ESET ENDPOINT SECURITY 6

Guide de l'utilisateur

Microsoft® Windows® 8.1/8/7/Vista/XP x86 SP3/XP x64 SP2

Cliquez ici pour télécharger la dernière version de ce document.

ENJOY SAFER TECHNOLOGY™

ESET **ENDPOINT SECURITY 6**

Assistance clientèle internationale : www.eset.com/support

RÉV. 2/23/2015

Table des matières

Table des matières

1. ESET Endpoint Security

ESET Endpoint Security 6 représente une nouvelle approche de sécurité informatique véritablement intégrée. La dernière version du moteur d'analyse ThreatSense®, associée à un pare-feu personnel et à un module antispam personnalisés, garantissent la sécurité de votre ordinateur avec grande précision et rapidité. Le résultat est un système intelligent et constamment en alerte, qui protège votre ordinateur des attaques et des programmes malveillants.

ESET Endpoint Security 6 est une solution complète de sécurité ; c'est le résultat d'un effort de longue haleine qui associe protection maximale et encombrement minimal. Des technologies avancées basées sur l'intelligence artificielle sont capables de faire barrage de manière proactive à l'infiltration de virus, de logiciels espions, de chevaux de Troie, de vers, de logiciels publicitaires, de rootkits et d'autres attaques provenant d'Internet, sans réduire les performances ni perturber votre ordinateur.

ESET Endpoint Security 6 est essentiellement destiné aux postes de travail des entreprises de petites tailles. Il peut être utilisé avec ESET Remote Administrator, vous permettant de facilement gérer des stations de travail clientes, quel que soit leur nombre, d'appliquer des règles et des stratégies, de surveiller les détections et de configurer à distance à partir de n'importe quel ordinateur du réseau.

1.1 Nouveautés

L'interface utilisateur graphique d'ESET Endpoint Security a été repensée pour offrir une meilleure visibilité et un environnement plus intuitif. Parmi les nombreuses améliorations apportées à ESET Endpoint Security version 6, citons notamment :

Améliorations fonctionnelles et d'utilisation

- Filtrage Internet : définissez une règle pour plusieurs URL ou des stratégies différentes pour différents emplacements réseau. Les stratégies de blocage souples sont une nouvelle fonctionnalité de la version 6 avec la possibilité de personnaliser partiellement le blocage et la page d'avertissement.
- Pare-feu personnell : vous pouvez désormais créer directement des règles à partir du journal ou de la fenêtre de notification IDS et attribuer des profils aux interfaces réseau.
- Nouvelle protection anti-botnet - contribue à la découverte de logiciels malveillants par l'analyse de ses schémas et protocoles de communication réseau.
- Contrôle de périphérique : ce module permet désormais de déterminer le type et le numéro de série du périphérique et de définir des règles pour plusieurs périphériques.
- Nouveau mode intelligent pour HIPS - placé entre les modes automatique et interactif. Possibilité d'identifier des activités suspectes et des processus malveillants dans le système.
- Améliorations du programme de mise à jour/miroir : vous pouvez désormais reprendre les téléchargements qui ont échoué de la base des signatures de virus et/ou des modules du produit.
- Nouvelle approche de la gestion à distance de vos ordinateurs à l'aide d'ESET Remote Administrator : renvoyez des journaux en cas de nouvelle installation d'ERA ou à des fins de test, installez à distance les solutions de sécurité ESET, obtenez une vue d'ensemble de l'état de la sécurité de l'environnement réseau et triez différentes données en vue de les utiliser ultérieurement.
- Améliorations de l'interface utilisateur : exécution en un seul clic des mises à jour de la base des signatures de virus et des modules à partir de la partie système de la barre des tâches Windows. Prise en charge des écrans tactiles et des affichages haute résolution.
- Amélioration de la détection et de la suppression des solutions de sécurité tierces.

Nouvelles fonctionnalités

- Antihameçonnage : vous protège des tentatives d’acquisition de mots de passe et d'autres informations sensibles en limitant l'accès des sites Web malveillants se faisant passer pour des sites légitimes.
- Améliorations de la vitesse d'analyse : utilisation du cache local partagé dans les environnements virtualisés.

Technologies de détection et de protection

- Amélioration de la vitesse et de la fiabilité de l'installation.
- Scanner de mémoire avancé : surveille le comportement des processus et analyse les processus malveillants lorsqu'ils désactivent le masquage en mémoire.
- Bloqueur d'exploit amélioré : conçu pour renforcer les types d'applications connues pour être très vulnérables aux exploits (navigateurs, lecteurs de fichiers PDF, clients de messagerie et composants MS Office). Le bloqueur d'exploit prend désormais en charge Java et contribue à améliorer la détection de ces types de vulnérabilités et la protection contre elles.
- Amélioration de la détection et de la suppression des rootkits.
- Bouclier anti-vulnérabilités : options de filtrage encore plus avancées pour détecter les différents types d'attaques et de vulnérabilités.
- Analyse en cas d'inactivité : analyse silencieuse effectuée sur tous les disques locaux lorsque l'ordinateur est dans un état inactif.

1.2 Configuration système

Pour garantir le fonctionnement correct d'ESET Endpoint Security, le système doit répondre à la configuration suivante :

Processeurs pris en charge : Intel® ou AMD x86 - x64

Systèmes d'exploitation : Microsoft® Windows® 8.1/8/7/Vista/XP SP3 32 bits/XP SP2 64 bits

1.3 Prévention

Lorsque vous travaillez sur votre ordinateur et particulièrement lorsque vous surfez sur Internet, gardez toujours à l'esprit qu'aucun antivirus au monde ne peut complètement éliminer le risque d'infiltrations et attaques. Pour bénéficier d'une protection maximale, il est essentiel d'utiliser votre solution antivirus correctement et de respecter quelques règles essentielles :

Mise à jour régulièrement

Selon les statistiques d'ESET Live Grid, des milliers de nouvelles infiltrations sont créées chaque jour pour contourner les dispositifs de sécurité existants et servir leurs auteurs, aux dépens des autres utilisateurs. Les spécialistes du laboratoire d'ESET analysent ces menaces chaque jour et conçoivent des mises à jour pour améliorer continuellement le niveau de protection des utilisateurs. Pour assurer l'efficacité maximale de ces mises à jour, il est important que les mises à jour soient configurées correctement dans votre système. Pour plus d'informations sur la procédure de configuration des mises à jour, reportez-vous au chapitre Configuration des mises à jour.

Télécharger les patchs de sécurité

Les auteurs de programmes malveillants exploitent souvent diverses failles du système pour assurer une meilleure propagation du code malveillant. Les sociétés qui commercialisent des logiciels recherchent donc activement les moindres failles dans leurs applications afin de concevoir des mises à jour de sécurité et d'éliminer régulièrement les menaces potentielles. Il est important de télécharger ces mises à jour de sécurité au moment de leur sortie. Microsoft Windows et les navigateurs Web, comme Internet Explorer, sont deux exemples de programmes pour lesquels des mises à jour sont régulièrement disponibles.

Sauvegarder les données importantes

Les concepteurs de programmes malveillants ne se soucient généralement pas des besoins des utilisateurs et l'activité de leurs programmes entraîne souvent un dysfonctionnement total du système d'exploitation et une perte importante au niveau des données. Il est essentiel de sauvegarder régulièrement vos données importantes et sensibles sur une source externe, telle qu'un DVD ou un disque dur externe. Ces précautions permettront de récupérer vos données beaucoup plus facilement et rapidement en cas de défaillance du système.

Rechercher régulièrement les virus sur votre ordinateur

La détection de virus, de vers, de chevaux de Troie et de rootkits, connus et inconnus, est gérée par le module de

protection du système de fichiers en temps réel. Cela signifie qu'à chaque fois que vous accédez à un fichier ou que vous l'ouvrez, il est analysé afin de détecter toute trace de logiciels malveillants. Nous vous recommandons de lancer une analyse complète de l'ordinateur au moins une fois par mois, car les logiciels malveillants peuvent varier et la base de signatures des virus est quotidiennement mise à jour.

Suivre les règles de sécurité de base

Cette règle est la plus utile et la plus efficace de toutes : soyez toujours prudent. Actuellement, de nombreuses infiltrations nécessitent l'intervention de l'utilisateur pour être exécutées et propagées. Si vous êtes prudent lorsque vous ouvrez de nouveaux fichiers, vous éviterez de perdre un temps et une énergie considérables à nettoyer des infiltrations. Voici quelques conseils qui pourront vous être utiles :

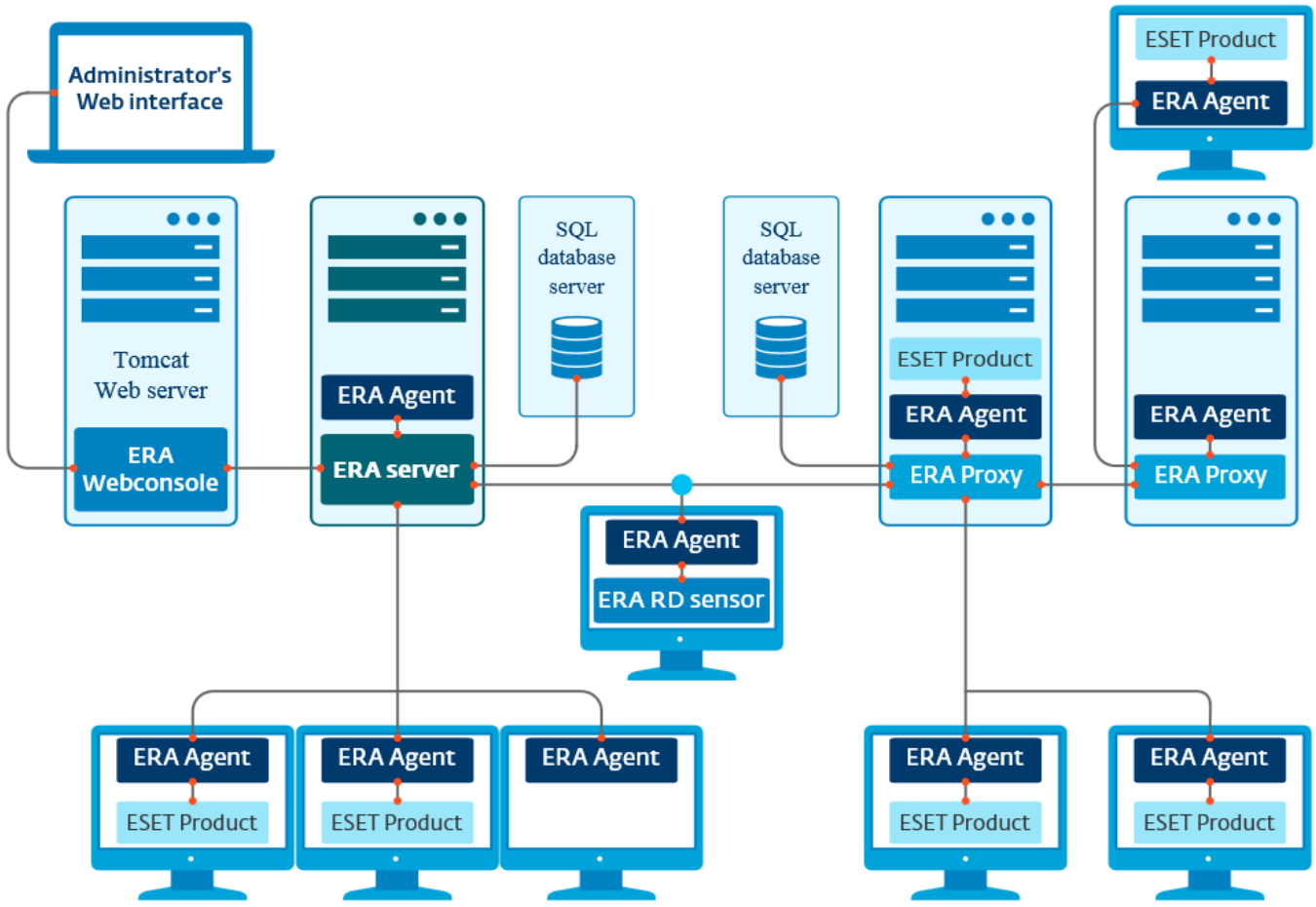
- Ne consultez pas les sites Web suspects comportant de nombreuses fenêtres publicitaires et annonces clignotantes.
- Soyez vigilant lorsque vous installez des logiciels gratuits, des packs codec, etc. N'utilisez que des programmes sécurisés et ne visitez que les sites Web sécurisés.
- Soyez prudent lorsque vous ouvrez les pièces jointes des messages électroniques, en particulier celles de messages provenant de mailing ou d'expéditeurs inconnus.
- N'utilisez pas de compte Administrateur pour le travail de tous les jours sur votre ordinateur.

2. Documentation pour les utilisateurs connectés via ESET Remote Administrator

ESET Remote Administrator (ERA) 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 offre la possibilité d'installer les solutions de sécurité ESET sur des ordinateurs distants et de réagir rapidement face aux nouveaux problèmes et menaces. ESET Remote Administrator n'offre pas de protection contre les codes malveillants ; le produit repose sur la présence d'une solution de sécurité ESET 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 MAC OS et de systèmes d'exploitation qui s'exécutent sur des périphériques 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 au Guide de l'utilisateur d'ESET Remote Administrator.

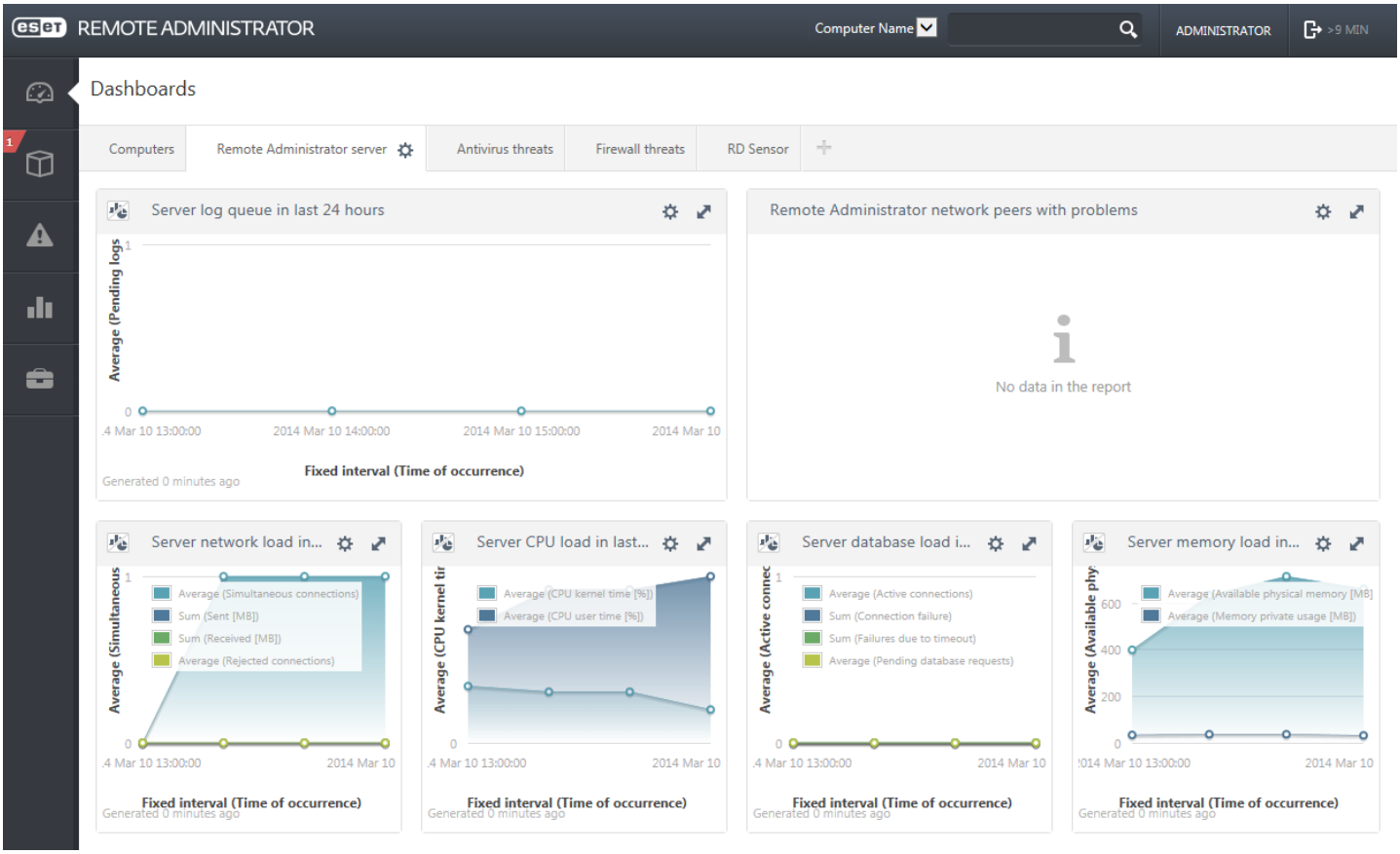
2.1 ESET Remote Administrator Server

ESET Remote Administrator Server est un composant principal d'ESET Remote Administrator. Il s'agit de l'application d'exécution qui traite toutes les données reçues des clients se connectant à cette dernière (par le biais d'ERA Agent). ERA Agent simplifie la communication entre le client et le serveur. Les données (journaux clients, configuration, réplication de l'agent et autres) sont stockées dans une base de données. Pour traiter correctement les données, ERA Server requiert une connexion stable à un serveur de base de données. Pour des performances optimales, Il est recommandé d'installer ERA Server et la base de données sur des serveurs distincts. L'ordinateur sur lequel ERA Server est installé doit être configuré pour accepter toutes les connexions des Agent/Proxy/RD Sensor qui sont vérifiées à l'aide de certificats. Après l'installation, vous pouvez ouvrir ERA Web Console qui se connecte à ERA Server (comme le montre le diagramme). À partir de la console Web, toutes les opérations d'ERA Server sont effectuées lors de la gestion des solutions de sécurité ESET dans votre environnement.

2.2 Console Web

ERA Web Console est une application dotée d'une interface utilisateur Web qui présente les données d'ERA Server et qui vous permet de gérer les solutions de sécurité ESET dans votre réseau. La console Web est accessible à l'aide d'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 à partir de presque n'importe quel emplacement ou périphérique.

Voici 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**, saisissez votre chaîne de recherche dans le champ de texte, puis cliquez sur le symbole de loupe ou appuyez sur **Entrante** pour lancer la recherche. Vous êtes alors redirigé vers la section **Groupes** dans laquelle le résultat de votre recherche est affiché.

REMARQUE : pour plus d'informations, reportez-vous au Guide de l'utilisateur d'ESET Remote Administrator.

2.3 Proxy

ERA Proxy est un autre composant d'ESET Remote Administrator qui a un double objectif. Dans le cas d'un réseau d'entreprise de taille moyenne qui comprend de nombreux clients (10 000 clients ou plus), ERA Proxy peut servir à répartir la charge entre plusieurs ERA Proxy, et décharger ainsi ERA Server. L'autre avantage d'ERA Proxy est que vous pouvez l'utiliser lors de la connexion à une filiale distante qui possède une liaison faible. Cela signifie qu'ERA Agent sur chaque client ne se connecte pas directement à ERA Server mais par le biais d'ERA Proxy qui se trouve sur le même réseau local que la filiale. Il libère ainsi la liaison de la filiale. ERA Proxy accepte les connexions de tous les ERA Agents locaux, compile leurs données et les charge sur ERA Server (ou un autre ERA Proxy). Votre réseau peut ainsi prendre en charge davantage de clients sans compromettre les performances du réseau et des requêtes de base de données.

Selon votre configuration réseau, ERA Proxy peut être connecté à un autre ERA Proxy puis à ERA Server.

Pour qu'ERA Proxy fonctionne correctement, l'ordinateur hôte sur lequel vous avez installé ERA Proxy doit disposer d'un ESET Agent et être connecté au niveau supérieur (ERA Server ou ERA Proxy supérieur, 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 sur tous les clients distants à partir d'un seul emplacement. L'Agent collecte les informations du 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 s'effectuent 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 est directement connecté au serveur.
2. L'Agent du client est connecté par le biais d'un proxy connecté au serveur.
3. L'Agent du client est connecté au serveur par le biais de plusieurs proxys.

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

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

2.5 RD Sensor

RD (Rogue Detection) Sensor est un composant d'ESET Remote Administrator conçu pour rechercher des ordinateurs sur votre réseau. Il offre un moyen pratique d'ajouter de nouveaux ordinateurs à ESET Remote Administrator sans avoir à les rechercher et à 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 les ordinateurs clients.

