ESET ENDPOINT SECURITY pour ANDROID

Guide de l'utilisateur

(versions 2.0 et ultérieures)

Cliquez ici pour télécharger la dernière version de ce document.

ESET **ENDPOINT SECURITY**

Service client : www.eset.com/support

RÉV. 28. 8. 2015

Sommaire

1. Introduction

La nouvelle version d'ESET Endpoint Security pour Android (EESA) est conçue pour fonctionner avec ESET Remote Administrator (ERA) 6, la nouvelle console de gestion qui permet l'administration à distance de toutes les solutions de sécurité ESET. ESET Endpoint Security pour Android 2 est uniquement compatible avec ERA 6 et ultérieur.

ESET Endpoint Security pour Android est conçu pour protéger les appareils mobiles de l'entreprise contre les dernières menaces et sécuriser les données même en cas de perte ou de vol de l'appareil. Il permet également à l'administrateur d'assurer la conformité des équipements avec les stratégies de sécurité en place.

ESET Endpoint Security peut également être utilisé dans des PME sans nécessiter de gestion à distance via ESET Remote Administrator. Le technicien IT, l'administrateur système ou l'utilisateur d'Endpoint peut simplement partager sa configuration de ESET Endpoint Security avec ses collègues. Ainsi, il n'est presque plus nécessaire d'activer le produit ou d'effectuer une configuration manuelle pour chaque module, ce qui est sinon indispensable juste après l'installation d'ESET Endpoint Security.

1.1 Nouveautés de la version 2

Contrôle d'application

Le Contrôle d'application permet aux administrateurs de surveiller les applications installées, de bloquer l'accès à certaines applications et de réduire les risques en demandant aux utilisateurs de désinstaller certaines applications. Reportez-vous à la section Contrôle d'application pour en savoir plus.

Sécurité du périphérique

Cette fonction permet aux administrateurs d'exécuter des stratégies élémentaires de sécurité sur plusieurs appareils mobiles. Ils peuvent par exemple :

- Définir la complexité et le niveau de sécurité minimum des codes de verrouillage de l'écran
- Définir le nombre maximum d'échecs lors du déverrouillage
- Indiquer au bout de combien de temps les utilisateurs doivent changer leur code de verrouillage de l'écran
- Définir le minuteur pour le verrouillage
- Limiter l'utilisation de la caméra

Reportez-vous à la section Sécurité du périphérique pour en savoir plus.

Importer et exporter les paramètres

Pour transmettre facilement les paramètres d'un appareil mobile à un autre si ceux-ci ne sont pas gérés par ERA, ESET Endpoint Security 2 propose désormais une option pour les exporter et les importer. L'administrateur peut exporter manuellement les paramètres de l'appareil dans un fichier qui peut ensuite être partagé (par e-mail par exemple) et importé sur n'importe quel appareil exécutant l'application cliente. Lorsque l'utilisateur accepte le fichier de paramètres qu'il a reçu, cela définit automatiquement tous les paramètres et active l'application (si les informations sur la licence ont été incluses). Tous ces paramètres sont protégés par le mot de passe administrateur.

Antihameçonnage

Cette fonction empêche les utilisateurs d'accéder à des sites Web malveillants s'ils utilisent les navigateurs pris en charge (navigateur Android par défaut et Chrome).

La technologie de l'Anti-Phishing prévient les tentatives de récupération des mots de passe, des données bancaires ou de toute autre information sensible par des sites Web illégaux qui se font passer pour des sites dignes de confiance. Lorsqu'un appareil tente d'accéder à une URL, la fonction Anti-Phishing effectue une comparaison avec la base de données ESET des sites d'hameçonnage connus. Si elle y trouve cette adresse, la connexion à l'URL est suspendue et un message d'avertissement s'affiche.

Centre de notification

ESET Endpoint Security fournit aux utilisateurs un centre de notification centralisé où ils peuvent trouver toutes les notifications relatives aux fonctions de l'application qui requièrent leur attention. Ce centre de notification donne des informations sur différents événements, indique pour quelles raisons ils ne sont pas conformes aux stratégies de l'entreprise et explique comment y remédier. Les notifications sont classées par priorité, les plus importantes figurant en haut de la liste.

Nouveau système de licences

ESET Endpoint Security prend totalement en charge ESET License Administrator, le nouveau modèle de licences d'ESET Remote Administrator 6.

Cette nouvelle structure simplifie le déploiement et l'utilisation à long terme du logiciel de sécurité ESET. Lorsque le client demande une modification de sa licence, ce changement est reporté automatiquement et en toute transparence dans tous les produits concernés. Ainsi, le client peut utiliser son adresse e-mail et un mot de passe personnalisé pour s'identifier, au lieu du mot de passe et du nom d'utilisateur créés par ESET comme c'était le cas dans les anciens produits.

L'apparition des clés de licence et des mises à jour automatiques (lors du renouvellement ou d'une autre opération sur la licence) est un gage de sécurité pour le client. Le portail ESET License Administrator et la possibilité d'attribuer des droits de licence par adresse e-mail (selon les informations des comptes des clients) simplifient la gestion et le déploiement des licences. Avec ESET License Administrator, les titulaires des licences peuvent en déléguer la gestion à un autre responsable (même à un tiers, sans perdre le contrôle sur la licence).

Mise à jour gérée d'un produit vers une build plus récente

Les administrateurs système qui utilisent ERA et ne souhaitent pas mettre à jour ESET Endpoint Security pour Android pour avoir la dernière version dès qu'elle est disponible ont la possibilité de paramétrer les mises à jour.

Assistants de configuration

ESET Endpoint Security propose des assistants de configuration, à utiliser après l'installation, pour certaines fonctions. Cela simplifie la procédure.

Antivirus plus performant

- Optimisation des durées d'analyse en temps réel (lors des accès)
- Système ESET Live Grid intégré
- 2 niveaux d'analyse, intelligente et approfondie
- Options supplémentaires pour l'analyse à la demande : en arrière-plan et pause
- Analyse planifiée : l'administrateur peut planifier une analyse complète du périphérique
- Analyse sur chargeur : l'analyse démarre automatiquement lorsque l'appareil est en veille, entièrement chargé et branché sur un chargeur.
- Meilleure configuration des mises à jour de la base de données des virus : l'administrateur peut planifier les mises à jour périodiques et sélectionner le serveur de mise à jour que l'appareil doit user (version, préversion, miroir local)

Des journaux détaillés contenant les résultats des analyses sont envoyés à ERA. ESET Endpoint Security reprend des fonctions de ESET Endpoint Security version 1, notamment la détection des applications potentiellement dangereuses, la détection des applications potentiellement indésirables et USSD Control.

Amélioration du filtre de SMS et d'appels

Le filtre de SMS et des appels, anciennement l'antispam, met les utilisateurs à l'abri des appels, SMS et MMS indésirables. Cette fonction propose maintenant deux types de règles : celles de l'administrateur et celles de l'utilisateur, les premières ayant toujours la priorité.

Autres améliorations :

- Blocage en fonction de l'heure : l'utilisateur ou l'administrateur peut bloquer les appels et les messages pendant des périodes spécifiques
- Blocage instantané du dernier appelant ou expéditeur, d'un numéro de téléphone, d'un groupe de contacts, des numéros masqués ou inconnus

Amélioration de la fonction Antivol

Les administrateurs ont la possibilité de protéger et de localiser un appareil perdu ou volé. Les mesures antivol peuvent être déclenchées à partir d'ERA ou par le biais de commandes à distance.

ESET Endpoint Security 2 utilise les mêmes commandes à distance que la version 1 (Verrouiller, Effacer et Rechercher). Les commandes suivantes sont nouvelles :

- **Déverrouiller** : déverrouille l'appareil verrouillé
- **Réinitialisation améliorée des paramètres d'usine** : toutes les données accessibles sur le périphérique sont rapidement supprimées (les en-têtes des fichiers sont détruits) et les paramètres d'usine par défaut sont rétablis
- **Sirène** : l'appareil perdu est verrouillé et émet un son très fort, même si le son a été coupé

Pour renforcer la sécurité des commandes à distance, l'administrateur reçoit un unique code SMS de vérification, valable pendant une durée limitée, sur son téléphone portable (au numéro indiqué dans la liste des contacts Administrateur) lorsqu'il exécute une commande à distance. Ce code de vérification sert à vérifier une commande particulière.

Commandes d'Antivol à partir d'ERA

Désormais, toutes les commandes d'Antivol peuvent également être exécutées à partir d'ERA. La nouvelle fonction de gestion des appareils mobiles permet à l'administrateur d'envoyer ces commandes en seulement quelques clics. Les tâches sont immédiatement envoyées pour être exécutées via le Connecteur de périphérique mobile, un composant qui fait maintenant partie de l'infrastructure ERA.

Contacts Administrateur

C'est la liste des numéros de téléphone des administrateurs. Ces numéros sont protégés par le mot de passe administrateur. Les commandes d'Antivol ne peuvent être envoyées que depuis des numéros fiables.

Affichage d'un message à partir d'ERA

Dans le cadre de la gestion des appareils à distance, l'administrateur peut envoyer un message personnalisé à un appareil particulier ou à un groupe d'appareils. Cela permet de transmettre un message urgent aux utilisateurs concernés. Le texte s'affiche dans une fenêtre contextuelle, aussi l'utilisateur le voit forcément.

Informations personnalisées sur l'écran verrouillé

L'administrateur a la possibilité de définir des informations personnalisées (nom de la société, adresse e-mail, message) qui s'afficheront sur l'appareil verrouillé et permettront d'appeler un des contacts Administrateur de la liste.

Amélioration de la gestion à distance avec ESET Remote Administrator **6**

Il est désormais possible de configurer et de définir tous les paramètres d'application via une stratégie à distance, de l'Antivirus aux restrictions du Contrôle d'application en passant par les paramètres du filtrage d'appels et de SMS et de la sécurité du périphérique. L'administrateur peut ainsi appliquer la stratégie de sécurité de l'entreprise sur tout le réseau, y compris les appareils mobiles.

ESET Endpoint Security pour Android version 2 propose des rapports nettement améliorés accessibles via la console Web ERA. L'administrateur peut alors identifier rapidement les appareils suspects et trouver l'origine du problème.

La gestion des appareils Android est maintenant un composant à part entière d'ESET Remote Administrator 6, dont presque toutes les fonctions sont disponibles dans les produits bureautiques d'ESET tels qu'ESET Endpoint Antivirus 6 et ESET Endpoint Security 6.

Administration locale

ESET Endpoint Security pour Android propose aux administrateurs une option pour configurer et gérer les terminaux en local s'ils ne souhaitent pas utiliser ESET Remote Administrator. Tous les paramètres de l'application sont protégés par le mot de passe administrateur, aussi l'application reste entièrement et en permanence sous contrôle.

Optimisation de la distribution et de l'installation du produit

Outre les méthodes traditionnelles (télécharger et installer un package à partir du site Web ESET, distribuer le package d'installation par e-mail), les administrateurs et les utilisateurs ont la possibilité de télécharger et d'installer l'application depuis la boutique Google Play.

Amélioration de la procédure d'activation du produit

Après le téléchargement et l'installation, l'administrateur ou l'utilisateur a plusieurs options pour activer le produit :

- Il peut utiliser le nouveau système de licences et fournir manuellement la clé de licence ou le compte de l'administrateur de la sécurité.
- Il peut cliquer sur le lien que l'administrateur a envoyé par e-mail. Le produit configure automatiquement la connexion à ERA et les informations sur la licence sont transmises (méthode push) à l'appareil depuis ERA.
- L'administrateur peut fournir manuellement les informations de connexion ERA.
- L'importation du fichier contenant les paramètres de l'application (avec les informations sur la licence) aura pour effet d'activer l'application.

Meilleure identification de l'appareil mobile dans ERA

Lors de l'inscription, les appareils Android sont placés dans la liste blanche. Ainsi, seuls les appareils admis peuvent se connecter à ERA. Cela améliore la sécurité et simplifie l'identification de chaque appareil, puisqu'ils sont tous identifiés par leurs nom, description et numéro IMEI. Les appareils exclusivement WiFi sont identifiés par leur adresse MAC WiFi.

Refonte de l'interface utilisateur graphique

ESET Endpoint Security offre une meilleure expérience utilisateur, similaire à celle que l'on retrouve dans toutes les solutions ESET pour les professionnels.

Simplicité d'utilisation

Grâce à la nouvelle interface, le produit est plus facile à utiliser. La structure de la GUI est alignée sur la nouvelle génération de solutions ESET Endpoint et ESET Remote Administrator.

