ESET MOBILE SECURITY

POUR ANDROID

Guide de l'utilisateur

(pour version 3.0 et versions ultérieures)

Cliquez ici pour télécharger la dernière version de ce document.

ESET **MOBILE SECURITY**

Service client : http://support.athena-gs.fr/demande_de_support.php?editeur=eset

Rév. 31. 7. 2014

Sommaire

1. Introduction

ESET Mobile Security est une solution de sécurité complète qui protège votre appareil contre les nouvelles menaces et les pages de hameçonnage, qui filtre les appels et les messages non sollicités, et qui contrôle votre appareil à distance en cas de perte ou de vol.

1.1 Nouveautés

Les mises à jour et améliorations suivantes ont été introduites dans ESET Mobile Security version 3 :

- Intégration d'ESET Antivol dans le portail my.eset.com
- Suivi de la position : l'emplacement de l'appareil s'affiche désormais sur une carte
- Photos de l'appareil photo : les clichés pris avec l'appareil photo avant et l'appareil photo arrière sont désormais pris automatiquement lorsque l'appareil est marqué comme étant manquant
- Message à l'écran : possibilité d'envoyer un message personnalisé à la personne qui a trouvé l'appareil
- Verrouillage automatique : l'appareil est verrouillé lorsqu'une activité suspecte est détectée ou que l'appareil est marqué comme étant manquant
- Batterie faible : lorsque la batterie de votre appareil est sur le point d'atteindre un niveau critique, ESET Mobile Security envoie son dernier emplacement à my.eset.com
- Retentissement de sirène : déclenchez une sirène à distance depuis my.eset.com si vous pensez que votre appareil se trouve dans les alentours
- Changement du mot de passe de sécurité : possibilité de changer le mot de passe de sécurité depuis my.eset.com si vous l'oubliez
- Suppression à distance : supprimez toutes les données importantes de votre appareil depuis my.eset.com
- Menaces ignorées : la liste des menaces sera ignorée dans les prochaines analyses
- Analyse sur chargeur : l'analyse démarre automatiquement lorsque l'appareil est en veille et est connecté à un chargeur.

1.2 Configuration système requise

Pour installer ESET Mobile Security, votre appareil Android doit disposer de la configuration minimale requise suivante :

Système d'exploitation : Android 2.3 (Gingerbread) et versions ultérieures.
Résolution de l'écran tactile : minimum 240 x 320 p, 320 x 480 p recommandés
Processeur : 500 MHz (ARM7+)
Mémoire : 128 Mo
Espace de stockage interne disponible : 20 Mo
Connexion Internet

REMARQUE : les appareils « rootés » ne sont pas pris en charge. Certaines fonctionnalités (Antivol et Filtre de SMS et d'appels, par exemple, ne sont pas disponibles pour les tablettes ne prenant pas en charge les appels et les messages.

2. Installation

Pour installer ESET Mobile Security, choisissez l'une des méthodes suivantes.

REMARQUE : si vous disposez déjà d'un nom d'utilisateur et d'un mot de passe actifs ou d'une clé d'activation fournie par ESET, téléchargez ESET Mobile Security depuis le site Web d' ESET.

2.1 Installation depuis le site Internet d'ESET

Téléchargez ESET Mobile Security en numérisant le code QR ci-dessous à l'aide de votre appareil mobile et d'une application comme QR Droid ou Barcode Scanner :

Vous pouvez également télécharger le fichier d'installation de ESET Mobile Security, APK sur votre ordinateur :

1. Téléchargez le fichier à partir du site Internet d'ESET.
2. Copiez le fichier sur votre appareil par Bluetooth ou USB.
3. Appuyez sur l'icône de lancement dans l'écran d'accueil Android ou sélectionnez **Accueil** > **Menu** et appuyez sur **Paramètres** > **Applications**. Veillez à ce que les **sources inconnues** soient autorisées sur votre appareil.
4. Recherchez le fichier APK à l'aide d'une application du type ASTRO File Manager ou ES File Explorer.
5. Ouvrez le fichier et appuyez sur **Installer**. Une fois l'application installée, appuyez sur **Ouvrir**.

2.2 Installation depuis Google Play

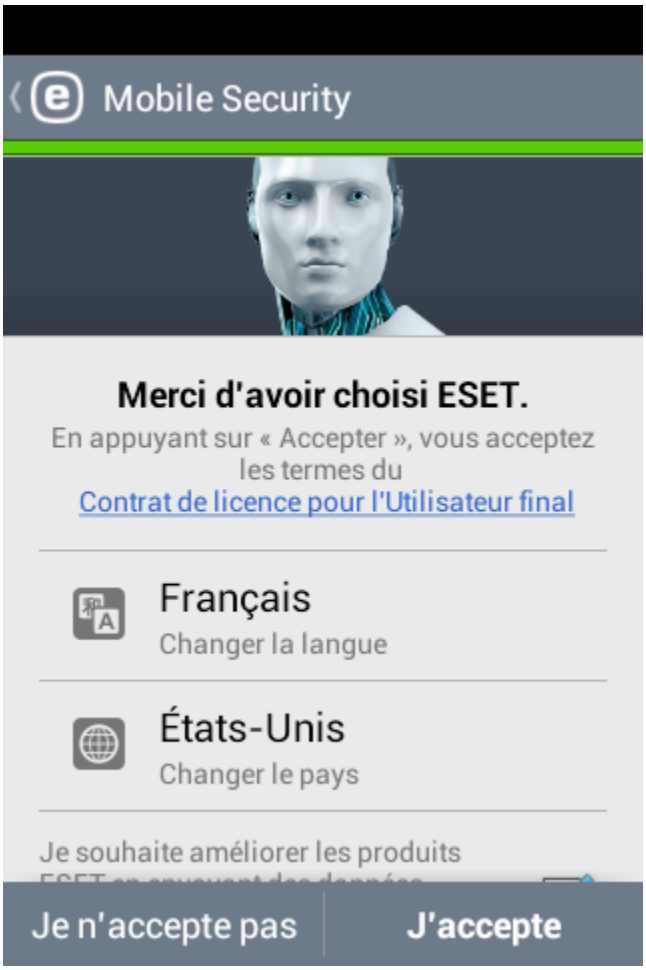
Ouvrez l'application Google Play Store sur votre appareil Android et recherchez ESET Mobile Security (ou simplement Eset).

Vous pouvez également installer le programme en numérisant le code QR ci-dessous à l'aide de votre appareil mobile et d'une application comme QR Droid ou Barcode Scanner :

2.3 Installation depuis Amazon

Ouvrez l'application Amazon sur votre appareil Android et recherchez ESET Mobile Security (ou simplement Eset).