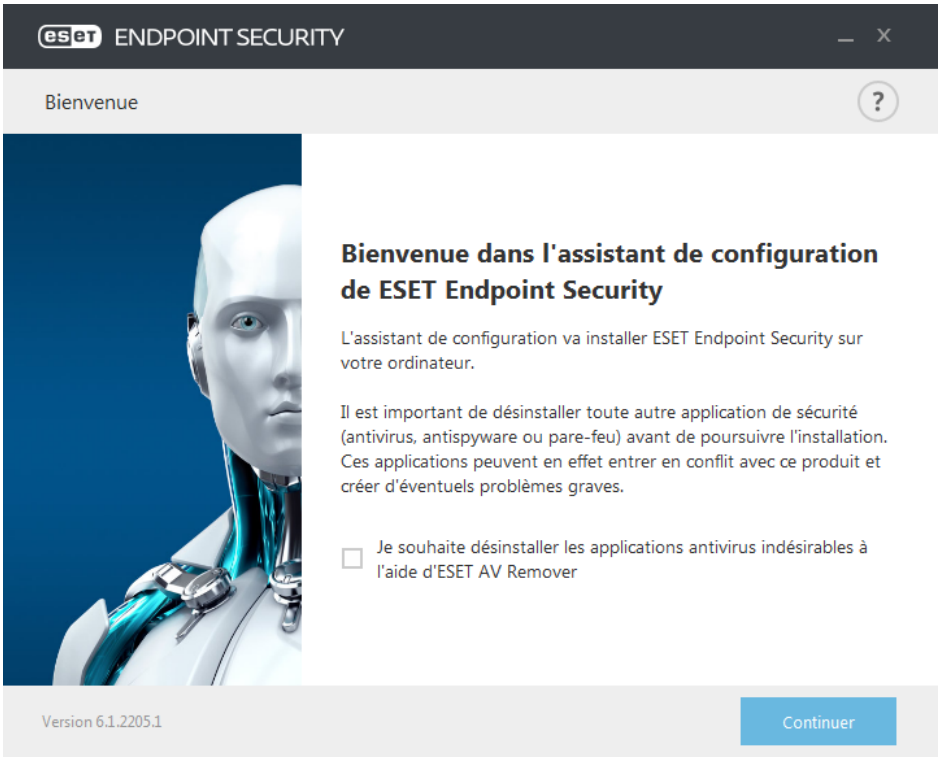
RD Sensor est un écouteur passif qui détecte les ordinateurs qui se trouvent sur le réseau et envoie des informations sur ces derniers à ERA Server. ERA Server évalue ensuite si les ordinateurs trouvés sur le réseau sont inconnus ou déjà gérés.

3. Utilisation d'ESET Endpoint Security uniquement

Cette section du guide de l'utilisateur est destinée aux utilisateurs qui emploient ESET Endpoint Security sans ESET Remote Administrator. Toutes les fonctions et fonctionnalités d'ESET Endpoint Security sont entièrement accessibles selon les droits du compte de l'utilisateur.

3.1 Installation à l'aide d'ESET AV Remover

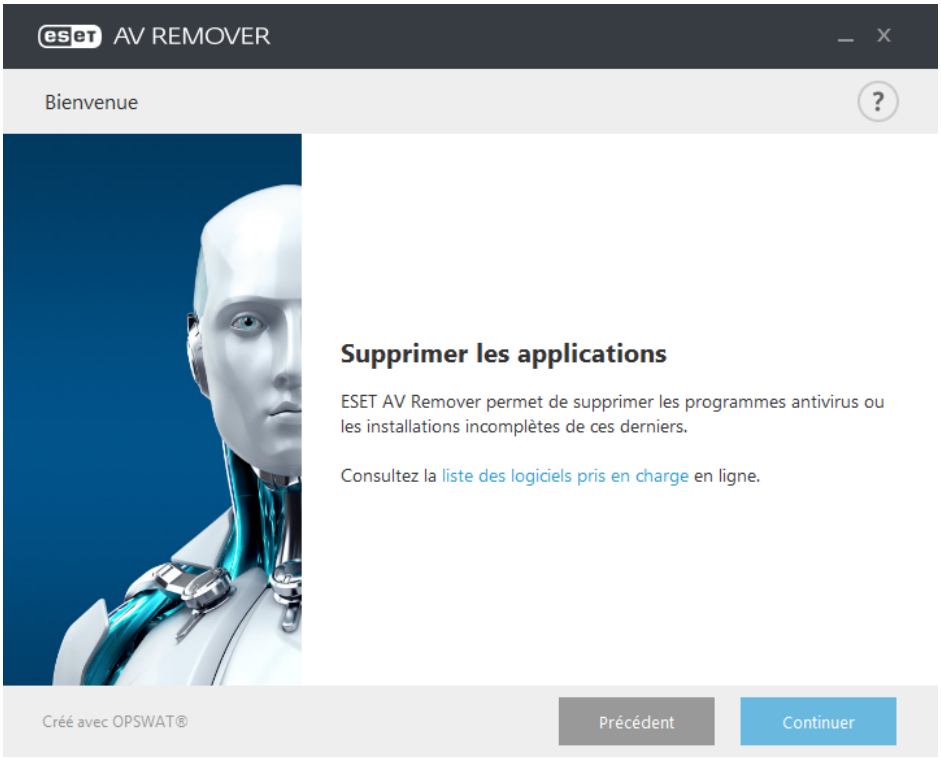
Avant de continuer la procédure d'installation, il est important de désinstaller toutes les applications de sécurité de l'ordinateur. Cochez la case en regard de l'option **Je souhaite désinstaller les applications antivirus indésirables à l'aide d'ESET AV Remover** pour qu'ESET AV Remover recherche toutes les applications de sécurité prises en charge sur votre système et les désinstalle. Ne cochez pas la case et cliquez sur **Continuer** pour installer ESET Endpoint Security sans exécuter ESET AV Remover.



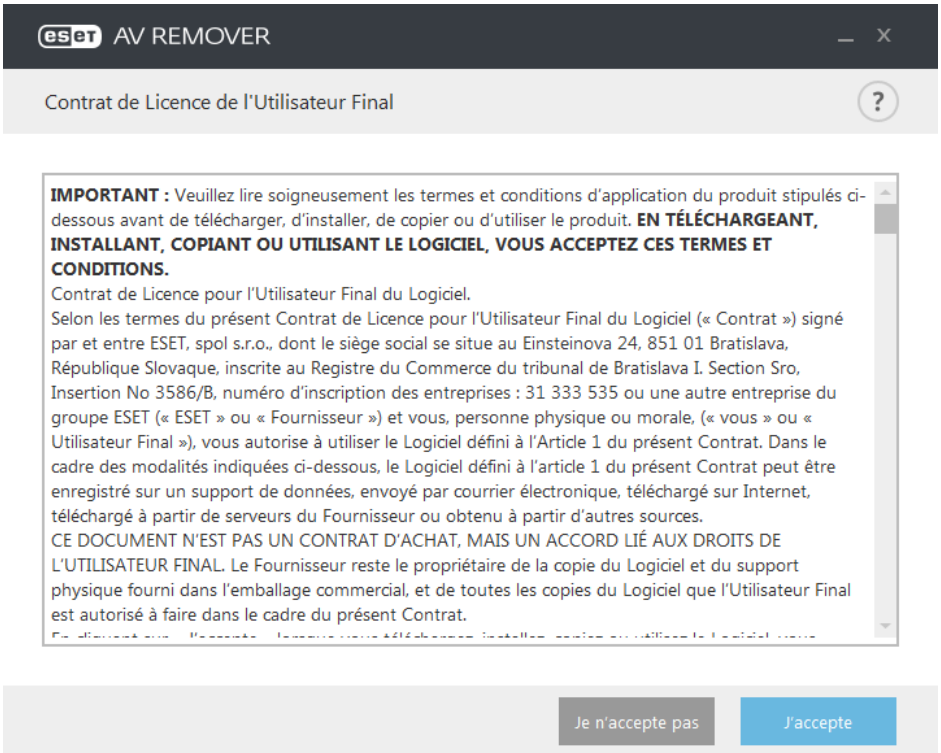
3.1.1 ESET AV Remover

L'outil ESET AV Remover permet de supprimer presque tous les logiciels antivirus précédemment installés sur votre système. Pour supprimer un programme antivirus existant à l'aide d'ESET AV Remover, suivez les instructions ci-après.

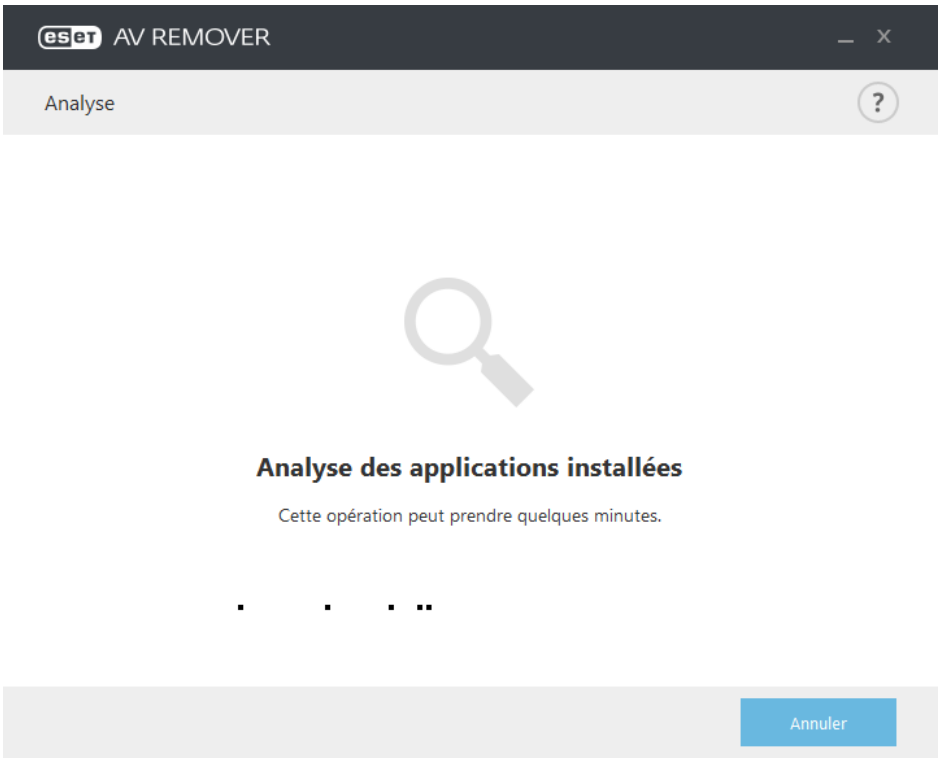
1. Pour afficher la liste des logiciels antivirus qu'ESET AV Remover peut supprimer, consultez l'article de la base de connaissances ESET.



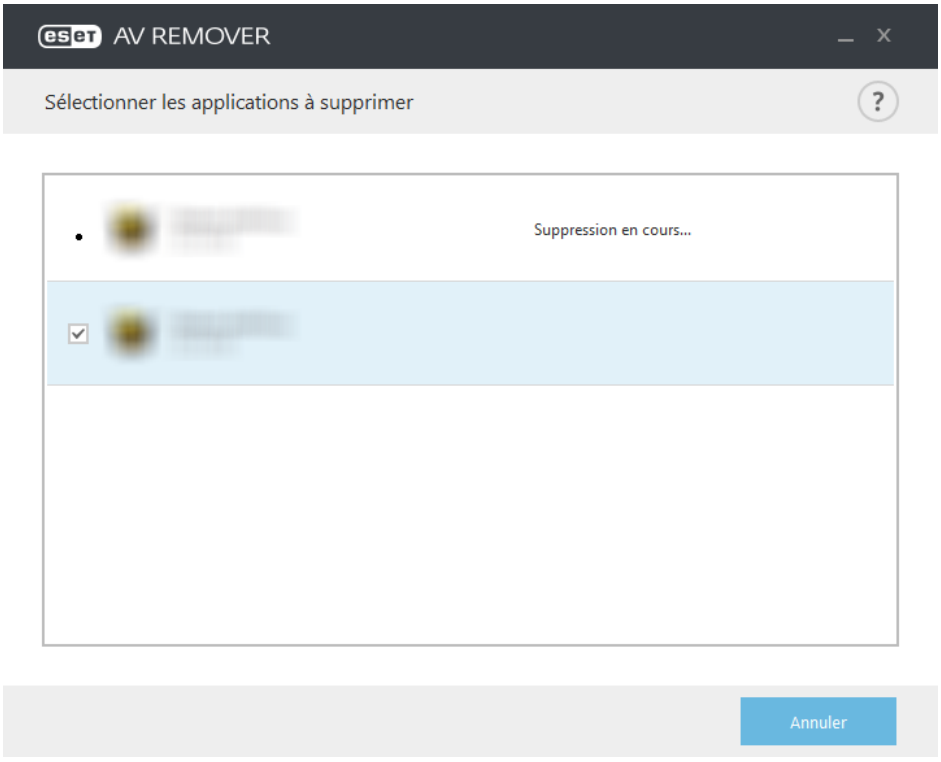
2. Lisez les termes du contrat de licence de l'utilisateur final, puis cliquez sur **Accepter** pour confirmer que vous les acceptez. Si vous cliquez sur **Refuser**, l'installation de ESET Endpoint Security continue sans la suppression des applications de sécurité existantes sur l'ordinateur.



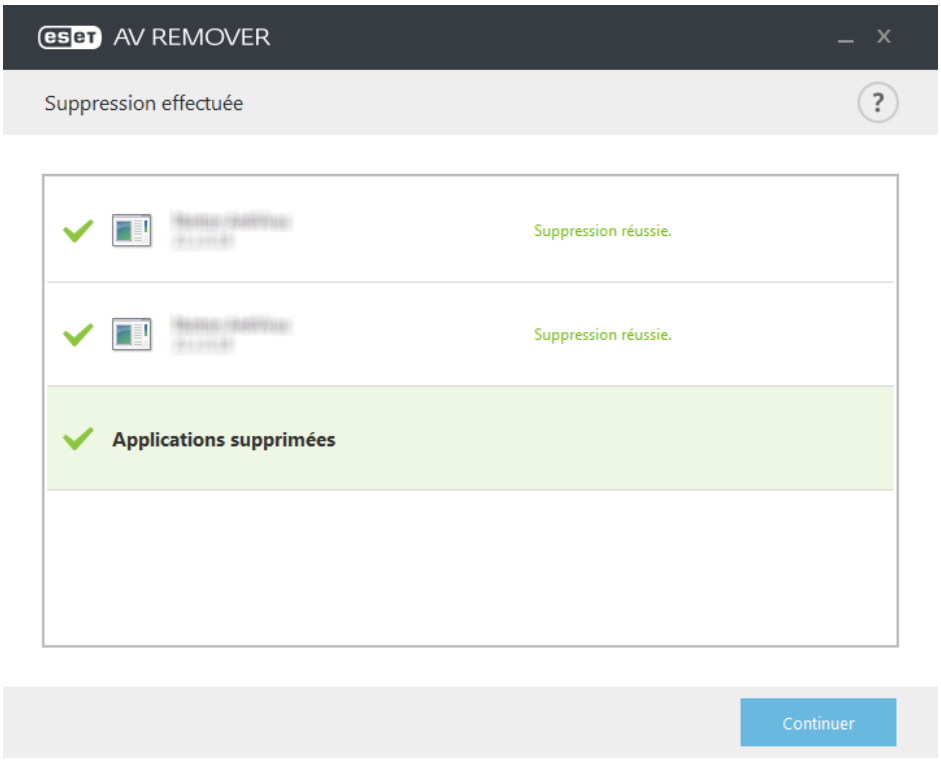
3. ESET AV Remover commence à rechercher les logiciels antivirus sur votre système.



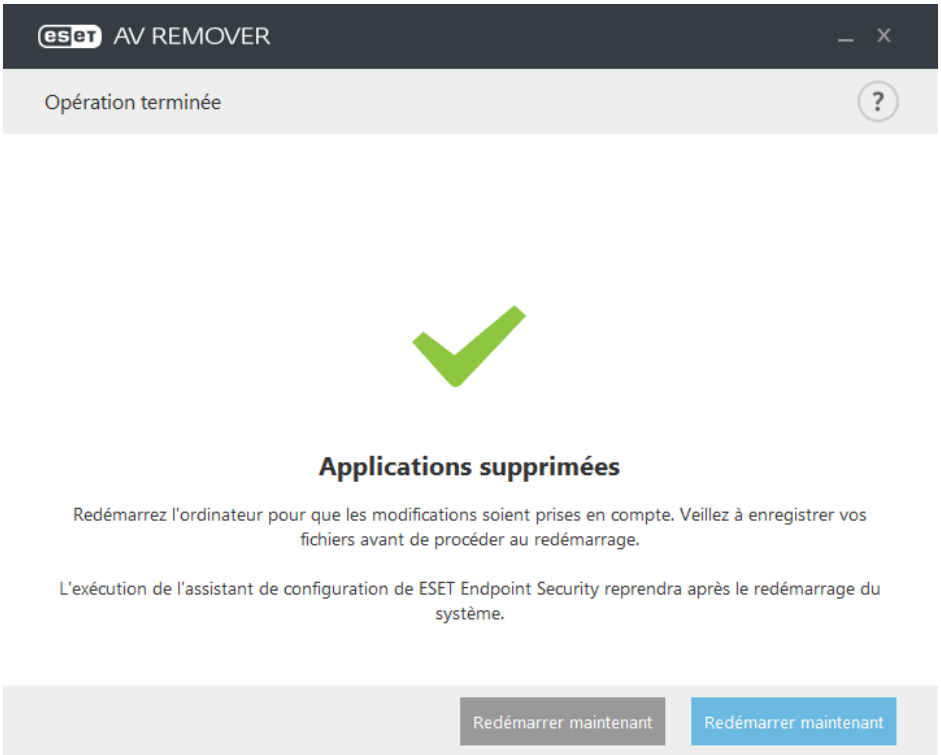
4. Sélectionnez les applications antivirus répertoriées, puis cliquez sur Supprimer. La suppression peut prendre quelques instants.



5. Lorsque la suppression est terminée, cliquez sur **Continuer**.



6. Redémarrez votre ordinateur pour que les modifications soient prises en compte, puis continuez l'installation de ESET Endpoint Security. Si la désinstallation échoue, reportez-vous à la section La désinstallation à l'aide d'ESET AV Remover a entraîné une erreur de ce guide.



3.1.2 La désinstallation à l'aide d'ESET AV Remover a entraîné une erreur

Si vous ne parvenez pas à désinstaller un programme antivirus à l'aide d'ESET AV Remover, une notification s'affiche pour vous signaler que l'application que vous essayez de désinstaller n'est peut-être pas prise en charge par ESET AV Remover. Consultez la liste des produits pris en charge ou les programmes de désinstallation pour les logiciels antivirus Windows courants dans la base de connaissances ESET pour déterminer si ce programme spécifique peut être désinstallé.

En cas d'échec de la désinstallation d'un produit de sécurité ou d'une désinstallation partielle de certains de ses composants, vous êtes invité à **redémarrer et relancer une analyse** de l'ordinateur. Confirmez le Contrôle de compte d'utilisateur (UAC) après le démarrage et continuez la procédure d'analyse et de désinstallation.

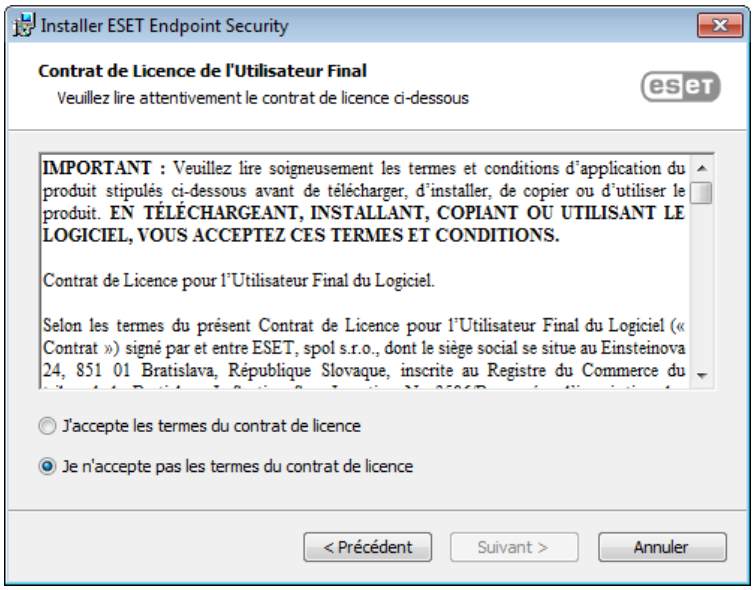
Si nécessaire, contactez le service client ESET pour effectuer une demande d'assistance. Ayez à disposition le fichier **AppRemover.log** pour aider les techniciens ESET. Le fichier **AppRemover.log** est situé dans le dossier **eset**. Naviguez jusqu'au répertoire *%TEMP%* dans l'Explorateur Windows pour accéder à ce dossier. Le service client ESET tentera le plus rapidement possible de résoudre votre problème.

3.2 Installation

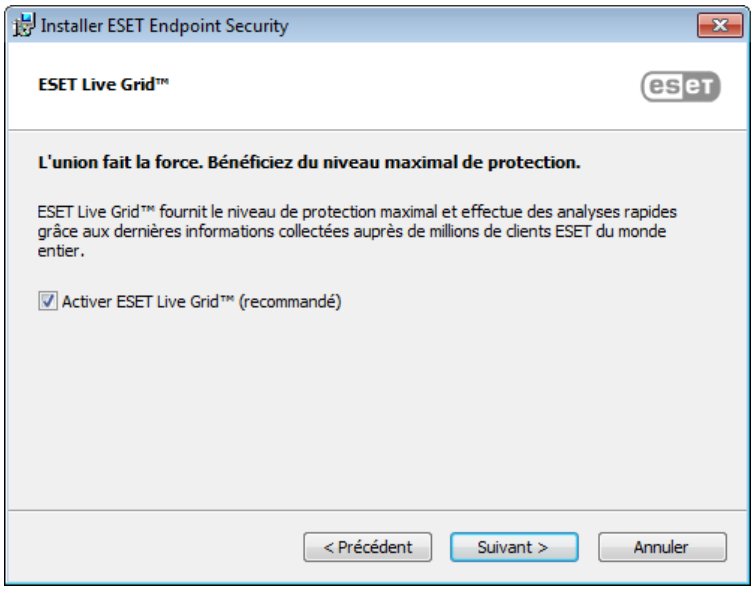
Lorsque vous lancez le programme d'installation, l'assistant d'installation vous guide tout au long du processus d'installation.