1.2 Configuration système minimale requise

Pour installer ESET Endpoint Security, assurez-vous que votre appareil Android correspond à la configuration minimale :

- Système d'exploitation : Android 4 (Ice Cream Sandwich) et versions ultérieures
- Résolution de l'écran tactile : 480 x 800 px
- CPU : ARM avec le jeu d'instructions ARMv7, x86 Intel Atom
- Espace de stockage disponible : 20 Mo
- Connexion Internet

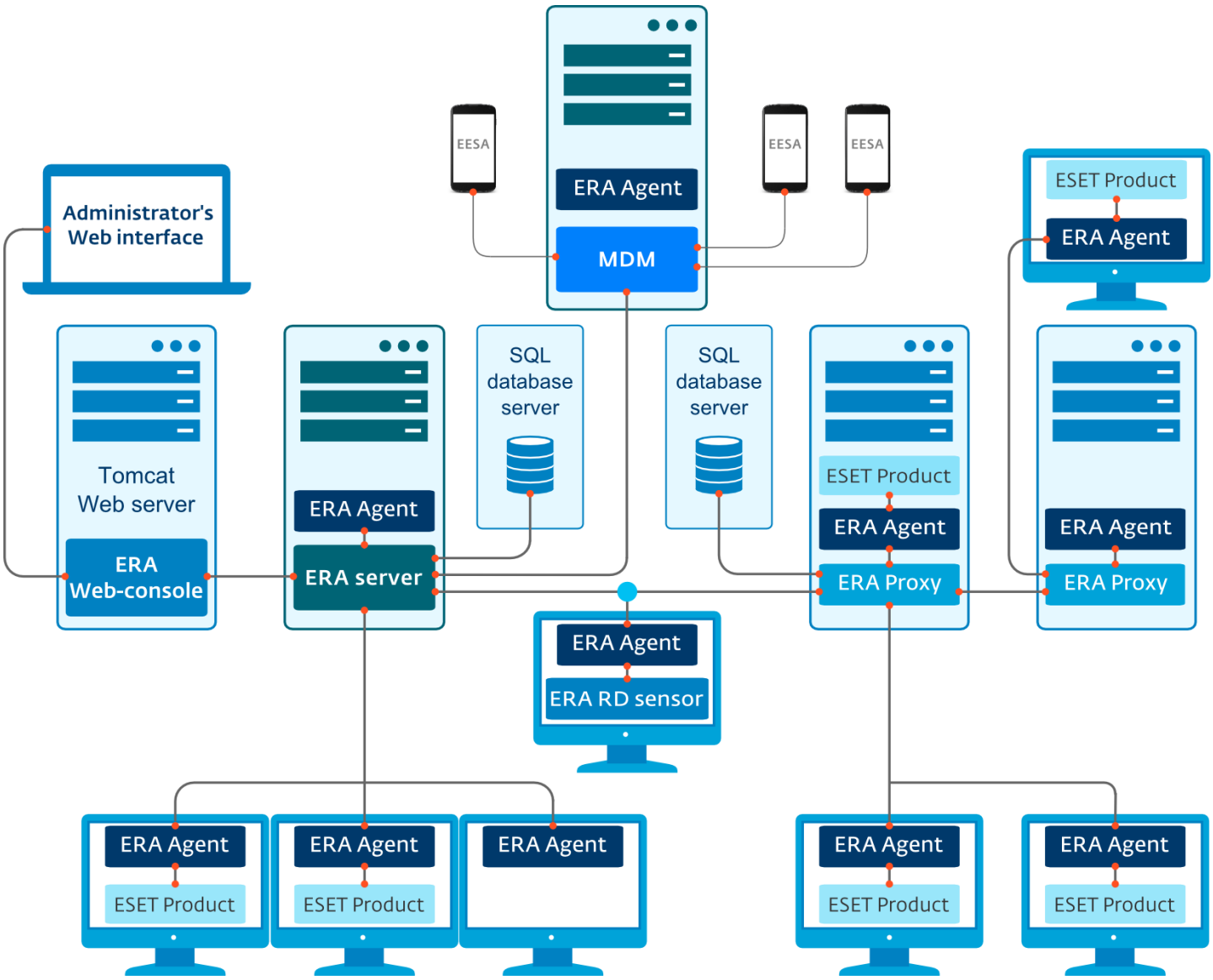
REMARQUE : les doubles SIM et le rootage ne sont pas pris en charge. Certaines fonctions (comme Antivol et le filtrage des SMS et des appels) ne sont pas disponibles sur les tablettes qui ne gèrent pas les appels et les messages.

2. Utilisateurs se connectant à ESET Remote Administrator

ESET Remote Administrator (ERA) 6 est une application qui permet de gérer les produits ESET de manière centralisée dans un environnement réseau. Le système de gestion des tâches ESET Remote Administrator donne la possibilité d'installer les solutions de sécurité ESET sur des ordinateurs distants et de réagir rapidement aux nouveaux problèmes et menaces. ESET Remote Administrator n'offre pas directement de protection contre les codes malveillants ; il s'appuie sur la solution de sécurité ESET installée sur chaque client.

Les solutions de sécurité ESET prennent en charge les réseaux qui comprennent plusieurs types de plateformes. Votre réseau peut comprendre une combinaison de systèmes d'exploitation Microsoft, Linux et OS X et de systèmes d'exploitation qui s'exécutent sur des appareils mobiles (téléphones mobiles et tablettes).

L'illustration suivante montre un exemple d'architecture pour un réseau protégé par les solutions de sécurité ESET gérées par ERA :



REMARQUE : pour plus d'informations, reportez-vous à la documentation en ligne d'ESET Remote Administrator.

2.1 ESET Remote Administrator Server

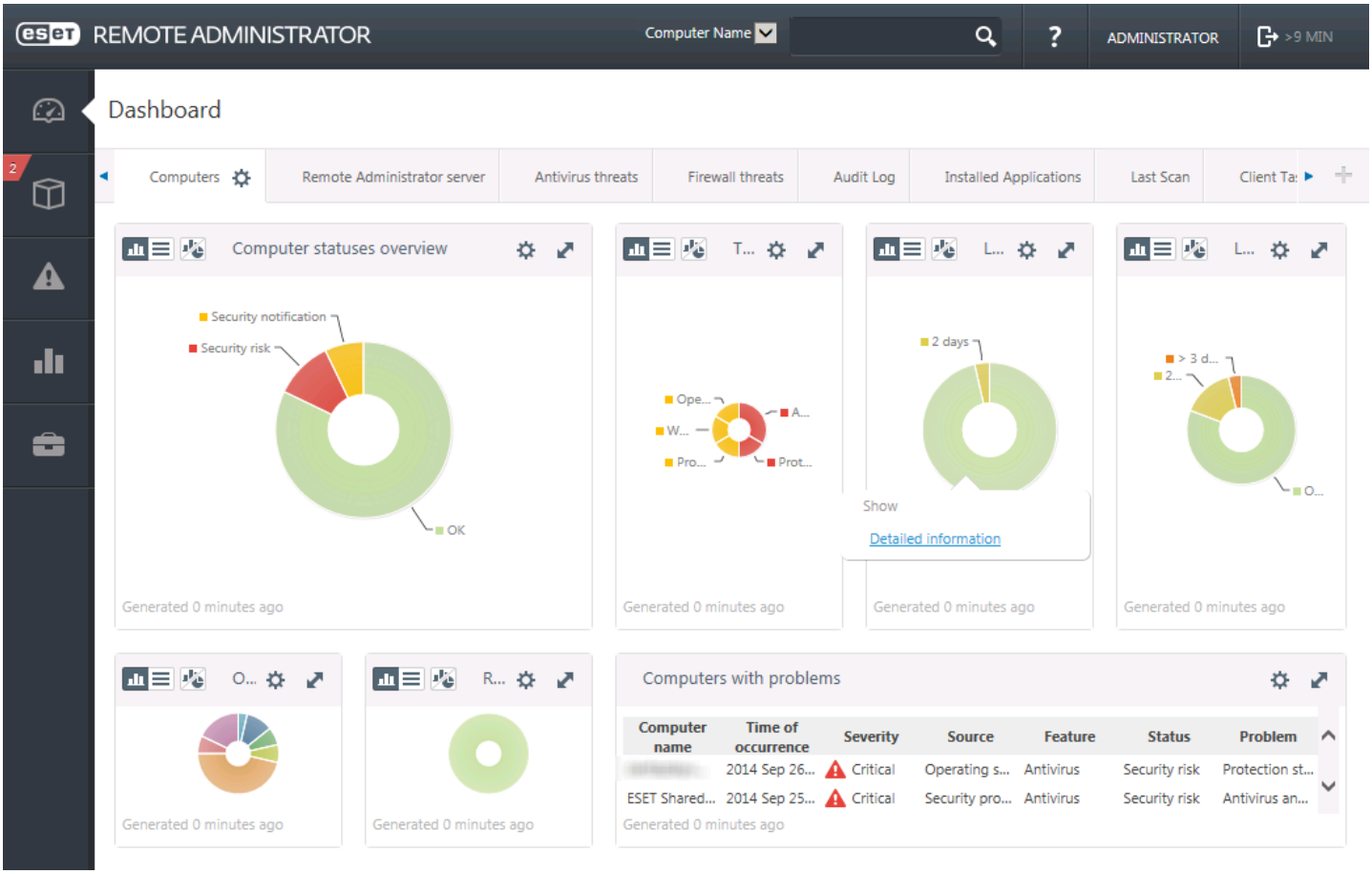
ESET Remote Administrator Server est le composant principal d'ESET Remote Administrator. Il traite toutes les données reçues des clients qui se connectent au serveur (par le biais de l'Agent ERA). L'Agent ERA facilite la communication entre le client et le serveur. Les données (journaux des clients, configuration, réplication de l'agent, etc.) sont stockées dans une base de données à laquelle ERA accède pour ses rapports.

Pour traiter correctement les données, le serveur ERA a besoin d'une connexion stable avec un serveur de bases de données. Pour optimiser les performances, nous vous conseillons d'installer le serveur ERA et la base de données sur des serveurs distincts. L'ordinateur sur lequel le serveur ERA est installé doit être configuré pour accepter toutes les connexions des agents/proxys/capteurs RD qui sont vérifiées à l'aide de certificats. Après avoir installé le serveur ERA, vous pouvez ouvrir la console Web ERA. Celle-ci permet de gérer les postes de travail sur lesquels des solutions ESET sont installées.

2.2 Console Web

La **console Web ERA** est une interface utilisateur Web qui présente les données d'ERA Server et vous permet de gérer les solutions de sécurité ESET sur votre réseau. Cette console Web est accessible via un navigateur. Elle affiche une vue d'ensemble de l'état des clients sur le réseau et peut être utilisée pour déployer à distance les solutions ESET sur des ordinateurs non gérés. Vous pouvez décider de rendre le serveur Web accessible à partir d'Internet pour permettre l'utilisation d'ESET Remote Administrator depuis presque n'importe quel emplacement ou appareil.

Le tableau de bord de la console Web :



L'outil **Recherche rapide** figure dans la partie supérieure de la console Web. Dans le menu déroulant, sélectionnez **Nom de l'ordinateur**, **Adresse IPv4/IPv6** ou **Nom de la menace**, tapez votre chaîne de recherche dans le champ de texte, puis cliquez sur le symbole de la loupe ou appuyez sur **Entrée** pour lancer la recherche. Vous êtes alors redirigé vers la section **Groupes** dans laquelle le résultat de votre recherche est affiché.

2.3 Proxy

Le **proxy ERA** est un autre composant d'ESET Remote Administrator qui a un double objectif. Dans le cas d'un réseau d'entreprise ou de PME qui comprend de nombreux clients (10 000 ou plus), cette fonction peut servir à répartir la charge entre plusieurs proxys ERA et soulager ainsi le serveur ERA. L'autre avantage du proxy ERA, c'est que vous pouvez l'utiliser dans le cadre d'une connexion de qualité médiocre à une filiale distante. Dans ce cas, l'Agent ERA de chaque client ne se connecte pas directement au serveur ERA. Il passe par le proxy ERA, qui se trouve sur le même réseau local que la filiale. Cette configuration permet de soulager la liaison avec la filiale. Le proxy ERA accepte les connexions en provenance de tous les Agents ERA locaux, compile leurs données et les envoie sur le serveur ERA (ou un autre proxy ERA). Votre réseau peut ainsi prendre en charge davantage de clients sans subir de dégradation de ses performances ni de celles des requêtes de base de données.

Selon votre configuration réseau, le proxy ERA peut se connecter à un autre proxy ERA, puis au serveur ERA.

Pour que le proxy ERA fonctionne correctement, l'ordinateur hôte sur lequel vous l'avez installé doit disposer d'un Agent ESET et être connecté au niveau supérieur (serveur ERA ou proxy ERA situé plus haut dans la hiérarchie, le cas échéant) du réseau.

2.4 Agent

ERA Agent est un composant essentiel du produit ESET Remote Administrator. Les solutions de sécurité ESET (ESET Endpoint Security, par exemple) sur les ordinateurs clients communiquent avec ERA Server par le biais de l'Agent. Ces communications permettent de centraliser la gestion des solutions de sécurité ESET installées sur tous les clients distants. L'Agent collecte les informations sur le client et les envoie au serveur. Lorsque le serveur envoie une tâche au client, celle-ci passe par l'Agent qui communique ensuite avec le client. Toutes les communications réseau ont lieu entre l'Agent et la partie supérieure du réseau ERA, à savoir le serveur et le proxy.

L'Agent ESET utilise l'une des trois méthodes suivantes pour se connecter au serveur :

1. L'Agent du client se connecte directement au serveur.
2. L'Agent du client se connecte par le biais d'un proxy lui-même connecté au serveur.
3. L'Agent du client se connecte au serveur par le biais de plusieurs proxys.

L'Agent ERA communique avec les solutions ESET installées sur un client, collecte les informations à partir des programmes de ce client et transmet au client les données de configuration reçues du serveur.

REMARQUE : le proxy ESET possède son propre Agent qui gère toutes les tâches de communication entre les clients, les autres proxys et le serveur ERA.

2.5 Capteur RD

Le **capteur RD (Rogue Detection)** est un composant d'ESET Remote Administrator conçu pour chercher des ordinateurs sur votre réseau. Il permet d'ajouter facilement de nouveaux ordinateurs à ESET Remote Administrator sans avoir à les rechercher et les ajouter manuellement. Chaque ordinateur trouvé sur le réseau est affiché dans la console Web et ajouté au groupe Tous par défaut. À ce stade, vous pouvez effectuer d'autres actions sur chaque ordinateur client.

