proximus

Manuel Utilisateur

Mobile Threat Defense (MTD)

Datum	26/04/2023
Onze referentie	**Manuel Utilisateur MTD**
Contact	**Bart Callens**
E-mail	**b.callens@proximus.com**

Contenu

Aperçu

Le présent document a pour but d'aider l'utilisateur final lors des principales étapes de l'installation et de l'utilisation de l'option MTD sur les plans tarifaires mobiles de Proximus. Remarque : la disponibilité de certaines fonctions décrites dépend de la configuration de l'option MTD par votre administrateur.

Les différences éventuelles entre les types d'appareils (Android et iOS) sont mentionnées. Un guide plus complet pour Android et iOS est disponible en anglais sur https://proximus.be/mtduser.

1. Description du service

Pour contrer les menaces, Proximus propose une option de sécurité sur ses plans tarifaires mobiles destinés aux entreprises : MTD (Mobile Threat Defense). Cette option de sécurité protège votre smartphone au moyen d'une app (disponible pour iOS et Android). Cette app sécurise votre appareil contre les attaques pouvant cibler le réseau, le système ou les applications.

Votre administrateur a accès à un portail sécurisé où il peut configurer la politique de l'entreprise et gérer les menaces courantes.

Le présent manuel utilisateur décrit pour vous, l'utilisateur final, comment installer et activer l'app et comment l'utiliser sur des tablettes ou smartphones iOS et Android.

2. Installation et activation

2.1 Remarque préalable

Vérifiez la version de votre smartphone Android ou iOS. La version utilisée doit être au moins Android 5.1 ou iOS 11 sur un appareil 64 bits.

Votre administrateur doit demander à Proximus l'option Mobile Threat Defense pour ses employés. Si vous souhaitez bénéficier de cette option en tant qu'employé de votre entreprise, veuillez contacter l'administrateur de votre entreprise.

Ce dernier contactera alors Proximus ou un partenaire agréé de Proximus, qui ajoutera l'option MTD au contrat mobile conclu entre votre organisation et Proximus.

2.2 Installation et activation de l'app MTD sur votre smartphone

Dès que l'option MTD pour votre appareil mobile sera reprise dans le contrat mobile conclu entre votre organisation et Proximus, vous recevrez un e-mail pour installer et activer l'app MTD sur votre appareil mobile. Vous recevrez cet e-mail à l'adresse e-mail indiquée par votre administrateur.

Si vous ne recevez pas d'email, veuillez vérifier le dossier "spam" ou "courrier indésirable" de votre client de messagerie..

Cher,

nous sommes heureux de confirmer que l'option Mobile Threat Defense (MTD) pour votre appareil mobile est provisionnée et sera facturée à partir de maintenant sur le contrat mobile de votre organisation. Veuillez suivre les étapes ci-dessous pour protéger votre appareil mobile. Vous pouvez trouver une assistance supplémentaire ici ou contacter le gestionnaire de flotte de votre organisation.

Téléchargement et activation de votre application MTD

1. Téléchargez l'application MTD depuis le Google Play Store ou l'Apple Store sur votre appareil mobile :

Lien
MTD- iOS
MTD - Android

2. Activez l'application MTD sur votre appareil mobile en cliquant sur le lien ci-dessous sur votre appareil mobile ou scannez le code QR avec votre appareil mobile avec l'application MTD :

Lien	Code QR
Activez l'app MTD	

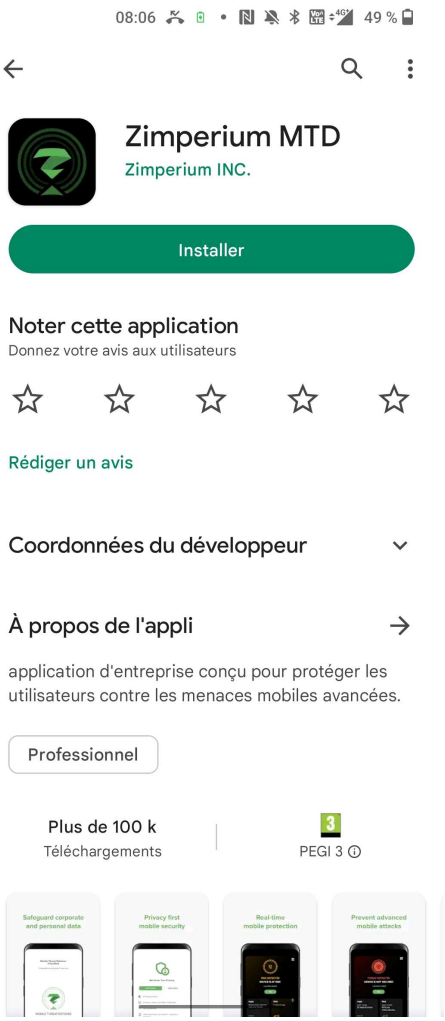
Veuillez agréer, Madame, Monsieur, l'expression de mes sentiments distingués,

Proximus

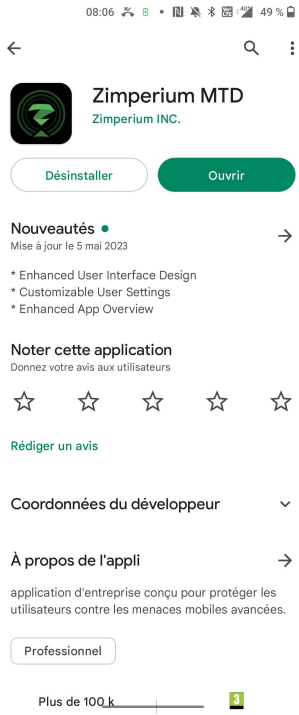
Si votre organisation dispose d'un environnement MDM (Mobile Device Management), la première étape (téléchargement de l'app MTD) sera automatique. Dans ce cas, passez immédiatement à la 2e étape (activation de l'app MTD).