Important : Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si plusieurs solutions antivirus sont installées sur un même ordinateur, elles risquent de provoquer des conflits. Nous recommandons de désinstaller tout autre antivirus de votre système. Reportez-vous à notre article de la base de connaissances pour obtenir une liste des outils de désinstallation des logiciels antivirus courants (disponible en anglais et dans plusieurs autres langues).

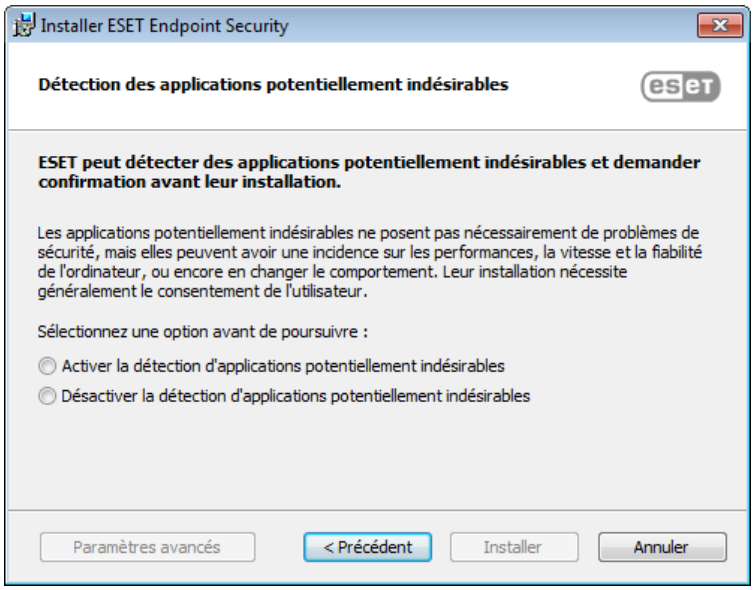
Le contrat de licence de l'utilisateur final (CLUF) apparaît à l'étape suivante. Veuillez en prendre connaissance, puis cliquez sur **Accepter** pour confirmer que vous acceptez les clauses du contrat de licence de l'utilisateur final. Après avoir accepté les termes du contrat, cliquez sur **Suivant** pour poursuivre l'installation.



Une fois que vous avez sélectionné J'accepte... et cliqué sur **Suivant**, vous êtes invité à configurer ESET Live Grid. ESET Live Grid contribue à garantir qu'ESET est informé immédiatement et en continu des nouvelles infiltrations, afin de protéger ses clients. Le système permet de soumettre les nouvelles menaces au laboratoire d'ESET, où elles sont analysées, traitées, puis ajoutées à la base des signatures de virus.



L'étape suivante du processus d'installation consiste à configurer la détection des applications potentiellement indésirables qui ne sont pas nécessairement malveillantes, mais peuvent avoir une incidence négative sur le comportement du système d'exploitation. Reportez-vous au chapitre Applications potentiellement indésirables pour plus d'informations. Vous pouvez accéder à d'autres paramètres en cliquant sur **Paramètres avancés** (pour installer par exemple votre produit ESET dans un dossier spécifique ou activer l'analyse automatique après l'installation).



La dernière étape consiste à confirmer l'installation en cliquant sur **Installer**.

3.2.1 Installation avancée

L'installation avancée permet de personnaliser certains paramètres d'installation qui ne sont pas disponibles lors d'une installation standard.

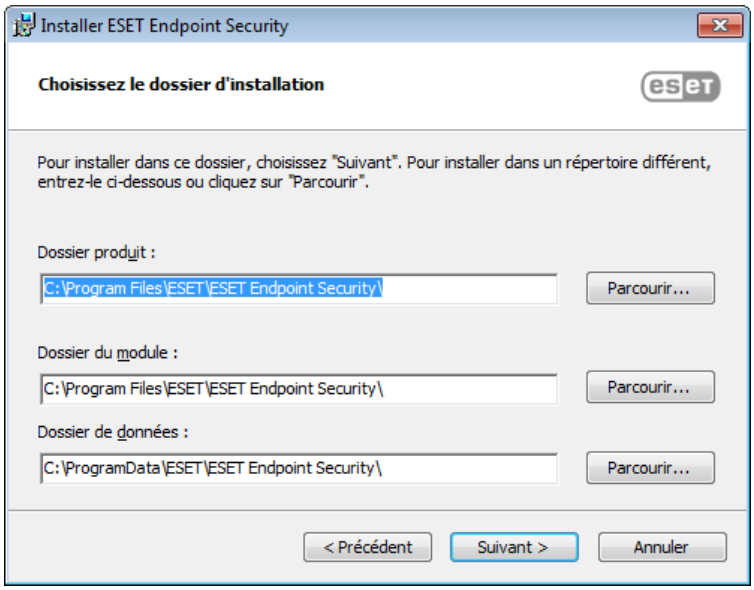
Une fois que vous avez sélectionné votre préférence pour la détection des applications potentiellement indésirables et que vous avez cliqué sur **Paramètres avancés**, vous êtes invité à sélectionner un emplacement pour le dossier d'installation du produit. Par défaut, le système installe le programme dans le répertoire suivant :

C:\Program Files\ESET\ESET Endpoint Security

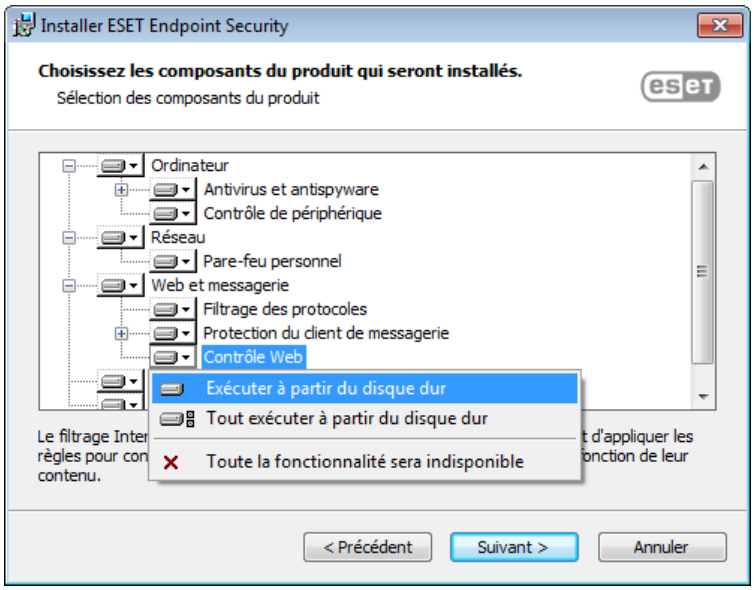
Vous pouvez indiquer un emplacement pour les modules et les données du programme. Par défaut, ils sont installés dans les répertoires respectifs suivants :

C:\Program Files\ESET\ESET Endpoint Security
C:\ProgramData\ESET\ESET Endpoint Security

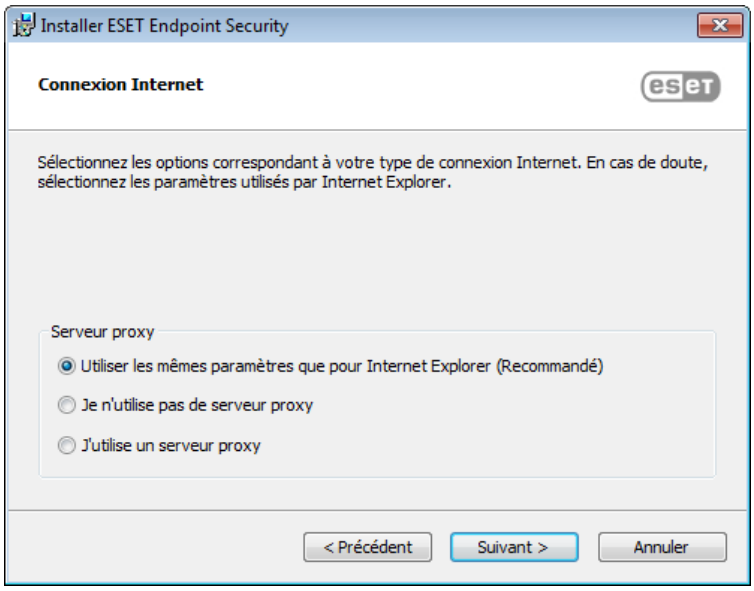
Cliquez sur **Parcourir...** pour changer ces emplacements (non recommandé).



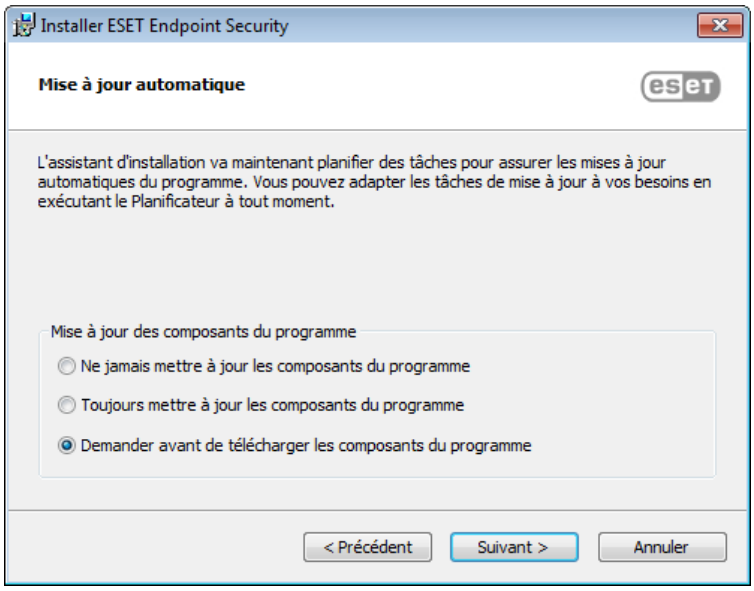
Dans la fenêtre suivante, vous pouvez sélectionner quels composants du produit à installer. Les composants du produit de la section Ordinateur comprennent la protection en temps réel du système de fichiers, l'analyse d'ordinateur, la protection des documents et le contrôle de périphérique. Notez que les deux premiers composants sont obligatoires pour que la solution de sécurité puisse fonctionner. La section Réseau permet d'installer le pare-feu personnel qui surveille toutes les connexions au réseau entrantes et sortantes et applique des règles pour chaque connexion au réseau. Le pare-feu personnel offre aussi une protection contre les attaques d'ordinateurs distants. Les composants de la section Internet et messagerie sont chargés de votre protection lorsque vous naviguez sur Internet et communiquez par messagerie. Le composant Miroir de mise à jour peut être utilisé pour mettre à jour les autres ordinateurs du réseau. La section Prise en charge de Microsoft NAP fournit un agent d'ESET pour assurer une compatibilité complète avec l'architecture NAP.



Pour configurer les paramètres du serveur proxy, sélectionnez l'option **J'utilise un serveur proxy** et cliquez sur **Suivant**. Entrez l'adresse IP ou l'adresse URL de votre serveur proxy dans le champ **Adresse**. Si vous ne savez pas exactement si vous utilisez ou non un serveur proxy pour la connexion à Internet, sélectionnez **Utiliser les mêmes paramètres qu'Internet Explorer (option recommandée)** et cliquez sur **Suivant**. Si vous n'utilisez pas de serveur proxy, sélectionnez **Je n'utilise pas de serveur proxy**. Pour plus d'informations, reportez-vous à la section Serveur proxy.

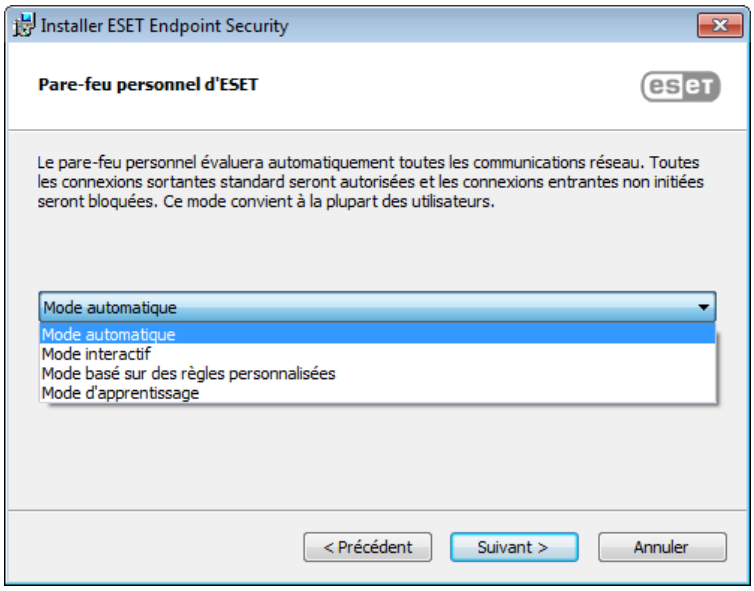


L'installation personnalisée permet de définir la façon dont le système gère les mises à jour automatiques du programme. Cliquez sur **Changer...** pour accéder aux paramètres avancés.

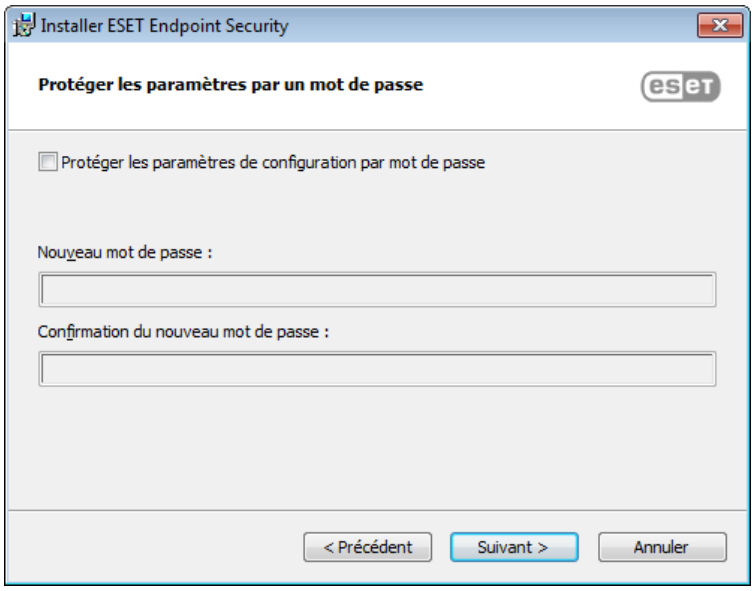


Si vous ne voulez pas que les composants du programme soient mis à jour, sélectionnez **Ne jamais mettre à jour les composants du programme**. Sélectionnez **Demander avant de télécharger les composants du programme** pour afficher une fenêtre de confirmation chaque fois que le système essaie de télécharger les composants du programme. Pour télécharger les mises à niveau des composants du programme, sélectionnez **Toujours mettre à jour les composants du programme**.

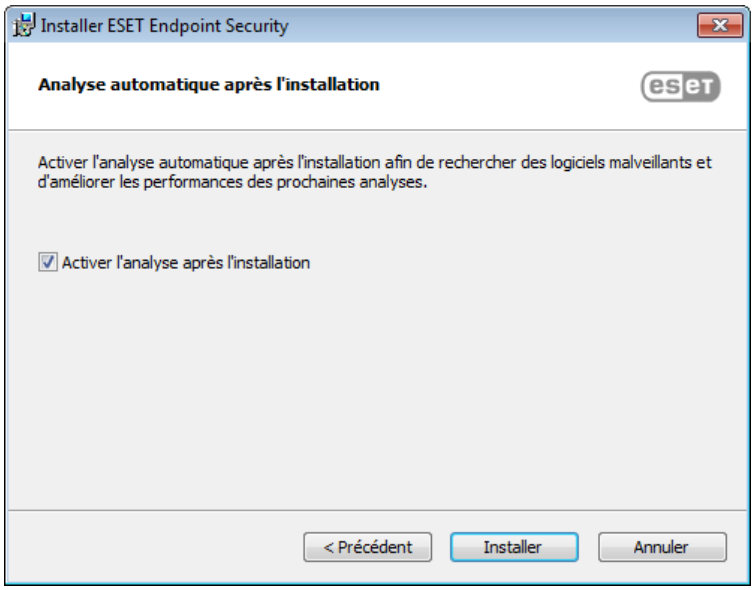
Sélectionnez ensuite un mode de filtrage pour le pare-feu personnel ESET. Quatre modes de filtrage sont disponibles pour le pare-feu personnel d'ESET Endpoint Security. Le comportement du pare-feu change en fonction du mode sélectionné. Les modes de filtrage affectent également le niveau d'interaction de l'utilisateur.



La fenêtre suivante de l'installation permet d'indiquer un mot de passe afin de protéger les paramètres du programme. Sélectionnez **Protéger la configuration par mot de passe** et entrez votre mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**. Ce mot de passe vous sera demandé pour modifier les paramètres d'ESET Endpoint Security ou pour y accéder. Si les deux mots de passe correspondent, cliquez sur **Suivant** pour continuer.



Pour désactiver la première analyse après l'installation qui est normalement exécutée après l'installation, désactivez la case à cocher en regard de **Activer l'analyse après l'installation**.



Cliquez sur **Installer** pour démarrer l'installation.

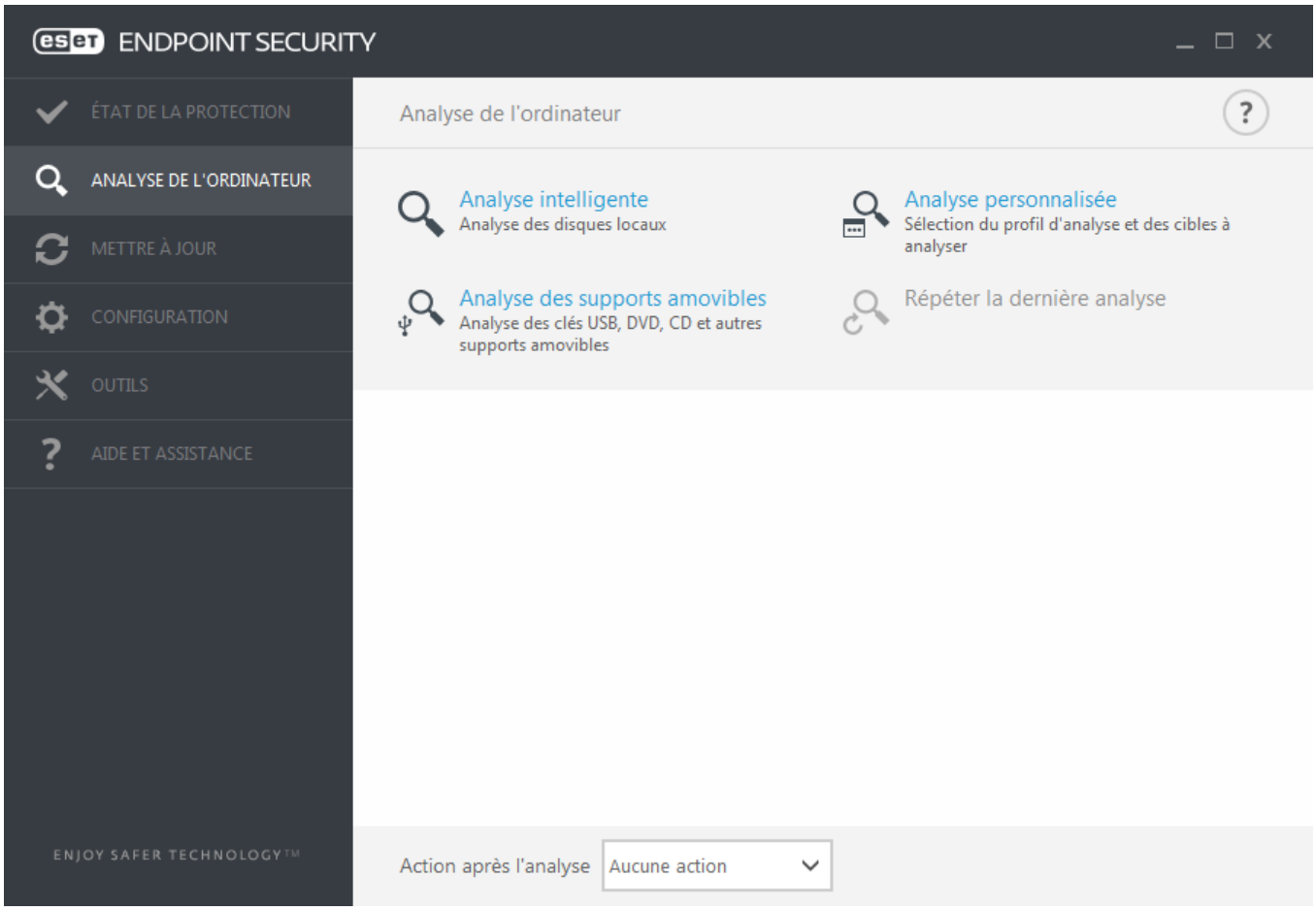
3.3 Activation du produit

Une fois l'installation terminée, vous êtes invité à activer le produit.

Sélectionnez l'une des méthodes disponibles pour activer ESET Endpoint Security. Pour plus d'informations, reportez-vous à la section Comment activer ESET Endpoint Security.

3.4 Analyse d'ordinateur

Dans les 15 minutes qui suivent l'installation (un redémarrage de l'ordinateur peut être nécessaire), ESET Endpoint Security effectue automatiquement une analyse de l'ordinateur. En plus de l'analyse initiale, il est recommandé d'effectuer des analyses régulières de l'ordinateur ou de planifier une analyse régulières pour détecter les menaces éventuelles. Dans la fenêtre principale du programme, cliquez sur **Analyse d'ordinateur**, puis sur **Analyse intelligente**. Pour plus d'informations sur l'analyse d'ordinateur, reportez-vous à la section Analyse d'ordinateur.



