demo.Android C RFII.demo.Android C Connected Services P Properties D BRIE.demo.Android
	Android 6.0 (niveau d'API 23 - Marshmallow) 🗸	Assets
	Version Android cible : Android 9.0 (niveau d'API 28 - Pie)	▶ ■ Resources ▶ C <sup>ass</sup> MainActivity.cs
	Autorisations nécessaires :	Contractions de solutions - Trace Contaces
	ACCEPT_HANDOVER  ACCESS_CHECKIN, PROPERTIES  ACCESS_COARSE_LOCATION  ACCESS_INE_LOCATION  ACCESS_INE_LOCATION  ACCESS_LOCATION_EXTRA_COMMANDS  ACCESS_MOCK_LOCATION	Proprietés

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 ».

RFIT.demo.Android 😔 X MainPage.xam		<ul> <li>Explorateur de solutions</li> </ul>
Application	Configurations (Palasse) attice as Distances (Ams CDID attice as	○ ○ 🏠 📅 - Ĭo - ≒ 🖒 @ 🛙
Manifeste Android	Configuration : (Release) active v Platforme : (Any CPO) active v	Rechercher dans Explorateur de solutions
Options Android		Solution 'RFIT.demo' (2 sur 2 projets
Signature du paquet Android	exemple : .dll;.mp3	C# KFII.demo     Dépendances
Build	Options de débogage	A DP.xaml
Événements de build	Activer l'instrumentation du dévelopmeur (débogage et profilage)	C= App.xaml.cs
Chemins d'accès des références	Dékenunger	C# AssemblyInfo.cs
	Net (Xamarin)	P C= MainPage.xaml.cs
	in set (second in )	A 🗄 RFIT.demo.Android
	Génération de code et runtime	Connected Services
	Activer le suivi au démarrage	Properties ▶ ■ ■ Références
	✓ Utiliser le récupérateur de mémoire concurrent	Assets
	Propriétés de l'éditeur de liens	Resources
	-	C* MainActivity.cs
	Édition des liens en cours	
	Assemblys de SDK et assemblys d'utilisateur v	
	Assemblys de SDK uniquement	
	Aucun	Explorateur de solutions Team Explorer
	Assemblys de SDK et assemblys d'utilisateur	Propriétés
	En envirolue	
	<u>en savoir pids</u>	🔠 💱 🏓
	Aurora	
	Avance	×
	- 1	

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.

Gestionnaire d'archives 😕 🗙 RFIT.demo.Android MainPage.xam	nl		Explorateur de solutions
Rechercher P DEIT domo			୦୦☆∺·bo-5¢
Distribuer		X Tout	Rechercher dans Explorateur de solut
Détails de l'applicatio Canal de d RFT demo Android Date de création : 19/12/2019 Version : 1.0 © Sélectionner le canal	listribution 1 de distribution : Ad Hoc Google Play	Android	Solution RFIT demoi (2 sur 2 pr  RFIT.demo  RFIT.demo
		Distribuer	Explorateur de solutions Team Explo
		Ouvrir la distribution	Propriétés
		Ouvrir le dossier	
		Annuler	

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

r Distribuer Détails de l'applicatio	Identité de signatur	e	>	< undroid گ	Solution 'RFIT.demo' (2 sur 2 projets
RFIT.demo.Android Date de création : 19/12/2019 Version : 1.0	Rechercher Nom	Expiration	ې Type		C# AssemblyInfo.cs
Ad Hoc Identité de signature	RfitTools	Sun Dec 29 15:05:33 CET 2047		undroid	
0	+         -         Cy Importer           Spécifier une autorité d'horodatage :	http://example.timestampauth.com		ition ier	Explorateur de solutions Team Explorer Propriétés
Pourquoi ai-je besoin d'un magasin de clés ?		Précédent Enregistrer sou	ıs Annuler		8

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 <u>www.tinymdm.fr</u> 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).





< <li>Console d'administrati</li>	n	🌲 jvinay@rfit-tech.com
G Apps approuvées par l'entreprise	Utilisateurs	Ajouter un utilisateur Importer des utilisateurs Rafraîchir
Utilisateurs		
OS Politiques de sécurité		
Appareils	/ coblentz	
Contacts partagés	robin     robin     Pas de group     Ajouter un utilisateur	
Lo Gestionnaires	test   🗱 Entrez les informations du nouvel utilisateur, il recevra son mot de passe ou son code QR pour d	enröler son appareil.
Mon Compte	Appareit : 1051	
Support	test 1	
	Annuler Ok	

## **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.



Aucun appareil enrôlé

## **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).





n	A	jvinay@rfit-tech.com
✓ Ø Securite_test		Retour
Vitilisateurs concernés par la politique de sécurité Ajouter ou supprimer des utilisateurs de cette politique		
□ & Guinot   📽 (1) □ for Groupe_test   📽 (1) □ jvinay □ coblentz		
Sestion des mots de passe		
Définir le type de mot de passe     Définir la taille minimale du mot de passe     Définir le délai d'expiration du mot de passe       Pas de restriction <ul> <li>Aucune taille minimale requities</li> <li>Illimité</li> <li>Illimité</li> <li>Illimité</li> <li>Illimité</li> <li>Illimité</li> <li>Illimité</li> <li>Illimité</li> <li>Illimité</li> <li>Illimité</li> <li> </li></ul>		
IIII Profil de travail uniquement (Work Profile).		
Définir le type de mot de passe pour accèder au profil de travail Des de sesticies y au profil de travail Des de sesticies y au profil de travail		
Pras de resulction Aucune taille minimale require		

Nous paramettrerons 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 <u>afw#tinymdm\_</u>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.

