ESET Mobile Security

Windows Mobile

Manuel d'installation et Guide de l'utilisateur

ESET Mobile Security

Service client Monde : www.eset.eu/support
Service client Amérique du Nord : www.eset.com/support

Rév. 10/28/2010

Sommaire

1. Installation d'ESET Mobile Security

1.1 Configuration minimum requise

Pour que vous puissiez installer ESET Mobile Security pour Windows Mobile, votre appareil mobile doit disposer de la configuration système suivante :

	Configuration minimum requise
Système d'exploitation	Windows Mobile 5.0 et versions ultérieures
Processeur	200 MHz
Mémoire	16 Mo
Espace disque disponible	2,5 Mo

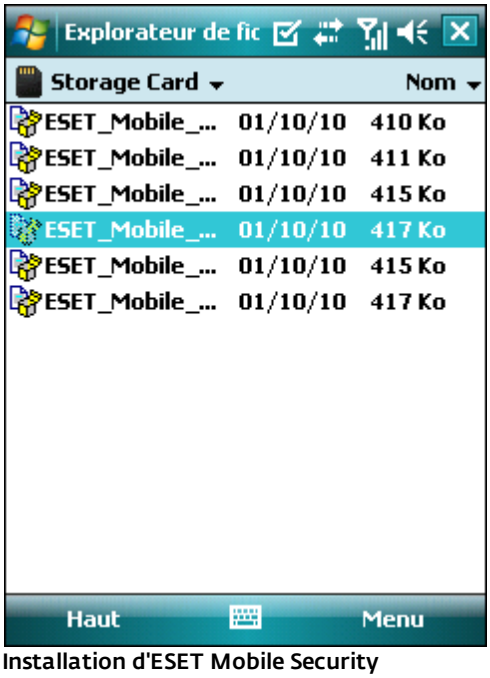
1.2 Installation

Enregistrez tous les documents ouverts et quittez toutes les applications avant d'effectuer l'installation. Vous pouvez installer ESET Mobile Security directement sur votre appareil ou utiliser votre ordinateur pour l'installer.

Une fois ESET Mobile Security installé, vous devez l'activer en suivant les étapes mentionnées dans la section Activation de produit 5.

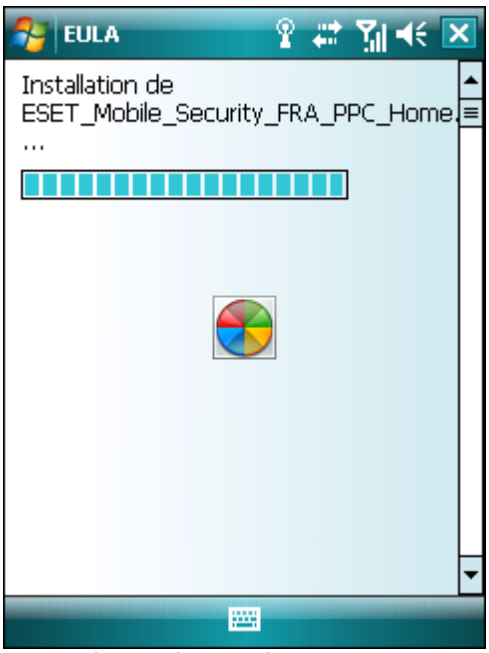
1.2.1 Installation sur votre appareil

Pour installer ESET Mobile Security directement sur votre appareil, téléchargez le fichier d'installation *.cab* sur votre appareil par transfert Wi-Fi ou Bluetooth, ou encore en l'insérant en pièce jointe d'un message. Choisissez **Démarrer > Programmes > Explorateur de fichiers** pour localiser le fichier. Touchez le fichier pour lancer le programme d'installation, puis suivez les instructions de l'assistant d'installation.



Installation d'ESET Mobile Security

REMARQUE : l'interface utilisateur peut varier en fonction du système d'exploitation (il s'agit dans votre cas de Windows Mobile) et du modèle de l'appareil. Le fichier d'installation peut s'afficher dans un autre menu ou dans un autre dossier sur votre appareil.

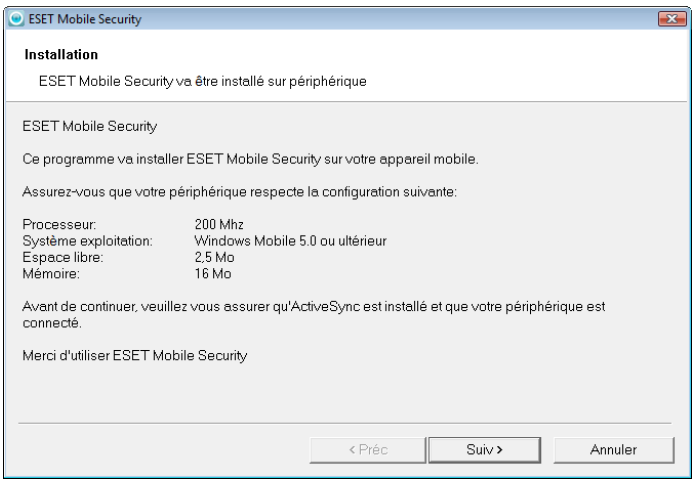


Progression de l'installation

Après l'installation, vous pouvez modifier les paramètres du programme. Toutefois, la configuration par défaut fournit déjà le niveau maximum de protection contre les programmes malveillants.

1.2.2 Installation à partir de votre ordinateur

Pour installer ESET Mobile Security à l'aide de votre ordinateur, connectez votre appareil mobile à l'ordinateur par ActiveSync (sous Windows XP) ou à l'aide du Gestionnaire pour appareils Windows Mobile (sous Windows 7 et Vista). Une fois l'appareil reconnu, exécutez le module d'installation que vous avez téléchargé (fichier *exe*) et suivez les instructions de l'assistant d'installation.



Lancement du programme d'installation sur votre ordinateur

Suivez ensuite les invites qui s'affichent sur votre appareil mobile.

1.3 Désinstallation

Pour désinstaller ESET Mobile Security de votre appareil mobile, touchez les options **Démarrer > Paramètres**, puis l'onglet **Système** et l'icône de **suppression des programmes**.

REMARQUE : l'interface utilisateur peut varier en fonction du système d'exploitation (il s'agit dans votre cas de Windows Mobile) et du modèle de l'appareil. Ces options peuvent être légèrement différentes sur votre appareil.

Suppression d'ESET Mobile Security

Sélectionnez ESET Mobile Security et touchez l'option **Suppr**. Touchez **Oui** lorsque le système vous invite à confirmer la désinstallation.

Suppression d'ESET Mobile Security

2. Activation de produit

La fenêtre principale d'ESET Mobile Security (**Démarrer > Applications > ESET Mobile Security**) est le point de départ de toutes les instructions de ce manuel.