2.4 Assistant de démarrage

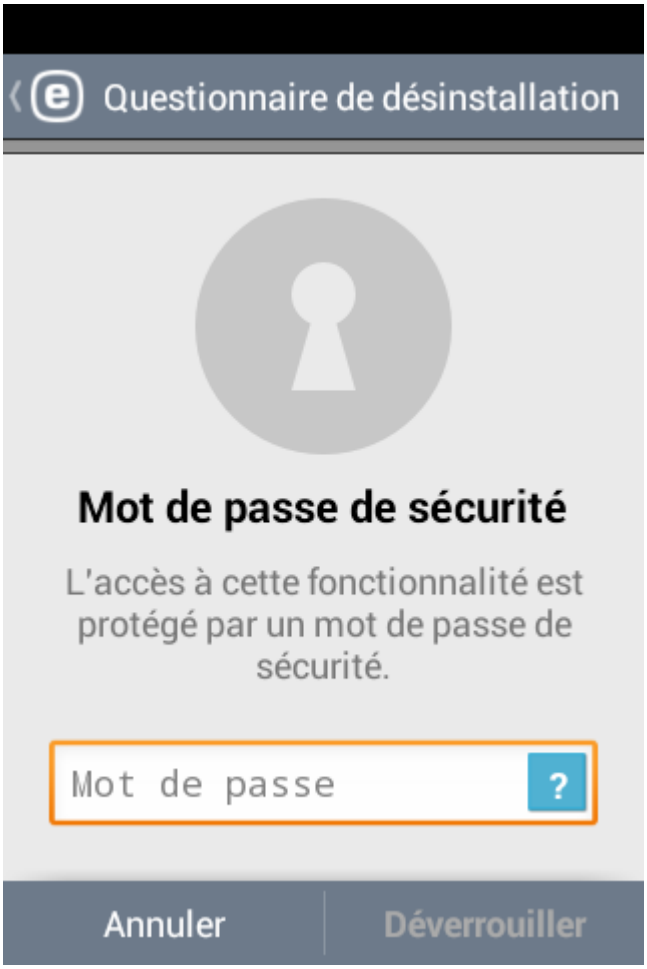


Une fois l'application installée sur votre appareil, suivez les invites de l'assistant de démarrage :

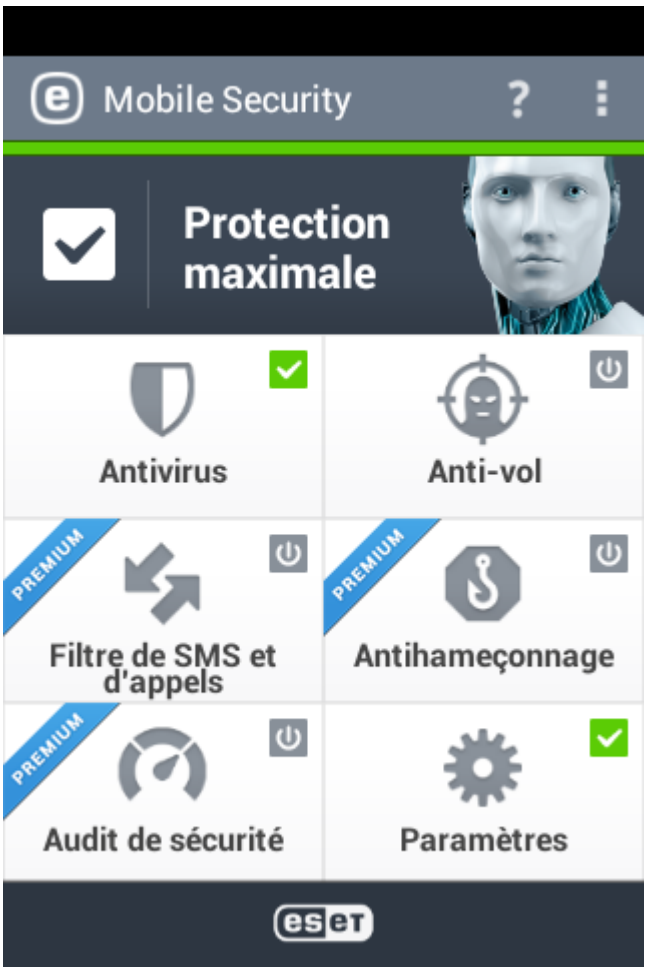
1. Sélectionnez la langue à utiliser dans ESET Mobile Security.
2. Sélectionnez votre pays de résidence.
3. Si vous souhaitez contribuer à l'amélioration des produits ESET en envoyant des données anonymes sur l'utilisation des applications, sélectionnez l'option correspondante.
4. Appuyez sur **J'accepte**. En appuyant sur Accepter, vous acceptez les termes du Contrat de licence pour l'Utilisateur final.
5. Choisissez si vous souhaitez participer à ESET Live Grid. Pour en savoir plus sur ESET Live Grid, consultez cette section 9.
6. Appuyez sur **Suivant**.
7. Choisissez si vous souhaitez que ESET Mobile Security détecte les applications potentiellement indésirables Pour en savoir plus sur de telles applications, reportez-vous à cette section 9.
8. Appuyez sur **Suivant**.
9. Appuyez sur **Terminer**.

2.5 Désinstallation

Pour désinstaller ESET Mobile Security, utilisez l'assistant de désinstallation disponible dans le menu principal d'ESET Mobile Security sous **Paramètres** > **Désinstaller**. Si vous avez activé la protection contre les désinstallations, vous serez invité à saisir votre mot de passe de sécurité.



3. Licence



Après son installation, ESET Mobile Security doit être activé.

Pour ouvrir la section **Licence**, appuyez sur l'icône Menu sur l'écran principal d'ESET Mobile Security (ou appuyez sur le bouton **MENU** de votre appareil), puis appuyez sur **Licence**.

Les méthodes d'activation varient selon que vous téléchargiez ESET Mobile Security depuis le site Internet d'ESET, depuis Amazon ou depuis Google Play.

- **Version d'essai** - Sélectionnez cette option si vous ne disposez pas d'une licence et si vous souhaitez tester ESET Mobile Security avant d'en faire l'acquisition. Indiquez votre **Adresse électronique** pour activer ESET Mobile Security pendant une période limitée. Vous recevrez un message de confirmation vous informant du succès de l'activation du produit. Vous pouvez activer une version d'essai une seule fois par appareil.
- **Activer l'application à l'aide d'un nom d'utilisateur et d'un mot de passe** - Si vous avez acheté votre produit auprès d'un revendeur ESET, vous avez reçu un nom d'utilisateur et un mot de passe au moment de l'achat. Saisissez ensuite les informations que vous avez reçues dans les champs **Nom d'utilisateur** et **Mot de passe**.
- **Activer l'application à l'aide d'une clé d'activation** - Si vous avez fait l'acquisition de votre produit avec un nouvel appareil (ou dans un boîtier), vous avez reçu une clé d'activation au moment de l'achat. Saisissez les informations que vous avez reçues dans le champ **Clé d'activation**, puis indiquez votre adresse électronique dans le champ **Adresse électronique**. Les nouvelles données d'authentification (Nom d'utilisateur et Mot de passe) remplaceront automatiquement la clé d'activation et seront envoyées à l'adresse électronique que vous avez indiquée.
- **Acheter une licence** - Sélectionnez cette option si vous n'avez pas de licence et souhaitez en acheter une. Vous serez redirigé vers la page Internet de votre revendeur ESET local.