Le capteur RD est un dispositif d'écoute passive qui détecte les ordinateurs présents sur le réseau et envoie des informations sur ces derniers au serveur ERA. Ce serveur ERA évalue ensuite si les ordinateurs détectés sur le réseau sont inconnus ou déjà gérés.

3. Installation à distance

L'installation à distance d'ESET Endpoint Security à partir d'ERA nécessite :

- L'installation du Connecteur de périphérique mobile
- L'inscription des périphériques mobiles

L'installation d'ESET Endpoint Security peut s'effectuer de deux manières :

1. L'administrateur envoie le lien pour l'inscription aux utilisateurs finaux par e-mail, avec le fichier APK d'installation et quelques instructions. Ce lien ouvre le navigateur Internet par défaut de leur Android et ESET Endpoint Security est inscrit et connecté à ERA. Si ESET Endpoint Security n'est pas installé sur l'appareil, l'utilisateur est automatiquement redirigé vers la boutique Google Play pour télécharger l'application. Ensuite, l'installation standard a lieu.
2. L'administrateur envoie le fichier des paramètres de l'application aux utilisateurs finaux par e-mail, avec le fichier APK d'installation et quelques instructions. Il peut aussi les inviter à télécharger le fichier APK depuis la boutique Google Play en leur fournissant le lien. Après l'installation, les utilisateurs ouvrent le fichier des paramètres de l'application. Tous ces paramètres sont importés et l'application est activée (du moins si les informations sur la licence sont incluses).

4. Installation en local sur l'appareil

ESET Endpoint Security propose aux administrateurs une option pour configurer et gérer Endpoint en local s'ils ne souhaitent pas utiliser ESET Remote Administrator. Tous les paramètres de l'application sont protégés par le mot de passe administrateur, aussi l'application reste entièrement et en permanence sous contrôle.

Si l'administrateur d'une petite entreprise décide de ne pas utiliser ESET Remote Administrator mais qu'il souhaite malgré tout protéger les équipements et appliquer des stratégies élémentaires de sécurité, il dispose de deux méthodes pour gérer les appareils en local :

1. Il peut accéder physiquement à chaque appareil de l'entreprise et configurer manuellement les paramètres.
2. Il peut préparer la configuration souhaitée sur son appareil Android (où ESET Endpoint Security est installé) et exporter ces paramètres dans un fichier. Reportez-vous à la section Importer/exporter les paramètres pour en savoir plus). Il lui suffit ensuite de communiquer ce fichier exporté aux utilisateurs (par e-mail par exemple), et ceux-ci l'importeront sur tout appareil exécutant ESET Endpoint Security. Lorsque l'utilisateur ouvre et accepte le fichier de paramètres qu'il a reçu, il importe automatiquement tous les paramètres et active l'application (si les informations sur la licence sont incluses). Tous les paramètres sont protégés par le mot de passe administrateur.

4.1 Télécharger depuis le site Web d'ESET

Téléchargez ESET Endpoint Security en scannant le code QR ci-dessous avec votre appareil mobile si vous disposez de l'application prévue à cet effet :

Vous pouvez aussi télécharger le fichier APK d'installation d'ESET Endpoint Security à partir du site Web d'ESET :

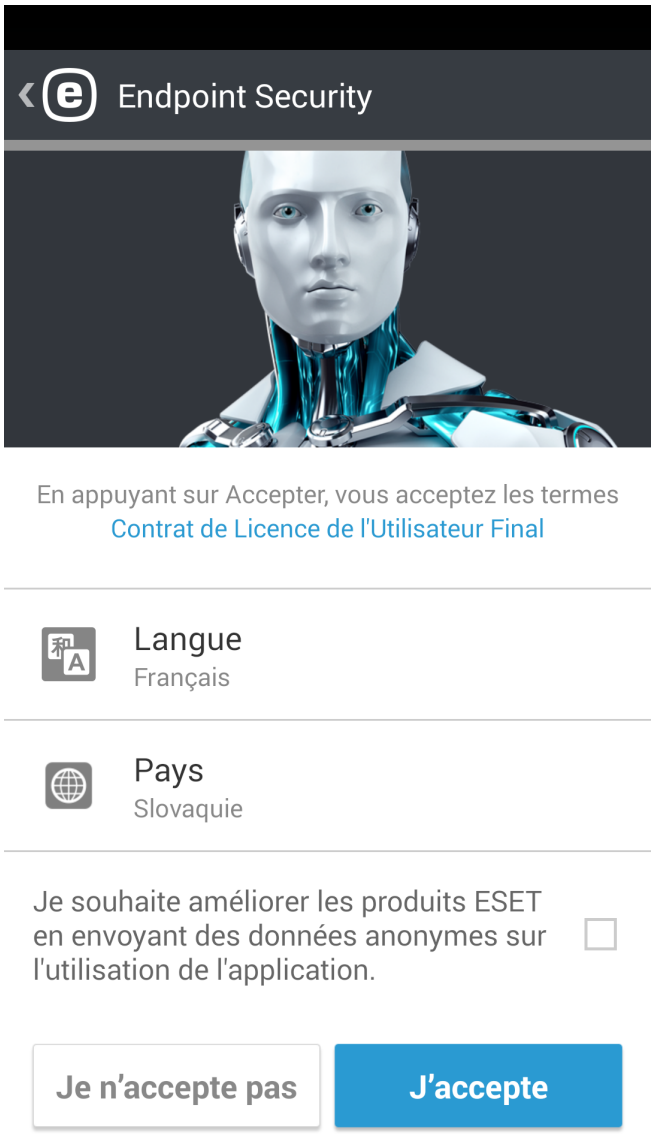
1. Téléchargez le fichier d'installation depuis le site Web d'ESET.
2. Ouvrez le fichier à partir de la zone de notification de l'Android ou cherchez-le à l'aide d'une application d'exploration des fichiers. Ce fichier est généralement enregistré dans le dossier des téléchargements.
3. Assurez-vous que les applications provenant de sources inconnues sont autorisées sur votre appareil. Pour cela, appuyez sur l'icône du lanceur d'applications de l'écran d'accueil de l'Android ou sélectionnez **Accueil** > **Menu**. Appuyez sur **Paramètres** > **Sécurité**. L'option **Sources inconnues** doit autoriser ces sources.
4. Après avoir ouvert le fichier, appuyez sur **Installer**.

4.2 Télécharger depuis Google Play

Ouvrez l'application de la boutique Google Play Store sur votre Android et recherchez ESET Endpoint Security (ou simplement ESET).

Vous pouvez aussi télécharger ce logiciel en scannant le code QR ci-dessous avec votre appareil mobile si vous disposez de l'application prévue à cet effet :

4.3 Assistant Démarrage



Une fois l'application installée, appuyez sur **Configuration de l'administrateur** et suivez les instructions de l'assistant Démarrage. Cette procédure doit être effectuée exclusivement par un administrateur :

1. Sélectionnez la **Langue** à utiliser dans ESET Endpoint Security.
2. Sélectionnez le **Pays** dans lequel vous travaillez ou résidez.
3. Si vous souhaitez nous aider à améliorer les produits ESET en envoyant des données anonymes sur l'utilisation de l'application, sélectionnez l'option prévue à cet effet.
4. Appuyez sur **J'accepte**. Vous indiquez alors que vous acceptez le Contrat de licence de l'utilisateur final.
5. Indiquez si vous souhaitez connecter ESET Endpoint Security à ESET Remote Administrator ou effectuer une configuration manuelle. Si vous optez pour la deuxième option, vous devez créer un mot de passe administrateur et activer la protection contre les désinstallations.
6. À l'étape suivante, indiquez si vous souhaitez participer à ESET Live Grid. Pour en savoir plus sur ESET Live Grid, cliquez ici.
7. Indiquez si vous souhaitez qu'ESET Endpoint Security détecte les applications potentiellement indésirables. Cliquez ici pour en savoir plus sur ces applications.
8. Activez le produit.

5. Désinstallation

ESET Endpoint Security peut être désinstallé à l'aide de l'Assistant de désinstallation proposé dans le menu principal, sous **Paramètres** > **Désinstaller**. Si la protection contre la désinstallation est activée, vous êtes invité à fournir le mot de passe administrateur.

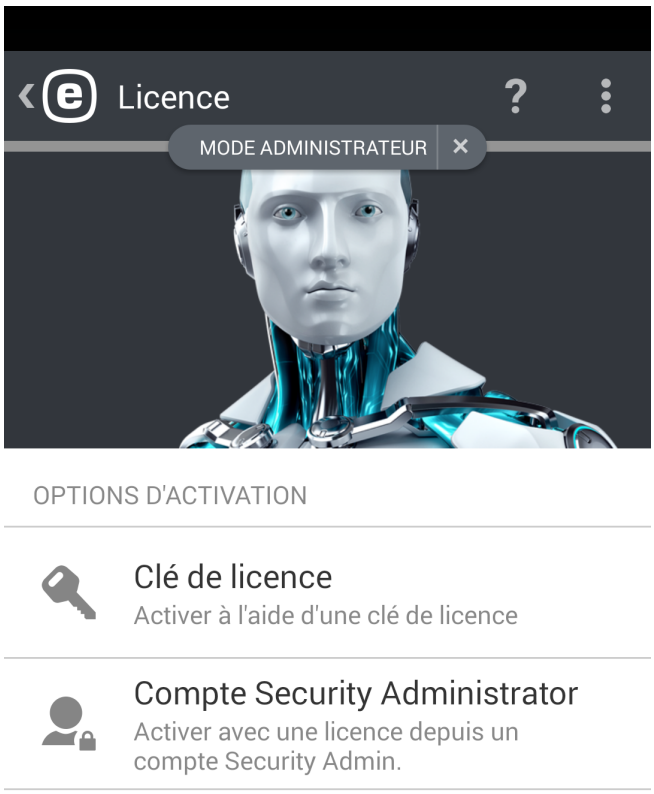
Vous pouvez aussi désinstaller le produit manuellement :

1. Appuyez sur l'icône du Lanceur dans l'écran d'accueil Android (ou sélectionnez **Accueil** > **Menu**) et appuyez sur **Paramètres** > **Sécurité** > **Administrateurs de l'appareil**. Désactivez ESET Endpoint Security en appuyant sur **Désactiver**. Appuyez sur **Déverrouiller** et fournissez le mot de passe administrateur. Si vous n'avez pas encore défini ESET Endpoint Security comme étant l'administrateur de l'appareil, ignorez cette étape.
2. Revenez au menu **Paramètres** et appuyez sur **Gérer les applications** > ESET Endpoint Security > **Désinstaller**.

6. Activation du produit

Il y a plusieurs manières d'activer ESET Endpoint Security. Les méthodes disponibles peuvent varier en fonction du pays, ainsi que les moyens de distribution (pages Web ESET, etc.) de votre produit.

Pour activer ESET Endpoint Security directement sur l'appareil Android, appuyez sur l'icône **Menu** dans l'écran principal d'ESET Endpoint Security (ou appuyez sur le bouton **MENU** de l'appareil) et sélectionnez **Licence**.



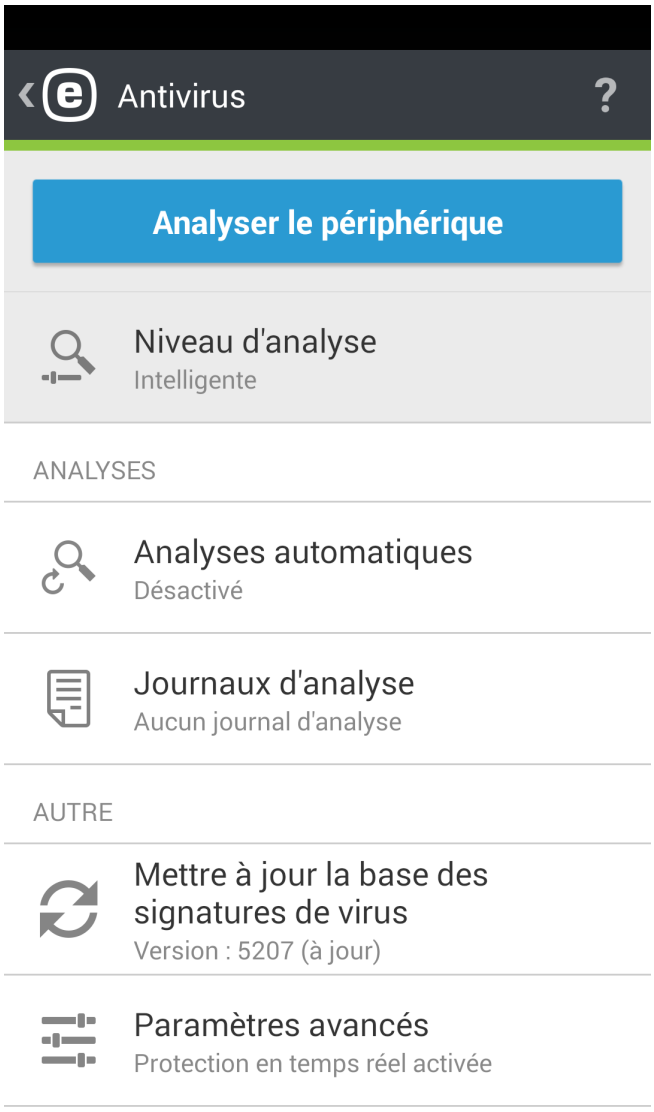
Pour activer ESET Endpoint Security, vous pouvez utiliser l'une des méthodes suivantes :

- **Clé de licence** : il s'agit d'une chaîne unique au format XXXX-XXXX-XXXX-XXXX-XXXX. Elle permet d'identifier le titulaire de la licence et d'activer celle-ci.
- **Compte d'administrateur de la sécurité** : compte créé sur le portail ESET License Administrator avec les informations d'identification (adresse e-mail et mot de passe). Cette méthode permet de gérer plusieurs licences à partir d'un même emplacement.