Fenêtre principale d'ESET Mobile Security

Après son installation, ESET Mobile Security doit être activé. Si vous ne recevez aucun message vous invitant à activer le produit, touchez les options **Menu > Activer**.

Activation du programme

Il existe deux méthodes d'activation en fonction du mode d'acquisition de votre produit ESET Mobile Security.

2.1 Activation à l'aide d'un login et d'un mot de passe

Si vous avez acheté votre produit auprès d'un revendeur, vous avez reçu un login et un mot de passe au moment de l'achat. Sélectionnez l'option **Login/MdP** et saisissez les informations que vous avez reçues dans les champs **Login** et **MdP**. Saisissez votre adresse dans le champ **Email**. Touchez l'option **Activer** pour terminer l'activation.

2.2 Activation à l'aide d'une clé d'enregistrement

Si vous avez fait l'acquisition de votre produit ESET Mobile Security avec un nouvel appareil (ou indépendamment dans un coffret), vous avez reçu une clé d'enregistrement au moment de l'achat. Sélectionnez l'option **Clé enregistr.** et saisissez les informations que vous avez reçues dans le champ **Clé**, ainsi que votre adresse dans le champ **Email**. Touchez l'option **Activer** pour terminer l'activation. Les nouvelles données d'authentification (Login et MdP) remplaceront automatiquement la clé d'enregistrement et seront envoyées à l'adresse électronique que vous avez indiquée.

Dans les deux cas, vous recevrez un message de confirmation vous informant du succès de l'activation du produit.

Chaque activation n'est valide que pour une durée déterminée. Une fois l'activation expirée, vous devrez renouveler la licence du programme (le programme vous en avertira à l'avance).

REMARQUE : pendant l'activation, l'appareil doit être connecté à Internet. Des données seront téléchargées. Le montant de ces transferts dépend du contrat de service que vous avez signé avec votre opérateur de téléphonie mobile.

3. Mise à jour (MAJ)

Par défaut, ESET Mobile Security est installé avec une tâche de mise à jour qui garantit la mise à jour régulière du programme. Vous pouvez également effectuer des mises à jour manuellement.

Après l'installation, il est recommandé d'exécuter la première mise à jour manuellement. Pour ce faire, touchez les options **Action > MAJ**.

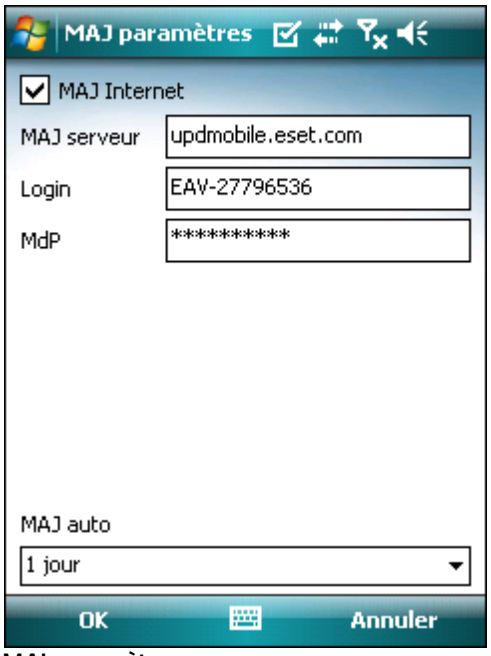
3.1 Paramètres (Param.)

Pour configurer les paramètres de mise à jour, touchez les options **Menu > Param. > MAJ**.

L'option **MAJ Internet** active ou désactive les mises à jour automatiques.

Vous pouvez indiquer le serveur de mise à jour **MAJ serveur** depuis lequel les mises à jour sont téléchargées (il est recommandé de conserver le paramètre par défaut *updmobile.eset.com*).

Pour définir la fréquence des mises à jour automatiques, utilisez l'option **MAJ auto**.



MAJ paramètres

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

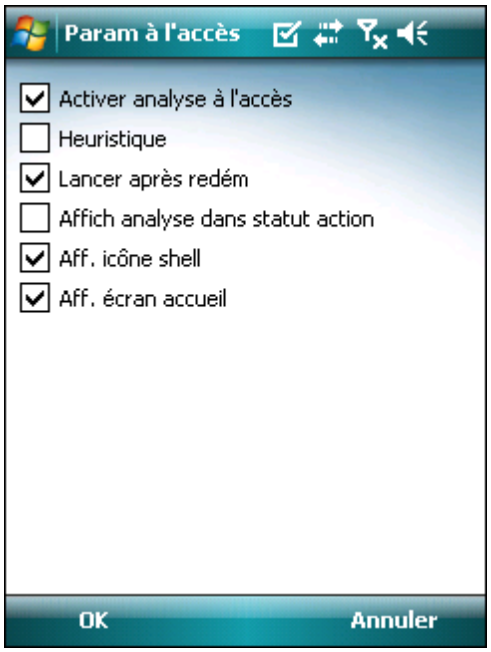
4. Analyse à l'accès

L'analyse à l'accès vérifie en temps réel les fichiers que vous manipulez. Les fichiers exécutés, ouverts ou enregistrés sont automatiquement vérifiés afin de détecter toute menace éventuelle. L'analyse s'effectue avant toute opération réalisée sur le fichier, ce qui garantit une protection maximale avec les paramètres par défaut. L'analyse à l'accès est lancée automatiquement au démarrage du système.

4.1 Paramètres (Param.)

Touchez les options **Menu > Param. > À l'accès** pour activer ou désactiver les options suivantes :

- **Activer analyse à l'accès** : si cette option est activée, l'analyse à l'accès s'exécute en arrière-plan.
- **Heuristique** : sélectionnez cette option pour afficher les techniques d'analyse heuristique. L'analyse heuristique identifie de manière proactive les nouveaux logiciels malveillants que la version actuelle de la base des signatures de virus ne détecte pas encore : elle analyse le code et reconnaît le comportement typique des virus. Les analyses de ce type sont en revanche plus longues que les analyses classiques.
- **Lancer après redém** : si cette option est sélectionnée, l'analyse à l'accès démarre automatiquement au redémarrage de l'appareil.
- **Affich analyse dans statut action** : sélectionnez cette option pour afficher le statut de l'analyse dans l'angle inférieur droit pendant le déroulement de l'analyse.
- **Aff. icône shell** : affiche l'icône d'accès rapide aux paramètres d'analyse à l'accès (dans l'angle inférieur droit de l'écran d'accueil Windows Mobile).
- **Aff. écran accueil** : cette option permet de désactiver l'écran d'accueil d'ESET Mobile Security pendant le démarrage de l'appareil.



Paramètres de l'analyse à l'accès

5. Analyse à la demande

Vous pouvez utiliser l'analyse à la demande afin de rechercher toute présence éventuelle d'infiltrations dans votre appareil mobile. Certains types de fichiers prédéfinis sont analysés par défaut.