Chaque licence n'est valide que pour une durée déterminée. Après l'expiration de la licence, vous serez invité à la renouveler. Le programme affichera une notification à l'avance.

REMARQUE : pendant l'activation, l'appareil doit être connecté à Internet. Des données seront téléchargées.

4. Antivirus

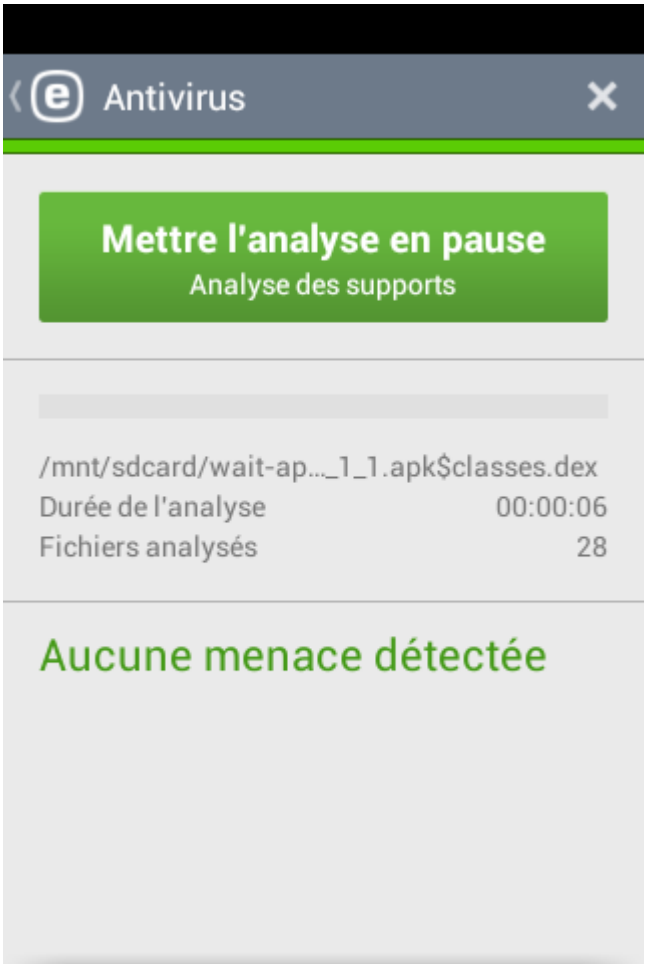
Le module Antivirus protège votre appareil contre les codes malveillants en bloquant les menaces et en les supprimant ou en les plaçant en quarantaine.

Analyser l'appareil

Analyser l'appareil permet de rechercher la présence éventuelle d'infiltrations sur votre appareil mobile.

Certains types de fichiers prédéfinis sont analysés par défaut. Une analyse complète de l'appareil vérifie la mémoire, les processus en cours, les DLL (bibliothèques de liaison dynamiques) qui en dépendent, ainsi que les fichiers faisant partie de la zone de stockage interne et des supports amovibles. Un résumé de l'analyse est enregistré dans un fichier journal disponible dans la section **Journaux d'analyse** .

Si vous souhaitez interrompre une analyse en cours, appuyez sur l'icône .



Type d'analyse

Vous avez le choix entre trois niveaux d'analyse :

- **Rapide** - si vous sélectionnez cette option, ESET Mobile Security n'analyse que les applications installées, les fichiers DEX (fichiers exécutables pour Android OS), les fichiers SO (bibliothèques) et les fichiers ZIP contenant un maximum de 3 archives imbriquées.
- **Intelligente** - l'analyse intelligente analyse le contenu de la carte SD en plus des types de fichiers analysés par l'analyse rapide.
- **Approfondie** - quelle que soit leur extension, tous les fichiers stockés dans la mémoire interne et sur la carte SD sont analysés.

Analyses automatiques

Outre l'analyse à la demande de l'appareil, ESET Mobile Security propose également des analyses automatiques. Pour en savoir plus sur l'analyse sur chargeur et l'analyse planifiée, consultez cette section 8.

Quarantaine

La principale fonction de la quarantaine consiste à stocker les fichiers infectés en toute sécurité. Pour en savoir plus, reportez-vous à la section Quarantaine 8.

Menaces ignorées

Pour en savoir plus sur cette fonctionnalité, consultez cette section 8.

Journaux d'analyse

La section **Journaux d'analyse** contient des informations complètes sur les tâches d'analyse réalisées sous forme de fichiers journaux. Pour en savoir plus, reportez-vous à ce chapitre 8.

Mettre à jour la base de données de menaces

Par défaut, ESET Mobile Security inclut une tâche qui garantit la mise à jour régulière du programme. Pour exécuter la mise à jour manuellement, appuyez sur **Mettre à jour la base de données de menaces**.

REMARQUE : afin d'éviter toute utilisation superflue de la bande passante, les mises à jour sont publiées uniquement lorsque cela est nécessaire, c'est-à-dire lorsqu'une nouvelle menace est ajoutée. Les mises à jour sont gratuites avec votre licence active, mais votre opérateur de téléphonie mobile peut facturer le transfert des données.

Des descriptions détaillées des **paramètres avancés** de l'antivirus sont disponibles dans la section Paramètres avancés 8.

4.1 Analyses automatiques

Type d'analyse

Vous avez le choix entre trois niveaux d'analyse. Ce paramètre s'applique à l'analyse sur chargeur et à l'analyse planifiée :

- **Rapide** - si vous sélectionnez cette option, ESET Mobile Security n'analyse que les applications installées, les fichiers DEX (fichiers exécutables pour Android OS), les fichiers SO (bibliothèques) et les fichiers ZIP contenant un maximum de 3 archives imbriquées.
- **Intelligente** - l'analyse intelligente analyse le contenu de la carte SD en plus des types de fichiers analysés par l'analyse rapide.
- **Approfondie** - quelle que soit leur extension, tous les fichiers stockés dans la mémoire interne et sur la carte SD sont analysés.

Analyse sur chargeur

Lorsque cette option est sélectionnée, l'analyse démarre automatiquement lorsque l'appareil est en veille, entièrement chargé et connecté à un chargeur.