REMARQUE : ESET Remote Administrator peut activer des périphériques clients de manière transparente en utilisant les licences fournies par l'administrateur.

7. Antivirus

Le module Antivirus protège votre appareil contre les codes malveillants en bloquant les menaces, puis en les éradiquant ou en les mettant en quarantaine.



Analyser le périphérique

Cette commande peut être utilisée pour vérifier si votre appareil a été victime d'une intrusion.

Certains types de fichiers prédéfinis sont analysés par défaut. Lors d'une analyse complète, la mémoire, les processus en cours et les bibliothèques de liens dynamiques associées, ainsi que les fichiers stockés en interne ou sur support amovible, sont vérifiés. Une brève synthèse de l'analyse est enregistrée dans un fichier journal qui est conservé avec les autres journaux d'analyse.

Pour interrompre une analyse en cours, appuyez sur l'icône .

Niveau d'analyse

Vous avez le choix entre 2 niveaux d'analyse :

- **Intelligente** : l'analyse intelligente examine les applications installées, les fichiers DEX (fichiers exécutables pour le système d'exploitation Android), les fichiers SO (bibliothèques) et les fichiers ZIP en allant jusqu'à 3 niveaux d'imbrication des archives et du contenu de la carte SD.
- **Approfondie** : tous les types de fichiers, quelle que soit leur extension, sont analysés dans la mémoire interne et sur la carte SD.

Analyses automatiques

En plus de l'analyse à la demande, ESET Endpoint Security propose aussi les analyses automatiques. Pour apprendre à utiliser l'analyse sur chargeur et l'analyse planifiée, lisez cette section.

Journaux d'analyse

La section Journaux d'analyse contient des données complètes, sous forme de fichiers journaux, sur les analyses effectuées. Reportez-vous à la section Fichiers journaux de l'antivirus pour en savoir plus.

Mettre à jour la base des signatures de virus

Par défaut, ESET Endpoint Security inclut une tâche de mise à jour pour garantir que le programme est mis à jour régulièrement. Pour effectuer manuellement la mise à jour, appuyez sur **Mettre à jour la base des signatures de virus**.

REMARQUE : pour éviter de consommer inutilement de la bande passante, les mises à jour sont mises à disposition quand une nouvelle menace apparaît. Ces mises à jour sont fournies gratuitement avec votre licence active. Toutefois, votre opérateur de téléphonie mobile peut vous facturer des frais de transfert de données.

Pour plus de détails sur les paramètres avancés de l'antivirus, reportez-vous à la section Paramètres avancés.

7.1 Analyses automatiques

Niveau d'analyse

Vous avez le choix entre 2 niveaux d'analyse. Ce paramètre est valable pour les deux types d'analyse, planifiée et sur chargeur :

- **Intelligente** : l'analyse intelligente examine les applications installées, les fichiers DEX (fichiers exécutables pour le système d'exploitation Android), les fichiers SO (bibliothèques) et les fichiers ZIP en allant jusqu'à 3 niveaux d'imbrication des archives et du contenu de la carte SD.
- **Approfondie** : quelle que soit leur extension, tous les fichiers stockés dans la mémoire interne et sur la carte SD sont analysés.

Analyse sur chargeur

Quand cette option est sélectionnée, l'analyse démarre automatiquement lorsque l'appareil est en veille, entièrement chargé et branché sur un chargeur.

Analyse planifiée

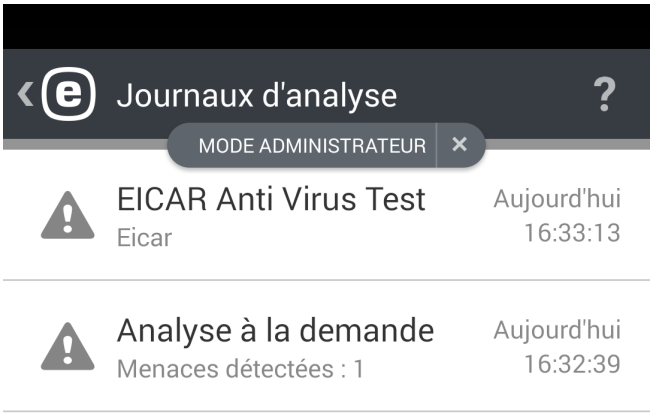
Cette option vous permet d'exécuter l'analyse de l'appareil automatiquement à une heure prédéfinie. Pour planifier une analyse, appuyez sur le bouton  à côté de l'option **Analyse planifiée** et spécifiez les dates et les heures de démarrage de l'analyse. Par défaut, elle a lieu tous les lundis à 4 heures du matin.

7.2 Journaux d'analyse

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

Chacun d'eux 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 pendant celle-ci



7.3 Paramètres avancés

Protection en temps réel

Cette option permet d'activer ou de désactiver l'analyse en temps réel qui démarre automatiquement en même temps que le système et analyse les fichiers avec lesquels vous interagissez. Le dossier des téléchargements, les fichiers d'installation APK et tous les fichiers de la carte SD une fois qu'elle est montée sont automatiquement analysés.

ESET Live Grid

Fondée sur le système d'avertissement anticipé avancé ThreatSense.net, la fonctionnalité ESET Live Grid est conçue pour offrir des niveaux de sécurité supplémentaires à votre appareil. Elle surveille en permanence les programmes et processus en cours d'exécution sur votre système en se basant sur les dernières informations collectées auprès des millions d'utilisateurs ESET à travers le monde. Les analyses gagnent en rapidité et en précision au fur et à mesure du développement de la base de données ESET Live Grid. Cela nous permet d'offrir à tous nos utilisateurs une meilleure protection proactive et des analyses plus rapides. Nous recommandons d'activer cette fonctionnalité. Merci pour votre soutien.

Détecter les applications potentiellement indésirables

Une application indésirable est un programme qui contient un logiciel publicitaire, installe des barres d'outils, piste les résultats de vos recherches ou dont les objectifs ne sont pas clairs. Dans certains cas, vous pouvez estimer que les avantages offerts par une application indésirable dépassent de loin les risques. Pour cette raison, ESET classe les applications de ce type dans une catégorie à faible risque par rapport aux autres types de logiciels malveillants.

Détecter les applications potentiellement dangereuses

Il existe de nombreuses applications authentiques qui permettent de simplifier l'administration des appareils en réseau. Toutefois, si elles tombent entre de mauvaises mains, elles sont susceptibles d'être utilisées à mauvais escient dans un but malveillant. L'option Détecter les applications potentiellement dangereuses vous permet de surveiller ces types d'applications et de les bloquer si vous le souhaitez. La classification *Applications potentiellement dangereuses* s'utilise pour des logiciels authentiques du commerce. Elle englobe des programmes tels que les outils d'accès à distance, les applications de décodage des mots de passe et les enregistreurs de frappe (keyloggers en anglais).

Bloquer les menaces non résolues

Ce paramètre détermine l'action à exécuter lorsque l'analyse est terminée et que des menaces ont été détectées. Si vous activez cette option, le fichier infecté ne sera pas exécutable.

Mises à jour de la base des signatures de virus

Cette option vous permet de définir l'intervalle entre les téléchargements automatiques des mises à jour de la base de données de menaces. Ces mises à jour sont publiées dès qu'une nouvelle menace est ajoutée à la base de données. Il est recommandé de conserver le paramètre par défaut (tous les jours).

Âge maximal personnalisé de la base de données

Par défaut, ESET Endpoint Security remplace la base des signatures de virus tous les 7 jours même si une mise à jour n'a pas été publiée.

Serveur de mise à jour

Cette option permet de mettre à jour votre appareil à partir du **serveur de préversion**. Ces mises à jour ont subi des tests internes poussés et seront disponibles très prochainement. Vous pouvez activer ces versions bêta afin d'accéder aux dernières méthodes de détection et aux derniers correctifs. Toutefois, ces mises à jour ne sont peut-être pas suffisamment stables pour être utilisées en permanence. La liste des modules actuels figure dans la section **À propos** : appuyez sur l'icône Menu  dans l'écran principal de ESET Endpoint Security, puis sur **À propos** > ESET Endpoint Security. Il est préférable que les utilisateurs non avertis laissent l'option **Serveur de version** sélectionnée par défaut.

ESET Endpoint Security permet de créer des copies des fichiers de mises à jour afin de les utiliser pour la mise à jour d'autres appareils du réseau. L'utilisation d'un **miroir local**, copie des fichiers de mise à jour dans l'environnement du réseau local, s'avère pratique puisque les fichiers de mise à jour doivent être téléchargés du serveur de mise à jour du fournisseur de manière répétée, pour tous les appareils mobiles. Vous trouverez dans ce document des informations détaillées sur la configuration d'un serveur miroir à l'aide des produits ESET Endpoint pour Windows.

8. Antivol

La fonction **Antivol** protège votre appareil mobile contre les accès non autorisés.

Si vous le perdez ou si quelqu'un le vole et remplace votre carte SIM par une autre (non fiable), ESET Endpoint Security le verrouille automatiquement et une alerte est envoyée par SMS aux numéros de téléphone que vous aviez définis. Ce message contient le numéro de téléphone de la carte SIM actuellement insérée, le numéro IMSI (International Mobile Subscriber Identity) et le numéro IMEI (International Mobile Equipment Identity) du téléphone. L'utilisateur non autorisé ne se rend pas compte de l'envoi de ce message, car celui-ci est automatiquement supprimé sur l'appareil. Vous pouvez également demander les coordonnées GPS de votre mobile égaré ou effacer à distance toutes les données qui sont stockées dessus.

REMARQUE : certaines options de la fonction Antivol (commandes SMS et cartes SIM approuvées) ne sont pas disponibles sur les tablettes qui ne prennent pas en charge les messages.

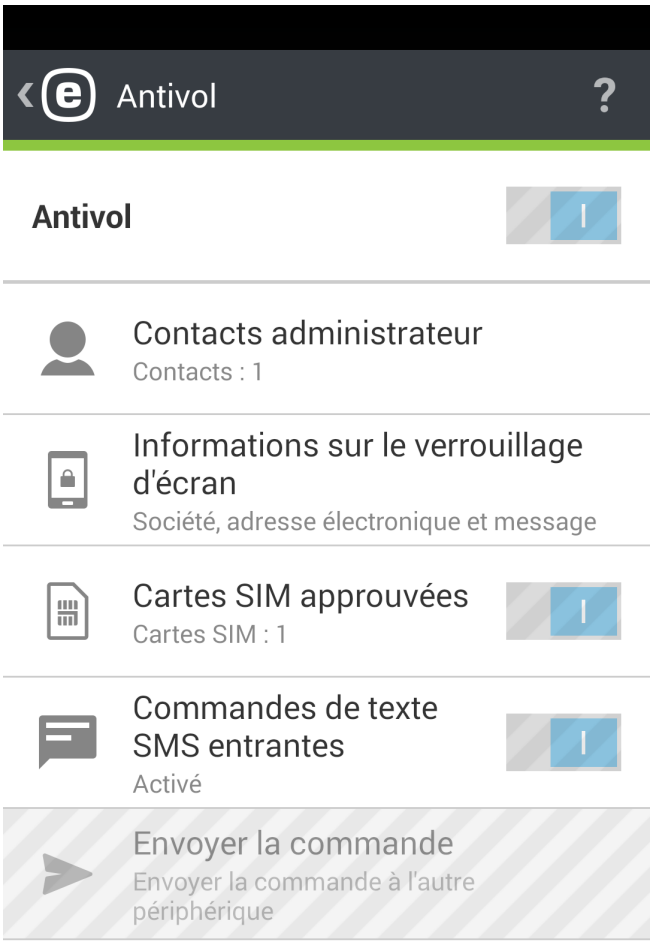
ESET Antivol aide les administrateurs à protéger les appareils et à retrouver les équipements perdus. Les actions peuvent être déclenchées via ERA ou des commandes SMS.

ESET Endpoint Security 2 utilise les mêmes commandes SMS que la version 1 (Verrouiller, Effacer et Rechercher). Les commandes suivantes sont nouvelles :

- **Déverrouiller** :déverrouille l'appareil verrouillé
- **Réinitialisation améliorée des paramètres d'usine** : toutes les données accessibles sur le périphérique sont rapidement supprimées (les en-têtes des fichiers sont détruits) et les paramètres d'usine par défaut sont rétablis
- **Sirène** : l'appareil perdu est verrouillé et émet un son très fort, même si le son a été coupé

Pour renforcer la sécurité des commandes SMS, l'administrateur reçoit un unique code SMS de vérification, valable pendant une durée limitée, sur son téléphone portable (au numéro indiqué dans la liste des contacts Administrateur) lorsqu'il exécute une commande SMS. Ce code de vérification sert à vérifier une commande particulière.

Par exemple, si un administrateur envoie un SMS à un appareil géré (tel qu'un téléphone portable égaré) avec le texte *eset lock,* il reçoit en retour un SMS avec un code de vérification pour cette commande. Il envoie alors un autre SMS au même numéro, cette fois avec le texte *eset lock* suivi du code de confirmation. Après ces actions, la commande est vérifiée, puis exécutée. Les commandes SMS peuvent être envoyées depuis n'importe quel téléphone portable et à n'importe quel numéro figurant dans la liste des contacts Administrateur.



Quand il exécute des commandes par SMS, l'administrateur reçoit un SMS confirmant qu'elles ont bien été envoyées. Quand il exécute ces commandes à partir d'ERA, il reçoit la confirmation dans ERA.