5.1 Exécution d'une analyse sur l'intégralité de l'appareil

Une analyse sur l'intégralité 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.

Pour exécuter une analyse sur l'intégralité de l'appareil, touchez les options **Action > Analyse > App. complet**.

REMARQUE : par défaut, la mémoire n'est pas analysée. Vous pouvez activer cette analyse dans **Menu > Param. > Général**.

Exécution d'une analyse sur l'intégralité de l'appareil

Le programme analyse d'abord la mémoire système (y compris les processus en cours et les fichiers DLL dépendants), puis analyse les fichiers et les dossiers. Le chemin complet et le nom de chaque fichier analysé sont affichés brièvement.

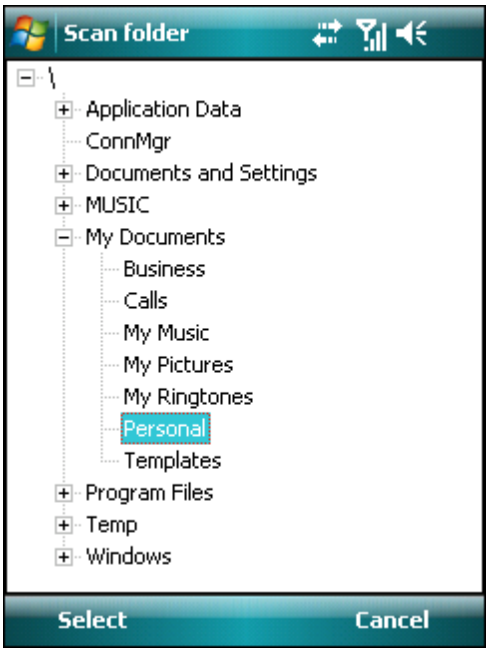
REMARQUE : pour annuler une analyse en cours, touchez les options **Action > Analyse > Arr analyse**.

5.2 Analyse d'un dossier

Pour analyser un dossier de votre appareil, touchez les options **Action > Analyse > Dossier**.

Analyse d'un dossier

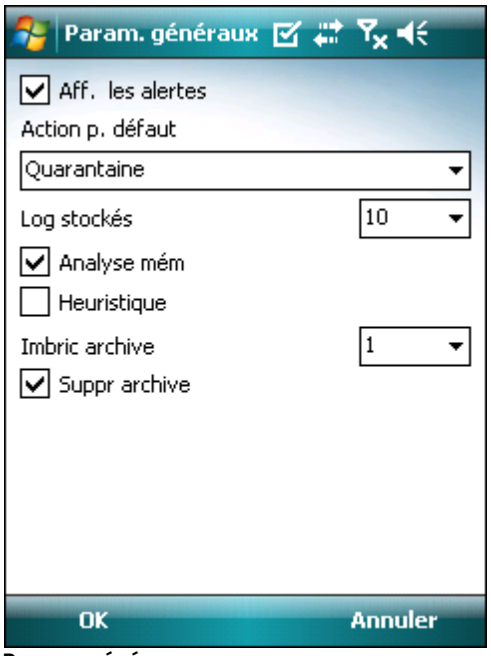
Touchez le dossier à analyser, puis l'option **Sélect**.



Sélection d'un dossier à analyser

5.3 Param. généraux

Pour modifier les paramètres d'analyse, touchez les options **Menu > Param. > Général**.



Param. généraux

Sélectionnez l'option **Aff. les alertes** pour afficher les notifications d'alerte de menace.

Vous pouvez indiquer une action par défaut qui sera exécutée automatiquement en cas de détection de fichiers infectés. Vous pouvez choisir parmi les options suivantes :

- **Quarantaine**
- **Suppr**
- **Ne rien faire (non recommandé)**

L'option **Log stockés** vous permet de définir le nombre maximum de journaux à stocker dans la section **Menu > Logs > Analyse**.

Si l'option **Analyse mém** est activée, l'analyse recherche les éventuels programmes malveillants dans la mémoire de l'appareil avant d'analyser les fichiers proprement dits.

Si l'option **Heuristique** est sélectionnée, ESET Mobile Security utilise les techniques d'analyse heuristique. L'heuristique est une détection basée sur un algorithme et qui analyse le code et recherche tout comportement typique de virus. Elle permet notamment d'identifier les logiciels malveillants qui ne sont pas encore identifiés par la version actuelle de la base des signatures de virus. Les analyses de ce type sont en revanche plus longues que les analyses classiques.

L'option **Imbric. archives** permet d'indiquer le nombre de niveaux d'imbrication des archives à analyser. (Plus le nombre est élevé, plus l'analyse « descend » dans les différents niveaux d'imbrication.)

Si l'option **Suppr archive** est activée, les fichiers d'archive (*zip*, *rar* et *jar*) contenant des objets infectés sont supprimés automatiquement.

5.4 Param extension

Pour spécifier les types de fichiers à analyser sur votre appareil mobile, touchez les options **Menu > Param. > Extensions**.

La fenêtre **Extensions** qui apparaît répertorie les types de fichiers qui risquent le plus d'être infiltrés. Sélectionnez les types de fichiers à analyser ou désélectionnez les extensions à exclure de l'analyse. Si vous activez l'option **Archives**, tous les fichiers d'archive pris en charge (*zip*, *rar* et *jar*) sont analysés.

Pour analyser tous les fichiers, désélectionnez la case **Sensible à extension**.

Param extension

6. Menace détectée

Lorsqu'une menace est détectée, ESET Mobile Security vous invite à sélectionner une action à entreprendre.

Boîte de dialogue d'alerte de menace

Il est recommandé de sélectionner **Suppr**. Si vous sélectionnez **Quarantaine**, le fichier est déplacé de son emplacement d'origine au dossier de quarantaine. Si vous sélectionnez **Ignorer**, aucune action n'est exécutée et le fichier infecté reste sur votre appareil mobile.

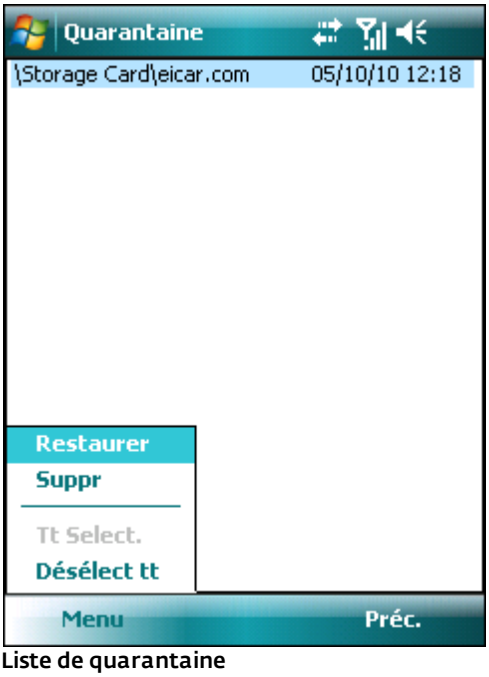
Si une infiltration est détectée dans une archive (fichier *.zip* par exemple), l'option **Suppr archive** est disponible dans la fenêtre d'alerte. Sélectionnez cette option et l'option **Suppr** pour supprimer tous les fichiers archivés.