Analyse planifiée

Analyse planifiée vous permet d'exécuter l'analyse de l'appareil automatiquement à une heure prédéfinie. Pour planifier une analyse, appuyez sur le bouton  en regard de l'option **Analyse planifiée** et indiquez les dates et les heures de démarrage de l'analyse. Par défaut, tous les jours de la semaine sont sélectionnés.

4.2 Quarantaine

Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer, ou encore s'ils sont détectés à tort par ESET Mobile Security.

Les fichiers stockés en quarantaine peuvent être affichés dans un journal qui indique le nom et l'emplacement d'origine des fichiers infectés, ainsi que la date et l'heure de leur mise en quarantaine.

Si vous souhaitez restaurer un fichier mis en quarantaine vers son emplacement d'origine, appuyez sur le fichier et sélectionnez l'icône  . Il n'est pas recommandé de restaurer régulièrement des fichiers mis en quarantaine.

Pour supprimer définitivement un fichier mis en quarantaine de votre appareil, appuyez sur le fichier et sélectionnez l'icône  .

REMARQUE : si vous mettez une application suspecte en quarantaine et décidez par la suite de l'installer, elle sera automatiquement retirée de la quarantaine.

4.3 Menaces ignorées

Pendant l'analyse, vous pouvez ajouter une nouvelle menace à la liste blanche. De cette manière, cette menace sera ignorée dans les prochaines analyses.

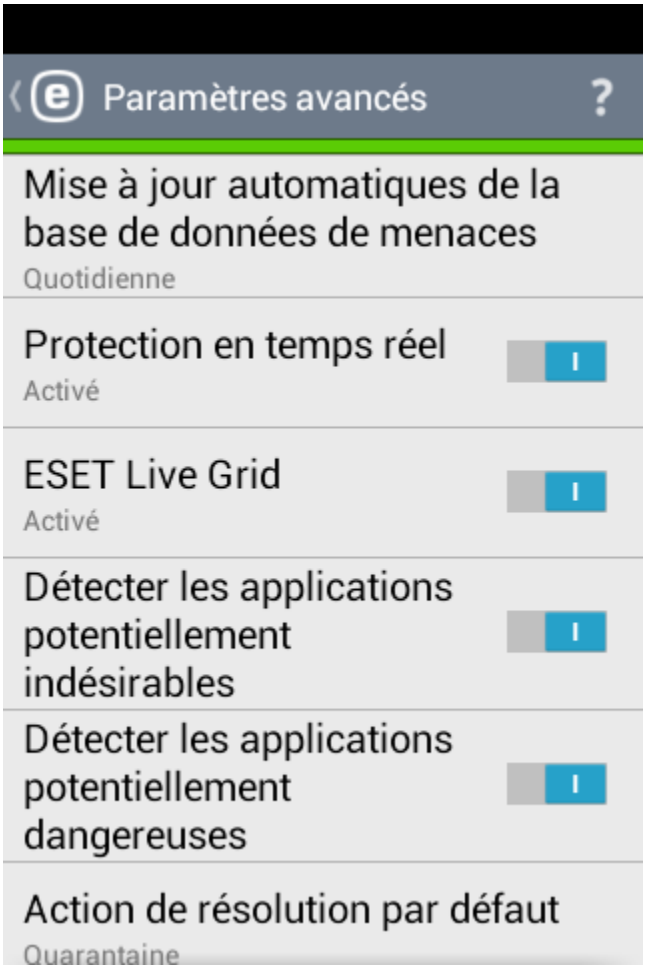
4.4 Journaux d'analyse

Des journaux d'analyse sont créés après chaque analyse planifiée ou analyse manuelle de l'appareil.

Chaque journal contient les éléments suivants :

- la date et l'heure de l'événement ;
- la durée de l'analyse ;
- le nombre de fichiers analysés ;
- le résultat de l'analyse ou les erreurs rencontrées au cours de l'analyse.

4.5 Paramètres avancés



Mise à jour automatiques de la base de données de menaces
Cette option permet de définir l'intervalle de téléchargement automatique des mises à jour de la base de données de menaces. Ces mises à jour sont publiées lorsqu'une nouvelle menace est ajoutée à la base de données. Il est recommandé de laisser ce paramètre à sa valeur par défaut (Quotidienne).

Protection en temps réel
Cette option vous permet d'activer ou de désactiver l'analyse en temps réel. Cette analyse démarre automatiquement au démarrage du système et analyse les fichiers avec lesquels vous interagissez. Elle analyse automatiquement le dossier *de téléchargements*, tous les fichiers d'installation *.apk* et tous les fichiers se trouvant sur la carte SD une fois qu'elle a été montée.

ESET Live Grid
Basé sur le système d'avertissement anticipé sophistiqué ThreatSense.Net, **ESET Live Grid** offre des niveaux de sécurité supplémentaires à votre appareil. Il surveille en permanence les programmes et processus exécutés, grâce à des informations collectées auprès de millions d'utilisateurs d'ESET dans le monde. De plus, vos analyses sont traitées plus rapidement et plus précisément à mesure que la base de données d' ESET Live Grid augmente. Cela nous permet d'offrir une protection proactive améliorée et une vitesse d'analyse accrue à tous les utilisateurs ESET. Nous recommandons d'activer cette fonctionnalité. Nous vous remercions pour votre soutien.

Détecter les applications potentiellement indésirables
Une application indésirable est un programme qui contient notamment des logiciels malveillants, qui installe des barres d'outils ou qui surveille les résultats de vos recherches. Dans certains cas, les avantages associés à une application indésirable l'emportent sur les risques. Par conséquent, ESET attribue à de telles applications une catégorie de risque inférieure à d'autres types de logiciels malveillants.

Détecter les applications potentiellement dangereuses
De nombreuses applications légitimes permettent de simplifier l'administration d'appareils en réseau. Elles peuvent cependant être utilisées à mauvais escient et à des fins malveillantes. L'option **Détecter les applications potentiellement dangereuses** vous permet de détecter de telles menaces. « Applications potentiellement dangereuses » est une classification utilisée pour les logiciels commerciaux et légitimes. Elle inclut les programmes tels que les outils d'accès à distance, les applications de décodage de mot de passe et les enregistreurs de frappe.

Action de résolution par défaut
Ce paramètre détermine l'action à exécuter lorsqu'une analyse se termine et des menaces ont été détectées. Si vous avez sélectionné **Supprimer**, le fichier infecté est supprimé. Si vous avez sélectionné **Quarantaine**, le fichier infecté est placé en quarantaine 8.