L'administrateur qui utilise ESET Remote Administrator reçoit les informations de localisation (commande Rechercher) sous forme de coordonnées GPS. S'il exécute la commande via SMS, il reçoit ces données (coordonnées GPS et un lien vers Google Maps) par SMS. S'il utilise l'interface utilisateur graphique (GUI) pour les commandes SMS (la fonction **Envoyer la commande**), il reçoit les informations dans la GUI dédiée.

Toutes les commandes d'Antivol peuvent également être exécutées à partir d'ERA. La nouvelle fonctionnalité de gestion des appareils mobiles permet aux administrateurs d'exécuter les commandes d'Antivol en quelques clics seulement. Les tâches sont immédiatement envoyées (pour être exécutées) via un nouveau composant de traitement des commandes push (Connecteur de périphérique mobile) qui fait maintenant partie de l'infrastructure ERA.

8.1 Contacts Administrateur

C'est la liste des numéros de téléphone des administrateurs. Ces numéros sont protégés par le mot de passe administrateur. Les commandes d'Antivol ne peuvent être envoyées que depuis des numéros fiables. Ces numéros servent également pour les notifications relatives aux actions d'Antivol.

8.1.1 Comment ajouter un contact administrateur

Le nom de l'administrateur et son numéro de téléphone sont en principe fournis dans l'Assistant Démarrage d'Antivol. Si le contact est associé à plusieurs numéros de téléphone, ceux-ci seront tous pris en compte.

Les contacts Administrateurs sont ajoutés ou modifiés dans la section **Antivol** > **Contacts Administrateur**.

8.2 Informations sur le verrouillage de l'écran

L'administrateur a la possibilité de définir des informations personnalisées (nom de la société, adresse e-mail, message) qui s'afficheront sur l'appareil verrouillé et permettront d'appeler un des contacts Administrateur de la liste.

Ces informations sont notamment :

- Nom de la société (facultatif)
- Adresse électronique (facultatif)
- Message personnalisé

8.3 Cartes SIM approuvées

La section **SIM approuvée** affiche la liste des cartes SIM approuvées qui seront acceptées par ESET Endpoint Security. Si vous introduisez une carte SIM qui ne figure pas dans cette liste, l'écran se verrouille et une alerte est envoyée par SMS à l'administrateur.

Pour ajouter une nouvelle carte SIM, appuyez sur l'icône ✚. Spécifiez un **Nom** pour cette carte SIM (par exemple Perso, Travail) et indiquez son numéro IMSI (International Mobile Subscriber Identity). Ce nombre à 15 chiffres est généralement imprimé sur la carte SIM. Il peut être plus court.

Pour retirer une carte SIM de la liste, appuyez sur l'entrée correspondante et maintenez la pression, puis appuyez sur l'icône 🗑.

REMARQUE : la fonction SIM approuvée n'est pas disponible sur les appareils CDMA, WCDMA et exclusivement Wi-Fi.

8.4 Commandes à distance

Les commandes à distance peuvent être déclenchées de trois manières différentes :

- directement à partir d'ERA Console ;
- à l'aide de la fonctionnalité **Envoyer la commande** d'ESET Endpoint Security installée sur l'appareil Android de l'administrateur ;
- en envoyant des messages texte SMS à partir de l'appareil de l'administrateur.

Pour faciliter l'exécution des commandes SMS si l'administrateur n'utilise pas ERA, il est possible de les déclencher à partir d'ESET Endpoint Security installé sur l'appareil Android de l'administrateur. Au lieu de taper manuellement le message texte et de vérifier la commande avec le code de vérification, l'administrateur peut utiliser la fonctionnalité **Envoyer la commande** (disponible exclusivement en mode Administrateur). Il peut entrer le numéro de téléphone ou choisir un contact et sélectionner la commande à envoyer dans le menu déroulant. ESET Endpoint Security exécute automatiquement et de manière silencieuse toutes les étapes nécessaires en arrière-plan.

Lors de l'envoi de commandes SMS, le numéro de téléphone de l'administrateur doit être un contact d'administrateur sur l'appareil cible. L'administrateur reçoit un code de vérification valide pendant une heure. Ce code peut être utilisé pour exécuter les commandes répertoriées ci-dessous. Le code doit être ajouté au message dans lequel la commande est envoyée en utilisant le format suivant : `eset find code`. L'administrateur reçoit une confirmation une fois que la commande a été exécutée sur l'appareil cible. Les commandes SMS suivantes peuvent être envoyées :

Rechercher
Commande SMS : `eset find`
Vous recevez un message texte avec les coordonnées GPS de l'appareil cible, ainsi qu'un lien vers cet emplacement sur Google Maps. S'il y a une localisation plus précise dans les 10 minutes, l'appareil renvoie un nouveau SMS.

Verrouiller
Commande SMS : `eset lock`
Cette commande verrouille l'appareil. Pour le déverrouiller, utilisez le mot de passe administrateur ou la commande Déverrouiller. Lorsque vous envoyez cette commande par SMS, vous pouvez ajouter un message personnalisé qui s'affiche sur l'écran de l'appareil verrouillé. Pour ce faire, utilisez le format suivant : `eset lock message de code`. Si vous laissez le paramètre de message vide, un message de la section Informations sur le verrouillage de l'écran s'affiche.

Déverrouiller
Commande SMS : `eset unlock`
Cette commande déverrouille l'appareil, et la carte SIM qui se trouve à l'intérieur est répertoriée comme SIM approuvée.

Sirène
Commande SMS : `eset siren`
Une sirène sonore se déclenche même si l'appareil est en mode silence.

Réinitialisation améliorée des paramètres d'usine
Commande SMS : `eset enhanced factory reset`
Cette option rétablit les paramètres d'usine de l'appareil. Toutes les données accessibles sont effacées et les en-têtes des fichiers sont supprimés. Ce processus peut prendre plusieurs minutes.

Effacer
Commande SMS : `eset wipe`
Tout ce qui est stocké dans les dossiers par défaut de l'appareil (contacts, messages, courrier électronique, comptes, contenu de la carte SD, images, musique et vidéos) est définitivement effacé. ESET Endpoint Security reste installé sur l'appareil.

REMARQUE : les commandes SMS ne font pas la distinction entre les majuscules et les minuscules.

9. Contrôle d'application

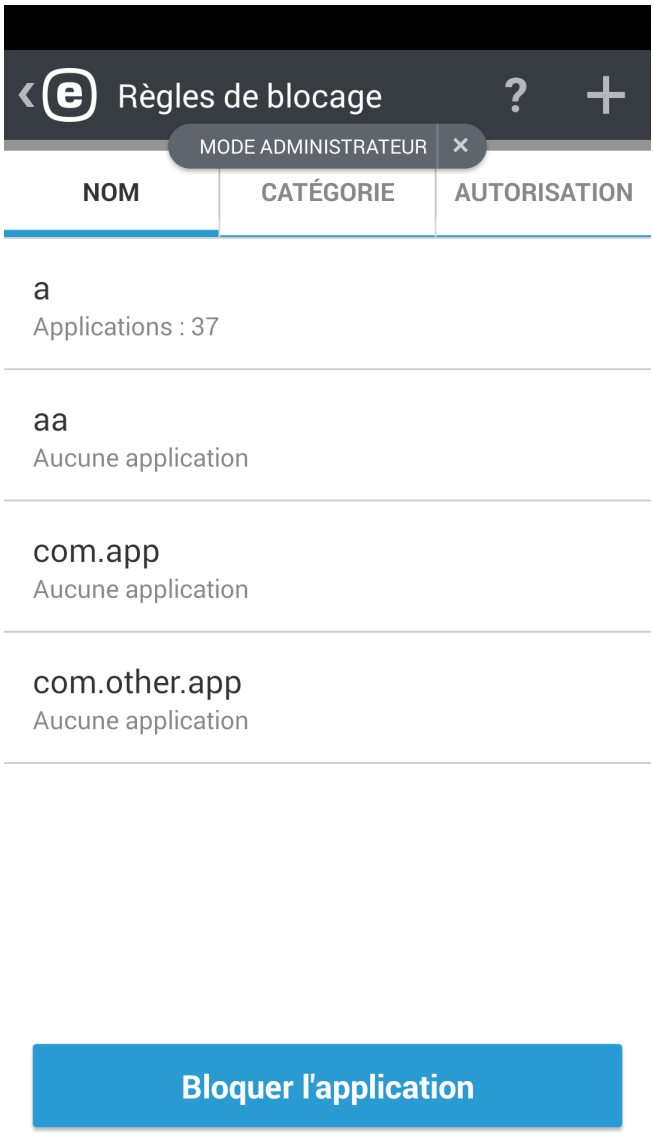
La fonction **Contrôle d'application** permet aux administrateurs de surveiller les applications installées, de bloquer l'accès à certaines applications et de réduire les risques en demandant aux utilisateurs de désinstaller certaines applications. L'administrateur a plusieurs méthodes de filtrage à sa disposition :

- Définir manuellement les applications à bloquer
- Bloquer par catégorie (jeux ou réseaux sociaux, par exemple)
- Bloquer en fonction des autorisations (par exemple, les applications qui utilisent la localisation)
- Bloquer d'après la source (par exemple, les applications installées à partir d'une autre source que la boutique Google Play)

9.1 Règles de blocage

Dans la section **Contrôle d'application** > **Blocage** > **Règles de blocage**, vous pouvez créer les règles de blocage d'application d'après les critères suivants :

- nom de l'application ou nom du package
- catégorie
- autorisations



9.1.1 Bloquer par nom d'application

ESET Endpoint Security permet aux administrateurs de bloquer une application en fonction de son nom ou du nom du package. La section **Règles de blocage** donne une vue d'ensemble des règles créées et affiche la liste des applications bloquées.

Pour modifier une règle existante, appuyez dessus et maintenez la pression, puis sélectionnez **Modifier** . Pour supprimer des règles de la liste, appuyez et maintenez la pression sur une des entrées, sélectionnez celles que vous souhaitez supprimer et appuyez sur **Supprimer** . Pour supprimer toute la liste, appuyez sur **SÉLECTIONNER TOUT**, puis sur **Supprimer** .

Lorsque vous bloquez une application par nom, ESET Endpoint Security recherche une correspondance exacte avec un nom d'application lancée. Si vous remplacez la langue de l'interface utilisateur graphique d'ESET Endpoint Security par une autre, vous devez retaper le nom de cette application dans cette langue pour continuer à la bloquer.

Pour éviter tout problème lié aux noms d'application traduits, il est recommandé de bloquer ces applications par nom de package, identifiant d'application unique qui ne peut pas être changé au moment de l'exécution ni réutilisé par une autre application.

Dans le cas d'un administrateur local, un utilisateur peut trouver le nom du package de l'application dans **Contrôle d'application** > **Surveillance** > **Applications autorisées**. Après avoir appuyé sur l'application, l'écran **Détails** affiche le nom du package de l'application. Pour bloquer l'application, suivez cette procédure.

9.1.1.1 Comment bloquer une application via son nom

1. Appuyez sur **Contrôle d'application** > **Blocage** > **Bloquer une application** > **Bloquer par nom**.
2. Indiquez s'il faut bloquer l'application par son nom ou celui du package.
3. Entrez les mots d'après lesquels l'application sera bloquée. Pour les séparer, utilisez une virgule (,).

Par exemple, le mot « *poker* » placé dans le champ **Nom de l'application** bloquera toutes les applications dont le nom contient « *poker* ». Si vous spécifiez « *com.poker.game* » dans le champ **Nom du package**, ESET Endpoint Security ne bloquera qu'une seule application.

9.1.2 Bloquer par catégorie d'application

ESET Endpoint Security donne à l'administrateur la possibilité de bloquer l'application d'après des catégories préalablement définies. La section **Règles de blocage** vous donne une vue d'ensemble des règles créées et affiche la liste des applications bloquées.

Pour modifier une règle existante, appuyez dessus et maintenez la pression, puis sélectionnez **Modifier** .

Pour supprimer des règles de la liste, appuyez et maintenez la pression sur une des entrées, sélectionnez celles que vous souhaitez supprimer et appuyez sur **Supprimer** . Pour supprimer toute la liste, appuyez sur **SÉLECTIONNER TOUT**.

9.1.2.1 Comment bloquer une application en fonction de sa catégorie

1. Appuyez sur **Contrôle d'application** > **Blocage** > **Bloquer une application** > **Bloquer par catégorie**.
2. Sélectionnez les catégories proposées en cochant les cases et appuyez sur **Bloquer**.

9.1.3 Bloquer selon les autorisations de l'application

ESET Endpoint Security donne à l'administrateur la possibilité de bloquer l'application d'après ses autorisations. La section **Règles de blocage** vous donne une vue d'ensemble des règles créées et affiche la liste des applications bloquées.

Pour modifier une règle existante, appuyez dessus et maintenez la pression, puis sélectionnez **Modifier** .

Pour supprimer des règles de la liste, appuyez et maintenez la pression sur une des entrées, sélectionnez celles que vous souhaitez supprimer et appuyez sur **Supprimer** . Pour supprimer toute la liste, appuyez sur **SÉLECTIONNER TOUT**.