Si vous désactivez l'option **Aff. les alertes**, aucune fenêtre d'alerte n'apparaît pendant la mise à jour (pour désactiver les alertes pour toutes les prochaines analyses, reportez-vous à la rubrique Param. généraux 9).

6.1 Quarantaine

La principale fonction de la quarantaine est le stockage en toute sécurité des fichiers infectés. Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer ou s'ils sont détectés erronément par ESET Mobile Security.

Les fichiers stockés dans le dossier de quarantaine peuvent être affichés dans un journal qui indique la date et l'heure de mise en quarantaine et l'emplacement d'origine des fichiers infectés. Pour ouvrir la quarantaine, touchez les options **Menu > Affich > Quarantaine**.



Liste de quarantaine

Vous pouvez restaurer les fichiers en quarantaine en touchant les options **Menu > Restaurer** (chaque fichier est restauré dans son emplacement d'origine). Si vous souhaitez supprimer les fichiers définitivement, touchez les options **Menu > Suppr**.

7. Anti-Theft

La fonction Anti-Theft protège votre téléphone mobile de tout accès non autorisé.

Si vous perdez votre téléphone ou si quelqu'un le vole et remplace votre carte SIM par une autre carte (non fiable), un SMS d'alerte est envoyé secrètement à certains numéros de téléphone indiqués par l'utilisateur. Ce message indique le numéro de téléphone 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) du téléphone. L'utilisateur non autorisé n'a pas conscience que ce message a été envoyé puisqu'il est supprimé automatiquement du dossier des éléments envoyés.

Pour effacer toutes les données (contacts, messages et applications) stockées sur votre appareil et tous les supports amovibles qui y sont insérés, vous pouvez envoyer un SMS de suppression à distance au numéro de téléphone de l'utilisateur non autorisé sous la forme suivante :
#RC# DS mot_de_passe
mot_de_passe étant votre propre mot de passe que vous avez défini dans **Menu > Param. > MdP**.

7.1 Paramètres (Param.)

Définissez d'abord votre mot de passe dans **Menu > Param. > MdP**. Ce mot de passe est nécessaire :

- pour l'envoi à votre appareil d'un SMS de suppression à distance ;
- pour l'accès aux paramètres Anti-Theft sur votre appareil ;
- pour la désinstallation d'ESET Mobile Security depuis votre appareil.

Pour définir un nouveau mot de passe, saisissez votre mot de passe dans les champs **Nouveau MdP** et **Ressaisissez MdP**. L'option **Rappel** (si elle est définie) affiche une astuce qui vous permet de vous remémorer votre mot de passe si vous l'avez oublié.

Pour changer de mot de passe, saisissez d'abord votre mot de passe dans **Entrez MdP actuel**, puis entrez le mot de passe.

IMPORTANT : choisissez votre mot de passe avec soin, car vous devrez le fournir si vous souhaitez éventuellement désinstaller ESET Mobile Security de votre appareil.

Définition d'un mot de passe de sécurité

Pour accéder aux paramètres Anti-Theft, touchez les options **Menu > Param. > Anti-Theft** et saisissez votre mot de passe.

Pour désactiver la vérification automatique de la carte SIM insérée dans l'appareil (et l'envoi éventuel d'un SMS d'alerte), désélectionnez l'option **Activer corresp SIM**.

Si la carte SIM qui est insérée dans votre appareil mobile est celle que vous souhaitez enregistrer comme étant fiable, cochez la case **SIM actuelle fiable** : la carte SIM est enregistrée dans la liste des cartes SIM fiables (onglet **SIM fiable**). La zone de texte **Alias SIM** est complétée automatiquement avec le numéro IMSI.

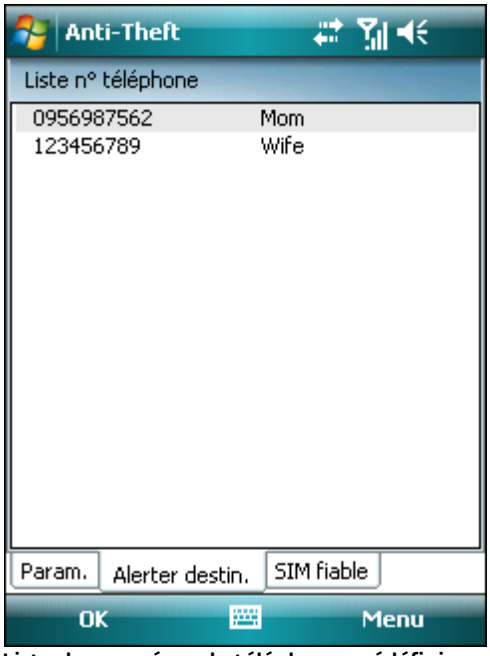
Si vous utilisez plusieurs cartes SIM, vous souhaiterez peut-être les différencier en modifiant l'option **Alias SIM** (en indiquant par exemple *Bureau*, *Maison*, etc.).

Dans la zone **Alerte SMS**, vous pouvez modifier le message qui sera envoyé aux numéros prédéfinis si une carte SIM non fiable est insérée dans votre appareil.

Anti-Theft paramètres

L'onglet **Alerte destin.** répertorie les numéros prédéfinis qui recevront le SMS d'alerte si une carte SIM non fiable est insérée dans votre appareil. Pour ajouter un nouveau numéro, touchez les options **Menu > Ajout**. Pour ajouter un numéro figurant dans la liste des contacts, touchez les options **Menu > Ajout contact**.

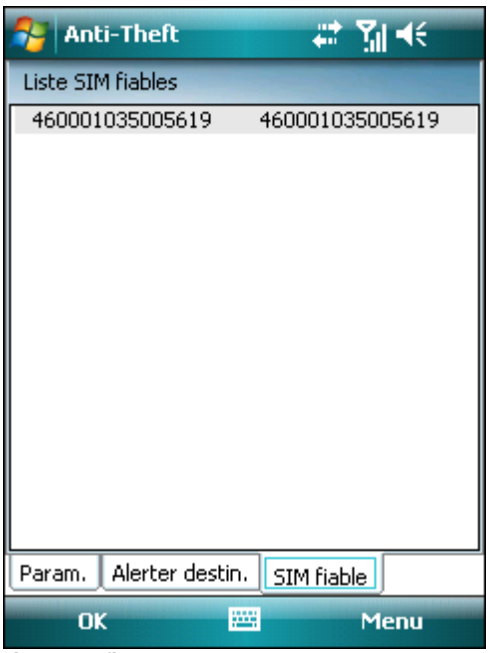
REMARQUE : le numéro de téléphone doit inclure l'indicatif international, suivi du numéro proprement dit (par exemple *+16105552000*).