3.5 Mise à niveau vers une nouvelle version

Les nouvelles versions d'ESET Endpoint Security offrent des améliorations ou apportent des solutions aux problèmes que les mises à jour automatiques des modules ne peuvent pas résoudre. La mise à niveau vers une nouvelle version peut s'effectuer de différentes manières :

1. Automatiquement, par l'intermédiaire d'une mise à jour du programme.
   Les mises à niveau du programme sont distribuées à tous les utilisateurs et peuvent avoir un impact sur certaines configurations système. Elles sont par conséquent mises à disposition après de longues périodes de test afin que leur fonctionnement correct soit garanti sur toutes les configurations système. Pour effectuer la mise à niveau vers une nouvelle version dès que celle-ci est disponible, utilisez l'une des méthodes ci-dessous.
2. Manuellement, en téléchargeant la nouvelle version et en l'installant sur l'installation précédente.
3. Manuellement, avec déploiement automatique sur un réseau par l'intermédiaire d'ESET Remote Administrator.

3.6 Guide du débutant

Ce chapitre donne un premier aperçu d'ESET Endpoint Security et de ses paramètres de base.

3.6.1 Interface utilisateur

La fenêtre principale d'ESET Endpoint Security est divisée en deux sections principales. La fenêtre principale de droite affiche les informations correspondant à l'option sélectionnée dans le menu principal à gauche.

Voici une description des options disponibles dans le menu principal :

État de la protection - Fournit des informations sur l'état de protection d'ESET Endpoint Security.

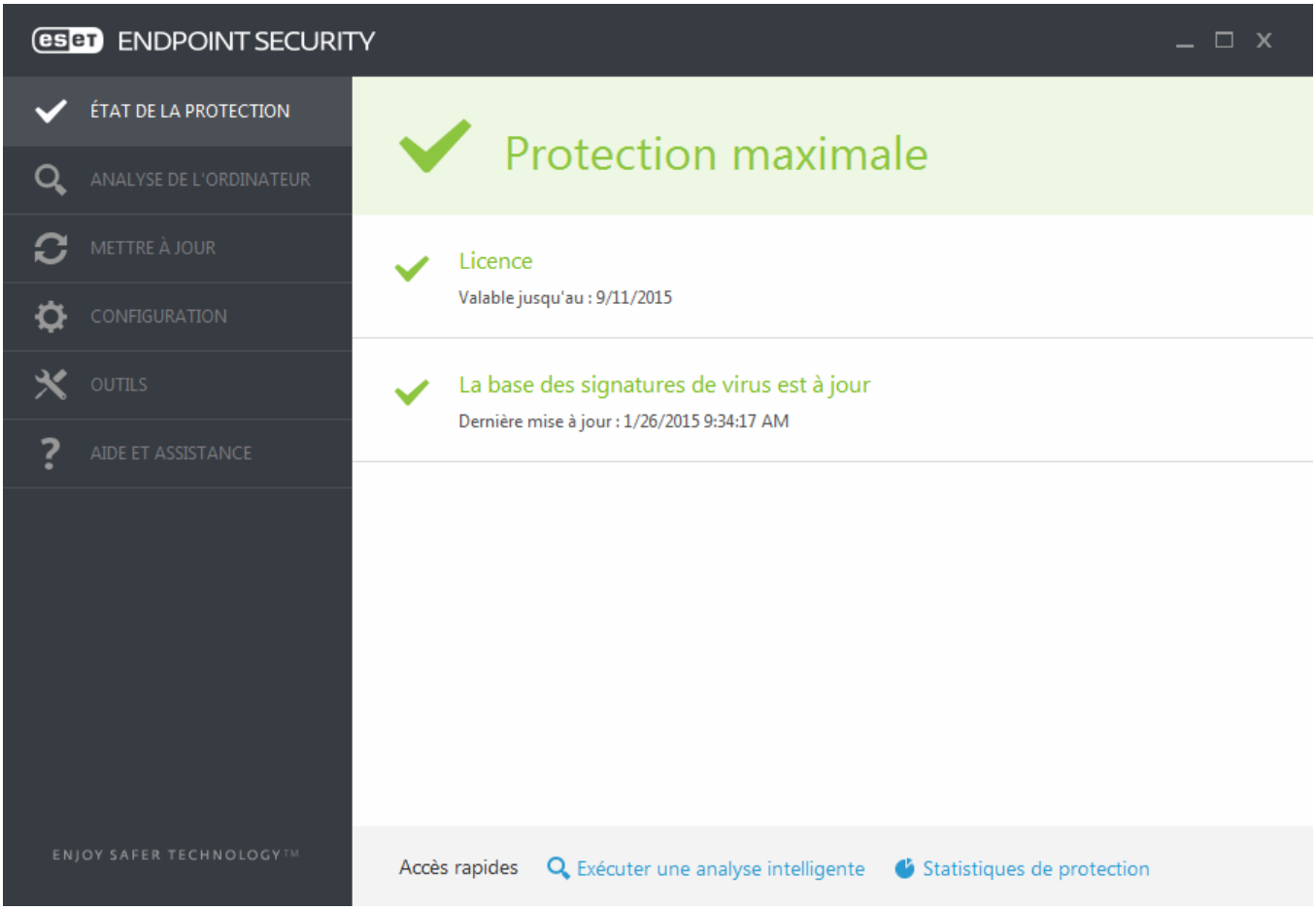
Analyse de l'ordinateur - Cette option permet de configurer et de lancer l'analyse intelligente, l'analyse personnalisée ou l'analyse de supports amovibles. Vous pouvez également répéter la dernière analyse effectuée.

Mise à jour - Affiche des informations sur la base des signatures de virus.

Configuration - Sélectionnez cette option pour régler les paramètres de sécurité de l'ordinateur, du réseau ou de l'Internet et de la messagerie.

Outils - Permet d'accéder aux fichiers journaux, aux statistiques de protection, à la surveillance de l'activité, aux processus en cours, à la quarantaine, aux connexions réseau, à ESET SysInspector et à ESET SysRescue pour créer un CD de sauvetage. Vous pouvez également soumettre un échantillon pour analyse.

Aide et assistance - Permet d'accéder aux fichiers d'aide, à la base de connaissances ESET et au site Web d'ESET. Des liens sont également proposés pour ouvrir une requête auprès du service client et pour accéder à des outils d'assistance et des informations sur l'activation du produit.



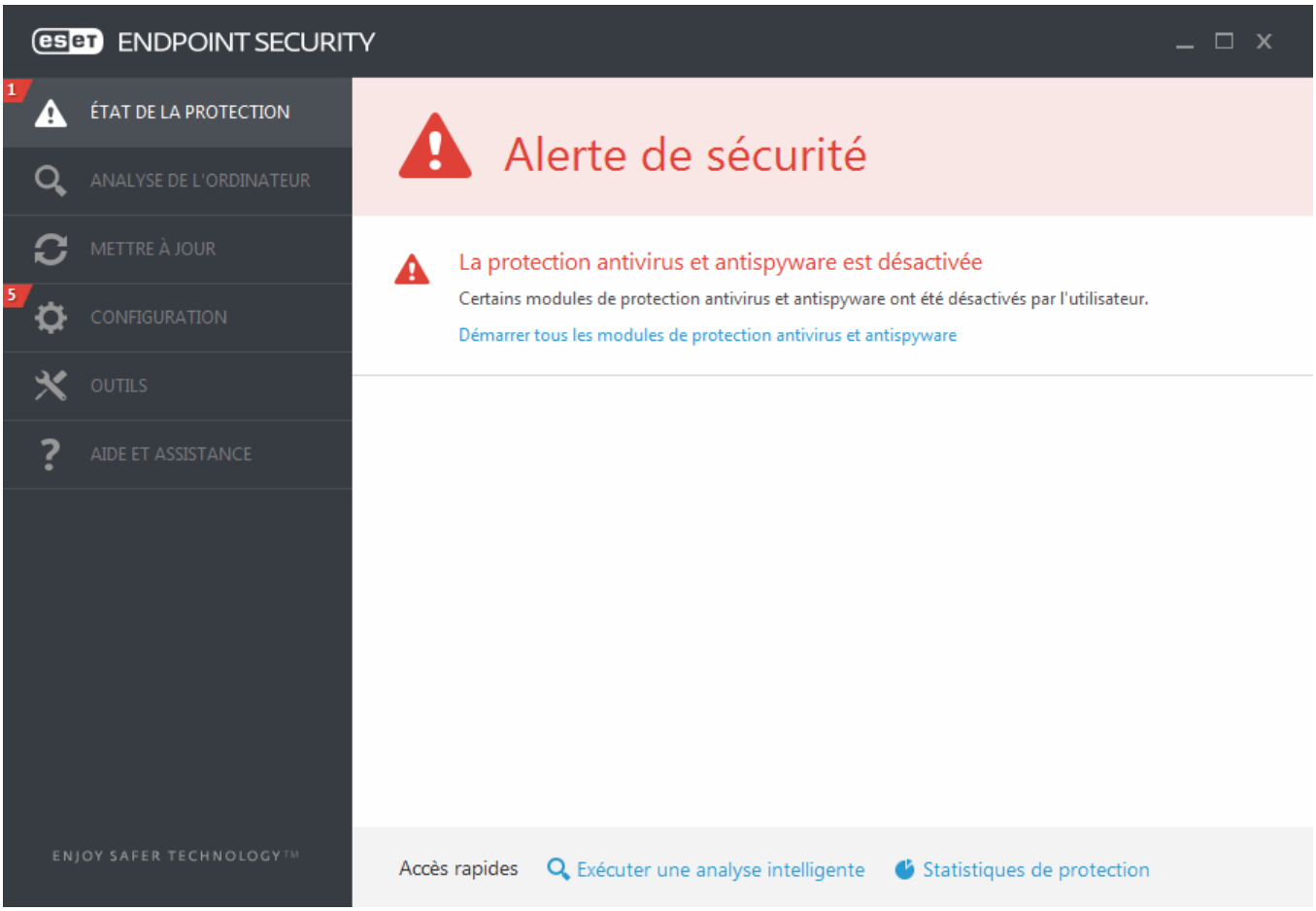
L'écran **État de la protection** vous informe sur le niveau actuel de sécurité et de protection de l'ordinateur. L'icône verte d'état **Protection maximale** indique qu'une protection maximale est assurée.

La fenêtre d'état contient également des liens rapides vers les fonctionnalités fréquemment utilisées dans ESET

Endpoint Security et des informations sur la dernière mise à jour.

Que faire lorsque le programme ne fonctionne pas correctement ?

Une coche verte s'affiche en regard de chaque module activé et fonctionnant correctement. Dans le cas contraire, un point d'exclamation rouge ou orange s'affiche. Des informations supplémentaires sur le module s'affichent dans la partie supérieure de la fenêtre. Une suggestion de solution pour corriger le module est également affichée. Pour changer l'état d'un module, cliquez sur **Configuration** dans le menu principal puis sur le module souhaité.



L'icône rouge contenant un point d'exclamation « ! » signale des problèmes critiques ; la protection maximale de votre ordinateur n'est pas assurée. Les raisons possibles sont les suivantes :

- **Protection antivirus et antispyware désactivée** - Vous pouvez réactiver la protection antivirus et antispyware en cliquant sur **Activer la protection en temps réel** dans le volet **État de la protection** ou sur **Activer la protection antivirus et antispyware** dans le volet **Configuration** de la fenêtre principale du programme.
- **Le pare-feu personnel d'ESET est désactivé** - Ce problème est signalé par une icône rouge et une notification de sécurité en regard de l'élément **Réseau**. Vous pouvez réactiver la protection réseau en cliquant sur **Activer le mode de filtrage**.
- **La base des signatures de virus n'est plus à jour** - Vous utilisez une base des signatures de virus obsolète.
- **Le produit n'est pas activé** ou **Licence arrivée à expiration** - Cette information est indiquée par l'icône d'état de la protection qui devient rouge. Le programme ne peut plus effectuer de mise à jour après expiration de la licence. Nous vous recommandons de suivre les instructions de la fenêtre d'alerte pour renouveler la licence.

L'icône orange contenant un « i » signale que votre produit ESET nécessite votre attention en raison d'un problème non critique. Les raisons possibles sont les suivantes :

- **La protection de l'accès Web est désactivée** - Vous pouvez réactiver la protection de l'accès Web en cliquant sur la notification de sécurité, puis sur **Activer la protection de l'accès Web**.
- **Votre licence va arriver prochainement à expiration** - Cette information est donnée par l'icône d'état de protection qui affiche un point d'exclamation. Après l'expiration de votre licence, le programme ne peut plus se

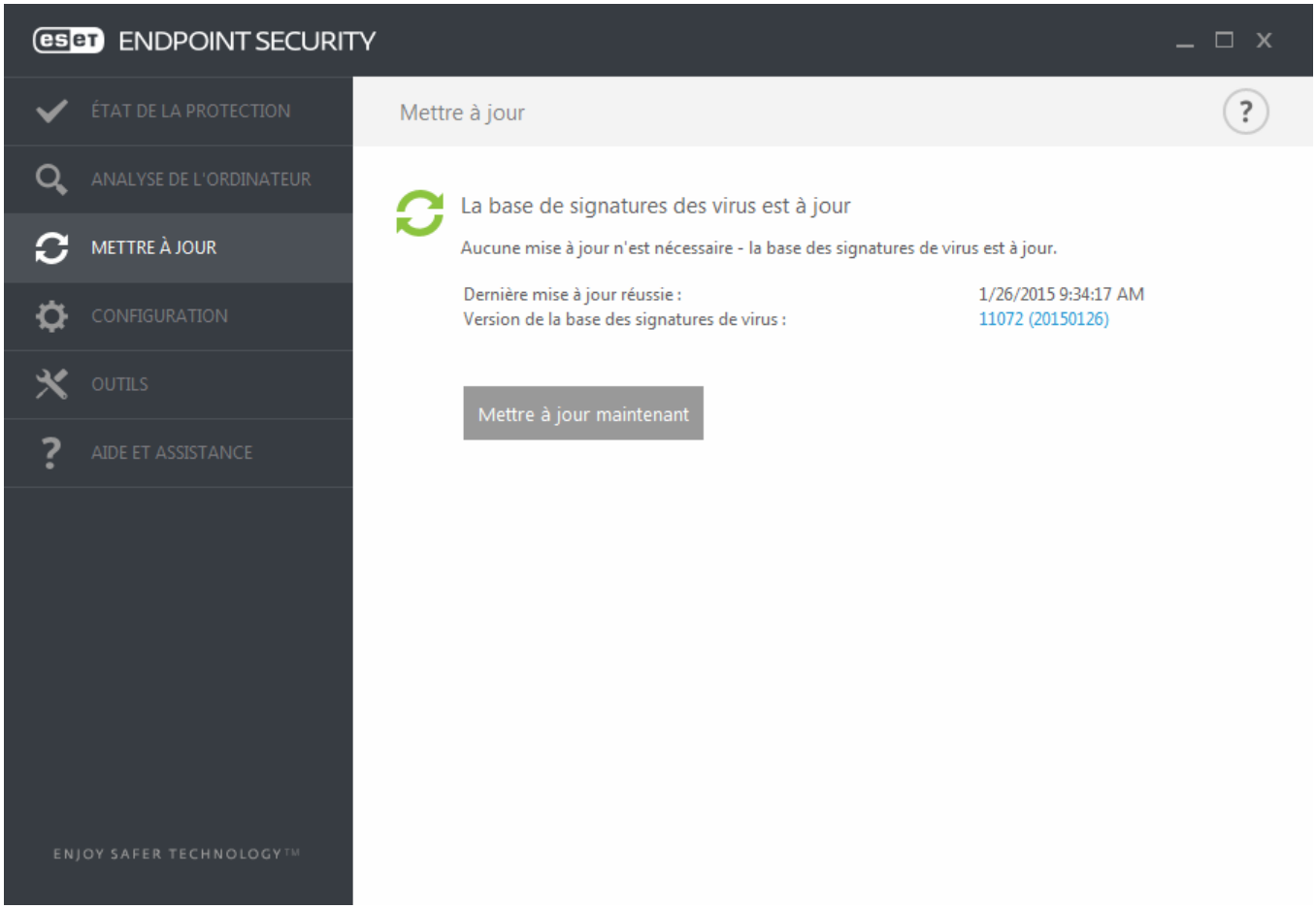
mise à jour et l'icône d'état de la protection devient rouge.

Si vous ne parvenez pas à résoudre le problème à l'aide des solutions suggérées, cliquez sur **Aide et assistance** pour accéder aux fichiers d'aide ou pour effectuer des recherches dans la base de connaissances ESET. Si vous avez encore besoin d'aide, vous pouvez soumettre une demande au service client d'ESET. Ce dernier répondra très rapidement à vos questions et vous permettra de trouver une solution.

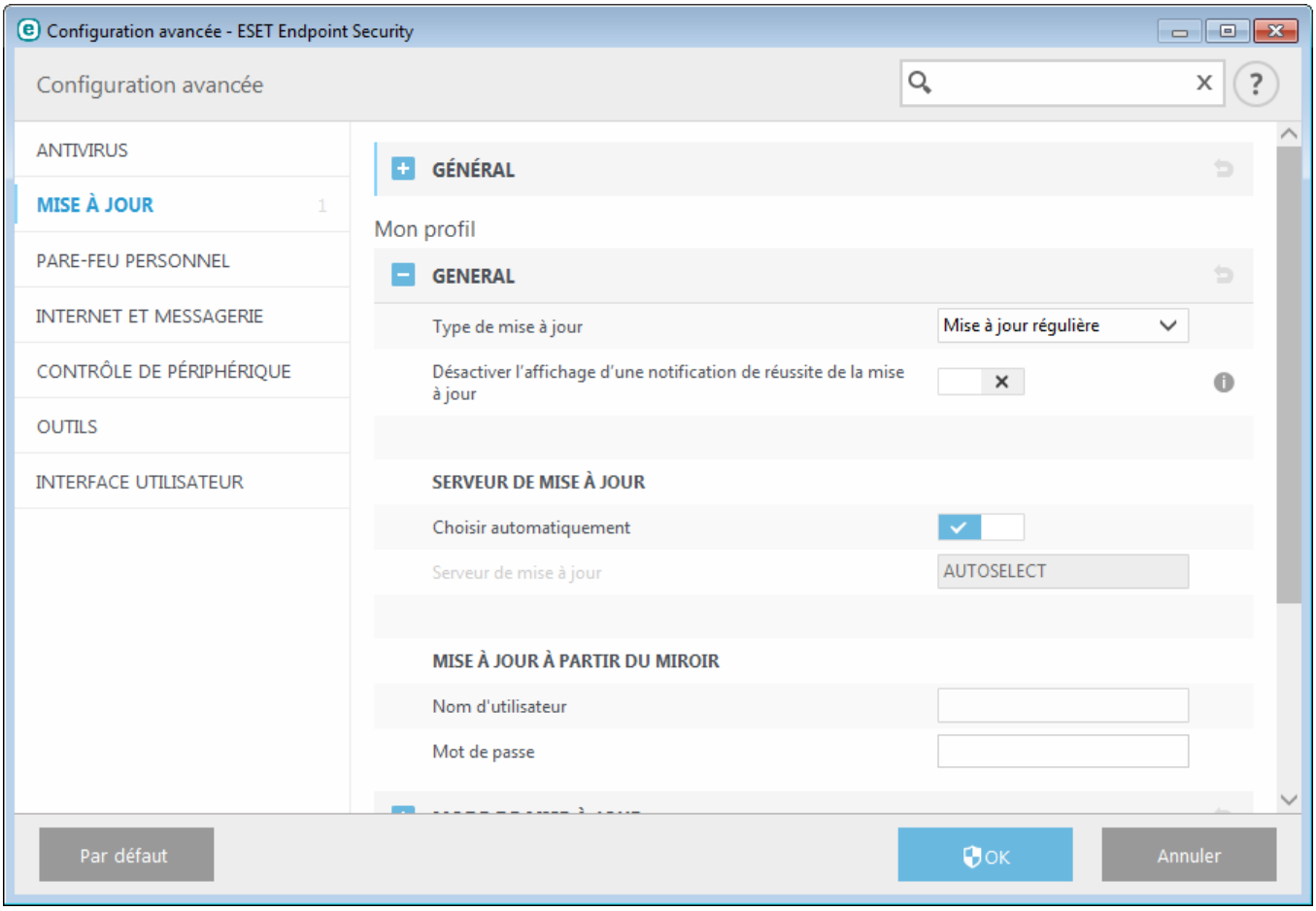
3.6.2 Configuration des mises à jour

La mise à jour de la base des signatures de virus et celle des composants du programme sont des opérations importantes qui assurent la protection totale contre les attaques des codes malveillants. Il convient donc d'apporter une grande attention à la configuration et au fonctionnement des mises à jour. Dans le menu principal, sélectionnez **Mettre à jour** > **Mettre à jour maintenant** pour rechercher toute nouvelle mise à jour de la base de données.

Si votre **clé de licence** n'est pas encore saisie, vous ne serez pas en mesure de recevoir de nouvelles mises à jour. Vous serez en outre invité à activer votre produit.