9.1.3.1 Comment bloquer une application selon ses autorisations

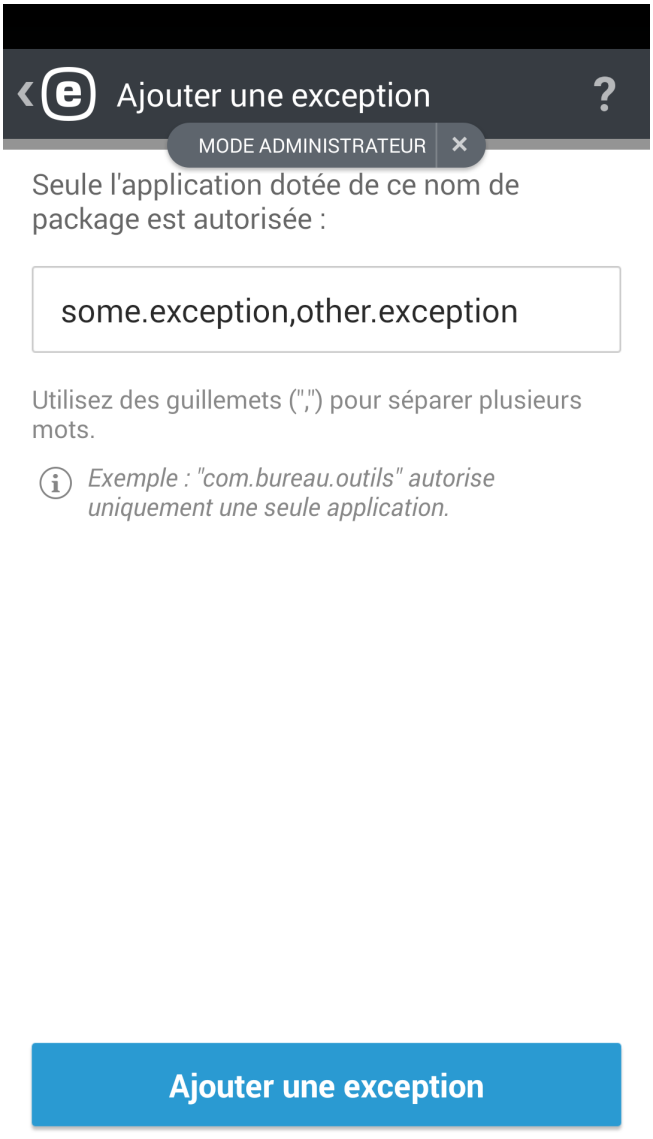
1. Appuyez sur **Contrôle d'application** > **Blocage** > **Bloquer une application** > **Bloquer par autorisation**.
2. Sélectionnez les autorisations en cochant les cases et appuyez sur **Bloquer**.

9.1.4 Bloquer les sources inconnues

Par défaut, ESET Endpoint Security ne bloque pas les applications lorsqu'elles proviennent d'Internet ou d'une autre source que la boutique Google Play. La section **Applications bloquées** vous donne une vue d'ensemble des applications bloquées (nom du package, règle appliquée). Vous pouvez les désinstaller ou les ajouter dans la liste blanche (section **Exceptions**).

9.2 Exceptions

Vous pouvez créer des exceptions pour exclure une application particulière de la liste des applications bloquées. Cette fonctionnalité permet aux administrateurs qui gèrent ESET Endpoint Security à distance de déterminer si un appareil respecte bien la politique de l'entreprise en ce qui concerne les applications installées.

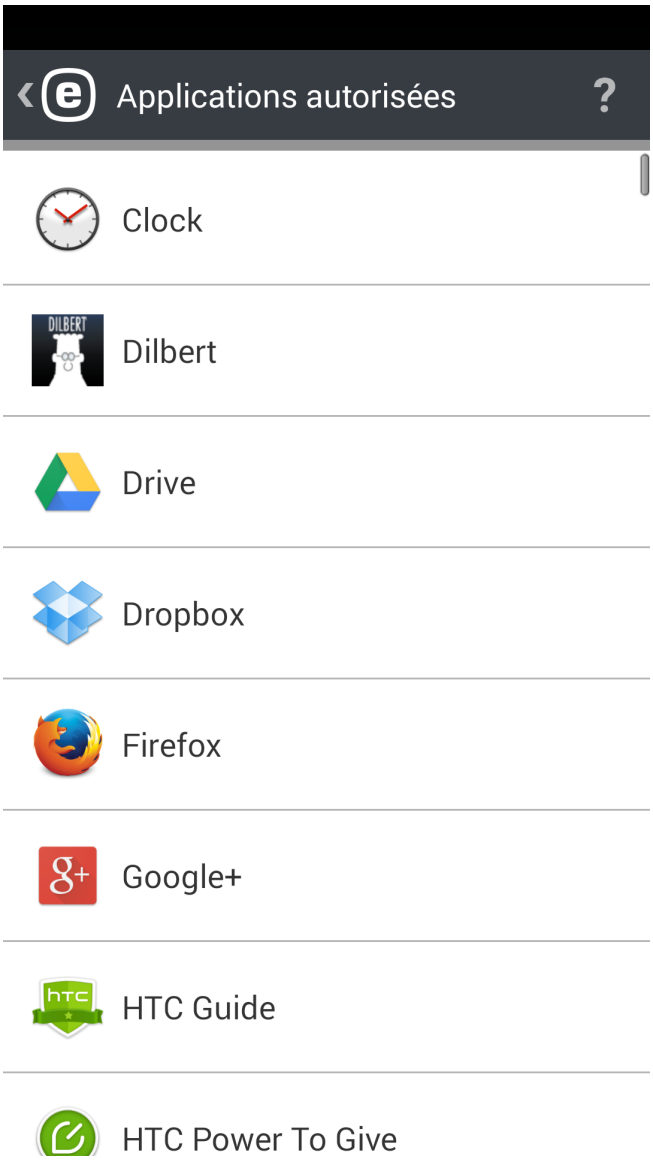


9.2.1 Comment ajouter des exceptions

Outre l'ajout de la nouvelle exception (en spécifiant le nom du package d'application), il est également possible de placer des applications dans la liste blanche en les retirant de la liste des **applications bloquées**.

9.3 Applications autorisées

Cette section vous donne une vue d'ensemble des applications installées qui ne sont pas bloquées par des règles de blocage. Si vous souhaitez bloquer l'une des applications répertoriées dans cette section, appuyez sur l'icône **Menu** dans le coin supérieur droit de l'écran, puis sur **Bloquer**. L'application sera déplacée vers la liste **Applications bloquées** (dans **Contrôle d'application** > **Blocage**).

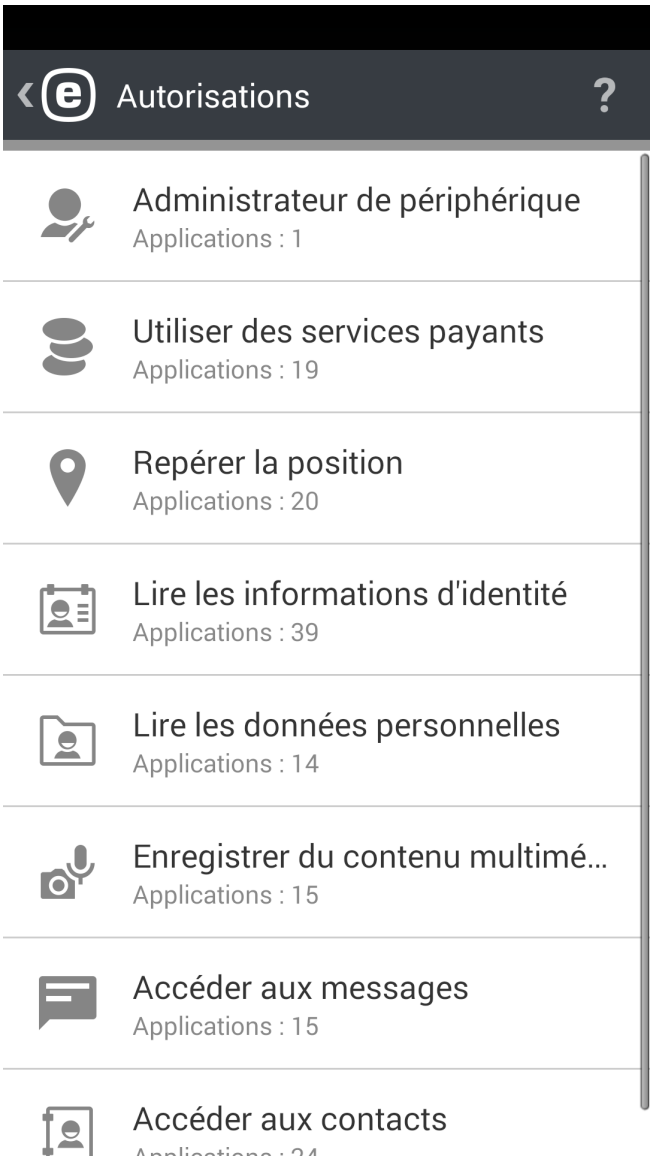


9.4 Autorisations

Cette fonction contrôle le comportement des applications ayant accès à des données personnelles ou à celles de l'entreprise. Elle permet à l'administrateur de surveiller l'accès des applications d'après des catégories d'autorisations préalablement définies.

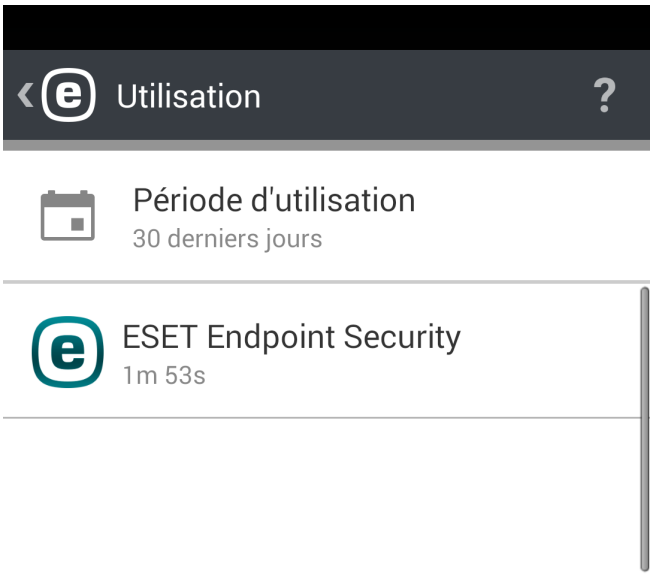
Certaines applications installées sur votre appareil peuvent avoir accès à des services payants, suivre votre position ou lire vos informations d'identité, vos contacts ou vos messages texte. ESET Endpoint Security présente un audit de ces applications.

Cette section contient la liste des applications triées par catégorie. Appuyez sur chaque catégorie pour afficher une description détaillée. Vous pouvez obtenir des informations sur les autorisations d'une application en appuyant sur celle-ci.



9.5 Utilisation

Dans cette section, l'administrateur peut surveiller la durée d'utilisation de certaines applications. Pour filtrer la liste des applications selon leur période d'utilisation, utilisez l'option **Période d'utilisation** et indiquez si vous voulez voir les applications utilisées ces 30 ou 7 derniers jours, ou ces dernières 24 heures.

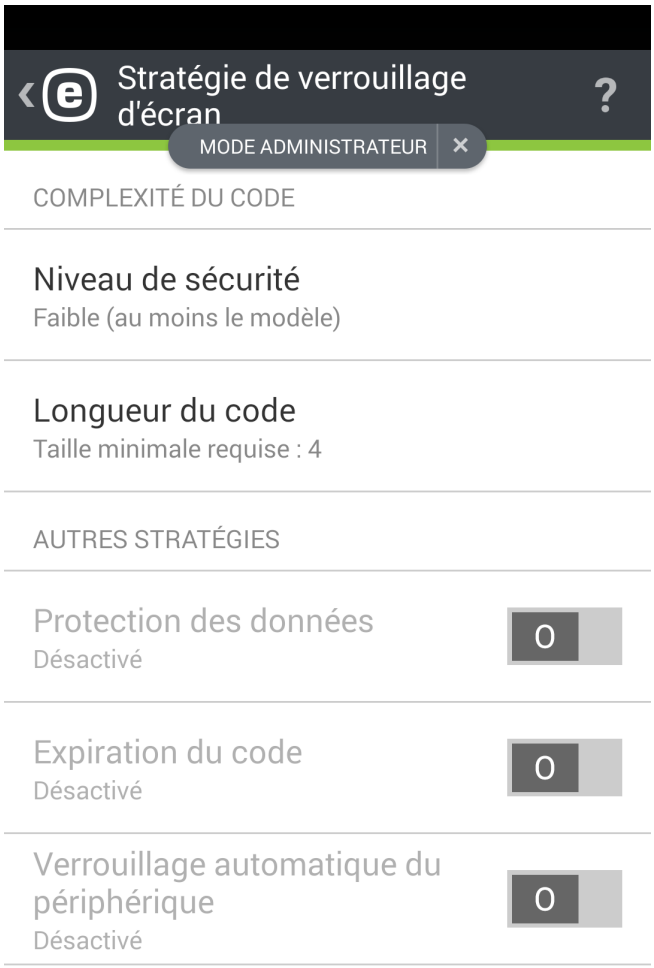


10. Sécurité du périphérique

La fonction **Sécurité du périphérique** permet aux administrateurs d'effectuer les opérations suivantes :

- Exécuter des stratégies de sécurité de base sur l'ensemble des appareils mobiles et définir des stratégies pour les paramètres importants
- Spécifier la complexité requise du verrouillage de l'écran
- Limiter l'utilisation de la caméra intégrée

10.1 Stratégie de verrouillage de l'écran



Dans cette section, l'administrateur a plusieurs possibilités :

- Définir un niveau de sécurité minimum (motif, numéro secret, mot de passe) pour le code de verrouillage de l'écran et définir sa complexité (longueur minimale par exemple)
- Définir le nombre maximum d'échecs lors du déverrouillage (avant que l'appareil ne revienne aux paramètres d'usine)
- Définir la longévité maximale du code de verrouillage de l'écran
- Définir le minuteur pour le verrouillage

ESET Endpoint Security informe automatiquement l'utilisateur et l'administrateur si les paramètres actuels de l'appareil sont conformes aux stratégies de sécurité de l'entreprise. Dans le cas contraire, l'utilisateur reçoit automatiquement des suggestions sur ce qui doit changer pour que l'appareil soit à nouveau conforme.