Serveur de mise à jour
Dans cette option, vous pouvez mettre à jour la base de données des menaces depuis le **serveur de préversion**. Les mises à jour des préversions font l'objet de tests en interne et seront très prochainement à la disposition du grand public. Vous pouvez bénéficier de ces mises à jour de préversions en accédant aux dernières méthodes de détection et aux derniers correctifs. Toutefois, la stabilité de ces mises à jour de préversions n'est pas garantie. La liste des modules en cours est disponible dans la section À propos : appuyez sur l'icône de menu dans l'écran principal de ESET Mobile Security (ou appuyez sur le bouton **MENU** de votre appareil) et appuyez sur **À propos** > **Version d'application**. Il est recommandé aux utilisateurs débutants de laisser l'option **Serveur de version** sélectionnée par défaut.

5. Antivol

La fonctionnalité Antivol protège votre appareil mobile de tout accès non autorisé.

Si vous perdez votre appareil ou si quelqu'un vous le dérobe et remplace votre carte SIM par une autre carte non fiable, ESET Mobile Security verrouille automatiquement l'alerte et une alerte est envoyée par SMS à un ou plusieurs numéros de téléphone que vous définissez. Ce message indique le numéro de la carte SIM insérée dans l'appareil, le numéro IMSI (numéro d'identité internationale d'abonné mobile), ainsi que le numéro IMEI (numéro d'identité internationale d'équipement mobile) de l'appareil mobile. L'utilisateur non autorisé n'a pas conscience que ce message a été envoyé puisqu'il est supprimé automatiquement des fils des messages de l'appareil. Vous pouvez également demander les coordonnées GPS de l'appareil perdu, ou effacer à distance toutes les données stockées dessus.

REMARQUE : Certaines fonctionnalités Antivol (Protection SIM, Amis de confiance et Commandes de texte SMS) ne sont pas disponibles sur les tablettes ne prenant pas en charge les messages.

La version 3 de ESET Mobile Security s'intègre complètement avec la protection ESET Antivol par l'intermédiaire de my.eset.com. Vous pouvez ainsi surveiller l'activité de votre appareil depuis le portail en ligne ESET Antivol, verrouiller l'appareil, envoyer des messages personnalisés à la personne qui l'a trouvé, déclencher une sirène ou effacer à distance les données de l'appareil.

Pour commencer à utiliser la fonctionnalité Antivol, appuyez sur **Antivol** dans le menu principal du programme. Un assistant très simple vous accompagne dans la création de votre mot de passe de sécurité, l'activation de l'option Protection contre les désinstallations, l'ajout de votre carte SIM comme étant fiable, l'ajout d'un ami fiable, la saisie de vos coordonnées et l'activation des commandes par SMS. Une fois ces étapes effectuées, vous pouvez associer votre appareil à votre compte my.eset.com.

5.1 my.eset.com

Si vous avez déjà un compte my.eset.com, appuyez sur **Vous avez déjà un compte ?** et saisissez votre adresse e-mail et votre mot de passe pour vous connecter.

Si vous n'avez pas de compte my.eset.com, appuyez sur **Enregistrement** et complétez le formulaire d'enregistrement. Recherchez dans votre boîte de réception le message de confirmation, ouvrez-le et cliquez sur le lien pour activer votre compte. Vous pouvez désormais utiliser les fonctionnalités de sécurité d'Antivol gérées depuis my.eset.com.

Pour obtenir de l'aide sur l'utilisation d'Antivol sur my.eset.com , reportez-vous à l'aide en ligne en cliquant sur **Aide** dans l'angle supérieur droit de l'écran.

5.2 Optimisation

L'optimisation d'ESET Antivol est une évaluation technique mesurable de l'état de sécurité de votre appareil. La protection ESET Antivol examine votre système et y recherche les problèmes suivants :

- Services de localisation désactivés
- Satellites GPS inutilisés
- Verrouillage de l'écran non sécurisé
- Données mobiles non activées
- Services Google Play absents

Pour chaque problème de sécurité, vous pouvez appuyer sur **Modifier les paramètres** afin d'accéder à l'écran dans lequel vous pouvez résoudre ce problème. Si vous ne souhaitez pas que ESET Mobile Security signale un problème, appuyez sur **Ignorer ce problème**.

5.3 Protection SIM

La section **Protection SIM** affiche la liste de cartes SIM de confiance acceptées par ESET Mobile Security. Si vous insérez une carte SIM qui n'est pas définie dans cette liste, l'écran se verrouille et un SMS d'alerte est envoyé à vos **Amis de confiance**.

Pour ajouter une nouvelle carte SIM, appuyez sur l'icône  . Pour en savoir plus, reportez-vous à la section suivante 10.

Pour supprimer une carte SIM de la liste, maintenez le doigt appuyé sur l'entrée correspondante et appuyez sur l'icône  .

REMARQUE : La fonction Protection SIM n'est pas disponible sur certains appareils mobiles CDMA et WCDMA.

5.3.1 Ajout d'une carte SIM de confiance

Saisissez un **Nom de la carte SIM** (Maison, Travail, par exemple), ainsi que son numéro **IMSI** (International Mobile Subscriber Identity). Le numéro IMSI contient généralement 15 chiffres et est imprimé sur la carte SIM. Il peut être plus court dans certains cas.

5.4 Amis de confiance

Dans la liste **Amis de confiance**, vous pouvez ajouter ou supprimer les numéros de téléphone qui recevront le SMS d'alerte si une carte SIM non fiable est insérée dans votre appareil. Pour ajouter un nouvel ami de confiance, appuyez sur **Ajouter à partir des contacts** et sélectionnez un contact dans la liste.

Si la personne n'est pas incluse dans votre liste de contacts, appuyez sur l'icône . Pour en savoir plus, reportez-vous à la section suivante 11.

Pour supprimer un contact de la liste, maintenez le doigt appuyé sur l'entrée correspondante et appuyez sur l'icône  .

REMARQUE : si vous vous trouvez à l'étranger, tous les numéros de téléphone inclus dans la liste doivent inclure le code du pays, suivi du numéro de téléphone (+1610100100, par exemple).

5.4.1 Ajout d'un ami de confiance

Saisissez le nom d'un ami, ainsi que son numéro de téléphone. Si le contact comporte plusieurs numéros de téléphone, le SMS d'alerte est envoyé à tous les numéros associés. Si vous souhaitez autoriser cet ami à réinitialiser votre mot de passe en cas d'oubli, sélectionnez l'option **Autoriser la réinitialisation à distance du mot de passe**.

5.5 Commandes de texte SMS

Les commandes à distance SMS (« siren », « wipe », « lock » et « find ») ne fonctionnent que si l'option **Commandes de texte SMS** est sélectionnée.