La fenêtre Configuration avancée (dans le menu principal, cliquez sur **Configuration** > **Configuration avancée** ou appuyez sur la touche F5 de votre clavier) comporte d'autres options de mise à jour. Pour configurer les options avancées de mise à jour telles que le mode de mise à jour, l'accès au serveur proxy, les connexions LAN et les paramètres de création de copies de signature de virus, cliquez sur **Mettre à jour** dans l'arborescence Configuration avancée. En cas de problème de mise à jour, cliquez sur **Effacer** pour effacer le cache de mise à jour temporaire. Le menu **Serveur de mise à jour** est défini par défaut sur **SÉLECTION AUTOMATIQUE**. Lors de l'utilisation d'un serveur ESET, il est recommandé de conserver l'option **Choisir automatiquement**. Si vous ne souhaitez pas afficher les notifications de la barre d'état système dans l'angle inférieur droit de l'écran, sélectionnez **Désactiver l'affichage d'une notification de réussite de la mise à jour**.



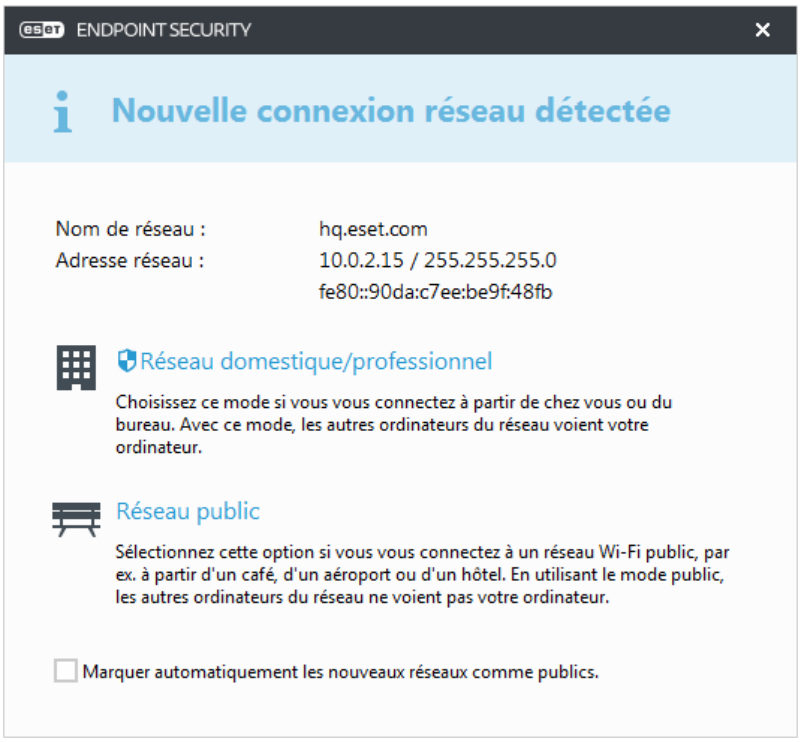
Le programme doit être mis à jour automatiquement pour assurer un fonctionnement optimal. Cela n'est possible que si la **clé de licence** correcte est entrée dans **Aide et assistance** > **Activer le produit**.

Si vous n'avez pas entré votre clé de licence après l'installation, vous pouvez le faire à tout moment. Pour plus d'informations sur l'activation, reportez-vous à la section Comment activer ESET Endpoint Security, puis entrez les informations d'identification que vous avez reçues avec votre produit de sécurité ESET dans la fenêtre Détails de la licence.

3.6.3 Configuration de zones

Des zones Fiables doivent être configurées pour que la protection de votre ordinateur dans un réseau soit activée. Vous pouvez autoriser d'autres utilisateurs à accéder à votre ordinateur en configurant une zone Fiable et en autorisant le partage. Cliquez sur **Configuration avancée** (F5) > **Pare-feu personnel** > **Zones** pour accéder aux paramètres des zones Fiables.

La détection de la zone Fiable s'effectue après l'installation de ESET Endpoint Security et dès que votre ordinateur se connecte à un nouveau réseau. Il n'est donc généralement pas nécessaire de définir la zone Fiable. Par défaut, la boîte de dialogue s'ouvre à la détection d'une nouvelle zone et vous permet d'en définir le niveau de protection.



Avertissement : une configuration incorrecte de la zone Fiable peut compromettre la sécurité de votre ordinateur.

REMARQUE : par défaut, les postes de travail d'une zone Fiable sont autorisés à accéder aux fichiers et imprimantes partagés, disposent de la communication RPC entrante activée et peuvent bénéficier du partage de bureau à distance.

3.6.4 Outils du filtrage Internet

Si vous avez activé le filtrage Internet dans ESET Endpoint Security, vous devez encore le configurer pour les comptes d'utilisateur souhaités afin que le filtrage Internet fonctionne correctement. Reportez-vous au chapitre Filtrage Internet pour obtenir des instructions afin de créer des restrictions spécifiques pour les stations de travail clientes en vue de les protéger contre tout contenu pouvant être choquant.

3.7 Questions fréquentes

Ce chapitre traite des questions et des problèmes les plus fréquents. Cliquez sur l'intitulé d'une rubrique pour savoir comment résoudre le problème :

Comment mise à jour ESET Endpoint Security
Comment activer ESET Endpoint Security
Comment utiliser les informations d'identification actuelles pour activer un nouveau produit
Comment éliminer un virus de mon PC
Comment autoriser la communication pour une certaine application
Comment créer une tâche dans le Planificateur
Comment programmer une tâche d'analyse (toutes les 24 heures)
Comment connecter mon produit à ESET Remote Administrator
Comment configurer un miroir

Si votre problème n'est pas traité dans les pages d'aide répertoriées ci-dessus, essayez d'effectuer une recherche par mot-clé ou expression décrivant votre problème dans les pages d'aide d'ESET Endpoint Security.

Si vous ne trouvez pas la solution à votre problème dans les pages d'aide, consultez la base de connaissances ESET qui contient les réponses aux problèmes et questions courants.

Comment supprimer le cheval de Troie Sirefef (ZeroAccess) ?
Mettre à jour la liste de contrôle pour le dépannage du miroir
Quels ports et adresses dois-je ouvrir sur mon pare-feu tiers pour autoriser les fonctionnalités complètes du produit ESET ?

Au besoin, vous pouvez contacter notre centre d'assistance technique en ligne pour soumettre vos questions ou problèmes. Vous trouverez le lien vers notre formulaire de contact en ligne dans le volet **Aide et assistance** de la fenêtre principale du programme.

3.7.1 Comment mettre à jour ESET Endpoint Security

La mise à jour de ESET Endpoint Security peut être effectuée manuellement ou automatiquement. Pour déclencher la mise à jour, cliquez sur **Mettre à jour maintenant** dans la section **Mise à jour** du menu principal.

Les paramètres d'installation par défaut créent une tâche de mise à jour automatique qui s'exécute chaque heure. Pour changer l'intervalle, accédez à **Outils** > **Planificateur** (pour plus d'informations sur le Planificateur, cliquez ici).

3.7.2 Comment activer ESET Endpoint Security

Une fois l'installation terminée, vous êtes invité à activer le produit.

Plusieurs méthodes permettent d'activer le produit. Certains scénarios d'activation proposés dans la fenêtre d'activation peuvent varier en fonction du pays et selon le mode de distribution (CD/DVD, page Web ESET, etc.).

Pour activer votre copie d'ESET Endpoint Security directement à partir du programme, cliquez sur l'icône dans la partie système de la barre des tâches, puis sélectionnez **Activer la licence du produit** dans le menu. Vous pouvez également activer le produit dans le menu principal sous **Aide et assistance** > **Activer le produit** ou **État de la protection** > **Activer le produit**.

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

- **Clé de licence** : chaîne unique au format XXXX-XXXX-XXXX-XXXX-XXXX qui sert à identifier le propriétaire de la licence et à activer la licence.
- **Security Admin** : compte créé sur le portail ESET License Administrator à l'aide d'informations d'identification (adresse électronique + mot de passe). Cette méthode permet de gérer plusieurs licences à partir d'un seul emplacement.
- **Licence hors ligne** : fichier généré automatiquement qui est transféré au produit ESET afin de fournir des informations de licence. Si une licence vous permet de télécharger un fichier de licence hors ligne (.lf), ce dernier peut être utilisé pour effectuer une activation hors ligne. Le nombre de licences hors ligne sera soustrait du

nombre total de licences disponibles. Pour plus d'informations sur la génération d'un fichier hors ligne, reportez-vous au Guide de l'utilisateur d'ESET License Administrator.

Cliquez sur **Activer ultérieurement** si votre ordinateur est membre d'un réseau géré et si votre administrateur effectuera une activation à distance via ESET Remote Administrator. Vous pouvez également utiliser cette option si vous souhaitez activer le client ultérieurement.

Pour changer de licence de produit à tout moment, cliquez sur **Aide et assistance** > **Gérer la licence** dans la fenêtre principale du programme. Vous verrez un ID de licence publique à communiquer à l'assistance ESET pour l'identification de la licence. Le nom d'utilisateur sous lequel l'ordinateur est enregistré dans le système des licences est stocké dans la section **À propos** et est visible en cliquant avec le bouton droit sur l'icône dans la partie système de la barre des tâches.

REMARQUE : ESET Remote Administrator peut activer des ordinateurs clients en silence à l'aide des licences fournies par l'administrateur.

3.7.3 Comment utiliser les informations d'identification actuelles pour activer un nouveau produit

Si vous disposez déjà de votre nom d'utilisateur et de votre mot de passe et souhaitez recevoir une clé de licence, accédez au portail ESET License Administrator sur lequel vous pouvez convertir vos informations d'identification en nouvelle clé de licence.

3.7.4 Comment éliminer un virus de mon PC

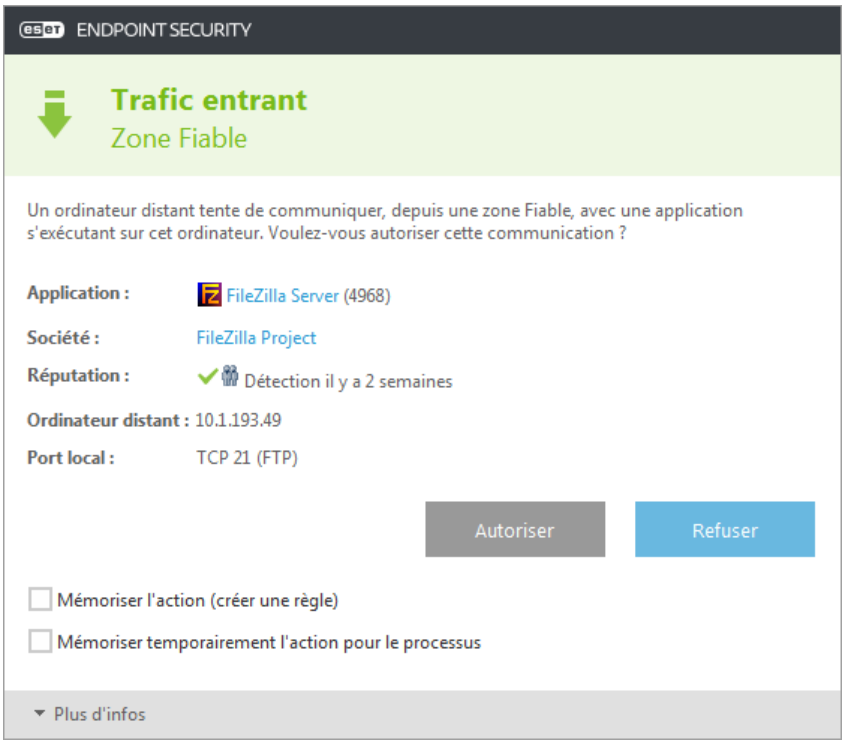
Si votre ordinateur montre des signes d'infection par un logiciel malveillant (ralentissement, blocages fréquents, par exemple), nous recommandons d'effectuer les opérations suivantes :

1. Dans la fenêtre principale du programme, cliquez sur **Analyse de l'ordinateur**.
2. Cliquez sur **Analyse intelligente** pour démarrer l'analyse de votre système.
3. Une fois l'analyse terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés.
4. Si vous ne souhaitez analyser qu'une certaine partie de votre disque, cliquez sur **Analyse personnalisée** et sélectionnez des cibles à analyser.

Pour plus d'informations, veuillez consulter notre article de la base de connaissances ESET régulièrement mis à jour.

3.7.5 Comment autoriser la communication pour une certaine application

Si une nouvelle connexion est détectée en mode interactif et qu'aucune règle ne correspond, le système vous demande d'autoriser ou de refuser la connexion. Si vous souhaitez que ESET Endpoint Security exécute la même action chaque fois que l'application tente d'établir la connexion, cochez la case **Mémoriser l'action (créer une règle)**.



Vous pouvez créer des règles de pare-feu personnel pour les applications avant leur détection par ESET Endpoint Security en cliquant sur **Modifier** dans la fenêtre Configuration du pare-feu personnel située sous **Configuration avancée** > **Pare-feu personnel** > **Général** > **Règles**.

Cliquez sur **Ajouter** pour ajouter la règle. Dans l'onglet **Général**, entrez le nom, le sens et le protocole de communication de la règle. Cette fenêtre permet de définir l'action à entreprendre lorsqu'une règle est appliquée.

Dans l'onglet **Local**, entrez le chemin de l'exécutable de l'application et le port local de communication. Cliquez sur l'onglet **Distant** pour entrer l'adresse et le port distants (le cas échéant). La nouvelle règle est appliquée dès que l'application tente de nouveau de communiquer.

3.7.6 Comment créer une tâche dans le Planificateur

Pour créer une tâche dans **Outils** > **Planificateur**, cliquez sur **Ajouter une tâche** ou cliquez avec le bouton droit sur la tâche et sélectionnez **Ajouter...** dans le menu contextuel. Cinq types de tâches planifiées sont disponibles :

- **Exécuter une application externe** - Permet de programmer l'exécution d'une application externe.
- **Maintenance des journaux** - Les fichiers journaux contiennent également des éléments provenant d'enregistrements supprimés. Cette tâche optimise régulièrement les entrées des fichiers journaux pour garantir leur efficacité.
- **Contrôle des fichiers de démarrage du système** - Vérifie les fichiers autorisés à s'exécuter au démarrage du système ou lors de l'ouverture de session de l'utilisateur.
- **Créer un rapport de l'état de l'ordinateur** : crée un instantané ESET SysInspector de l'ordinateur et collecte des informations détaillées sur les composants système (pilotes, applications) et évalue le niveau de risque de chacun de ces composants.
- **Analyse de l'ordinateur à la demande** : effectue une analyse des fichiers et des dossiers de votre ordinateur.
- **Première analyse** : par défaut, 20 minutes après une installation ou un redémarrage, une analyse de l'ordinateur sera effectuée en tant que tâche de faible priorité.
- **Mise à jour** - Planifie une tâche de mise à jour en mettant à jour la base des signatures de virus et les modules de l'application.

La tâche planifiée la plus fréquente étant la **mise à jour**, nous allons expliquer comment ajouter une nouvelle tâche de mise à jour :

Dans le menu déroulant **Tâche planifiée**, sélectionnez **Mise à jour**. Saisissez le nom de la tâche dans le champ **Nom de la tâche**, puis cliquez sur **Suivant**. Sélectionnez la fréquence de la tâche. Les options disponibles sont les suivantes : **Une fois**, **Plusieurs fois**, **Quotidiennement**, **Hebdo** et **Déclenchée par un événement.** Sélectionnez **Ignorer la tâche en cas d'alimentation par batterie** pour diminuer les ressources système lorsque l'ordinateur portable fonctionne sur batterie. Cette tâche est exécutée à l'heure et au jour spécifiées dans les champs **Exécution de tâche**. Vous pouvez définir ensuite l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée. Les options disponibles sont les suivantes :

- **À la prochaine heure planifiée**
- **Dès que possible**
- **Immédiatement, si la durée écoulée depuis la dernière exécution dépasse la valeur spécifiée** (l'intervalle peut être spécifié dans la zone de liste déroulante **Durée écoulée depuis la dernière exécution**)

À l'étape suivante, une fenêtre de synthèse apparaît. Elle contient des informations sur la tâche planifiée actuelle. Lorsque vous avez terminé vos modifications, cliquez sur **Terminer**.

La boîte de dialogue qui apparaît permet de sélectionner les profils à utiliser pour la tâche planifiée. Vous pouvez y définir le profil principal et le profil secondaire. Le profil secondaire est utilisé si la tâche ne peut pas être terminée à l'aide du profil principal. Cliquez sur **Terminer** pour ajouter la nouvelle tâche planifiée à la liste des tâches actuellement planifiées.

3.7.7 Comment programmer une tâche d'analyse (toutes les 24 heures)

Pour planifier une tâche régulière, ouvrez la fenêtre principale du programme et cliquez sur **Outils** > **Planificateur**. Vous trouverez ci-dessous un guide abrégé indiquant comment planifier une tâche qui analyse les disques locaux toutes les 24 heures.

Pour programmer une tâche d'analyse :

1. Cliquez sur **Ajouter** dans l'écran principal du planificateur.
2. Sélectionnez **Analyse de l'ordinateur à la demande** dans le menu déroulant.
3. Saisissez un nom pour la tâche et sélectionnez **Plusieurs fois**.
4. Choisissez de lancer la tâche toutes les 24 heures.
5. Sélectionnez une action à effectuer en cas de non-exécution de la tâche planifiée, quelle qu'en soit le motif.
6. Passez en revue le résumé de la tâche planifiée, puis cliquez sur **Terminer**.
7. Dans le menu déroulant **Cibles**, sélectionnez **Disques locaux**.
8. Cliquez sur **Terminer** pour appliquer la tâche.

3.7.8 Comment connecter ESET Endpoint Security à ESET Remote Administrator

Lorsqu'ESET Endpoint Security est installé sur votre ordinateur et que vous souhaitez vous connecter via ESET Remote Administrator, vérifiez qu'ERA Agent est également installé sur la station de travail cliente. ERA Agent est un composant essentiel de chaque solution cliente qui communique avec ERA Server. ESET Remote Administrator utilise l'outil RD Sensor pour rechercher des ordinateurs sur le réseau. Chaque ordinateur détecté sur le réseau par RD Sensor est affiché dans la console Web.

Une fois l'Agent déployé, vous pouvez effectuer une installation à distance des produits de sécurité ESET sur votre ordinateur client. La procédure précise pour l'installation à distance est décrite dans le Guide de l'utilisateur d'ESET Remote Administrator.

3.7.9 Comment configurer un miroir

ESET Endpoint Security peut être configuré pour stocker des copies de fichiers de mise à jour des signatures de virus et distribuer les mises à jour à d'autres stations de travail exécutant ESET Endpoint Security ou ESET Endpoint Antivirus.

Configuration d'ESET Endpoint Security en tant que serveur miroir pour fournir les mises à jour via un serveur HTTP interne

Appuyez sur **F5** pour accéder à Configuration avancée, puis développez **Mise à jour** > **General**. Veillez à ce que **Serveur de mise à jour** soit défini sur **SÉLECTION AUTOMATIQUE**. Sélectionnez **Créer un miroir de mise à jour** et **Fournir les fichiers de mise à jour via un serveur HTTP interne** dans **Configuration avancée** > **Général** > **Miroir**.

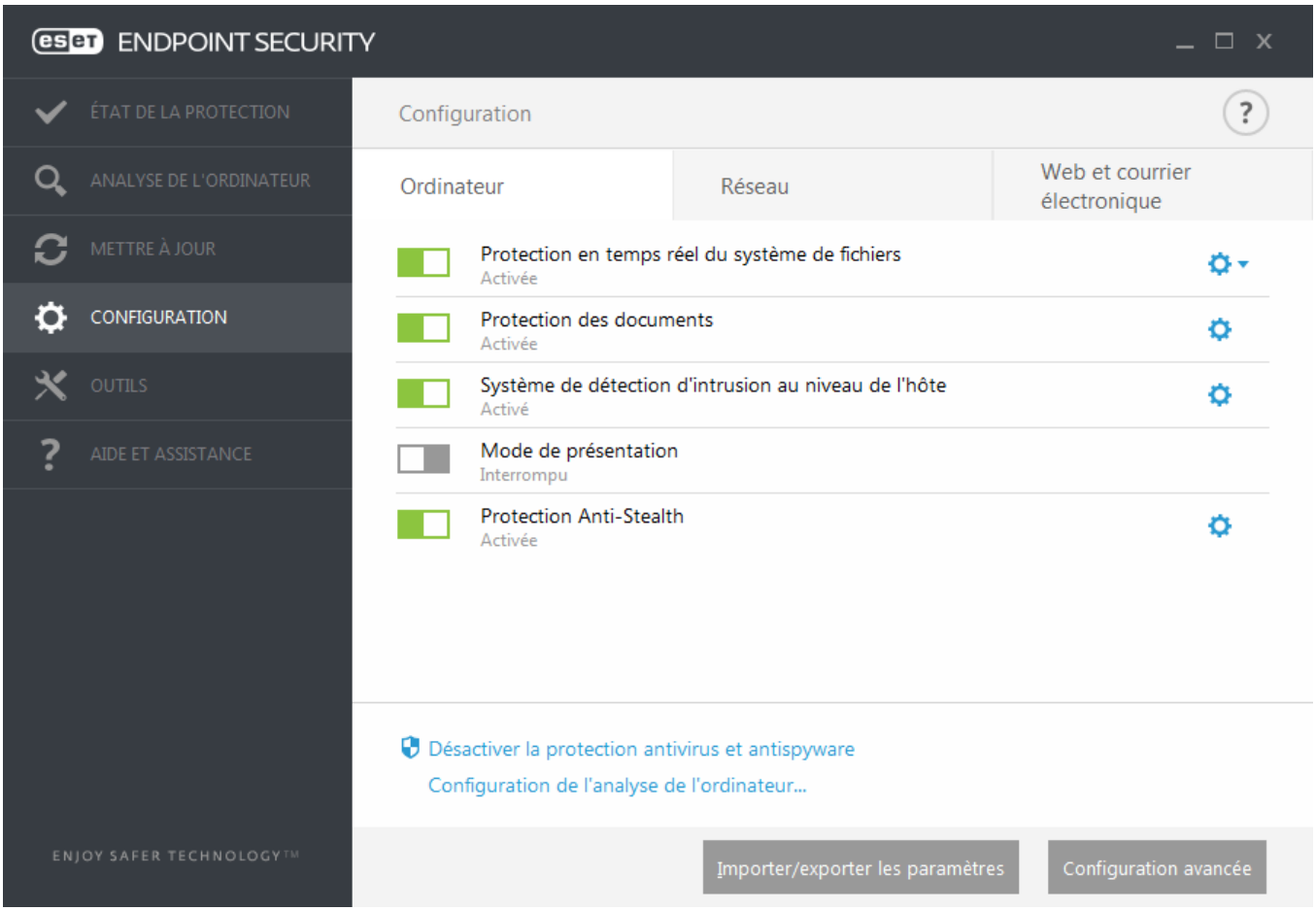
Configuration d'un serveur miroir pour fournir les mises à jour via un dossier réseau partagé

Créez un dossier partagé sur un périphérique local ou réseau. Ce dossier doit être accessible en lecture par tous les utilisateurs exécutant les solutions de sécurité ESET. Il doit également être accessible en écriture à partir du compte SYSTEM local. Activez **Créer un miroir de mise à jour** sous **Configuration avancée** > **General** > **Miroir**. Accédez au dossier partagé créé, puis sélectionnez-le.