Liste des numéros de téléphone prédéfinis

L'onglet **SIM fiable** répertorie les cartes SIM fiables. Chaque entrée se compose de l'alias SIM (colonne de gauche) et du numéro IMSI (colonne de droite).

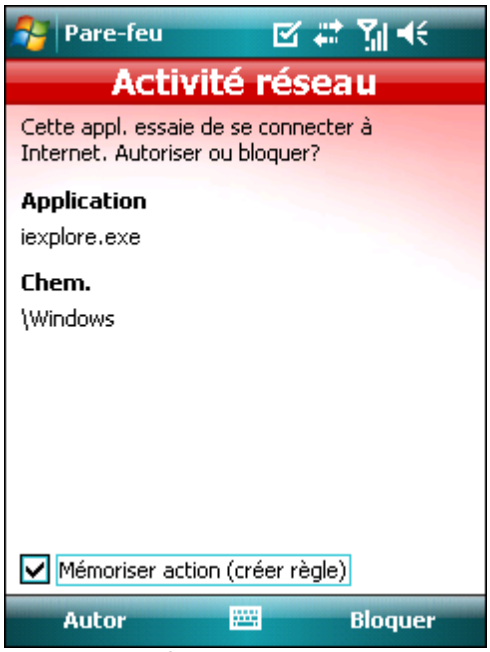
Pour supprimer un numéro SIM de la liste, sélectionnez le numéro et touchez les options **Menu > Supp**.



Liste SIM fiables

8. Pare-feu

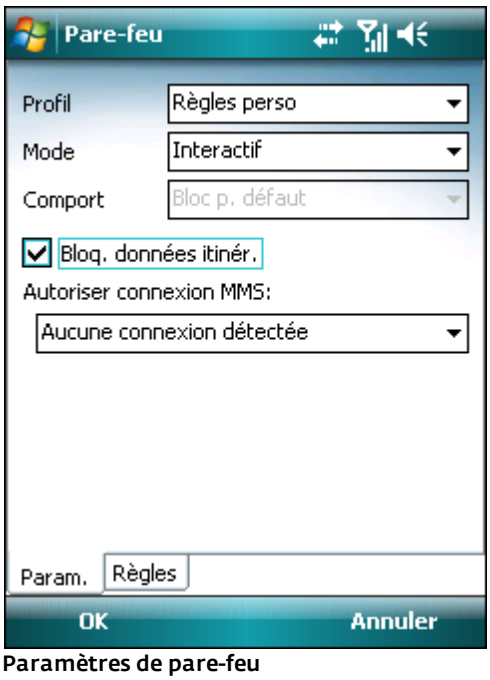
Le pare-feu contrôle tout le trafic réseau entrant et sortant, et autorise ou refuse les différentes connexions en fonction des règles de filtrage.



Alerte de pare-feu

8.1 Paramètres (Param.)

Pour modifier les paramètres de pare-feu, touchez les options **Menu > Param. > Pare-feu**.



Paramètres de pare-feu

Vous pouvez choisir parmi les profils suivants :

- **Tt autor.** : autorise tout le trafic réseau.
- **Tt bloquer** : bloque tout le trafic réseau.
- **Règles perso** : permet de définir vos propres règles de filtrage.

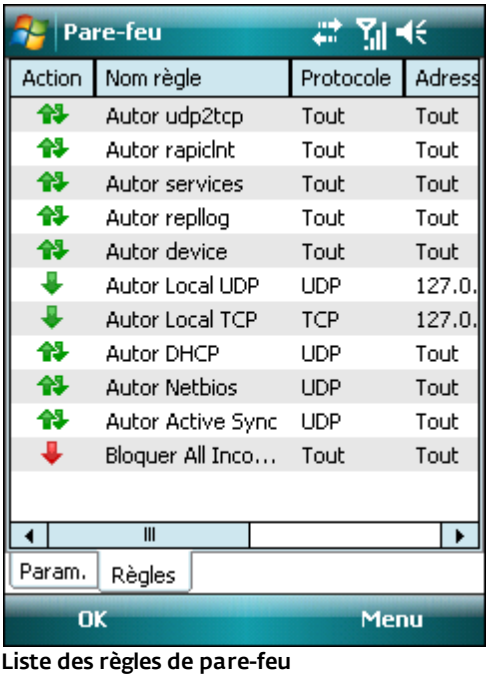
Vous pouvez choisir l'un des deux modes de filtrage dans le profil **Règles perso** :

- **Auto.** : convient aux utilisateurs qui préfèrent l'utilisation simple et pratique du pare-feu, sans définir de règles. Ce mode autorise tout le trafic sortant. Pour le trafic entrant, vous pouvez définir l'action par défaut (**Autor. p. déf.** ou **Bloc p. défaut**) dans l'option **Comport**.
- **Interactif** : vous permet de personnaliser votre pare-feu personnel. Lors de la détection d'une communication sans règle correspondante, une boîte de dialogue s'affiche pour signaler une connexion inconnue. La boîte de dialogue permet d'autoriser ou de bloquer la communication, et de créer une règle. Si vous choisissez de créer une règle, toutes les autres connexions de ce type seront autorisées ou bloquées, conformément à la règle. Si une application avec une règle existante a été modifiée, la boîte de dialogue permet d'accepter ou de refuser ce changement. En fonction de votre réponse, la règle existante est modifiée.

Bloq. données itinér. : si cette option est activée, ESET Mobile Security détecte automatiquement si votre appareil est connecté à un réseau itinérant et bloque les données entrantes et sortantes. Cette option ne bloque pas les données reçues par Wi-Fi ou GPRS.

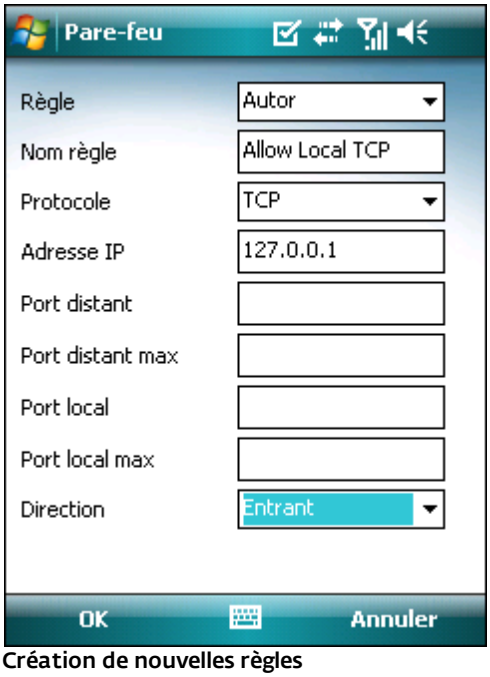
Autoriser connexion MMS : choisissez une connexion pour recevoir les messages MMS sur un réseau itinérant. Les messages MMS provenant d'autres connexions sont bloqués par ESET Mobile Security.