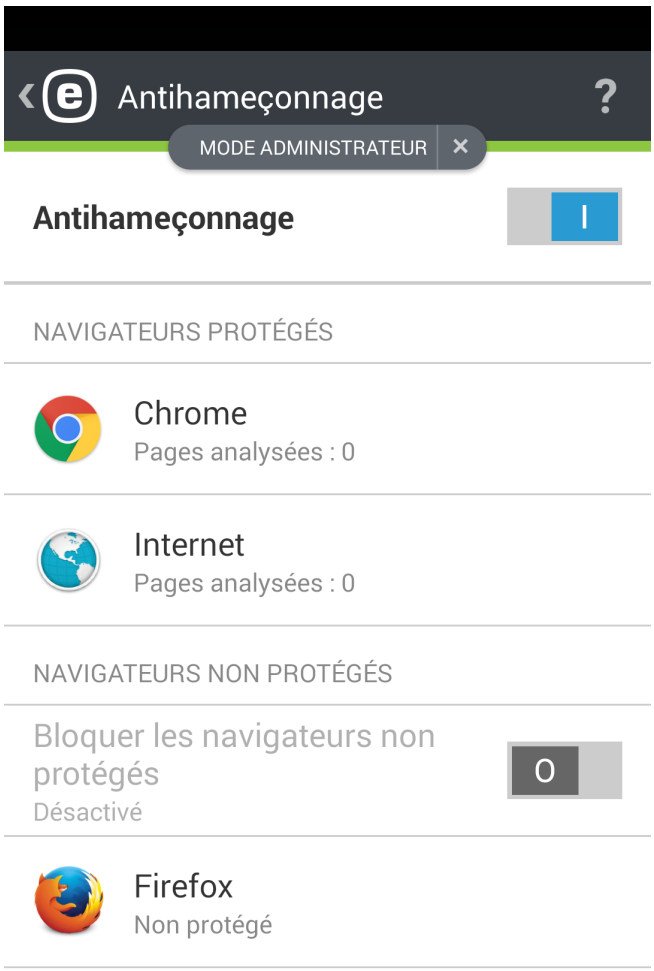
10.2 Stratégie relative aux paramètres de l'appareil

La fonction Sécurité du périphérique inclut également votre **stratégie relative aux paramètres de l'appareil** (qui faisait partie de la fonction Audit de sécurité). Celle-ci permet à l'administrateur système de surveiller les paramètres prédéfinis de l'appareil pour déterminer s'ils sont conformes aux recommandations.

Ces paramètres sont les suivants :

- Wi-Fi
- Satellites GPS
- Services de localisation
- Mémoire
- Itinérance des données
- Itinérance des appels
- Sources inconnues
- Mode débogage
- NFC
- Chiffrement du stockage
- Périphérique débloqué

11. Antihameçonnage



Le terme *hameçonnage* (phishing en anglais) désigne une activité frauduleuse impliquant des techniques d'ingénierie sociale (social engineering en anglais) qui consistent à manipuler les utilisateurs dans le but d'obtenir des informations confidentielles. L'hameçonnage est souvent utilisé pour accéder à des données sensibles, telles que numéros de comptes bancaires, codes des cartes bancaires, codes PIN ou noms d'utilisateur et mots de passe.

Il est recommandé de garder l'option **Antihameçonnage** activée. Toutes les attaques potentielles par hameçonnage provenant de sites Web ou de domaines inscrits dans la base de données ESET des logiciels malveillants seront bloquées et un avertissement s'affichera pour vous en informer.

La fonction Antihameçonnage s'intègre à la plupart des navigateurs Internet les plus utilisés sur le système d'exploitation Android (par exemple Chrome et le navigateur Internet par défaut d'Android). Les autres navigateurs seront indiqués comme n'étant pas protégés. Vous pouvez en interdire l'accès en cliquant sur le bouton  .

Pour exploiter pleinement la fonction Antihameçonnage, nous vous conseillons de bloquer tous les navigateurs Internet non pris en charge. Ainsi, les utilisateurs se serviront uniquement de ceux qui sont gérés.

REMARQUE : l'option Antihameçonnage ne vous protège pas lorsque vous optez pour la navigation privée (pour surfer incognito).

12. Filtre de SMS et d'appels

Le **filtre de SMS et d'appels** bloque les SMS/MMS entrants et les appels entrants et sortants en fonction des règles définies par l'utilisateur.

Les messages non sollicités contiennent généralement des publicités des opérateurs de téléphonie mobile ou proviennent d'utilisateurs inconnus ou non spécifiés. En fait, cette fonction place automatiquement le message entrant dans la section **Historique**. Aucune notification ne s'affiche pour un message ou un appel entrant bloqué. Cela présente un avantage : vous n'êtes plus dérangé par des informations non désirées, mais vous pouvez toujours consulter les journaux pour déceler les messages qui auraient été bloqués par erreur.

REMARQUE : le filtre de SMS et d'appels ne fonctionne pas sur les tablettes qui ne prennent pas en charge les appels et les messages. Il n'est pas disponible sur Android OS 4.4 (KitKat) et est désactivé sur les appareils où Google Hangouts est l'application principale pour les SMS.

Pour bloquer les appels et les messages en provenance du dernier numéro qui a cherché à vous contacter, appuyez sur **Bloquer le dernier appelant** ou **Bloquer le dernier expéditeur de SMS**. Cela va créer une nouvelle règle.

12.1 Règles

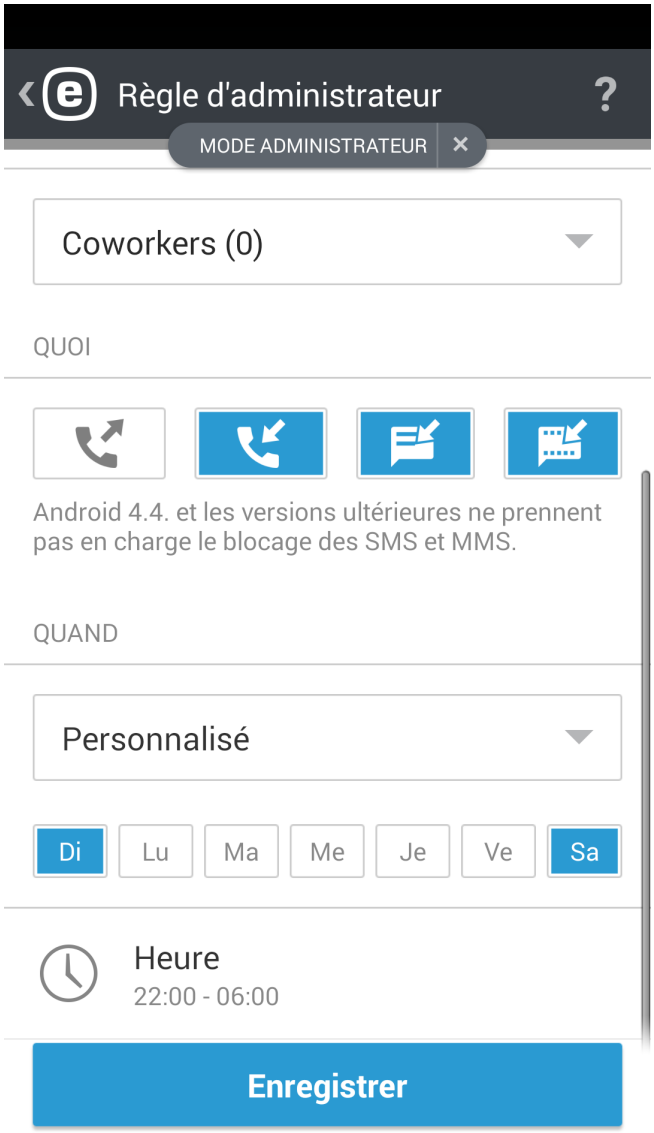
En tant qu'utilisateur, vous pouvez créer des règles sans avoir à fournir un mot de passe administrateur. En revanche, les règles d'administrateur ne peuvent être créées qu'en mode Administrateur et elles ont la priorité sur les règles d'utilisateur.

Pour en savoir plus sur la création des règles, reportez-vous à cette section.

Pour supprimer une règle existante de la liste **Règles**, appuyez sur l'entrée correspondante et maintenez la pression, puis appuyez sur l'icône **Supprimer**.

12.1.1 Comment ajouter une nouvelle règle

Pour ajouter une nouvelle règle, appuyez sur l'icône ➕ dans l'angle supérieur droit de l'écran **Règles**.



Selon l'action souhaitée, indiquez si les messages et les appels doivent être autorisés ou bloqués.

Spécifiez une personne ou un groupe de numéros de téléphone. ESET Endpoint Security reconnaîtra les groupes de contacts enregistrés dans vos Contacts (par exemple, Famille, Amis ou Collègues). La liste **Tous les numéros inconnus** contient les numéros qui ne sont pas enregistrés dans votre liste de contacts. Vous pouvez utiliser cette option pour bloquer les appels importuns (par exemple le démarchage) ou pour empêcher les employés de composer des numéros inconnus. L'option **Tous les numéros connus** correspond à tous les numéros enregistrés dans votre liste de contacts. Les **Numéros masqués** sont ceux des appelants qui ont choisi de masquer leur numéro via la fonction de restriction de l'identification de l'appelant (CLIR, Calling Line Identification Restriction).

Spécifiez ce que vous souhaitez bloquer ou autoriser :

- Appels sortants
- Appels entrants
- SMS entrants
- MMS entrants

Pour appliquer la règle seulement pendant une période spécifique, appuyez sur **Toujours** > **Personnaliser** et sélectionnez les jours de la semaine et une durée d'application. Par défaut, le samedi et le dimanche sont sélectionnés. Cette fonction peut être pratique si vous ne voulez pas être dérangé pendant les réunions, les déplacements professionnels, la nuit ou le week-end.

REMARQUE : Si vous êtes à l'étranger, tous les numéros de téléphone inscrits dans la liste doivent inclure le code international avant le numéro proprement dit (par exemple, +1610100100).

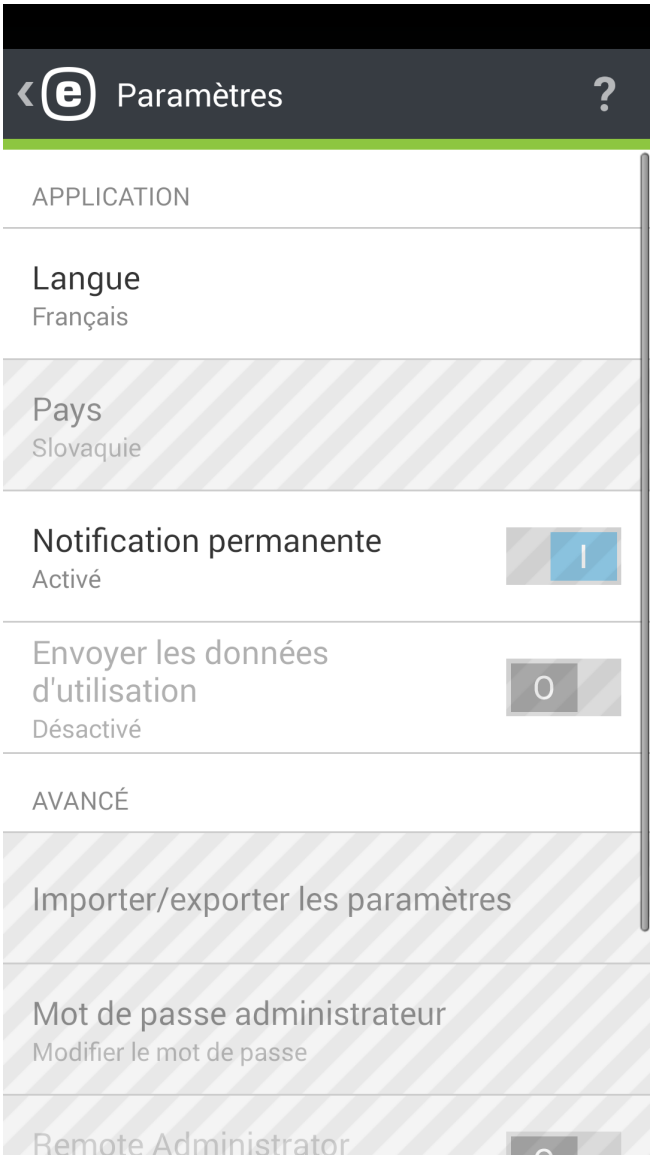
12.2 Historique

Dans la section **Historique**, vous pouvez voir les appels et les messages bloqués ou autorisés par le filtre de SMS et d'appels. Chaque journal contient le nom, et la date et l'heure de l'événement, ainsi que le numéro de téléphone correspondant. Le journal des SMS et MMS contient également le texte du message.

Si vous souhaitez modifier une règle associée à un numéro de téléphone ou à un contact qui a été bloqué, sélectionnez l'entrée en question dans la liste et appuyez sur l'icône .

Pour supprimer cette entrée, sélectionnez-la et appuyez sur l'icône . Pour en supprimer davantage, appuyez sur une des entrées et maintenez la pression, sélectionnez les autres et appuyez sur l'icône .

13. Paramètres



Langue
Par défaut, ESET Endpoint Security est installé dans la langue qui est définie comme paramètre régional sur votre appareil (dans les options du clavier et de la langue sur le système Android). Pour changer la langue de l'interface utilisateur de l'application, appuyez sur Langue et sélectionnez la langue de votre choix.