REMARQUE : si vous ne souhaitez pas effectuer la mise à jour via un serveur HTTP interne, désactivez **Fournir les fichiers de mise à jour via un serveur HTTP interne**.

3.8 Utilisation de ESET Endpoint Security

Les options de configuration d'ESET Endpoint Security permettent de régler le niveau de protection de votre ordinateur, d'Internet, de la messagerie et du réseau.



Le menu **Configuration** contient les sections suivantes :

- **Ordinateur**
- **Réseau**
- **Internet et messagerie**

La configuration de la protection de l'**ordinateur** permet d'activer ou de désactiver les composants suivants :

- **Protection en temps réel du système de fichiers** - Tous les fichiers ouverts, créés ou exécutés sur l'ordinateur sont analysés pour y rechercher la présence éventuelle de code malveillant.
- **Protection des documents** - La fonctionnalité de protection des documents analyse les documents Microsoft Office avant leur ouverture, ainsi que les fichiers téléchargés automatiquement par Internet Explorer, tels que les éléments Microsoft ActiveX.
- **HIPS** - Le système HIPS surveille les événements qui se produisent dans le système d'exploitation et réagit en fonction d'un ensemble de règles personnalisées.
- **Mode de présentation** - Fonctionnalité destinée aux utilisateurs qui ne veulent pas être interrompus lors de l'utilisation de leur logiciel. Ils ne souhaitent pas être dérangés par des fenêtres contextuelles et veulent réduire les contraintes sur l'UC. Vous recevez un message d'avertissement (risque potentiel de sécurité) et la fenêtre principale devient orange lorsque le mode de présentation est activé.
- **Protection Anti-Stealth** - Détecte les programmes dangereux tels que les rootkits, qui sont en mesure de se dissimuler du système d'exploitation. Il est impossible de les détecter à l'aide de techniques de test ordinaires.

La section **Réseau** permet d'activer ou de désactiver le **pare-feu personnel**.

La configuration de la protection **Internet et messagerie** permet d'activer ou de désactiver les composants suivants :

- **Filtrage Internet** - Bloque les pages Web dont le contenu est susceptible d'être choquant. Les administrateurs système peuvent en outre spécifier des préférences d'accès pour 27 catégories de sites Web prédéfinies.
- **Protection de l'accès Web** - Si cette option est activée, tout le trafic HTTP ou HTTPS est analysé afin d'y rechercher des codes malveillants.
- **Protection du client de messagerie** - Contrôle les communications reçues via les protocoles POP3 et IMAP.
- **Protection antispam** - Recherche les messages non sollicités.
- **Protection antihameçonnage** - Vous protège des tentatives d'acquisition de mots de passe, de données bancaires ou d'autres informations sensibles par des sites Web non légitimes se faisant passer pour des sites Web dignes de confiance.

Pour désactiver temporairement un module, cliquez sur le bouton bascule vert  en regard de celui-ci. Notez que cela pourrait abaisser le niveau de protection de l'ordinateur.

Pour réactiver la protection d'un composant de sécurité désactivé, cliquez sur le bouton bascule rouge  pour l'activer.

REMARQUE : toutes les mesures de protection désactivées de cette manière sont réactivées après le redémarrage de l'ordinateur.

Pour accéder aux paramètres détaillés d'un composant de sécurité spécifique, cliquez sur le symbole d'engrenage  situé en regard d'un composant**.**

D'autres options sont disponibles au bas de la fenêtre de configuration. Pour charger les paramètres de configuration à l'aide d'un fichier de configuration *.xml* ou pour enregistrer les paramètres de configuration actuels dans un fichier de configuration, utilisez l'option **Importer/exporter les paramètres**. Pour plus d'informations, consultez la section Importer/exporter les paramètres.

Pour afficher des options détaillées, cliquez sur **Configuration avancée** ou appuyez sur **F5**.

3.8.1 Ordinateur

Le module **Ordinateur** figure sous **Configuration** > **Ordinateur**. Il donne une vue d'ensemble des modules de protection décrits dans le chapitre précédent. Dans cette section, les paramètres suivants sont disponibles :

Cliquez sur l'engrenage ⚙ en regard de **Protection en temps réel du système de fichiers**, puis sur **Modifier les exclusions** pour ouvrir la fenêtre de configuration des exclusions qui permet d'exclure des fichiers et des dossiers de l'analyse.

REMARQUE : L'état de la protection des documents peut ne pas être disponible tant que vous n'avez pas activé **Configuration avancée** (F5) > **Antivirus** > **Protection des documents**. Une fois l'état activé, vous devez redémarrer votre ordinateur à partir du volet Configuration > Ordinateur en cliquant sur **Redémarrer** sous Contrôle de périphérique. Vous pouvez également effectuer le redémarrage à partir du volet État de la protection en cliquant sur **Redémarrer l'ordinateur**.

Interrompre la protection antivirus et antispywar : lorsque vous désactivez temporairement la protection antivirus et antispyware, vous pouvez sélectionner la durée de désactivation du composant sélectionné dans le menu déroulant et cliquer sur **Appliquer** pour désactiver le composant de sécurité. Pour réactiver la protection, cliquez sur **Activer la protection antivirus et antispyware**.

Configuration de l'analyse de l'ordinateur... : cliquez ici pour régler les paramètres d'analyse à la demande (analyse lancée manuellement).

3.8.1.1 Antivirus

La protection antivirus et antispyware vous protège des attaques contre le système en contrôlant les échanges de fichiers et de courrier, ainsi que les communications Internet. Si une menace est détectée, le module antivirus peut l'éliminer en la bloquant dans un premier temps, puis en nettoyant, en supprimant ou en mettant en quarantaine l'objet infecté.

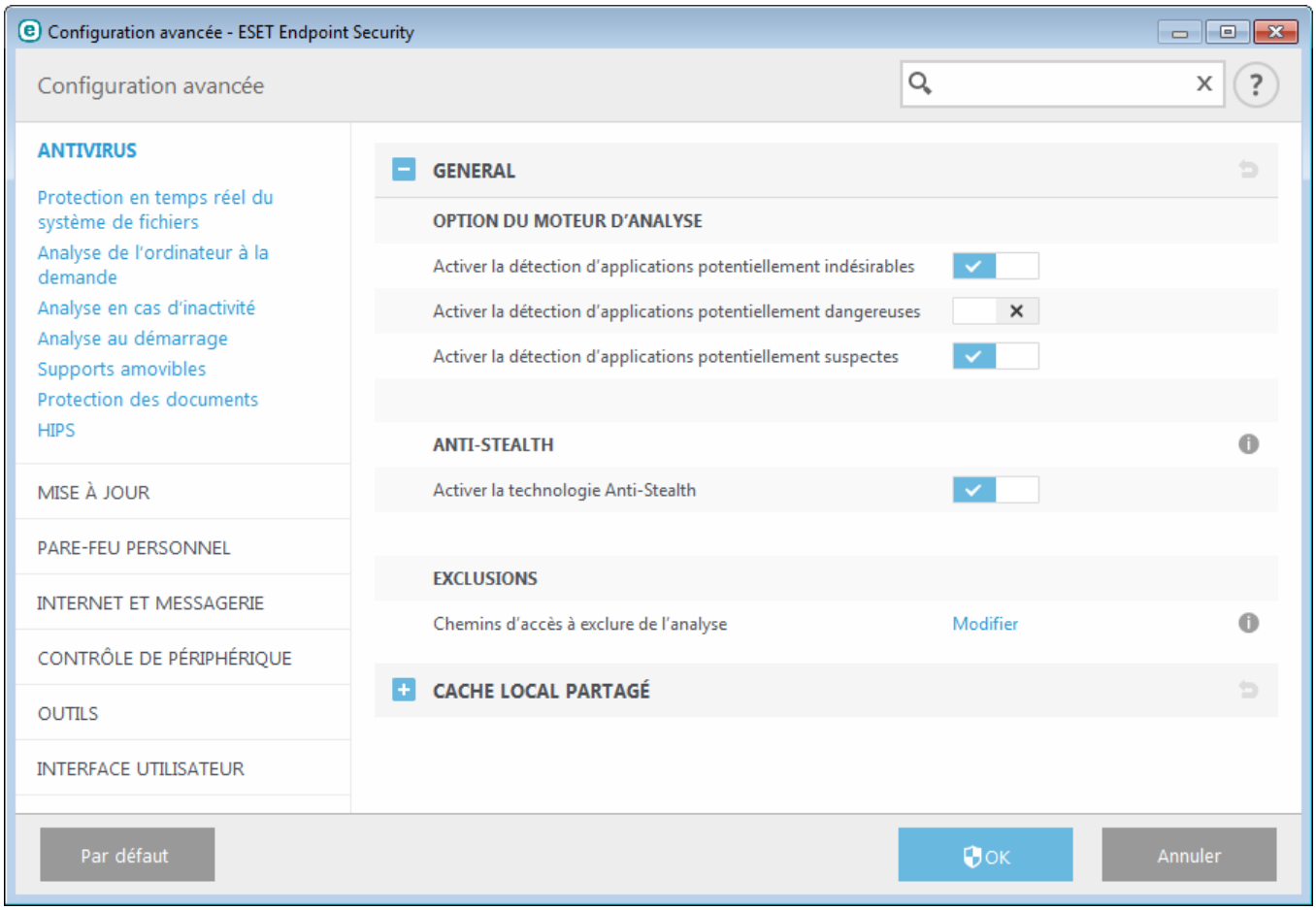
Pour configurer les paramètres du module antivirus, cliquez sur **Configuration avancée** ou appuyez sur **F5**.

Les options du scanner pour tous les modules de protection (par exemple, protection en temps réel du système de fichiers, protection de l'accès Web, etc.) vous permettent d'activer ou de désactiver la détection des éléments suivants :

- Les **applications potentiellement indésirables** ne sont pas nécessairement malveillantes, mais elles sont susceptibles d'affecter les performances de votre ordinateur.
  Pour en savoir plus sur ces types d'applications, consultez le glossaire.
- **Les applications potentiellement dangereuses** sont des logiciels commerciaux légitimes susceptibles d'être utilisés à des fins malveillantes. Cette catégorie comprend les programmes d'accès à distance, les applications de décodage des mots de passe ou les keyloggers (programmes qui enregistrent chaque frappe au clavier de l'utilisateur). Cette option est désactivée par défaut.
  Pour en savoir plus sur ces types d'applications, consultez le glossaire.
- **Les applications suspectes** comprennent des programmes compressés par des compresseurs ou par des programmes de protection. Ces types de protections sont souvent exploités par des créateurs de logiciels malveillants pour contourner leur détection.

La technologie Anti-Stealth est un système sophistiqué assurant la détection de programmes dangereux tels que les rootkits, qui sont à même de se cacher du système d'exploitation. Il est impossible de les détecter à l'aide de techniques de test ordinaires.

Les exclusions permettent d'exclure des fichiers et dossiers de l'analyse. Pour que la détection des menaces s'appliquent bien à tous les objets, il est recommandé de ne créer des exclusions que lorsque cela s'avère absolument nécessaire. Certaines situations justifient l'exclusion d'un objet. Par exemple, lorsque les entrées de bases de données volumineuses risquent de ralentir l'ordinateur pendant l'analyse ou lorsqu'il peut y avoir conflit entre le logiciel et l'analyse. Pour exclure un objet de l'analyse, reportez-vous à la section Exclusions.



3.8.1.1.1 Une infiltration est détectée

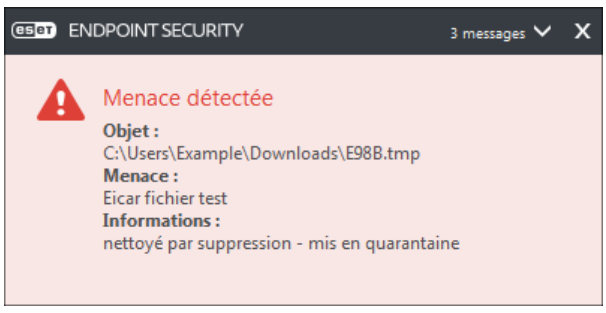
Des infiltrations peuvent atteindre le système à partir de différents points d'entrée : pages Web, dossiers partagés, courrier électronique ou périphériques amovibles (USB, disques externes, CD, DVD, disquettes, etc.).

Comportement standard

Pour illustrer de manière générale la prise en charge des infiltrations par ESET Endpoint Security, celles-ci peuvent être détectées à l'aide de :

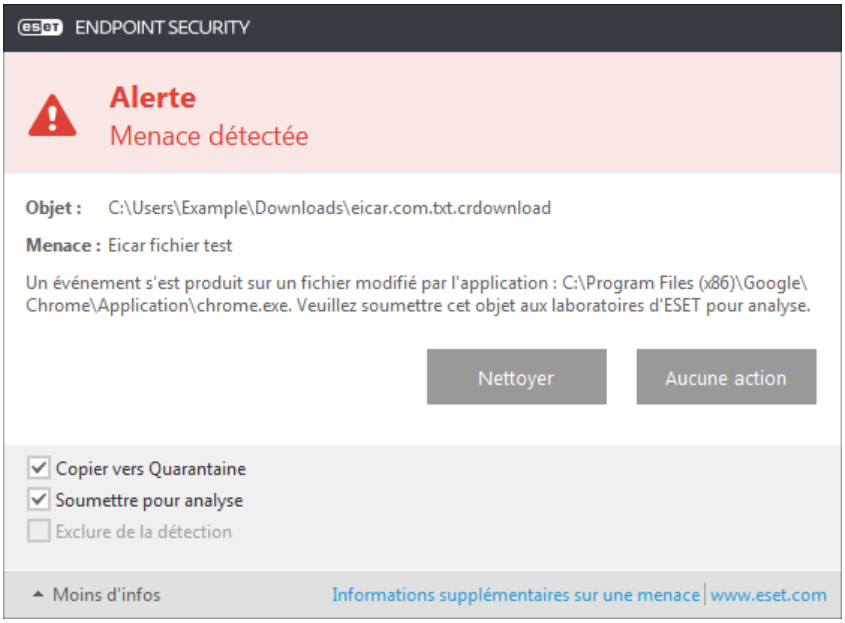
- Protection en temps réel du système de fichiers
- Protection de l'accès Web
- Protection du client de messagerie
- Analyse de l'ordinateur à la demande

Chaque fonction utilise le niveau de nettoyage standard et tente de nettoyer le fichier et de le déplacer en Quarantaine ou met fin à la connexion. Une fenêtre de notification s'affiche dans la zone de notification, dans l'angle inférieur droit de l'écran. Pour plus d'informations sur les niveaux et le comportement de nettoyage, voir Nettoyage.



Nettoyage et suppression

Si aucune action n'est prédéfinie pour le module de protection en temps réel du système de fichiers, vous êtes invité à sélectionner une option dans une fenêtre d'avertissement. Généralement, les options **Nettoyer**, **Supprimer** et **Aucune action** sont disponibles. Il n'est pas recommandé de sélectionner **Aucune action**, car cette option laissera les fichiers infectés non nettoyés. La seule exception concerne les situations où vous êtes sûr qu'un fichier est inoffensif et qu'il a été détecté par erreur.



Utilisez le nettoyage si un fichier sain a été attaqué par un virus qui y a joint du code malveillant. Dans ce cas, essayez d'abord de nettoyer le fichier infecté pour le restaurer dans son état d'origine. Si le fichier se compose uniquement de code malveillant, il est supprimé.

Si un fichier infecté est « verrouillé » ou utilisé par un processus système, il n'est généralement supprimé qu'après avoir été déverrouillé (normalement, après un redémarrage du système).

Menaces multiples

Si des fichiers infectés n'ont pas été nettoyés durant une analyse de l'ordinateur (ou si le niveau de nettoyage a été défini sur **Pas de nettoyage**), une fenêtre d'alerte s'affiche ; elle vous invite à sélectionner des actions pour ces fichiers. Sélectionnez des actions pour les fichiers (les actions sont définies pour chaque fichier de la liste), puis cliquez sur **Terminer**.

Suppression de fichiers dans les archives

En mode de nettoyage par défaut, l'archive complète n'est supprimée que si elle ne contient que des fichiers infectés et aucun fichier sain. Autrement dit, les archives ne sont pas supprimées si elles contiennent également des fichiers sains. Soyez prudent si vous choisissez un nettoyage strict ; dans ce mode, une archive sera supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

Si votre ordinateur montre des signes d'infection par un logiciel malveillant (ralentissement, blocages fréquents, etc.), nous recommandons d'effectuer les opérations suivantes :

- Ouvrez ESET Endpoint Security et cliquez sur Analyse de l'ordinateur
- Cliquez sur **Analyse intelligente** (pour plus d'informations, voir Analyse de l'ordinateur)
- Lorsque l'analyse est terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés

Si vous ne souhaitez analyser qu'une certaine partie de votre disque, cliquez sur **Analyse personnalisée** et sélectionnez des cibles à analyser.

3.8.1.2 Cache local partagé

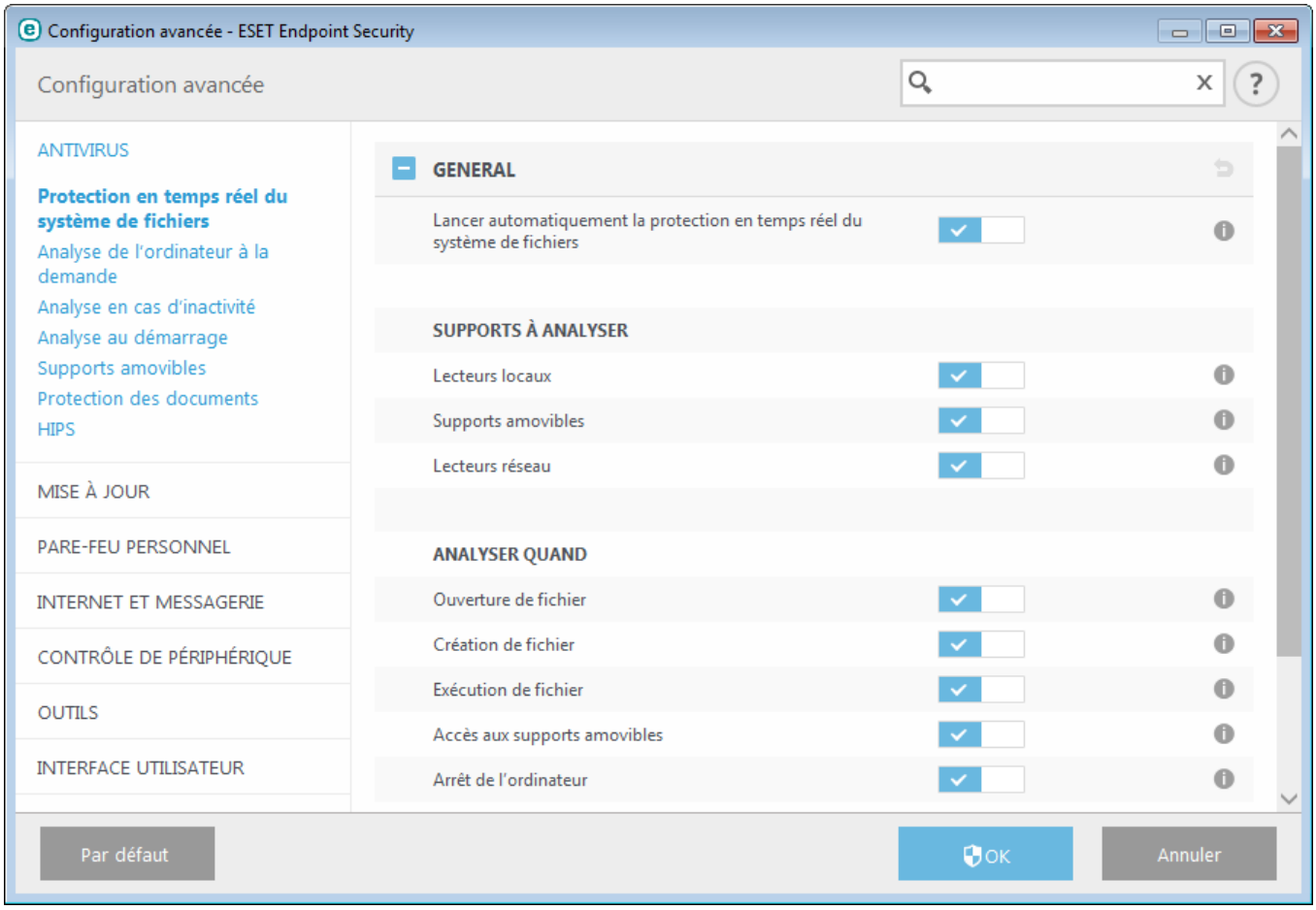
Le cache local partagé permet d'accroître considérablement les performances dans les environnements virtualisés en éliminant les analyses en double sur le réseau. Cela permet de s'assurer que chaque fichier est analysé une seule fois et stocké dans le cache partagé. Activez le bouton bascule **Option de mise en cache** pour enregistrer dans le cache local des informations sur les analyses des fichiers et des dossiers sur le réseau. Si vous effectuez une nouvelle analyse, ESET Endpoint Security recherche les fichiers analysés dans le cache. Si les fichiers correspondent, ils sont exclus de l'analyse.