2.2.1 Étape 1 : télécharger l'app MTD

Selon que vous disposez d'un smartphone Android ou iOS, appuyez sur le lien correspondant dans l'email reçu. Ouvrez Google Play ou l'Apple App Store et appuyez sur le bouton "**Installer**".

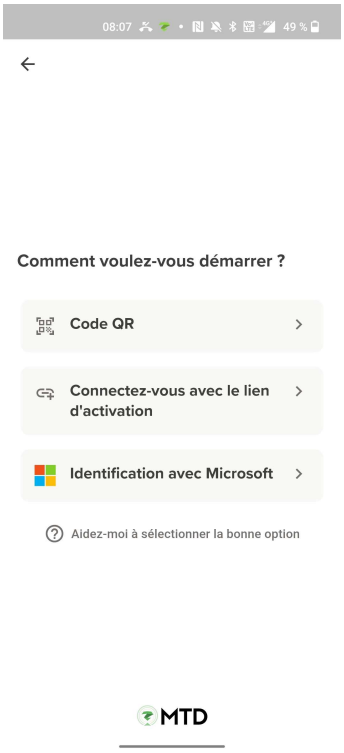


Appuyez sur le bouton "**Ouvrir**" :



L'écran suivant s'affiche. Si vous souhaitez obtenir plus d'informations sur les fonctionnalités de l'application, vous pouvez glisser vers la droite, sinon, cliquez sur "**Démarrer**":

L'écran suivant s'affiche :



Votre app MTD a été installée avec succès. Passez maintenant à l'étape 2.

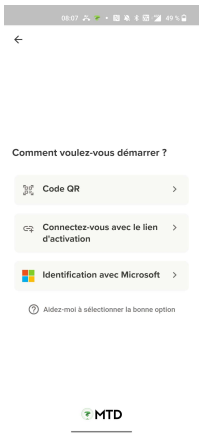
2.2.2 Étape 2 : activer l'app MTD

Pour activer l'app MTD, utilisez l'une des deux méthodes suivantes, la plus simple pour vous.

2.2.2.1 Activation via le QR code

Ouvrez l'e-mail reçu sur votre laptop ou PC. Dans l'écran d'accueil de l'app MTD installée sur votre smartphone (voir étape 1), appuyez sur le bouton "**QR Code**".

.



Si vous avez fermé l'app MTD entre-temps, ouvrez-la à nouveau. Le QR code doit être scanné avec l'app MTD.

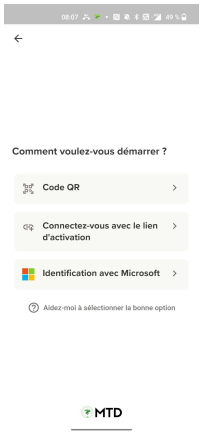
Remarque : le bouton "**Identification avec Microsoft**" n'est pas pertinent et ne doit dès lors pas être utilisé.

Afin de pouvoir scanner le QR code, vous devez autoriser l'app MTD à prendre des photos et enregistrer des vidéos.

Scannez le QR code figurant dans l'e-mail de bienvenue que vous avez reçu. Ensuite, passez à l'Etape 3.

2.2.2.2 Activation via l'URL

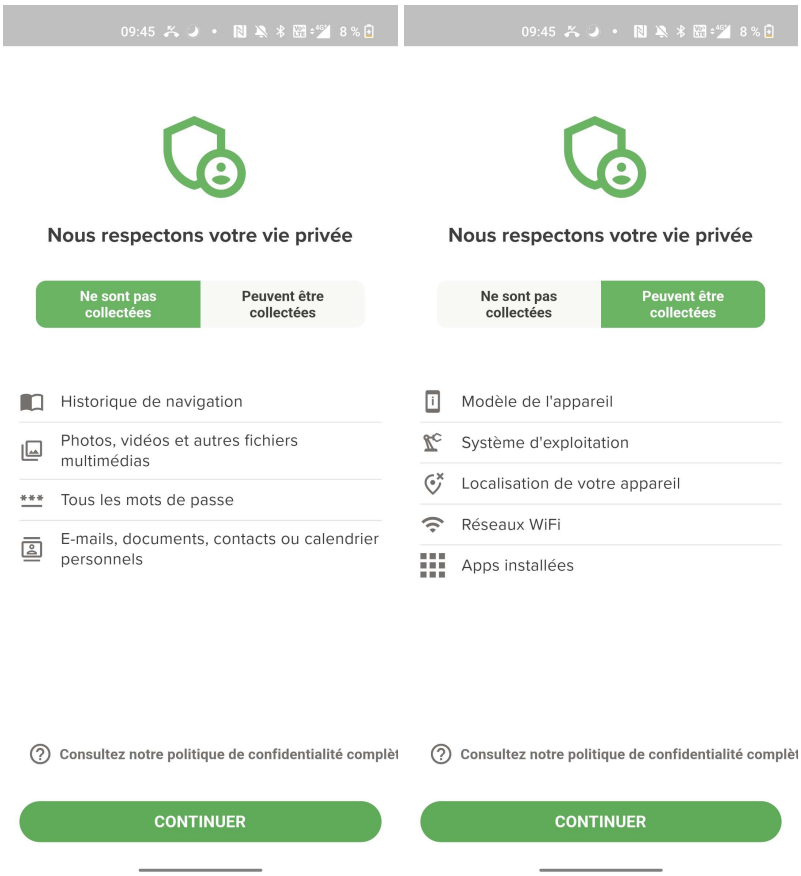
Ouvrez l'e-mail sur votre smartphone et appuyez sur le lien "**Activez MTD**". Vous pouvez également cliquer sur "**Connectez-vous avec le lien d'activation**" dans l'application MTD et copier/coller le lien d'activation de votre e-mail dans l'application MTD.:



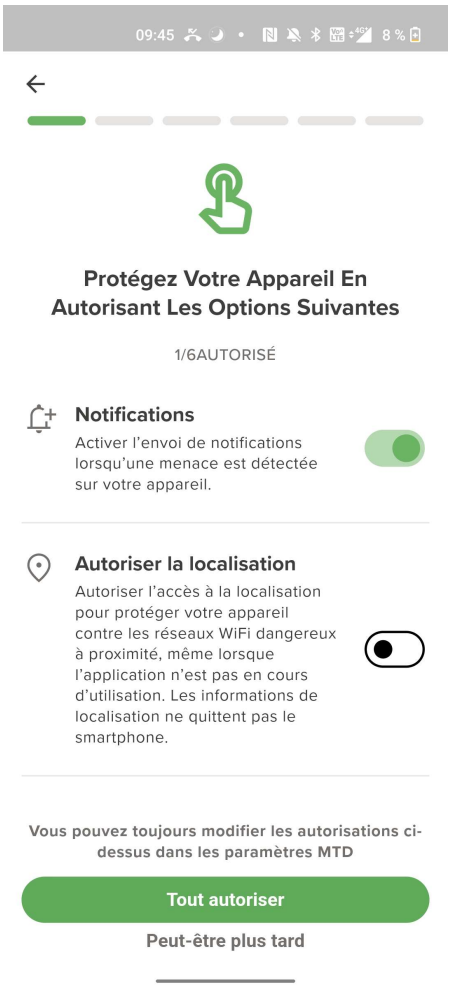
Ensuite, passez à l'étape 3.

2.2.3 Étape 3 : autoriser l'app MTD

Vous obtiendrez d'abord un aperçu des données de votre smartphone ou de votre tablette qui peuvent ou non être visibles par votre administrateur via la plateforme de l'administrateur MTD. Cet aperçu dépend de la politique de confidentialité définie par votre administrateur.



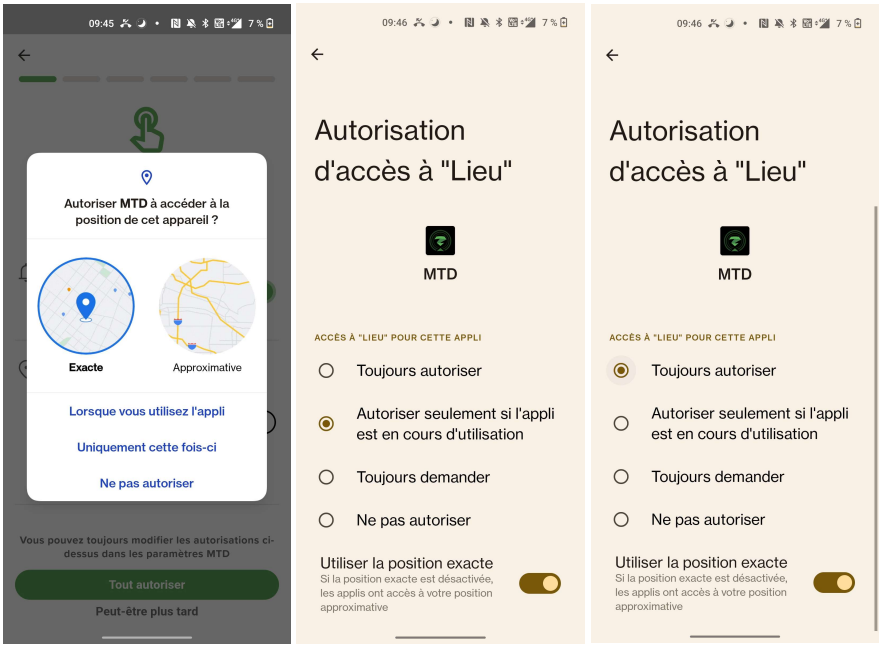
Cliquez sur **'Continuer'**:



Pour sécuriser au mieux votre appareil, il est nécessaire d'autoriser certaines permissions sur votre appareil. Cliquez sur "**Tout Autoriser** ".