Si vous avez perdu votre appareil et souhaitez le verrouiller, envoyez à votre numéro un SMS de verrouillage à distance depuis un appareil mobile. Le SMS doit avoir le format suivant :
eset lock mot_de_passe
Remplacez *mot_de_passe* par votre mot de passe de sécurité. Une fois l'appareil verrouillé, un utilisateur non autorisé devra saisir votre mot de passe pour le déverrouiller.

Pour verrouiller l'appareil et déclencher une sirène, envoyez à votre numéro un SMS au format suivant :
eset siren mot_de_passe
La sirène retentit, même si votre appareil est en mode silencieux.

Si vous souhaitez demander les coordonnées GPS de votre appareil mobile, envoyez un SMS à votre numéro ou au numéro de l'utilisateur non autorisé (selon que la carte SIM a déjà été remplacée ou non), au format suivant :
eset find mot_de_passe
Vous recevrez un SMS contenant les coordonnées GPS de l'appareil que vous avez perdu, ainsi qu'un lien vers cet emplacement sur Google Maps.

Si vous souhaitez effacer toutes les données stockées sur votre appareil et sur tous les supports amovibles qui y sont insérés, envoyez un SMS de suppression à distance au format suivant :
eset wipe mot_de_passe
Tous les contacts, tous les SMS, tous les messages électroniques, toutes les applications installées, ainsi que votre compte Google et le contenu de la carte SD, sont effacés de manière permanente de votre appareil. Si ESET Mobile Security n'est pas défini comme Administrateur de l'appareil, seuls les contacts, les messages et le contenu de la carte SD sont effacés.

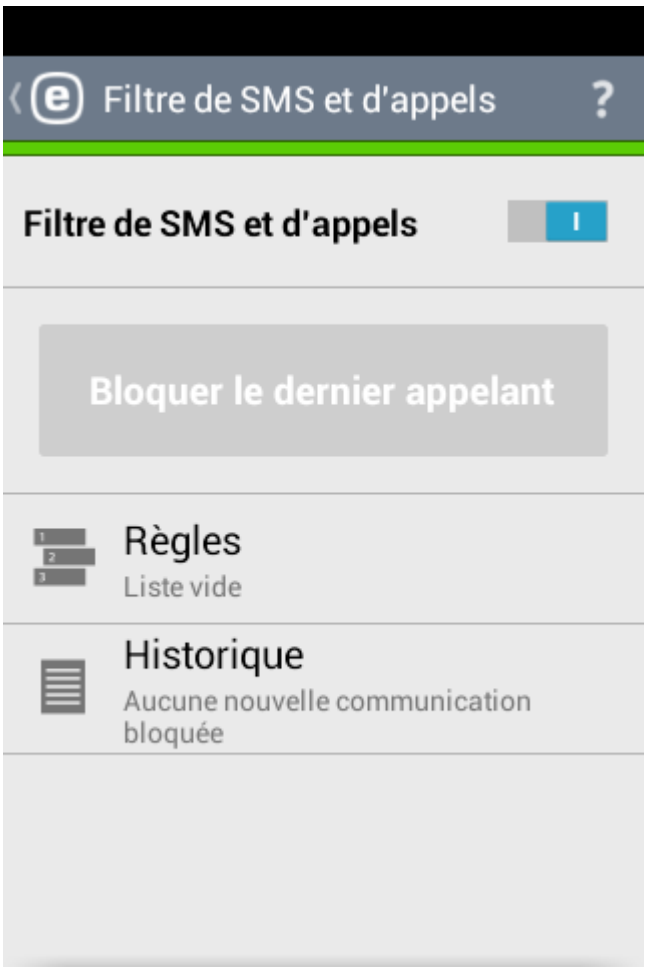
REMARQUE : votre mot de passe fait la différence entre les majuscules et les minuscules. Veillez par conséquent à le saisir exactement comme vous l'avez défini dans l'assistant de configuration d'Antivol.

5.6 Mes coordonnées

Si vous marquez votre appareil comme étant manquant sur my.eset.com, les informations figurant dans **Mes coordonnées** s'affichent sur l'écran de votre périphérique verrouillé et permettent à la personne qui a trouvé votre appareil de vous contacter.

Saisissez votre nom, la description de l'appareil, un numéro de contact secondaire (par exemple votre numéro professionnel ou privé) ou votre adresse électronique.

6. Filtre de SMS et d'appels



Filtre de SMS et d'appels bloque les SMS/MMS entrants, ainsi que les appels entrants/sortants en fonction des règles que vous déterminez.

Les messages non sollicités concernent habituellement des annonces de prestataires de service de téléphone portable, ou des messages d'inconnus ou d'utilisateurs non spécifiés. L'expression *blocage de message* fait référence au déplacement automatique d'un message entrant dans la section **Historique**. Aucune notification n'est affichée lorsqu'un message entrant est bloqué. Avec cette fonction, vous n'êtes pas dérangé par des informations non sollicitées, mais vous avez toujours la possibilité de consulter la liste des messages bloqués afin de vous assurer qu'aucun message n'a été bloqué par erreur.

REMARQUE : Filtre de SMS et d'appels ne fonctionne pas sur les tablettes ne prenant pas en charge les appels et les messages.

Pour bloquer les appels et les messages provenant du dernier numéro de téléphone reçu, appuyez sur **Bloquer le dernier appelant**. Cela permet de créer une règle de blocage de SMS et d'appels.

6.1 Règles

Pour ajouter une nouvelle règle, appuyez sur l'icône ✚. Pour en savoir plus sur la création d'une règle, reportez-vous à la section suivante 12.

Si vous souhaitez supprimer une règle dans la liste **Règles**, appuyez de manière prolongée sur l'entrée correspondante et appuyez sur l'icône 🗑.

6.1.1 Ajout d'une règle

Spécifiez un groupe de numéros de téléphones ou une personne. L'option **Tous les numéros inconnus** permet d'inclure les numéros de téléphone qui ne sont pas enregistrés dans votre liste de contacts. Vous pouvez utiliser cette option pour bloquer les appels indésirables ou pour empêcher vos enfants de composer des numéros inconnus. L'option **Tous les numéros connus** désigne tous les numéros de téléphone enregistrés dans votre liste de contacts. L'option **Numéros masqués** s'applique aux appelants dont le numéro est volontairement masqué par la fonction de refus de présentation de la ligne appelante.

Spécifiez les éléments à bloquer ou à autoriser :

-  appels sortants
-  appels entrants
-  messages texte entrants (SMS)
-  messages multimédia (MMS) entrants

Pour appliquer la règle pour une durée limitée, désélectionnez **Toujours** au bas de l'écran et sélectionnez les dates et heures d'application de la règle. Par défaut, tous les jours de la semaine sont sélectionnés. Cette fonctionnalité est utile si vous ne souhaitez pas être dérangé pendant la nuit ou le week-end.