Dans l'onglet **Règles**, vous pouvez modifier ou supprimer des règles de filtrage existantes.



Liste des règles de pare-feu

Pour créer une nouvelle règle, touchez les options **Menu > Ajout**, remplissez tous les champs obligatoires et touchez l'option **OK**.



Création de nouvelles règles

9. Vérification de sécurité

La Vérification de sécurité vérifie différentes données concernant le téléphone : niveau de la batterie, statut Bluetooth, espace disque disponible, etc.

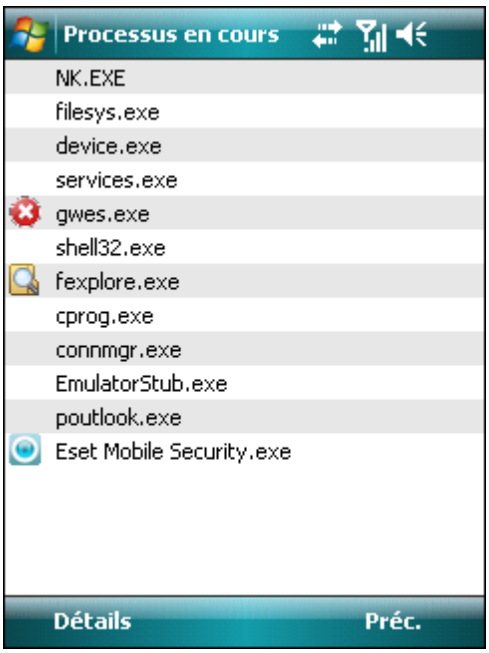
Pour exécuter une Vérification de sécurité manuellement, touchez les options **Action > Vérification de sécurité**. Un rapport détaillé apparaît.

Résultats de la Vérification de sécurité

La barre verte située à côté de chaque élément indique que la valeur est au-dessus du seuil ou que l'élément ne représente pas un risque de sécurité. La barre rouge indique que la valeur est au-dessous du seuil ou que l'élément pourrait représenter un risque de sécurité potentiel.

Si les options **Statut Bluetooth** ou **Visibilité appareil** sont repérées en rouge, vous pouvez désactiver le statut en sélectionnant l'élément et en touchant les options **Menu > Vérif**.

Pour afficher les détails de chaque élément, sélectionnez l'élément et touchez les options **Menu > Détails**.



Processus en cours

L'option **Processus en cours** répertorie tous les processus qui sont en cours d'exécution sur votre appareil.

Pour afficher les détails du processus (chemin d'accès complet du processus et utilisation de la mémoire), sélectionnez le processus et touchez l'option **Détails**.

9.1 Paramètres (Param.)

Pour modifier les paramètres de Vérification de sécurité, touchez les options **Menu > Param. > Vérification de sécurité**.

Paramètres de Vérification de sécurité

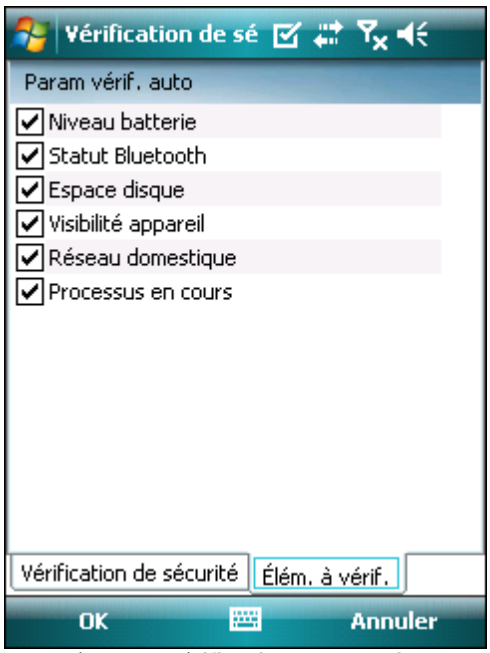
Si l'option **Correction auto** est activée, ESET Mobile Security essaie automatiquement de corriger les éléments présentant un risque (le statut Bluetooth, la visibilité de l'appareil par exemple) sans intervention de l'utilisateur.

Ce paramètre ne s'applique qu'à la vérification automatique (planifiée).

L'option **Période vérif** permet de choisir la fréquence de la vérification automatique. Si vous souhaitez désactiver la vérification automatique, sélectionnez **Jamais**.

Vous pouvez modifier la limite à partir de laquelle les options **Espace disque** et **Niveau batterie** sont considérées comme étant faibles.

Dans l'onglet **Élém. à vérif.**, vous pouvez sélectionner les éléments à vérifier au cours de la vérification de sécurité automatique (planifiée).



Paramètres de vérification automatique

10. Antispam

La protection antispam (courriers indésirables) bloque les messages SMS et MMS non sollicités qui sont envoyés à votre appareil mobile.

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.

10.1 Paramètres (Param.)

Touchez les options **Menu > Affich > Stats** pour afficher les statistiques relatives aux messages reçus et bloqués.

Les paramètres de protection antispam (**Menu > Param. > Antispam**) proposent les modes de filtrage suivants :

- **Bloquer contacts inconnus** : activez cette option pour accepter uniquement les messages provenant des contacts de votre carnet d'adresses.
- **Bloquer contacts connus** : activez cette option pour ne recevoir que les messages des expéditeurs qui ne figurent pas dans votre carnet d'adresses.
- Activez les deux options **Bloquer contacts inconnus** et **Bloquer contacts connus** pour bloquer automatiquement tous les messages entrants.
- Désactivez les deux options **Bloquer contacts inconnus** et **Bloquer contacts connus** pour désactiver la protection antispam. Tous les messages entrants seront acceptés.