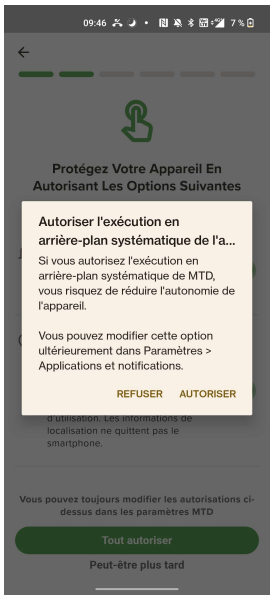
Ajustez les différentes autorisations sur votre appareil :

Autorisation de localisation : cela vous permet d'autoriser l'appli à transmettre la localisation de votre appareil à la plateforme de gestion MTD à laquelle votre administrateur a accès :

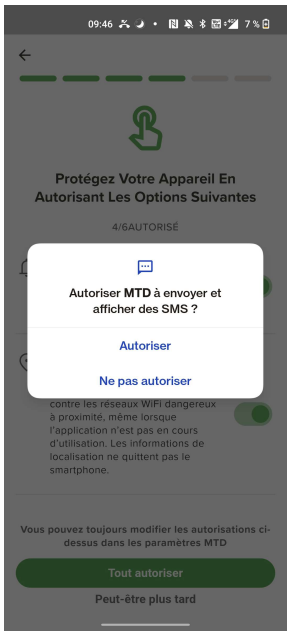


Optimisation de la batterie :

Pour une protection optimale, il est recommandé d'autoriser l'application MTD à être active en arrière-plan :

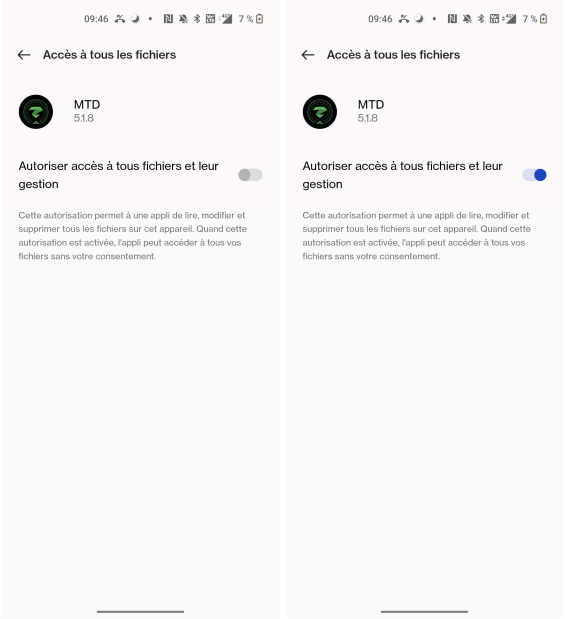


Autorisation SMS

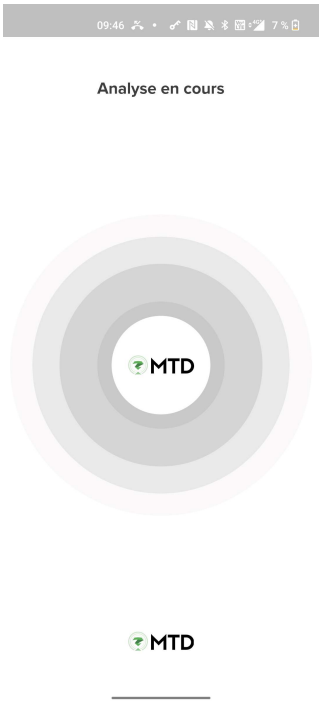


Accès VPN : Pour protéger votre appareil contre le phishing et les sites à risque, il est nécessaire d'accorder à l'application MTD un accès VPN :

Accès à tous les fichiers : Pour détecter les comportements malveillants sur votre appareil mobile, l'application MTD doit avoir accès aux fichiers présents sur votre appareil



Une fois toutes les autorisations accordées, l'application MTD procède à une première analyse de votre appareil mobile. Si une menace est détectée, par exemple une application malveillante, elle s'affiche et vous pouvez y remédier, par exemple en supprimant l'application malveillante en question.



À la fin de l'analyse, le tableau de bord de l'application MTD s'affiche. Votre application MTD est maintenant installée et activée avec succès :

3. Utilisation de l'app MTD

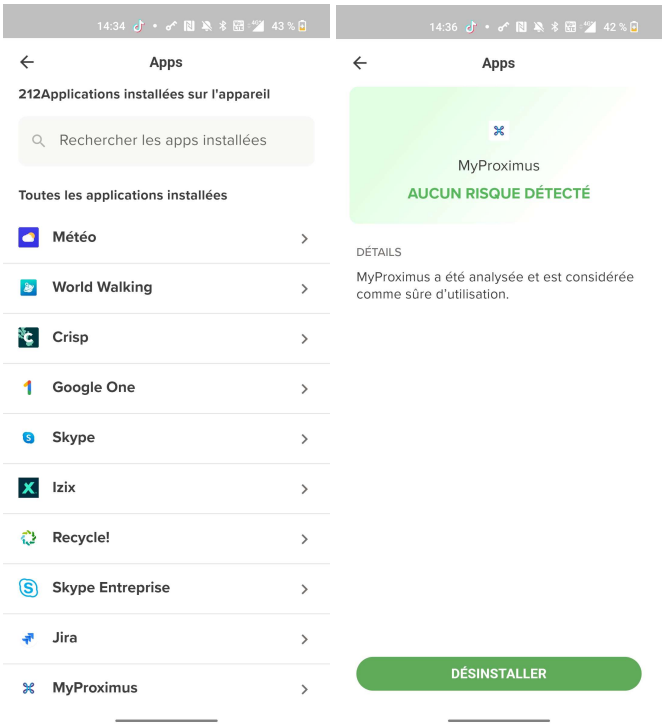
L'app MTD protège votre smartphone contre les menaces. En fonction des paramètres définis par votre administrateur, vous serez averti de certaines menaces et pourrez y réagir. Vous avez également la possibilité d'effectuer manuellement une analyse de sécurité sur votre appareil. Les interactions les plus courantes sont décrites ci-dessous.