REMARQUE : si vous vous trouvez à l'étranger, tous les numéros de téléphone inclus dans la liste doivent inclure le code du pays, suivi du numéro de téléphone (+1610100100, par exemple).

6.2 Historique

La section **Historique** contient les appels et les messages bloqués ou autorisés par le filtre de SMS et d'appels. Chaque journal contient le nom de l'événement, le numéro de téléphone correspondant, ainsi que la date et l'heure de l'événement. Les journaux des SMS et des MMS contiennent également le corps du message.

Si vous souhaitez modifier une règle relative au dernier numéro ou au dernier contact bloqué, sélectionnez l'entrée dans la liste et appuyez sur l'icône  .

Pour supprimer l'entrée de la liste, sélectionnez-la et appuyez sur l'icône  . Pour supprimer plus d'entrées, maintenez le doigt appuyé sur l'une d'elles, sélectionnez celles à supprimer et appuyez sur l'icône  .

7. Antihameçonnage

Le terme *hameçonnage* désigne une activité criminelle utilisant une ingénierie sociale (la manipulation d'utilisateurs dans le but d'obtenir des informations confidentielles). Le hameçonnage est souvent utilisé pour obtenir des données sensibles, comme des numéros de compte bancaire ou de carte de crédit, des codes PIN, des noms d'utilisateur ou des mots de passe.

Il est recommandé de garder la fonction **Antihameçonnage** activée. Toutes les attaques potentielles de hameçonnage en provenance de sites Internet ou de domaines répertoriés dans la base de données de logiciels malveillants d'ESET seront bloquées, et un message d'avertissement s'affichera pour vous informer de l'attaque.

Anti-hameçonnage s'intègre aux navigateurs les plus répandus disponibles pour Android (Chrome ou le navigateur Android par défaut, par exemple).

REMARQUE : Antihameçonnage ne vous offre pas de protection lors de la navigation en mode hors connexion (incognito).

7.1 Historique

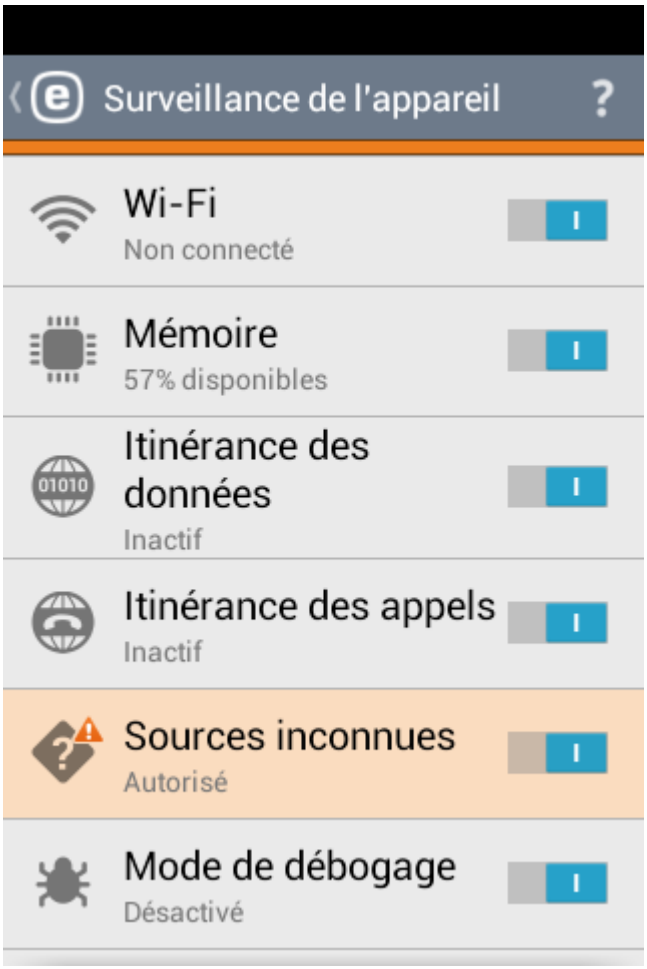
Dans la section **Historique**, vous pouvez consulter la liste de toutes les attaques de hameçonnage bloquées par ESET Mobile Security.

8. Audit de sécurité

Audit de sécurité vous permet de contrôler et de modifier des paramètres importants de l'appareil et des permissions des applications installées, pour prévenir les risques de sécurité.

Pour activer ou désactiver Audit de sécurité et ses composants spécifiques, utilisez les boutons suivants : 

8.1 Surveillance de l'appareil

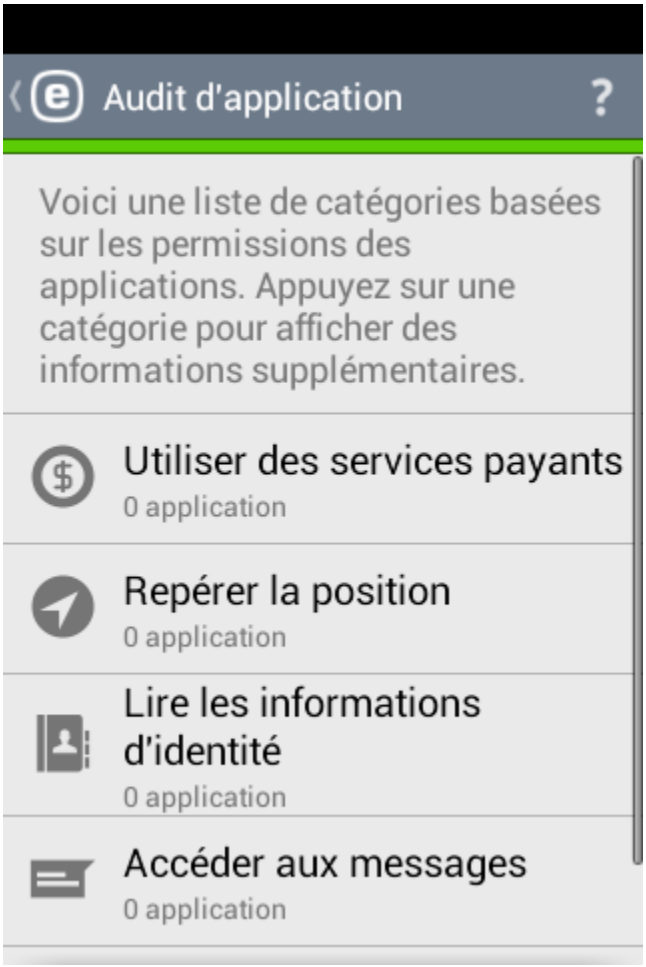


Dans la section **Surveillance de l'appareil**, vous pouvez définir les composants de l'appareil qui seront surveillés par ESET Mobile Security.

Appuyez sur chaque option pour afficher une description détaillée, ainsi que son état actuel.