#### Modèle - Robin DOC 20191220 Tiny MDM.docx







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.

#### APK DEVELOPPE EN INTERNE 7.1 Console d'administration 🔔 jvii G Apps approuvées par l'entrep G Enterprise Mobile Management Google pour Android Utilisateurs Pour utiliser les fonctionnalités EMM Android, votre entreprise doit être enregistrée C Politiques de sécurité Appareils Si vous ne souhaitez plus utiliser Enter prise Mobile Management Google pour Android sur vos appareils, vous pouvez annuler l'enre Modifier les paramètres Google de l'entreprise Contacts partagés Gestion des applications Applications approuvées par l'entreprise $\sim$ Lo Gestio A Mon Compte Approuver des applications depuis le Play Publier des applications privées et des applications Web Approuver une application avec son n package (exemple: com.google.an Nom du package d'applic C Support Parcourir les applications Liste des applications approuvées 6. Zebra ZETI RFID

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

≽ Google Play	,		P
Votre adresse e-ma	ail rcoblentz@rfit-tech.com	Mettre à jo	bur
Applications p Demo RFIT	privées CO testtooltrack		
			+

#### 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 <u>nas.rfit@gmail.com</u>, 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.

Partager avec d'autres utilisateurs	Obtenir le lien de partac	
	Obtenin le nen de partag	
Partage par lien activé En savoir plus		
Visible : utilisateurs avec le lien 🔻	Copier le lie	n
https://drive.google.com/file/d/17sh5QHEhZIGiG	SYPb63wZwsw2v_2iUr_8/view	/?usp=
Utilisateurs		
Saisir des noms ou des adresses e-mail		× -
Les suggestions et commentaires ajoutés à c lecteurs. <u>En savoir plus</u>	e fichier sont visibles par ses	
ок		Avancé
	Partager avec d'autres utilisateurs Partage par lien activé En savoir plus Visible : utilisateurs avec le lien • Inttps://drive.google.com/file/d/17sh5QHEhZIGiG Utilisateurs Saisir des noms ou des adresses e-mail Les suggestions et commentaires ajoutés à c lecteurs. En savoir plus	Partager avec d'autres utilisateurs       Obtenir le lien de partage         Partage par lien activé En savoir plus       Copier le lie         Visible : utilisateurs avec le lien •       Copier le lie         Inttps://drive.google.com/file/d/17sh5QHEhZIGiGYPb63wZwsw2v_2iUr_8/view         Utilisateurs         Saisir des noms ou des adresses e-mail         Les suggestions et commentaires ajoutés à ce fichier sont visibles par ses lecteurs. En savoir plus

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.

G Apps approuvées par l'entreprise	<b>G</b> Configuration du Play Sto	re			Retour
Ltilisateurs	Approuver des applicati	ons Ajouter de	s applications privées	Créer des applications Web	Personnaliser le Play Store
Q <sup>6</sup> Politiques de sécurité	Google Play				Ø
Appareils					^
Contacts partagés	Titre *	Livret accueil GUIN	ОТ		
Le Gestionnaires	URL*	https://drive.google.	com/file/d/17sh5QHEh2	ZIGiGYPb63wZwsw2v_	
Mon Compte		Plein écran	<ul> <li>Autonome</li> </ul>	O Interface utilisateur minimale	
Support			•••	c	
	Affichage	L'application Web s'afficher en plein écran	a Les barres de navigation e d'état du téléphone s'affict dans l'application Web	t Les barres de navigation, ent d'état et d'URL du téléphone, ainsi que le bouton	





## 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.

≡∙	Console d'administration	on				
G	Apps approuvées par l'entreprise	😂 Politiques d	e sécurité			
4	Utilisateurs					
			۵ 🖒 🗲		۵ 🖒 🖌	📌 🖓 🟛
•	Politiques de sécurité	🖋 Defaut		🖋 Guinot		Securite_test Modifier la politiques de sécurité
	Appareils	Aucune description	0.	Aucune description	0.	securite du groupe TEST
۵	Contacts partagés					
20	Gestionnaires					
٩	Mon Compte					

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.

Gestion des mots de passe					
Définir le type de mot de passe	Définir la taille minimale	e du mot de passe	Définir le délai	d'expiration du mot de passe	
Pas de restriction	Aucune taille minima	le requ 🗸	Illimité	~	
Profil de travail uniquement (Work Pr Définir le type de mot de passe pour a u profil de travail	ofile). ccéder Définir la taille pour accéder	e minimale du mot de pas au profil de travail	sse D	éfinir le délai d'expiration du our accéder au profil de trava	mot de passe il





### 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 fontionnalitées. 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.