3.1 Dashboard

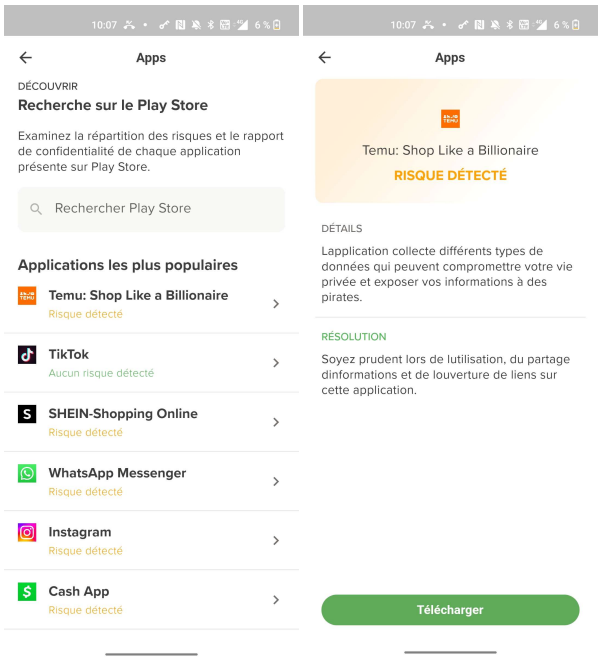
Le tableau de bord indique l'état de la sécurité pour chacune des catégories de menaces (applications, Web, appareils et réseau), ainsi que l'état général de la sécurité. Un code couleur indique si aucune menace n'a été détectée (vert), si des menaces non critiques ont été détectées (orange) ou si des menaces critiques ont été détectées (rouge)

3.1.1 Protection Apps

L'onglet “Apps” vous donne un aperçu de la sécurité de toutes les applications installées sur votre appareil.

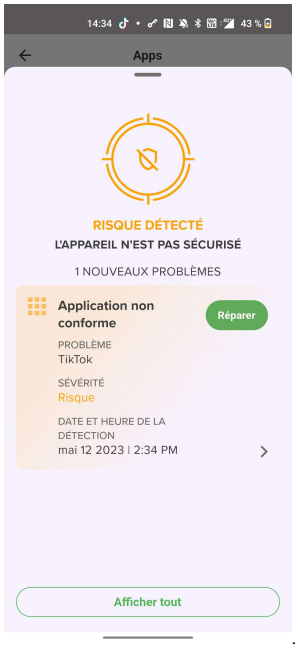


En outre, vous pouvez obtenir un rapport de sécurité d'une application à partir des magasins d'applications publics afin d'évaluer cette application avant de la télécharger :



En effet, certaines applications (par exemple TikTok) définies comme non conformes par votre administrateur, ces applications, lorsqu'elles sont installées sur votre appareil mobile, seront également

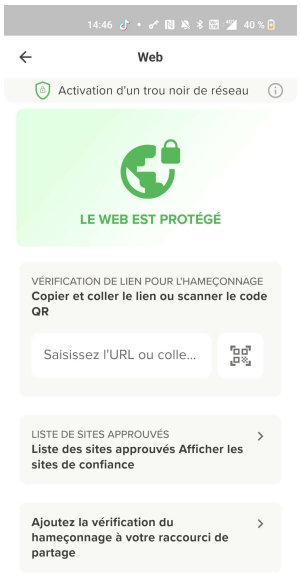
affichées ici. Vous pouvez rendre votre appareil conforme en désinstallant l'application concernée de votre appareil.



3.1.2 Protection Web

Dans l'onglet “Web”, vous pouvez voir quels sont les sites auxquels vous avez accordé votre confiance. Si votre administrateur l'a défini, vous recevrez également un message indiquant que le "network sinkhole” a été activé. Cette fonction protège activement votre appareil contre les contenus web malveillants. Vous pouvez demander un rapport sur les sites qui ont été bloqués par votre appareil au cours de la période écoulée.

En fonction des paramètres définis par votre administrateur, vous pourrez également vérifier si certaines URL et certains codes QR ne contiennent pas de contenu malveillant en les copiant et en les collant dans l'application MTD ou en scannant le code QR.