La configuration du **Serveur de cache** comprend les éléments suivants **:**

- **Nom de l'hôte** : nom ou adresse IP de l'ordinateur sur lequel se trouve le cache.
- **Port** : numéro de port utilisé pour les communications (identique à celui défini dans le cache local partagé).
- **Mot de passe** : indiquez le mot de passe du cache local partagé ESET si nécessaire.

3.8.1.3 Protection en temps réel du système de fichiers

La protection en temps réel du système de fichiers contrôle tous les événements liés à l'antivirus dans le système. Lorsque ces fichiers sont ouverts, créés ou exécutés sur l'ordinateur, elle les analyse pour y rechercher la présence éventuelle de code malveillant. La protection en temps réel du système de fichiers est lancée au démarrage du système.



Par défaut, la protection en temps réel du système de fichiers est lancée au démarrage du système et assure une analyse ininterrompue. Dans certains cas particuliers (par exemple, en cas de conflit avec un autre scanner en temps réel), la protection en temps réel peut être désactivée en désélectionnant **Démarrer automatiquement la protection en temps réel du système de fichiers** sous **Protection en temps réel du système de fichiers** > **General** dans **Configuration avancée**.

Supports à analyser

Par défaut, tous les types de supports font l'objet de recherches de menaces potentielles :

Disques locaux - Contrôle tous les disques durs système.
Supports amovibles - Contrôle les CD/DVD, les périphériques USB, les périphériques Bluetooth, etc.
Disques réseau - Analyse tous les lecteurs mappés.

Il est recommandé d'utiliser les paramètres par défaut et de ne les modifier que dans des cas spécifiques, par exemple lorsque l'analyse de certains supports ralentit de manière significative les transferts de données.

Analyser quand

Par défaut, tous les fichiers sont analysés lors de leur ouverture, création ou exécution. Il est recommandé de conserver ces paramètres par défaut, car ils offrent le niveau maximal de protection en temps réel pour votre ordinateur :

- **Ouverture de fichier** - Active/désactive l'analyse lorsque des fichiers sont ouverts.
- **Création de fichier** - Active/désactive l'analyse lorsque des fichiers sont créés.
- **Exécution de fichier** - Active/désactive l'analyse lorsque des fichiers sont exécutés.
- **Accès aux supports amovibles** : active ou désactive l'analyse déclenchée par l'accès à des supports amovibles spécifiques disposant d'espace de stockage.
- **Arrêt de l'ordinateur** - Active/désactive l'analyse déclenchée par l'arrêt de l'ordinateur.

La protection en temps réel du système de fichiers vérifie tous les types de supports. Elle est déclenchée par différents événements système, tels que l'accès à un fichier. Grâce aux méthodes de détection de la technologie ThreatSense (décrites dans la section Configuration des paramètres du moteur ThreatSense), la protection du système de fichiers en temps réel peut être configurée pour traiter différemment les nouveaux fichiers et les fichiers existants. Par exemple, vous pouvez configurer la protection en temps réel du système de fichiers pour surveiller plus étroitement les nouveaux fichiers.

Pour garantir un impact minimal de la protection en temps réel sur le système, les fichiers déjà analysés ne sont pas analysés plusieurs fois (sauf s'ils ont été modifiés). Les fichiers sont immédiatement réanalysés après chaque mise à jour de la base des signatures de virus. Ce comportement est contrôlé à l'aide de l'**optimisation intelligente**. Si l'**optimisation intelligente** est désactivée, tous les fichiers sont analysés à chaque accès. Pour modifier ce paramètre, appuyez sur **F5** pour ouvrir la configuration avancée, puis développez **Antivirus** > **Protection en temps réel du système de fichiers**. Cliquez ensuite sur **Paramètre ThreatSense** > **Autre**, puis sélectionnez ou désélectionnez **Activer l'optimisation intelligente**.

3.8.1.3.1 Autres paramètres ThreatSense

Autres paramètres ThreatSense pour les fichiers nouveaux et modifiés - La probabilité d'infection des nouveaux fichiers ou des fichiers modifiés est comparativement plus élevée que dans les fichiers existants. C'est la raison pour laquelle le programme vérifie ces fichiers avec des paramètres d'analyse supplémentaires. Outre les méthodes d'analyse basées sur les signatures, le système utilise également l'heuristique avancée qui permet de détecter les nouvelles menaces avant la mise à disposition de la mise à jour de la base des signatures de virus. Outre les nouveaux fichiers, l'analyse porte également sur les fichiers auto-extractibles (.sfx) et les fichiers exécutables compressés (en interne). Par défaut, les archives sont analysées jusqu'au dixième niveau d'imbrication et sont contrôlées indépendamment de leur taille réelle. Pour modifier les paramètres d'analyse d'archive, désactivez **Paramètres d'analyse d'archive par défaut**.

Pour plus d'informations sur les **fichiers exécutables compressés**, les **archives auto-extractibles** et l'**heuristique avancée**, reportez-vous à la section Configuration des paramètres du moteur ThreatSense.

Autres paramètres ThreatSense pour les fichiers exécutés : par défaut, l'heuristique avancée n'est pas utilisée lors de l'exécution des fichiers. Lorsque ce paramètre est activé, il est fortement recommandé de conserver les options Optimisation intelligente et ESET Live Grid activées pour limiter l'impact sur les performances système.

3.8.1.3.2 Niveaux de nettoyage

La protection en temps réel comporte trois niveaux de nettoyage (pour y accéder, cliquez sur **Configuration des paramètres du moteur ThreatSense** dans la section **Protection en temps réel du système de fichiers**, puis cliquez sur **Nettoyage**).

Pas de nettoyage - Les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche alors une fenêtre d'avertissement et laisse l'utilisateur choisir une action. Ce niveau est conçu pour les utilisateurs expérimentés qui connaissent les actions à entreprendre en cas d'infiltration.

Nettoyage normal - Le programme tente de nettoyer ou de supprimer automatiquement tout fichier sur la base d'une action prédéfinie (dépendant du type d'infiltration). La détection et la suppression d'un fichier infecté sont signalées par une notification affichée dans l'angle inférieur droit de l'écran. S'il n'est pas possible de sélectionner automatiquement l'action correcte, le programme propose plusieurs actions de suivi. C'est le cas également si une action prédéfinie ne peut pas être menée à bien.

Nettoyage strict - Le programme nettoie ou supprime tous les fichiers infectés. Les seules exceptions sont les fichiers système. S'il n'est pas possible de les nettoyer, l'utilisateur est invité à sélectionner une action dans une fenêtre d'avertissement.

Avertissement : si une archive contient un ou plusieurs fichiers infectés, elle peut être traitée de deux façons différentes. En mode standard (Nettoyage standard), toute l'archive est supprimée si tous ses fichiers sont infectés. En mode de **nettoyage strict**, l'archive est supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

3.8.1.3.3 Vérification de la protection en temps réel

Pour vérifier que la protection en temps réel fonctionne et détecte les virus, utilisez un fichier de test d'eicar.com. Ce fichier de test est un fichier inoffensif détectable par tous les programmes antivirus. Le fichier a été créé par la société EICAR (European Institute for Computer Antivirus Research) et permet de tester la fonctionnalité des programmes antivirus. Le fichier est téléchargeable à partir de la page http://www.eicar.org/download/eicar.com

REMARQUE : avant d'effectuer une vérification de la protection en temps réel, désactivez le pare-feu. S'il est activé, il détecte le fichier et empêche le téléchargement des fichiers de test. Veillez à réactiver le pare-feu immédiatement après la vérification de la protection en temps réel du système de fichiers.

3.8.1.3.4 Quand faut-il modifier la configuration de la protection en temps réel

La protection du système de fichiers en temps réel est le composant essentiel de la sécurisation du système. Procédez toujours avec prudence lors de la modification des paramètres de ce module. Il est recommandé de ne modifier les paramètres que dans des cas très précis.

Après l'installation d'ESET Endpoint Security, tous les paramètres sont optimisés pour garantir le niveau maximum de système de sécurité aux utilisateurs. Pour rétablir les paramètres par défaut, cliquez sur ↩ en regard de chaque onglet dans la fenêtre (**Configuration avancée** > **Antivirus** > **Protection du système de fichiers en temps réel**).

3.8.1.3.5 Que faire si la protection en temps réel ne fonctionne pas ?

Dans ce chapitre, nous décrivons des problèmes qui peuvent survenir lors de l'utilisation de la protection en temps réel et la façon de les résoudre.

La protection en temps réel est désactivée

Si la protection en temps réel a été désactivée par mégarde par un utilisateur, elle doit être réactivée. Pour réactiver la protection en temps réel, sélectionnez **Configuration** dans la fenêtre principale du programme et cliquez sur **Protection en temps réel du système de fichiers**.

Si la protection en temps réel ne se lance pas au démarrage du système, c'est probablement parce que **Lancer automatiquement la protection en temps réel du système de fichiers** est désactivé. Pour activer cette option, accédez à **Configuration avancée** (**F5**) et cliquez sur **Antivirus** > **Protection en temps réel du système de fichiers** > **Général**. Vérifiez que le bouton bascule **Lancer automatiquement la protection en temps réel du système de**

fichiers est activé.

Si la protection en temps réel ne détecte et ne nettoie pas les infiltrations

Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si deux programmes de protection en temps réel sont activés en même temps, il peut y avoir un conflit entre les deux. Nous recommandons de désinstaller tout autre antivirus de votre système avant d'installer ESET.

La protection en temps réel ne démarre pas

Si la protection en temps réel n'est pas lancée au démarrage du système (et si **Lancer automatiquement la protection en temps réel du système de fichiers** est activé), le problème peut provenir de conflits avec d'autres programmes. Afin d'obtenir une assistance pour résoudre ce problème, veuillez contacter le service client d'ESET.

3.8.1.4 Analyse de l'ordinateur à la demande

L'analyseur à la demande est un composant important d'ESET Endpoint Security. Il permet d'analyser des fichiers et des répertoires de votre ordinateur. Pour votre sécurité, il est essentiel que l'ordinateur soit analysé non seulement en cas de suspicion d'une infection, mais aussi régulièrement dans le cadre de mesures de sécurité routinières. Nous vous recommandons d'effectuer des analyses en profondeur de votre système de façon régulière (une fois par mois, par exemple) afin de détectés les virus qui ne l'ont pas été par la protection en temps réel du système de fichiers. Cela peut se produire si la protection en temps réel du système de fichiers est désactivée au moment de l'infection, si la base des signatures de virus n'est plus à jour ou si le fichier n'a pas été détecté comme virus lors de son enregistrement sur le disque.

Deux types d'**analyses de l'ordinateur** sont disponibles. L'**analyse intelligente** analyse le système sans exiger de reconfiguration des paramètres d'analyse. L'**analyse personnalisée** permet de sélectionner l'un des profils d'analyse prédéfinis et de sélectionner des cibles spécifiques à analyser.

Reportez-vous au chapitre sur la progression de l'analyse pour plus d'informations sur le processus d'analyse.

Analyse intelligente

L'analyse intelligente permet de lancer rapidement une analyse de l'ordinateur et de nettoyer les fichiers infectés sans intervention de l'utilisateur. L'analyse intelligente présente l'intérêt d'être facile à utiliser et de ne pas nécessiter de configuration détaillée. L'analyse intelligente vérifie tous les fichiers des disques locaux, et nettoie ou supprime automatiquement les infiltrations détectées. Le niveau de nettoyage est automatiquement réglé sur sa valeur par défaut. Pour plus d'informations sur les types de nettoyage, reportez-vous à la section Nettoyage.

Analyse personnalisée

L'analyse personnalisée est une solution optimale si vous souhaitez spécifier des paramètres d'analyse tels que les cibles et les méthodes d'analyse. L'analyse personnalisée a l'avantage de permettre la configuration précise des paramètres. Les configurations peuvent être enregistrées dans des profils d'analyse définis par l'utilisateur, qui sont utiles pour effectuer régulièrement une analyse avec les mêmes paramètres.

Pour sélectionner des cibles à analyser, sélectionnez **Analyse de l'ordinateur** > **Analyse personnalisée**, puis sélectionnez une option dans le menu déroulant **Cibles à analyser** ou sélectionnez des cibles spécifiques dans l'arborescence. Une cible à analyser peut également être spécifiée en indiquant le chemin d'accès au dossier ou aux fichiers à inclure. Si vous souhaitez effectuer uniquement une analyse du système sans actions de nettoyage supplémentaires, sélectionnez **Analyse sans nettoyage**. Lors d'une analyse, vous pouvez effectuer un choix parmi trois niveaux de nettoyage en cliquant sur **Configuration...** > **Paramètres ThreatSense** > **Nettoyage**.

L'exécution d'analyses personnalisées de l'ordinateur convient aux utilisateurs chevronnés qui maîtrisent l'utilisation de programmes antivirus.

Analyse de supports amovibles

Similaire à l'analyse intelligente, ce type d'analyse lance rapidement une analyse des supports amovibles (par ex. CD/DVD/USB) qui sont actuellement branchés sur l'ordinateur. Cela peut être utile lorsque vous connectez une clé USB à un ordinateur et que vous souhaitez l'analyser pour y rechercher les logiciels malveillants et autres menaces potentielles.

Pour lancer ce type d'analyse, vous pouvez aussi cliquer sur **Analyse personnalisée**, puis sélectionner **Supports amovibles** dans le menu déroulant **Cibles à analyser** et cliquer sur **Analyser**.

Vous pouvez utiliser le menu déroulant **Action après l'analyse** pour sélectionner l'action (Aucune action, Arrêt, Redémarrage et Veille) à exécuter après l'analyse.

Activer l'arrêt après l'analyse - Active un arrêt planifié à la fin de l'analyse à la demande de l'ordinateur. Une boîte de dialogue de confirmation d'arrêt affiche un compte à rebours de 60 secondes. Cliquez sur **Annuler** pour désactiver l'arrêt demandé.

REMARQUE : Nous recommandons d'exécuter une analyse d'ordinateur au moins une fois par mois. L'analyse peut être configurée comme tâche planifiée dans **Outils** > **Planificateur**.

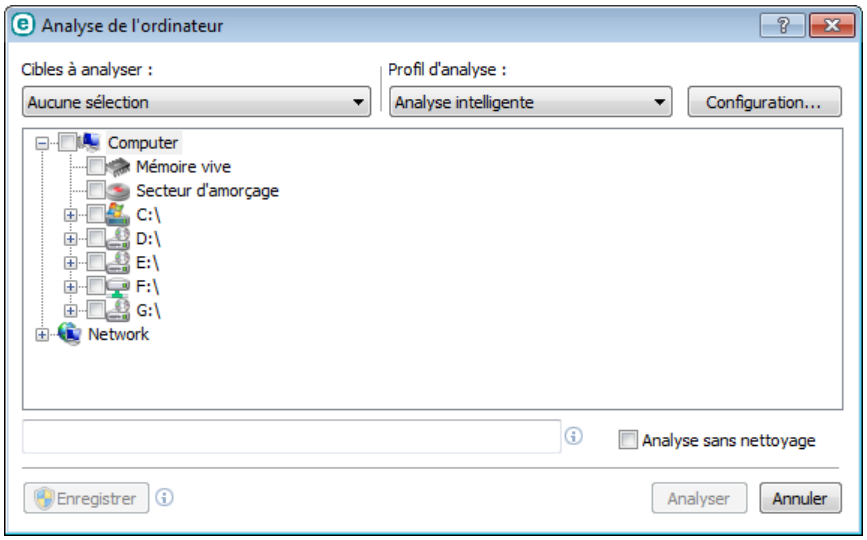
3.8.1.4.1 Lanceur d'analyses personnalisées

Si vous souhaitez analyser uniquement une cible spécifique, vous pouvez utiliser l'analyse personnalisée en cliquant sur **Analyse d'ordinateur** > **Analyse personnalisée** et sélectionner une option dans le menu déroulant **Cibles à analyser** ou des cibles particulières dans l'arborescence des dossiers.

La fenêtre des cibles à analyser permet de définir les objets (mémoire, lecteurs, secteurs, fichiers et dossiers) dans lesquels rechercher des infiltrations. Sélectionnez les cibles dans l'arborescence des périphériques disponibles sur l'ordinateur. Le menu déroulant **Cibles à analyser** permet de sélectionner des cibles à analyser prédéfinies :

- **Par les paramètres de profil** - Permet de sélectionner les cibles indiquées dans le profil d'analyse sélectionné.
- **Supports amovibles** - Permet de sélectionner les disquettes, les périphériques USB, les CD/DVD, etc.
- **Disques locaux** - Permet de sélectionner tous les disques durs du système.
- **Disques réseau** - Analyse tous les lecteurs réseau mappés.
- **Aucune sélection** - Annule toutes les sélections.

Pour accéder rapidement à une cible d'analyse ou ajouter directement une cible souhaitée (dossiers ou fichiers), entrez-la dans le champ vide sous la liste de dossiers. Aucune cible ne doit être sélectionnée dans la structure arborescente et le menu **Cibles à analyser** doit être défini sur **Aucune sélection**.



Les éléments infectés ne sont pas nettoyés automatiquement. Une analyse sans nettoyage permet d'obtenir un aperçu de l'état actuel de la protection. Si vous souhaitez effectuer uniquement une analyse du système sans actions de nettoyage supplémentaires, sélectionnez **Analyse sans nettoyage**. Vous pouvez aussi choisir parmi trois niveaux de nettoyage en cliquant sur **Configuration...** > **Paramètres ThreatSense** > **Nettoyage**. Les informations de l'analyse sont enregistrées dans un journal d'analyse.

Vous pouvez choisir un profil à utiliser pour l'analyse des cibles sélectionnées dans le menu déroulant **Profil d'analyse**. Le profil par défaut est **Analyse intelligente**. Il existe deux autres profils d'analyse prédéfinis nommés **Analyse approfondie** et **Analyse via le menu contextuel**. Ces profils d'analyse utilisent différents paramètres du moteur ThreatSense. Cliquez sur **Configuration...** pour configurer en détail le profil d'analyse de votre choix dans le menu Profil d'analyse. Les options disponibles sont décrites dans la section **Autre** de Configuration des paramètres du moteur ThreatSense.

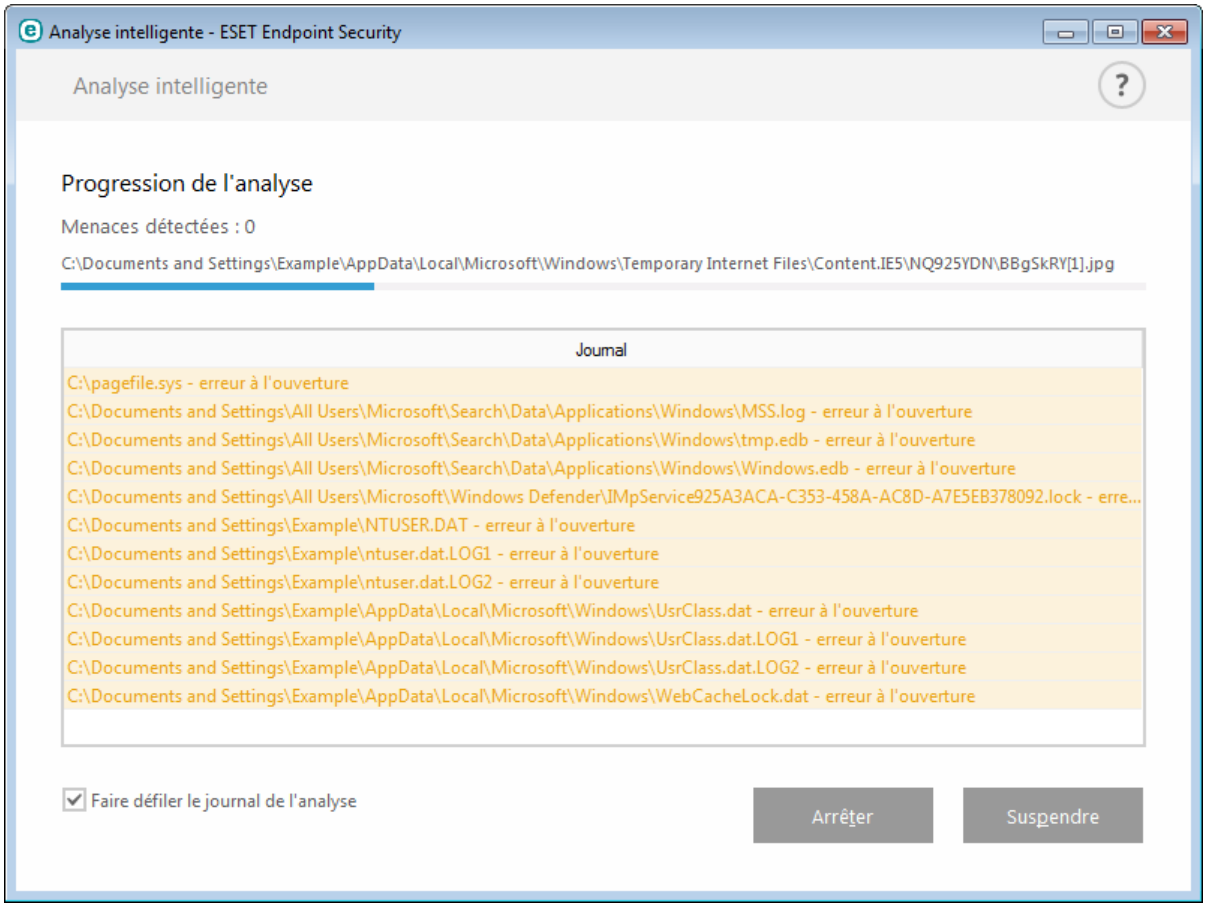
Cliquez sur **Enregistrer** pour enregistrer les modifications apportées à la sélection des cibles, y compris les sélections effectuées dans l'arborescence des dossiers.