Lettilisateurs	✓ securite du aroune TEST
S Politiques de sécurité	<ul> <li>Utilisataure concernáe nar la nolitinue de sécurité</li> </ul>
Annareils	Ajouter ou supprimer des utilisateurs de cette politique
	Politique de sécurité de l'appareil     Gestion des mots de passe
Contacts partagés	Gestion des applications Apolis autorisées dans cette politique (parmi celles approuvées au niveau de l'entreprise) pastion des permissions et configurations
Lo Gestionnaires	Définir les permissions des applications Définir le mode de mise à lour nar défaut La version actuelle de TinMDM est : 3.04551
Mon Compte	Accorder automatiquement  Accorder automatique Automatique Automatique
Support	☐ U Activer le mode klosque (Code admin : 87099 ) Rétablir le klosque après l'utilisation du code ▶ Réglages avancés du mode Klosque
	Applications approuvées en mode kiosque
	Tout désélectionner
	C Désinstaler les apps v i 📄 🕣 🎉
	Téléphone         Messages         Paramètres         Info         Outlis sim         Quiter         Demo RFIT           Ago intégrée         Ago intégrée

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

🛨 Téléchargements 🛛 🗙 🦉 Tinyl	MDM X 📮 Guide de démarrage rapide X   +	≂_0
< > C 88   VEN 🖨 WWV	بد <b>tinymdm.fr</b> /console/	0 🗸 🔊 🖉 🖢
Lo Gestionnaires	Contrôles généraux de l'appareil Mise à jour d'Android, blocage de la réinisialisation d'usine	
Mon Compte	♥ Appareils 100% managés uniquement.	
Support	Gestion du délai de mise à jour de l'OS Automatique	
	Empêcher l'ajout ou la suppression d'un compte Google sur les appareils	
	☑ Interdire l'Installation d'applications à partir de sources inconnues	
	Empêcher la réinitialisation d'usine	
	Désactiver la protection Google contre la réinitialisation (FRP) Qu'est ce que FRP ?	
	Empêcher l'utilisation du bluetooth	
	Empêcher l'itinérance des données (roaming)	
	Cption pour les développeurs	
	Filtrage Internet     Activer le filtrage des sites Web autorisés pour le travail, en liste blanche ou en liste noire	

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.

<ul> <li>Filtrage Internet</li> <li>Activer le filtrage des sites Web autorisés</li> </ul>	pour le travail, en liste blanche ou en liste noi	re	
D Appareils 100% managés uniquement.			
Niveau de sécurité	Sites autorisés	Sites interdits	Sites visités
Choisissez le niveau de filtrag	je internet ci-dessous		
O Liste blanche seulement Ce niveau donne seulement accès aux	sites spécifiquement autorisés.		
O Approprié pour le travail Ce niveau interdit l'accès aux sites non	appropriés pour le travail (drogue, porno, phi	shing, malware)	
O Anti-Phishing, anti-malware Ce niveau interdit seulement l'accès au	x sites répertoriés comme site de phishing ou	de malware	
Mode transparent (Aucun filtrage)     Ce mode spécial n'envoie pas les donn	ées de sites visités à notre serveur, mais ne c	ontribue pas à l'amélioration de notre base de d	lonnée

## 8.6 CONFIGURATION WIFI ET CONTACT PARTAGES

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

Contrôles généraux de l'appareil Mise à jour d'Android, blocage de la réinisialisation d'usine	
Siltrage Internet Activer le filtrage des sites Web autorisés pour le travail, en liste blanche	ou en liste noire
Configuration Wifi Configuration d'un réseau wifi, interdiction des réseaux wifi non sécurisés	3
Désactiver le Wifi	
🗌 Désactiver les réseaux wifi non sécurisés	
Ajouter des réseaux wifi prèconfigurés :	
Configurer un réseau wifi Configurer un réseau wifi EAP	
Configurer un réseau wifi Configurer un réseau wifi EAP Liste des wifis préconfigurés (ils seront automatiquement configurés sur les app	areils liés à cette politique de sécurité) :
Configurer un réseau wifi         Configurer un réseau wifi EAP           Liste des wifis préconfigurés (ils seront automatiquement configurés sur les app           La liste des wifis préconfigurés est vide.	areils liés à cette politique de sécurité) :
Configurer un réseau wifi         Configurer un réseau wifi EAP           Liste des wifis préconfigurés (ils seront automatiquement configurés sur les app           La liste des wifis préconfigurés est vide.	areils liés à cette politique de sécurité) :
Configurer un réseau wifi       Configurer un réseau wifi EAP         Liste des wifis préconfigurés (ils seront automatiquement configurés sur les app         La liste des wifis préconfigurés est vide.         Contacts partagés         Ajouter ou supprimer des contacts partagés par les utilisateurs de la politi	areils liés à cette politique de sécurité) : ique





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