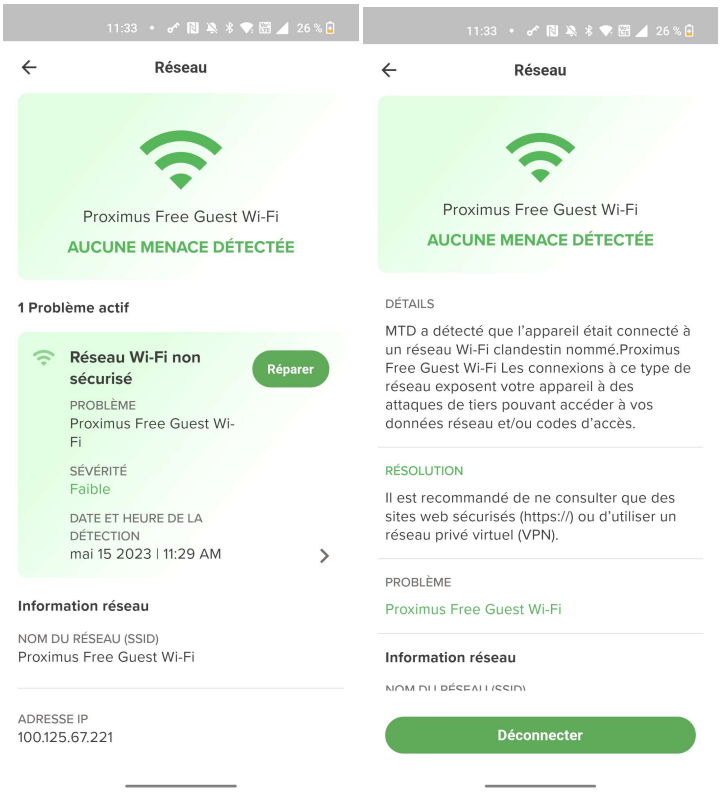
.

3.1.3 Protection appareil

L'onglet “appareil” répertorie les menaces liées aux appareils, telles qu'une version vulnérable d'Android ou un appareil rooté. Lorsqu'une menace a été détectée, vous pouvez la résoudre en cliquant sur "résoudre".

3.1.4 Protection réseau

L'onglet “Réseau” affiche l'état actuel de la sécurité du réseau mobile ou de la connexion WiFi. Les menaces critiques de cette catégorie sont, par exemple, les attaques MITM (Man-in-the-Middle), les faux certificats SSL et les faux points d'accès WiFi. Vous obtenez plus de détails sur les menaces et pouvez les résoudre si nécessaire, par exemple en déconnectant une connexion à un faux point d'accès WiFi.

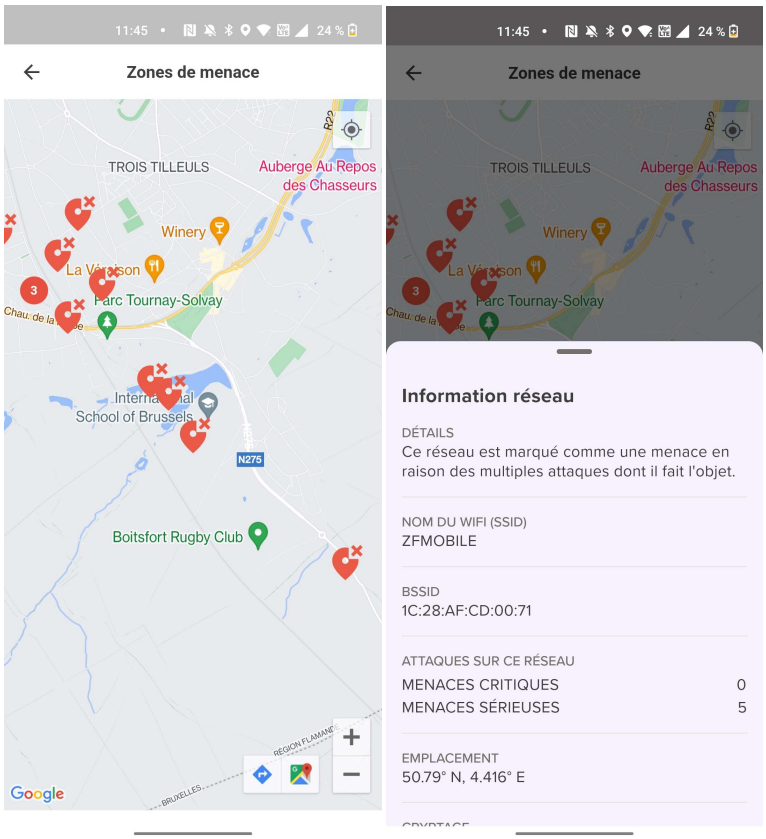


3.1.5 Zones de menace

La disponibilité de cette fonctionnalité dépend de la configuration effectuée par votre administrateur. En voyage ou en déplacement, vous pouvez parfois vous connecter à des réseaux wi-fi ouverts disponibles.

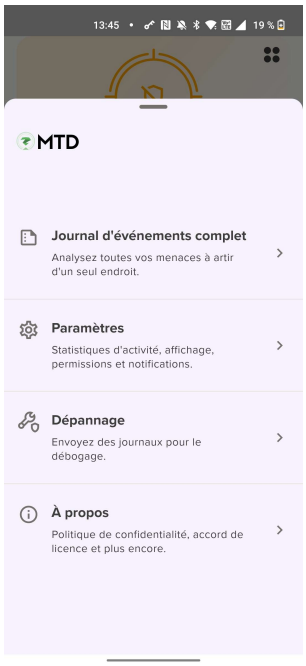
Cependant, bon nombre de ces réseaux wi-fi ouverts sont faux : les pirates informatiques essayent de piéger leurs victimes en les faisant se connecter à leur point d'accès wi-fi. La page “Zones de Menace” fournit des informations sur les réseaux disponibles à proximité qu'il vaut mieux éviter vu leur risque élevé en termes de sécurité. Avant de décider de vous connecter à un réseau, vous pouvez consulter la carte "Zones de menace" via votre app MTD. Sur cette carte, les réseaux à haut risque dans votre région sont marqués d'une icône rouge.