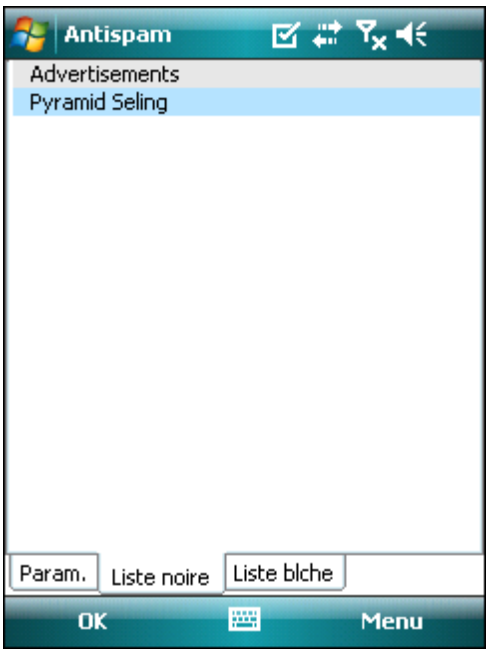
REMARQUE : les entrées de la liste blanche et de la liste noire ne tiennent pas compte de ces options (reportez-vous à la sectionListe noire/Liste blche 17).

Paramètres de protection antispam

10.2 Liste blanche/Liste noire

La **liste noire** est une liste de numéros de téléphone pour lesquels tous les messages sont bloqués. Les entrées répertoriées dans cette liste sont prioritaires sur les options définies dans les paramètres antispam (onglet **Param.**).

La **liste blanche** répertorie les numéros de téléphone pour lesquels tous les messages sont acceptés. Les entrées répertoriées dans cette liste sont prioritaires sur les options définies dans les paramètres antispam (onglet **Param.**).



Liste noire

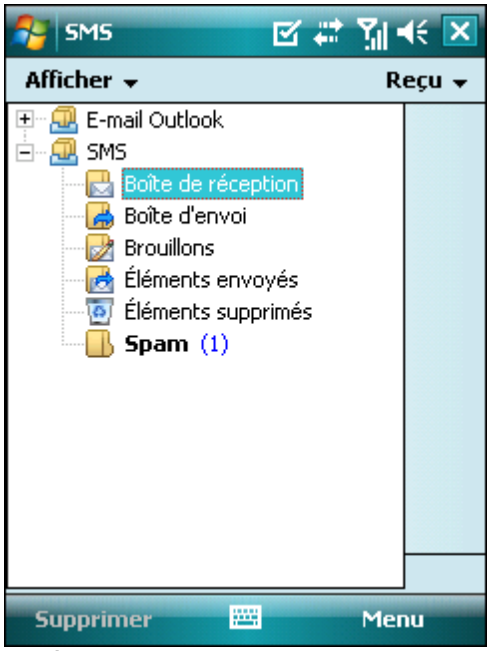
Pour ajouter un nouveau numéro à la liste blanche/liste noire, sélectionnez l'onglet de la liste à modifier et touchez les options **Menu > Ajout**. Pour ajouter un numéro figurant dans la liste des contacts, touchez les options **Menu > Ajout contact**.

Avertissement : l'ajout d'un numéro/contact à la liste noire déplace automatiquement les messages reçus de cet utilisateur dans le dossier **spam**.

10.3 Localisation des courriers indésirables

Le dossier **Spam** stocke les messages bloqués et les classe comme courriers indésirables en fonction des paramètres d'antispam. Le dossier est créé automatiquement à la réception du premier courrier indésirable. Pour localiser le dossier **Spam** et afficher les messages bloqués, suivez les étapes ci-dessous :

1. Ouvrez le programme qu'utilise votre appareil pour la messagerie depuis le menu **Démarrer**, **Messaging** par exemple.
2. Touchez l'option relative aux **messages texte** (ou aux **MMS** si vous souhaitez localiser le dossier de stockage des spams MMS).
3. Touchez les options **Menu > Accéder à > Dossiers...** (ou **Menu > Dossiers** sur les smartphones).
4. Sélectionnez le dossier **Spam**.



Dossier des spams

10.4 Suppression de courriers indésirables

Pour supprimer les courriers indésirables de votre appareil mobile, suivez les opérations ci-dessous :

1. Dans la fenêtre principale d'ESET Mobile Security, touchez les options **Menu >Settings > Antispam**.
2. Touchez l'option **Nettoyer le spam**.
3. Touchez l'option **Oui** pour confirmer la suppression de tous les courriers indésirables.

Suppression de courriers indésirables

11. Affichage des journaux et des statistiques

La section du **journal d'analyse** (**Menu > Logs > Analyse**) contient des journaux qui fournissent des informations complètes sur les tâches d'analyse réalisées. Les journaux sont créés à chaque analyse à la demande ou lorsqu'une infiltration a été détectée par l'analyse à l'accès. Tous les fichiers infectés sont identifiés en rouge. Chaque entrée du journal explique la raison pour laquelle le fichier a été inclus dans le journal.

Les journaux d'**analyse** contiennent les éléments suivants :

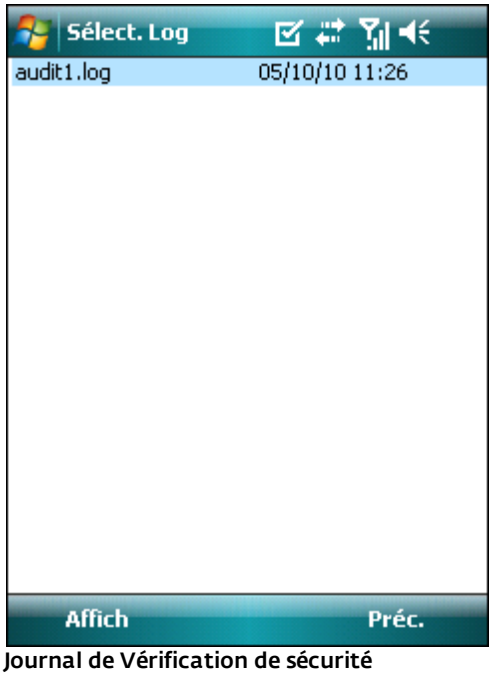
- le nom du fichier journal (généralement sous la forme *Analyse.Numéro.log*) ;
- la date et heure de l'événement ;
- la liste des fichiers analysés ;
- les actions exécutées ou les erreurs rencontrées lors de l'analyse.

Journal d'analyse

La section du journal de **Vérification de sécurité** (**Menu > Logs > Vérification de sécurité**) stocke tous les résultats de la vérification de sécurité des vérifications automatiques (planifiées) et déclenchées manuellement.

Les journaux de **Vérification de sécurité** contiennent les informations suivantes :

- le nom du fichier journal (sous la forme *vérificationNuméro.log*) ;
- la date et l'heure de la vérification ;
- les résultats détaillés.