Pays
Sélectionnez le pays dans lequel vous travaillez ou résidez.

Mettre à jour
Pour assurer une protection optimale, il est important d'utiliser la dernière version d'ESET Endpoint Security. Appuyez sur **Mettre à jour** pour voir s'il existe une version plus récente à télécharger à partir du site Web d'ESET. Cette option n'est pas disponible si vous avez téléchargé ESET Endpoint Security à partir de Google Play. Dans ce cas, le produit est mis à jour à partir de Google Play.

Notification permanente

ESET Endpoint Security affiche son icône de notification  dans l'angle supérieur gauche de l'écran (barre d'état Android). Si vous ne voulez pas voir cette icône, désactivez l'option **Notification permanente**.

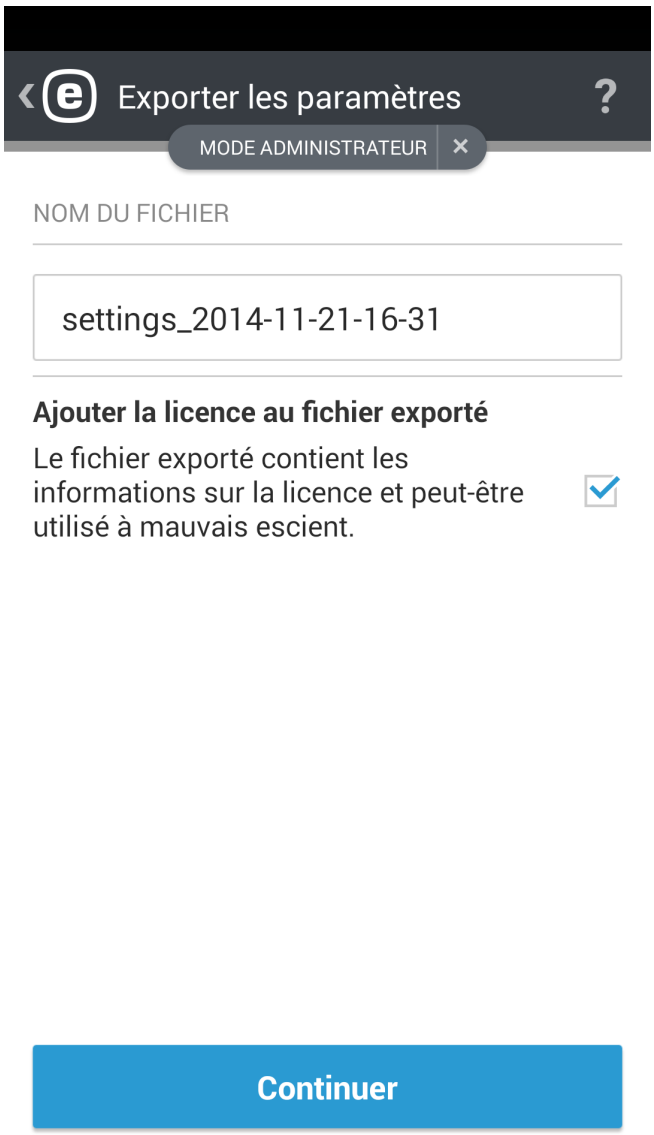
Envoyer les données d'utilisation
Cette option permet d'améliorer les produits ESET en envoyant des données anonymes sur l'utilisation de l'application. Si vous n'avez pas activer cette option dans Assistant Démarrage, vous pouvez le faire dans la section **Paramètres**.

Mot de passe administrateur
Cette option vous permet de définir un nouveau mot de passe administrateur ou de modifier celui qui existe déjà. Pour en savoir plus, lisez la section Mot de passe administrateur.

Désinstaller
Lorsque vous exécutez l'Assistant de désinstallation, ESET Endpoint Security et les dossiers de mise en quarantaine sont définitivement supprimés de l'appareil. Si la protection contre la désinstallation a été activée, vous êtes invité à fournir votre **mot de passe administrateur**.

13.1 Importer/exporter les paramètres

Pour transmettre facilement les paramètres d'un appareil mobile à un autre si ceux-ci ne sont pas gérés par ERA, ESET Endpoint Security 2 propose désormais une option pour les exporter et les importer. L'administrateur peut exporter manuellement les paramètres de l'appareil dans un fichier qui peut ensuite être partagé (par e-mail par exemple) et importé sur n'importe quel appareil exécutant l'application cliente. Lorsque l'utilisateur accepte le fichier de paramètres qu'il a reçu, cela définit automatiquement tous les paramètres et active l'application (si les informations sur la licence ont été incluses). Tous les paramètres sont protégés par le mot de passe administrateur.



13.1.1 Exporter les paramètres

Pour exporter les paramètres actuels d'ESET Endpoint Security, spécifiez le nom du fichier. La date et l'heure sont ajoutées automatiquement. Vous pouvez aussi ajouter les informations sur la licence (clé ou adresse e-mail et mot de passe du compte de l'administrateur de la sécurité) au fichier exporté, mais sachez que ces données ne sont pas chiffrées et peuvent donc être détournées.

À l'étape suivante, indiquez comment transmettre le fichier :

- Réseau Wi-Fi
- Bluetooth
- Adresse e-mail
- Gmail
- Explorateur de fichiers (par exemple le gestionnaire de fichiers ASTRO ou l'explorateur de fichiers ES)

13.1.2 Importer les paramètres

Pour importer les paramètres à partir d'un fichier se trouvant sur l'appareil, utilisez une application telle que le gestionnaire de fichiers ASTRO ou l'explorateur de fichiers ES, localisez le fichier des paramètres et choisissez ESET Endpoint Security.

Vous pouvez également importer les paramètres en sélectionnant un fichier dans la section **Historique**.

13.1.3 Historique

La section **Historique** fournit la liste des fichiers de paramètres importés et permet de les partager, de les importer ou de les supprimer.

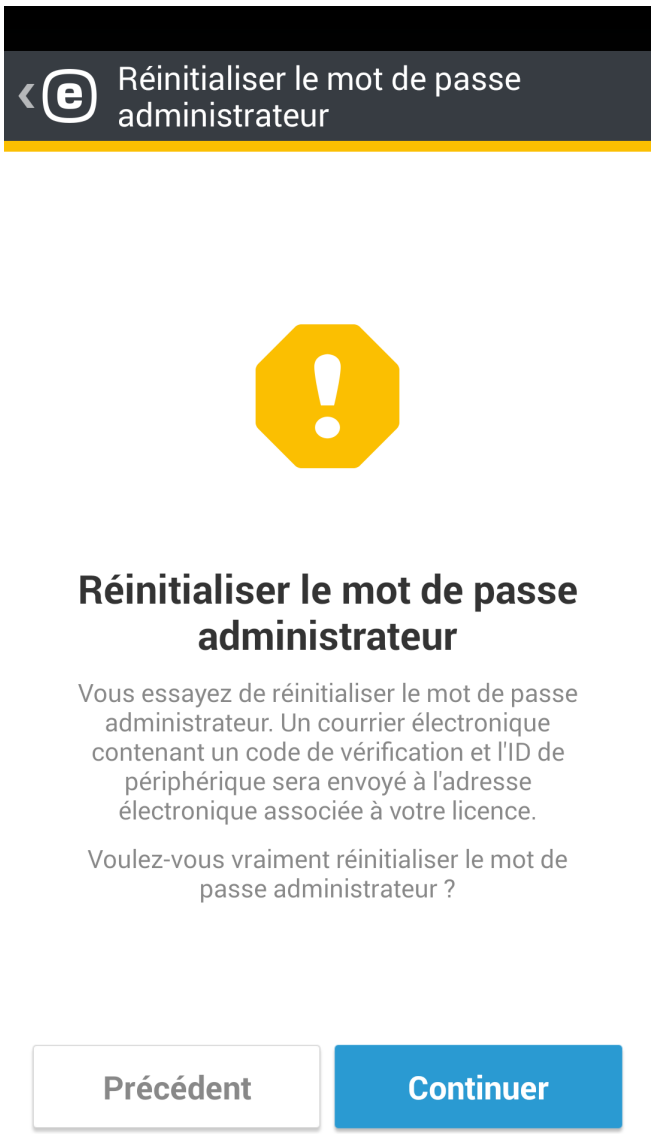
13.2 Mot de passe administrateur

Le **mot de passe administrateur** est nécessaire pour déverrouiller un appareil, envoyer des commandes d'Antivol, accéder aux fonctions protégées par mot de passe et désinstaller ESET Endpoint Security.

IMPORTANT : choisissez le mot de passe avec soin. Pour renforcer la sécurité et rendre le mot de passe plus difficile à deviner, combinez des lettres minuscules et majuscules avec des chiffres.

Pour réinitialiser le mot de passe administrateur sur un appareil dont l'écran est verrouillé :

1. Appuyez sur **Mot de passe oublié ?** > **Continuer** > **Demander le code de vérification**. Si l'appareil n'est pas connecté à Internet, appuyez sur le lien **choisissez la réinitialisation hors ligne** et contactez le service client ESET.
2. Vérifiez vos messages : un message électronique contenant un code de vérification et l'ID d'appareil est envoyé à l'adresse électronique associée à la licence ESET. Le code de vérification est actif pendant 1 heure après sa réception.
3. Saisissez le code de vérification et un nouveau mot de passe dans l'écran verrouillé de l'appareil.



13.3 Remote administrator

ESET Remote Administrator (ERA) vous permet de gérer ESET Endpoint Security dans un environnement réseau à partir d'un emplacement centralisé.

Utiliser ERA permet non seulement de renforcer la sécurité, mais aussi d'assurer la simplicité d'utilisation dans l'administration de tous les produits ESET installés sur les appareils mobiles et postes de travail clients. Les appareils disposant d'ESET Endpoint Security peuvent se connecter à ERA avec n'importe quel type de connexion Internet – WiFi, LAN, WLAN, cellulaire (3G, 4G, HSDPA, GPRS), etc. – pourvu qu'elle soit standard (sans proxy ni pare-feu) et à condition que les deux points de terminaison soient configurés correctement.

Le succès d'une connexion à ERA via un réseau cellulaire dépend de l'opérateur. Elle nécessite par ailleurs une connexion Internet totalement fonctionnelle.

Pour connecter un appareil à ERA, ajoutez-le à la liste **Ordinateurs** de la console Web ERA, inscrivez-le à l'aide de la tâche **Inscription de périphérique**, puis saisissez l'adresse du serveur Mobile Device Connector (MDC) :

- **Hôte du serveur** : spécifiez le nom DNS complet ou l'adresse IP publique du serveur exécutant Mobile Device Connector (MDC). Le nom d'hôte ne peut être utilisé que si vous effectuez la connexion via un réseau Wi-Fi interne.
- **Port du serveur** : permet de spécifier le port du serveur utilisé pour se connecter à Mobile Device Connector.

REMARQUE : pour plus d'informations sur la gestion du réseau à l'aide d'ESET Remote Administrator, reportez-vous à la documentation en ligne d'ESET Remote Administrator.

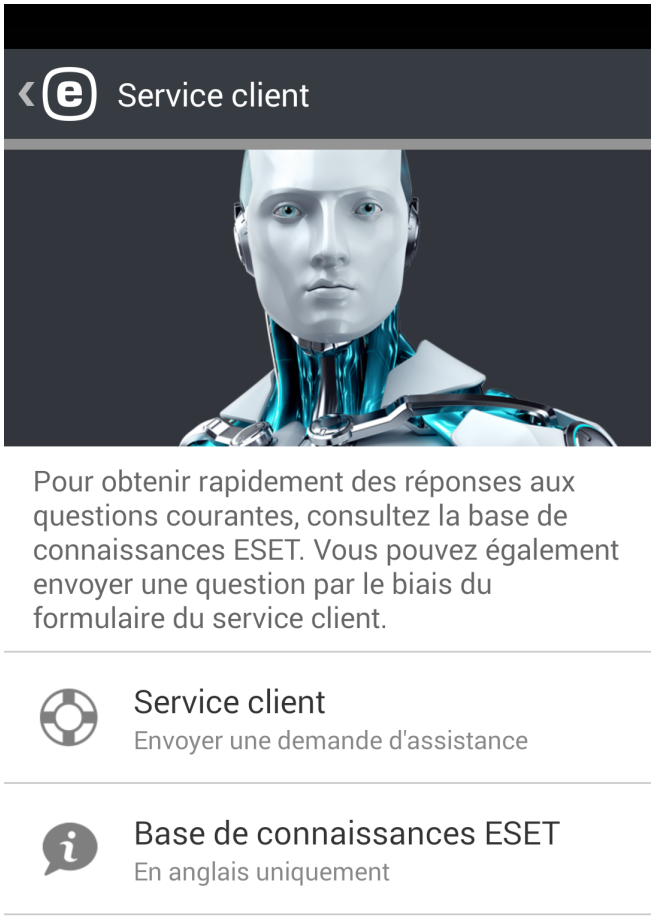
13.4 ID de périphérique

Cet ID permet à l'administrateur d'identifier votre appareil en cas de perte ou de vol.

14. Service client

Les spécialistes du service client ESET sont à votre disposition et assurent l'assistance administrative ou technique pour ESET Endpoint Security ou n'importe quel autre produit ESET.

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



ESET Endpoint Security propose des fonctions avancées de consignation dans les journaux qui permettent de mieux diagnostiquer les éventuels problèmes techniques. Pour fournir à ESET un journal détaillé, veillez à ce que l'option **Envoyer le journal de l'application** soit sélectionnée (elle l'est par défaut). Appuyez sur **Envoyer** pour envoyer la demande. Un spécialiste du service client ESET vous contactera à l'adresse e-mail que vous avez indiquée.