Si vous ne consultez pas l'app MTD avant de vous connecter, vous recevrez un avertissement de l'app MTD lorsque vous vous connecterez à un réseau à haut risque, avec des recommandations comme celle de se déconnecter de ce point d'accès.



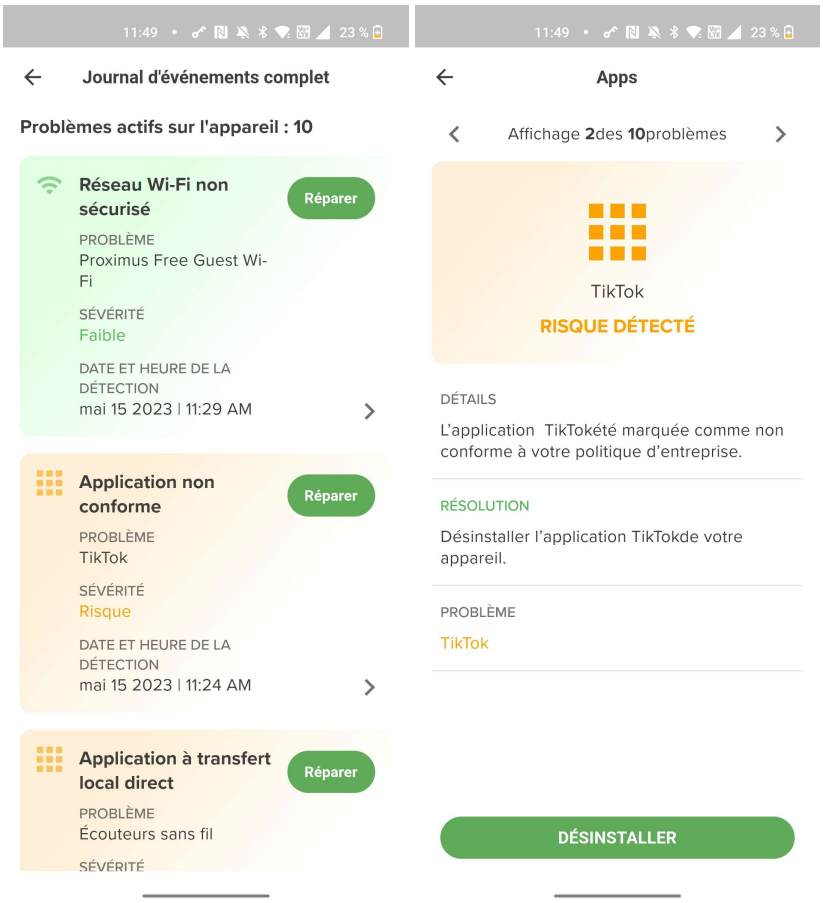
3.2 Paramètres

Als u in het dashboard op de 4 punten rechtsboven in het scherm klikt, krijgt U het volgende scherm :



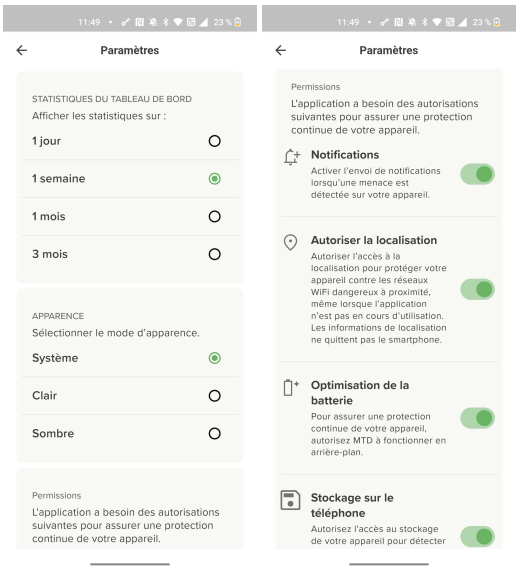
3.2.1 Journal d’événements complet

Ici, vous obtenez un aperçu complet de tous les événements sur votre appareil mobile. En cliquant sur « résoudre », vous pouvez afficher les détails de chaque événement et les résoudre, par exemple en supprimant une application non conforme à la politique de l’entreprise.



3.2.2 Paramètres

Sous paramètres, vous pouvez ajuster la période des rapports affichés dans l'application MTD, le mode d'affichage de l'application MTD et les autorisations de l'application configurées lors de l'installation de l'application.