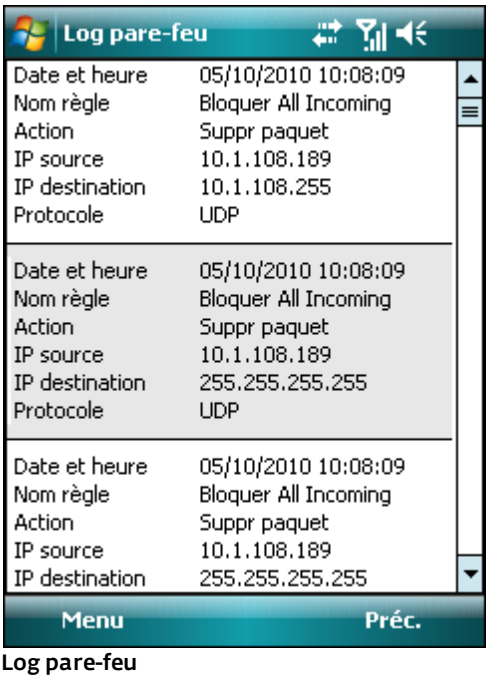


Journal de Vérification de sécurité

Le **Log pare-feu** (**Menu > Logs > Pare-feu**) contient des informations sur les événements relatifs au pare-feu et qui sont bloqués par ESET Mobile Security. Le journal est mis à jour après chaque communication qui passe par le pare-feu. Les nouveaux éléments apparaissent dans la partie supérieure du journal.

Le **Log pare-feu** contient les éléments suivants :

- la date et heure de l'événement ;
- le nom de la règle utilisée ;
- l'action réalisée (en fonction des paramètres de la règle) ;
- l'adresse IP source ;
- l'adresse IP de destination ;
- le protocole utilisé.



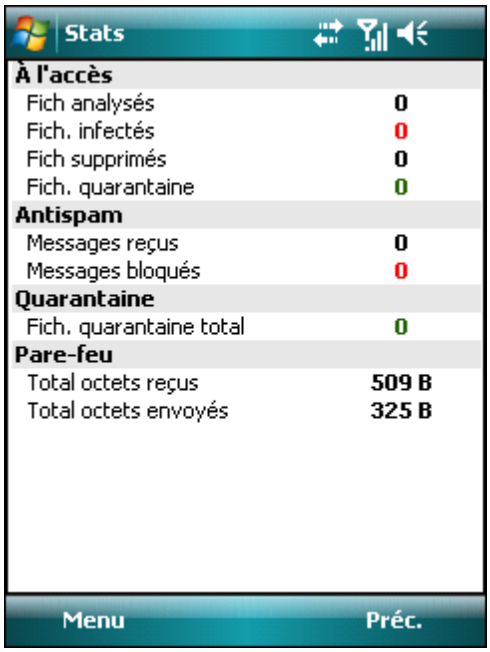
Log pare-feu

L'écran **Stats** (**Menu > Affich > Stats**) récapitule les éléments suivants :

- les fichiers analysés par l'analyse à l'accès ;
- les messages reçus et bloqués ;
- les fichiers en quarantaine ;
- les données envoyées et reçues et qui traversent le pare-feu.

Si vous souhaitez réinitialiser les statistiques, touchez les options **Menu > Réinit. Compteur**.

REMARQUE : toutes les données statistiques sont recalculées à partir du dernier redémarrage de l'appareil.

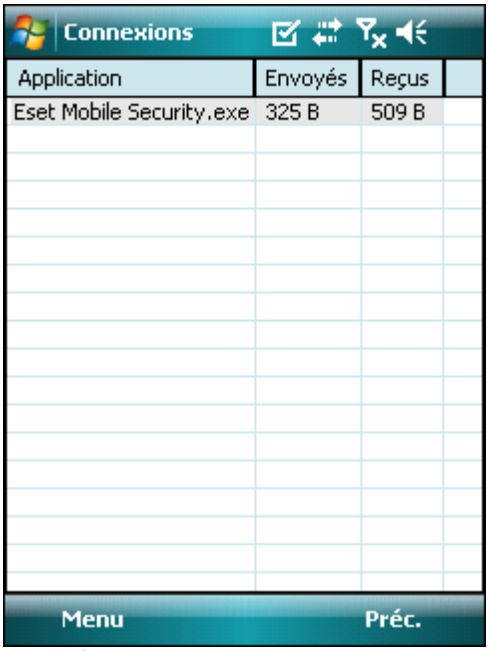


Stats

La section **Connexions** (**Menu > Affich > Connexions**) affiche les applications utilisées pour l'envoi et la réception des données.

Les informations sont les suivantes :

- nom du processus ;
- quantité de données envoyées ;
- quantité de données reçues.



Connexions

12. Résolution des problèmes et assistance

12.1 Résolution des problèmes

Cette section fournit des solutions aux questions communes concernant ESET Mobile Security.

12.1.1 Échec de l'installation

L'affichage de ce message d'erreur pendant l'installation s'explique généralement par le fait que la version d'ESET Mobile Security installée sur votre appareil n'est pas la version correcte. Lorsque vous téléchargez le fichier d'installation depuis le *site Internet d'ESET*, veillez à bien télécharger la version du produit correspondant à votre appareil.

12.1.2 Échec de la connexion au serveur de mise à jour

Ce message d'erreur apparaît après l'échec d'une tentative de mise à jour si le programme n'est pas en mesure de contacter les serveurs de mise à jour.

Essayez les opérations suivantes :

1. Vérifiez que vous êtes bien connecté à Internet : ouvrez votre navigateur Internet et accédez au site *http://www.eset.com*.
2. Vérifiez que le programme utilise le serveur de mise à jour correct. Touchez les options **Menu > Param. > MAJ** : les informations *updmobile.eset.com* doivent figurer dans le champ **MAJ serveur**.

12.1.3 Expiration téléch. fichier

La connexion Internet a été ralentie ou interrompue de façon inattendue pendant la mise à jour. Essayez de relancer la mise à jour ultérieurement.

12.1.4 Fich. de MAJ manquant

Si vous essayez d'installer une nouvelle base des signatures de virus depuis le fichier mis à jour (*esetav_wm.upd*), le fichier doit être stocké dans le dossier d'installation d'ESET Mobile Security (*Program Files\ESET\ESET Mobile Security*).

12.1.5 Fichier BdD endommagé

Le fichier mis à jour de la base des signatures de virus (*esetav_wm.upd*) est endommagé. Vous devez remplacer le fichier et exécuter de nouveau la mise à jour.

12.2 Assistance technique

Pour toute assistance administrative ou technique concernant ESET Mobile Security ou tout autre produit de sécurité ESET, notre service client est disponible pour vous aider. Pour trouver une solution à votre problème concernant l'assistance technique, vous pouvez choisir parmi les options suivantes :

Pour trouver des réponses aux questions les plus fréquentes, accédez à la base de connaissances ESET : *http://kb.eset.com*

La base de connaissances contient un grand nombre d'informations utiles pour résoudre les problèmes les plus courants. Elle est organisée en catégories et propose une fonction de recherche avancée.

Pour contacter le service client ESET, utilisez le formulaire de demande d'assistance disponible à cette adresse : *http://eset.com/support/contact.php*