Certaines options telles que **Sources inconnues** et **Mode de débogage** peuvent être modifiées en appuyant sur **Modifier les paramètres**. Vous serez redirigé vers l'écran des paramètres du système Android.

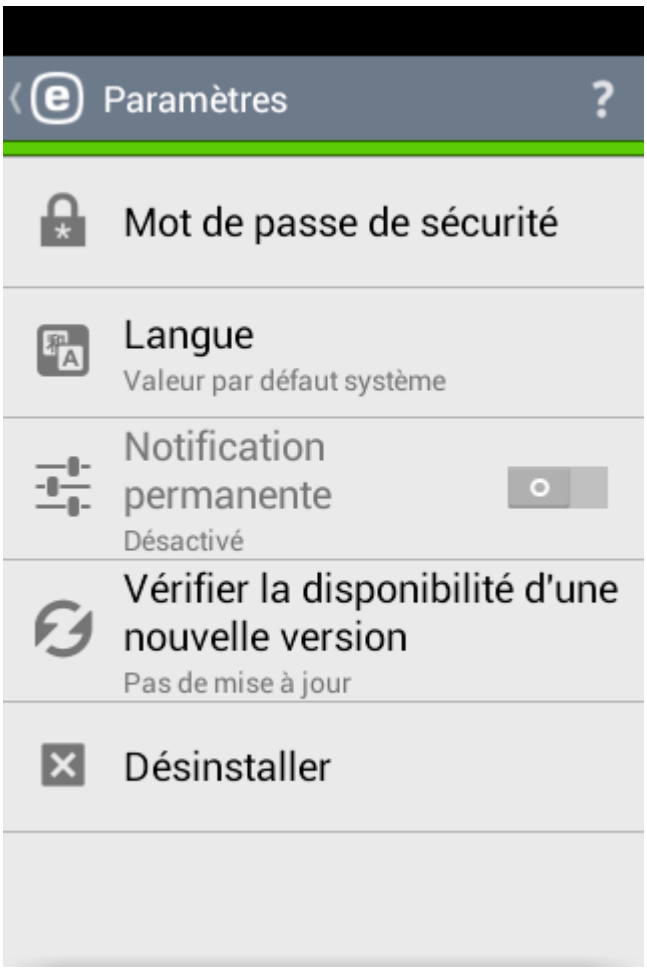
8.2 Audit d'application



Certaines applications installées sur votre appareil peuvent accéder à des services payants, qui repèrent votre emplacement ou qui lisent les informations liées à votre identité, les contacts et les SMS. ESET Mobile Security permet d'effectuer un audit de ces applications.

Dans la section **Audit d'application**, vous pouvez consulter la liste des applications, réparties en catégories. Appuyez sur chaque catégorie pour afficher une description détaillée. Appuyez sur une application particulière pour accéder aux détails de ses permissions.

9. Paramètres



Mot de passe de sécurité
Cette option vous permet de définir un nouveau mot de passe de sécurité ou de modifier le mot de passe existant. Pour en savoir plus, reportez-vous à la section Mot de passe de sécurité 16.

Langue
Par défaut, ESET Mobile Security est installé dans la langue qui est définie dans les paramètres régionaux de votre appareil (dans les paramètres de langue et de clavier d'Android). Pour changer la langue de l'interface utilisateur de l'application, appuyez sur **Langue** et sélectionnez la langue de votre choix.

Notification permanente

ESET Mobile Security affiche son icône de notification dans l'angle supérieur gauche de l'écran (barre d'état Android). Si vous ne souhaitez pas afficher cette icône, désélectionnez l'option **Notification permanente**.

Vérifier la disponibilité d'une nouvelle version
Pour une protection maximale, il est important d'utiliser la dernière version d'ESET Mobile Security. Appuyez sur **Vérifier la disponibilité d'une nouvelle version** pour vérifier si une nouvelle version est disponible au téléchargement.

Désinstaller
Pour désinstaller ESET Mobile Security, utilisez l'assistant **Désinstaller**. Les dossiers d'ESET Mobile Security et de quarantaine seront définitivement supprimés.

9.1 Mot de passe de sécurité

Votre **mot de passe de sécurité** est requis pour déverrouiller votre appareil, pour accéder aux fonctionnalités protégées par mot de passe (Antivol, par exemple) et pour désinstaller ESET Mobile Security. L'option **Expression de rappel** (si elle est définie) affiche une astuce qui vous permet de vous souvenir du mot de passe si vous l'avez oublié.

Si vous avez oublié votre mot de passe, vous pouvez envoyer à votre téléphone portable un SMS depuis un numéro de téléphone portable enregistré dans la liste Amis de confiance 10. Ce SMS doit avoir la forme suivante :
eset remote reset
Votre mot de passe sera réinitialisé et vous serez invité à définir un nouveau mot de passe.

Si vous n'aviez pas défini d'ami de confiance avant de verrouiller votre appareil, vous pouvez envoyer une demande de réinitialisation de mot de passe. Cette option s'activera sur l'écran de votre appareil verrouillé après 2 tentatives infructueuses de déverrouillage. Vous recevrez un message contenant le code de déverrouillage à l'adresse électronique de votre compte Google ou à l'adresse définie dans **Antivol** > **Mes coordonnées**. Saisissez le code de déverrouillage sur l'écran de votre appareil verrouillé. Une fois l'appareil déverrouillé, définissez un nouveau mot de passe de sécurité dans **Paramètres** > **Mot de passe**.

Vous pouvez également changer votre mot de passe de sécurité sur my.eset.com. Une fois que vous êtes connecté, sélectionnez votre appareil, cliquez sur **Paramètres** et saisissez un nouveau mot de passe.

IMPORTANT : choisissez votre mot de passe avec soin. Pour renforcer la sécurité et rendre votre mot de passe plus difficile à deviner pour les autres, utilisez une combinaison de majuscules, de minuscules et de chiffres.

10. Service client

ESET Les experts du service client sont disponibles pour vous apporter une assistance administrative ou technique concernant ESET Mobile Security ou tout autre produit ESET.

Pour envoyer une demande d'assistance directement depuis votre appareil, appuyez sur l'icône Menu  dans l'écran principal de ESET Mobile Security (ou appuyez sur le bouton **MENU** de votre appareil) et appuyez sur **Service client** > **Service client**. Remplissez tous les champs obligatoires.

ESET Mobile Security inclut une fonctionnalité de journalisation avancée qui contribue au diagnostic des problèmes techniques potentiels. Pour envoyer à ESET un journal détaillé de l'application, assurez-vous que l'option **Journal de l'application** sélectionnée (par défaut). Envoyez votre demande en appuyant sur **Soumettre**. Les spécialistes du service client ESET vous contacteront à l'adresse électronique que vous avez spécifiée.