11:49
23 %
Paramètres
STATISTIQUES DU TABLEAU DE BORD
Afficher les statistiques sur :
1 jour
1 semaine
1 mois
3 mois
APPARENCE
Sélectionner le mode d'apparence.
Système
Clair
Sombre
Permissions
L'application a besoin des autorisations suivantes pour assurer une protection continue de votre appareil.
11:49
23 %
Paramètres
Permissions
L'application a besoin des autorisations suivantes pour assurer une protection continue de votre appareil.
Notifications
Activer l'envoi de notifications lorsqu'une menace est détectée sur votre appareil.
Autoriser la localisation
Autoriser l'accès à la localisation pour protéger votre appareil contre les réseaux WiFi dangereux à proximité, même lorsque l'application n'est pas en cours d'utilisation. Les informations de localisation ne quittent pas le smartphone.
Optimisation de la batterie
Pour assurer une protection continue de votre appareil, autorisez MTD à fonctionner en arrière-plan.
Stockage sur le téléphone
Autorisez l'accès au stockage de votre appareil pour détecter

4. Questions fréquentes

4.1 Je scanne le QR code figurant dans mon e-mail d'activation et j'obtiens un écran de navigateur vide.

Veuillez vérifier si vous avez déjà installé l'app MTD sur votre smartphone (voir l'étape 1 de l'e-mail de bienvenue). Si tel est le cas, veuillez contacter votre administrateur pour obtenir une assistance supplémentaire.

4.2 Puis-je activer l'app MTD sur plusieurs appareils en même temps ?

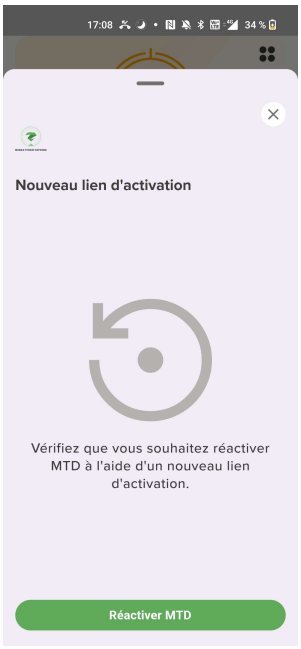
Non, vous ne pouvez activer l'app MTD que sur un seul appareil à la fois. Voir également ci-dessous 'Je change d'appareil mobile. Que dois-je faire ?.'

4.3 Je change d'appareil mobile. Que dois-je faire ?

- Désinstallez l'app MTD sur votre ancien appareil mobile
- Installez l'app MTD sur votre nouvel appareil mobile (à partir de Google Playstore ou de l'Apple Store ou par le biais d'une solution MDM de votre employeur).
- Activez l'app MTD sur votre nouvel appareil mobile. Veuillez utiliser le lien ou le QR code original que vous avez reçu initialement. Si vous ne possédez plus ce lien ou ce QR code, veuillez contacter votre administrateur. Ce dernier vous le fournira à nouveau.

4.4 Je quitte mon employeur actuel. Mon option MTD expire-t-elle ?

Si votre employeur actuel met un terme à votre abonnement de téléphonie mobile, l'option MTD prend fin automatiquement. Si votre nouvel employeur reprend votre abonnement GSM, il peut décider d'activer à nouveau l'option MTD. Vous recevrez alors un nouvel e-mail de bienvenue. Appuyez ensuite sur "Réactiver MTD" .

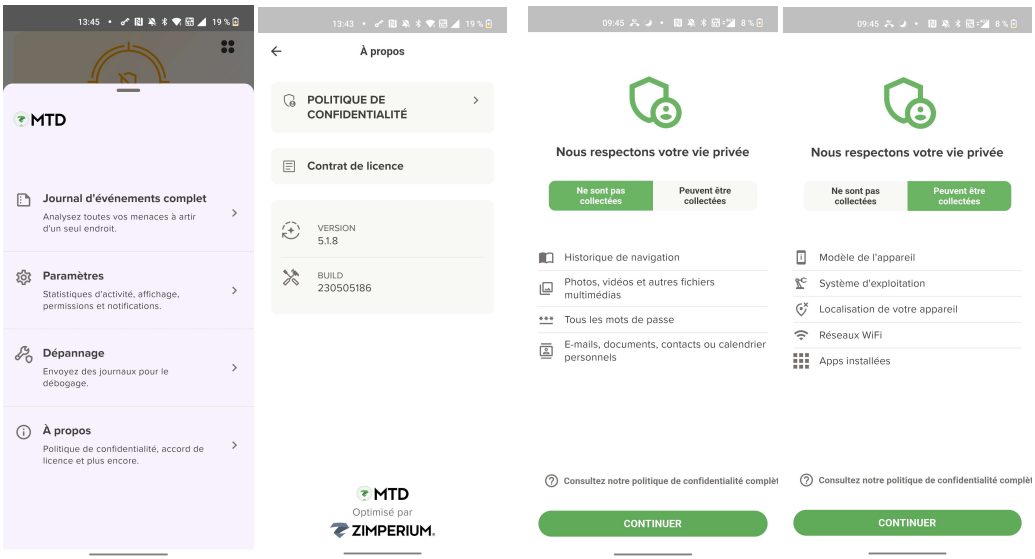


4.5 Quel contrôle mon administrateur a-t-il sur mon appareil ?

En fonction de la politique qu'il a définie, votre administrateur peut bloquer l'accès wi-fi, le Bluetooth ou l'accès à l'environnement de l'entreprise (p. ex. la messagerie) si certaines menaces sont détectées sur votre appareil mobile.

4.6 Qu'en est-il de ma vie privée ? À quelles données mon administrateur a-t-il accès ?

Les données accessibles ou non à votre administrateur à partir de votre appareil dépendent des paramètres de confidentialité de la solution définis par votre administrateur. Vous pouvez les consulter via la section Privacy Policy de l'app MTD .



4.7 Je reçois un message dans mon app MTD "Server verification incomplete"

Veuillez contacter votre administrateur. Il devra adapter la configuration.