Cliquez sur **Analyser** pour exécuter l'analyse avec les paramètres personnalisés que vous avez définis.

Analyser en tant qu'administrateur vous permet d'exécuter l'analyse sous le compte administrateur. Cliquez sur cette option si l'utilisateur actuel ne dispose pas des privilèges suffisants pour accéder aux fichiers à analyser. Remarquez que ce bouton n'est pas disponible si l'utilisateur actuel ne peut pas appeler d'opérations UAC en tant qu'administrateur.

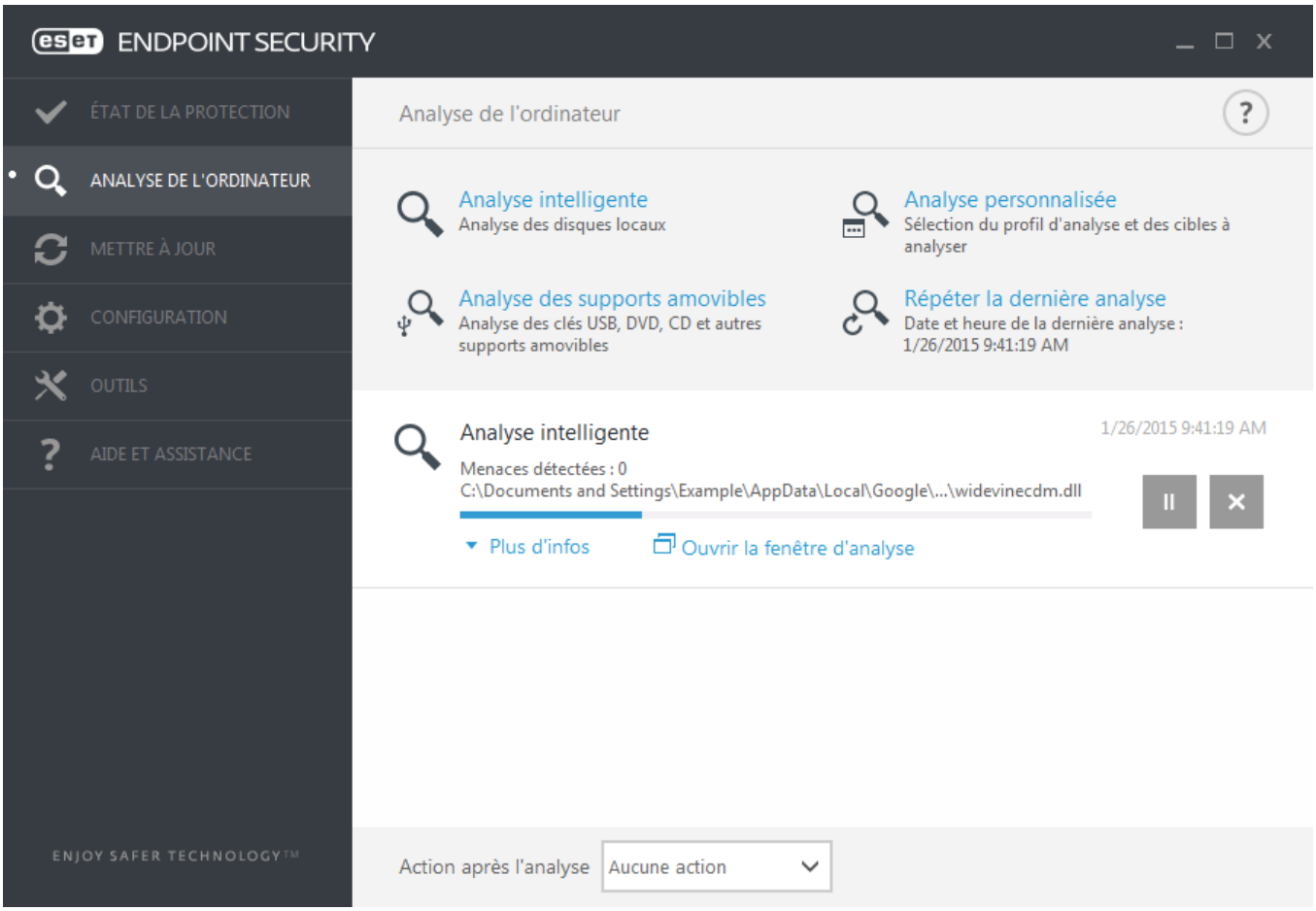
3.8.1.4.2 Progression de l'analyse

La fenêtre de progression de l'analyse indique l'état actuel de l'analyse, ainsi que des informations sur le nombre de fichiers contenant du code malveillant qui sont détectés.



REMARQUE : il est normal que certains fichiers, protégés par mot de passe ou exclusivement utilisés par le système (en général *pagefile.sys* et certains fichiers journaux), ne puissent pas être analysés.

Progression de l'analyse - La barre de progression indique l'état des objets déjà analysés par rapport aux objets qui ne sont pas encore analysés. L'état de progression de l'analyse est dérivé du nombre total d'objets intégrés dans l'analyse.
Cible - Taille de l'élément analysé et emplacement.
Menaces détectées - Indique le nombre total de menaces détectées pendant une analyse.
Interrompre - Interrompt une analyse.
Reprendre - Cette option est visible lorsque l'analyse est interrompue. Cliquez sur Reprendre pour poursuivre l'analyse.
Arrêter - Met fin à l'analyse.
Faire défiler le journal de l'analyse - Si cette option est activée, le journal de l'analyse défile automatiquement au fur et à mesure de l'ajout des entrées les plus récentes.



3.8.1.5 Contrôle de périphérique

ESET Endpoint Security permet un contrôle automatique des périphériques (CD/DVD/USB/...). Ce module permet d'analyser, de bloquer ou d'ajuster les filtres étendus/autorisations, et de définir les autorisations des utilisateurs à accéder à un périphérique et à l'utiliser. Ce procédé peut être utile si l'administrateur souhaite empêcher l'utilisation de périphériques avec du contenu non sollicité.

Périphériques externes pris en charge :

- Stockage sur disque (disque dur, disque amovible USB)
- CD/DVD
- Imprimante USB
- Stockage FireWire
- Périphérique Bluetooth
- Lecteur de carte à puce
- Périphérique d'image
- Modem
- Port LPT/COM
- Périphérique portable
- Tous les types de périphérique

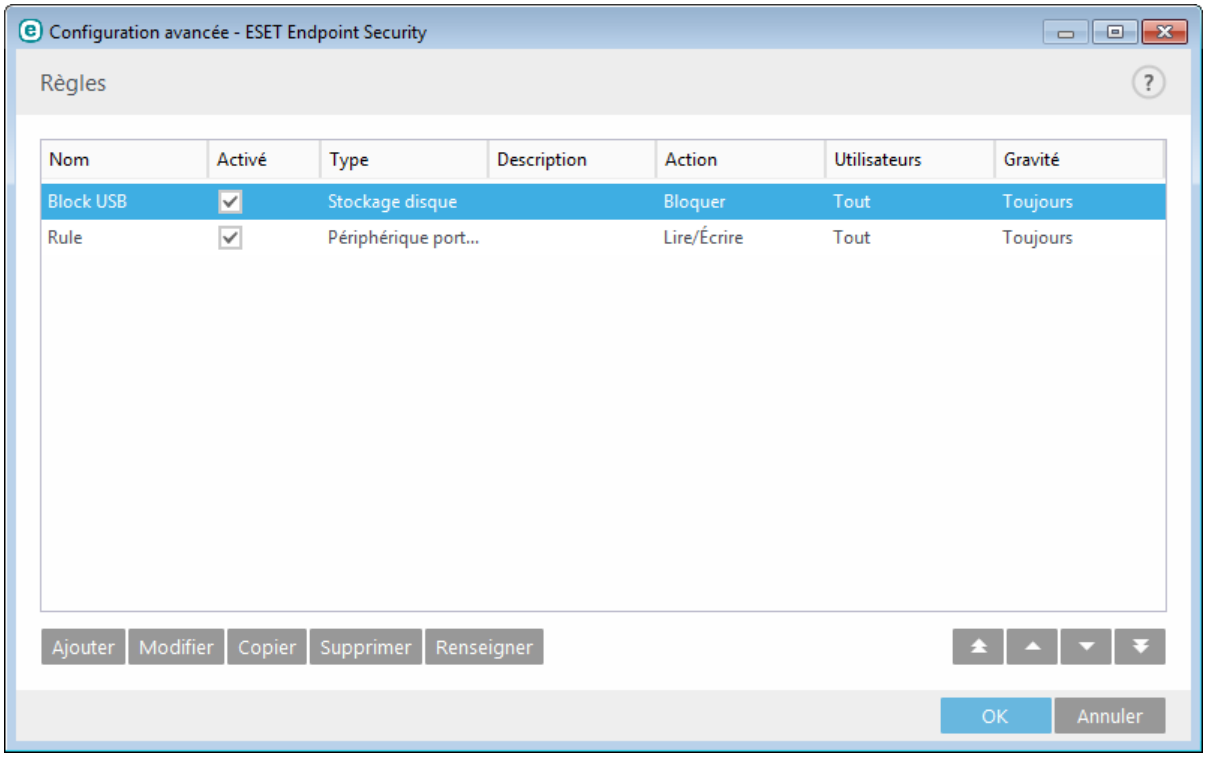
Les options de configuration du contrôle de périphérique peuvent être modifiées dans **Configuration avancée** (F5) > **Contrôle de périphérique**.

Si vous activez l'option **Intégrer au système**, la fonctionnalité de contrôle de périphérique est activée dans ESET Endpoint Security ; vous devrez redémarrer votre ordinateur pour que cette modification soit prise en compte. Une fois le contrôle de périphérique activé, les **règles** deviennent actives, ce qui vous permet d'ouvrir la fenêtre Éditeur de règles.

Si un périphérique bloqué par une règle existante est inséré, une fenêtre de notification s'affiche et l'accès au périphérique n'est pas accordé.

3.8.1.5.1 Éditeur de règles de contrôle de périphérique

La fenêtre **Éditeur de règles de contrôle de périphérique** affiche les règles existantes et permet un contrôle précis des périphériques externes que les utilisateurs peuvent connecter à l'ordinateur.



Des périphériques spécifiques peuvent être autorisés ou bloqués selon l'utilisateur, le groupe d'utilisateurs ou tout autre paramètre supplémentaire pouvant être spécifié dans la configuration des règles. La liste des règles contient plusieurs descriptions de la règle, telles que le nom, le type de périphérique externe, l'action à exécuter après la connexion d'un périphérique externe à l'ordinateur et le niveau de gravité d'après le journal.

Cliquez sur **Ajouter** ou **Modifier** pour gérer une règle. Décochez la case **Activé** en regard de la règle pour la désactiver jusqu'à ce que vous souhaitiez la réutiliser. Sélectionnez une ou plusieurs règles, puis cliquez sur **Supprimer** pour les supprimer définitivement.

Copier : cette option permet de créer une règle à l'aide d'options prédéfinies utilisées pour une autre règle sélectionnée.

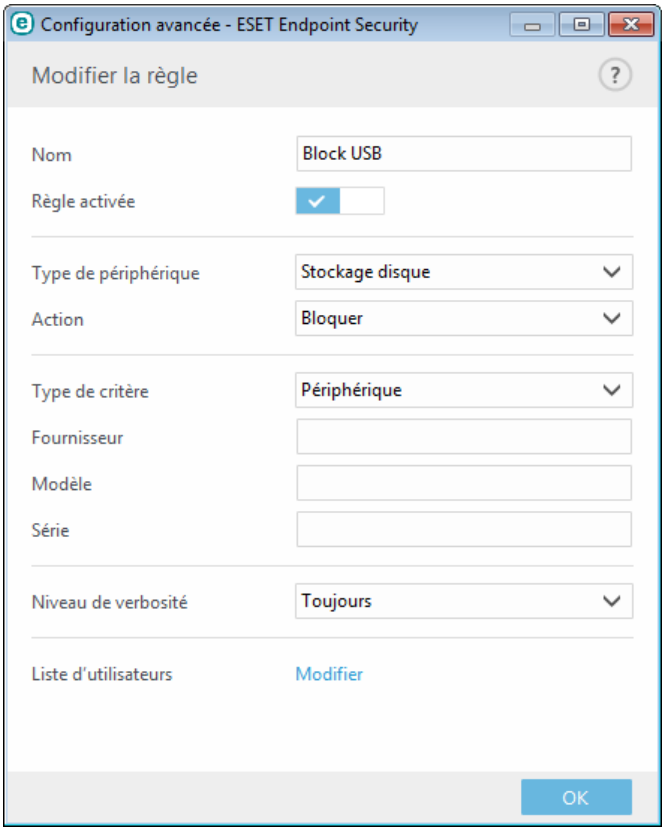
Cliquez sur l'option **Renseigner** pour renseigner automatiquement les paramètres des supports amovibles déjà connectés à votre ordinateur.

Les règles sont classées par ordre de priorité ; les règles de priorité supérieure sont dans la partie supérieure de la liste. Les règles peuvent être déplacées, séparément ou en groupe, en cliquant sur **Haut/Monter/Bas/Descendre**.

Le journal du contrôle de périphérique enregistre toutes les occurrences où le contrôle de périphérique est déclenché. Les entrées de journaux peuvent être affichées dans la fenêtre principale du programme ESET Endpoint Security dans **Outils** > **Fichiers journaux**.

3.8.1.5.2 Ajout de règles de contrôle de périphérique

Une règle de contrôle de périphérique définit l'action qui sera exécutée lorsqu'un périphérique répondant aux critères de la règle est connecté à l'ordinateur.



Entrez une description de la règle dans le champ **Nom** afin de mieux l'identifier. Cliquez sur le bouton bascule situé en regard de l'option **Règle activée** pour désactiver ou activer cette règle ; cette option peut être utile si vous ne souhaitez pas supprimer la règle de façon définitive.

Type de périphérique

Choisissez le type de périphérique externe dans le menu déroulant (Stockage disque/Périphérique portable/ Bluetooth/FireWire/...). Les informations sur le type de périphérique sont collectées à partir du système d'exploitation et sont visibles dans le Gestionnaire de périphériques système lorsqu'un périphérique est connecté à l'ordinateur. Les périphériques de stockage comprennent les disques externes ou les lecteurs de carte mémoire conventionnels connectés via USB ou FireWire. Les lecteurs de carte à puce regroupent tous les lecteurs de carte avec circuit intégré embarqué, telles que les cartes SIM ou d'authentification. Les scanners et les caméras sont des périphériques d'image. Comme ces périphériques fournissent uniquement des informations sur leurs actions, et non sur les utilisateurs, ils peuvent être bloqués uniquement de manière globale.

Action

L'accès aux périphériques autres que ceux de stockage peut être autorisé ou bloqué. En revanche, les règles s'appliquant aux périphériques de stockage permettent de sélectionner l'un des paramètres des droits suivants :

- **Lire/Écrire** - L'accès complet au périphérique sera autorisé.
- **Bloquer** - L'accès au périphérique sera bloqué.
- **Lecture seule** - L'accès en lecture seule au périphérique sera autorisé.
- **Avertir** - À chaque connexion d'un périphérique, l'utilisateur est averti s'il est autorisé/bloqué, et une entrée est enregistrée dans le journal. Comme les périphériques ne sont pas mémorisés, une notification continuera de s'afficher lors des connexions suivantes d'un même périphérique.

Il convient de noter que toutes les actions (autorisations) ne sont pas disponibles pour tous les types de périphériques. S'il s'agit d'un périphérique de stockage, les quatre actions sont disponibles. Pour les périphériques autres que les périphériques de stockage, seules trois actions sont disponibles (par exemple, l'action **Lecture seule**

n'étant pas disponible pour Bluetooth, un tel périphérique ne peut être qu'autorisé ou sujet à un avertissement).

Type de critère - Sélectionnez **Groupe de périphériques** ou **Périphérique**.

Les autres paramètres indiqués ci-dessous peuvent être utilisés pour optimiser les règles et les adapter à des périphériques. Tous les paramètres sont indépendants de la casse :

- **Fabricant** - Permet de filtrer par nom ou ID de fabricant.
- **Modèle** - Nom du périphérique.
- **N° de série** - Les périphériques externes ont généralement leur propre numéro de série. Dans le cas d'un CD/DVD, Il s'agit du numéro de série du support et pas du lecteur.

REMARQUE : si ces paramètres ne sont pas définis, la règle ignore ces champs lors de la recherche de correspondances. Les paramètres de filtrage de tous les champs de texte ne respectent pas la casse et les caractères génériques (*, ?) ne sont pas pris en charge.

CONSEIL : pour afficher des informations sur un périphérique, créez une règle pour ce type de périphérique, connectez le périphérique à votre ordinateur, puis consultez les informations détaillées du périphérique dans le journal du contrôle de périphérique.

Gravité

- **Toujours** - Consigne tous les événements.
- **Diagnostic** - Consigne les informations nécessaires au réglage du programme.
- **Informations** - Enregistre tous les messages d'information, y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissement** - Enregistre les erreurs critiques et les messages d'avertissement.
- **Aucune** - Aucun journal n'est enregistré.

Les règles peuvent être limitées à certains utilisateurs ou groupes d'utilisateurs en les ajoutant à la **Liste des utilisateurs** :

- **Ajouter** - Ouvre la boîte de dialogue **Types d'objet : utilisateurs ou groupes** qui permet de sélectionner les utilisateurs voulus.
- **Supprimer** - Supprime l'utilisateur sélectionné du filtre.

REMARQUE : tous les périphériques peuvent être filtrés par les règles de l'utilisateur (par exemple, les périphériques d'image ne fournissent pas d'informations sur les utilisateurs, uniquement sur les actions effectuées).

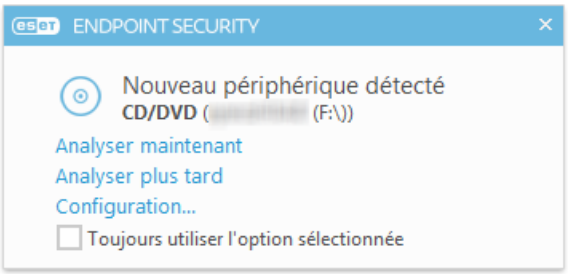
3.8.1.6 Supports amovibles

ESET Endpoint Security permet d'analyser automatiquement les supports amovibles (CD/DVD/USB...). Ce module permet d'analyser un support inséré. Cela peut être utile si l'administrateur souhaite empêcher les utilisateurs d'utiliser des supports amovibles avec du contenu non sollicité.

Action à entreprendre après l'insertion de support amovible - Sélectionnez l'action par défaut qui sera exécutée lors de l'insertion d'un support amovible (CD/DVD/USB). Si l'option **Afficher les options d'analyse** est sélectionnée, une notification vous autorise à choisir l'action adéquate :

- **Ne pas analyser** - Aucune action n'est exécutée et la fenêtre **Nouveau périphérique détecté** se ferme.
- **Analyse automatique de périphérique** - Le support amovible inséré fait l'objet d'une analyse à la demande.
- **Afficher les options d'analyse** - Ouvre la section de configuration des supports amovibles.

Lorsqu'un support amovible est inséré, la boîte de dialogue suivante s'affiche :



Analyser maintenant - Cette option déclenche l'analyse du support amovible.

Analyser ultérieurement - L'analyse du support amovible est reportée.

Configuration - Ouvre la boîte de dialogue Configuration avancée.

Toujours utiliser l'option sélectionnée - Lorsque cette option est sélectionnée, la même action sera exécutée lorsqu'un support amovible sera inséré plus tard.

En outre, ESET Endpoint Security offre la fonctionnalité de contrôle des périphériques qui permet de définir des règles d'utilisation de périphériques externes sur un ordinateur donné. Pour plus de détails sur le contrôle des périphériques, reportez-vous à la section Contrôle des périphériques.

3.8.1.7 Analyse en cas d'inactivité

Vous pouvez activer l'analyse en cas d'inactivité dans **Configuration avancée** sous **Antivirus** > **Analyse en cas d'inactivité** > **Général**. Placez le bouton bascule en regard de l'option **Activer l'analyse en cas d'inactivité** sur **Activer** pour activer cette fonctionnalité. Lorsque l'ordinateur n'est pas utilisé, une analyse silencieuse de l'ordinateur est effectuée sur tous les disques locaux. Consultez la section Déclencheurs de détection d'inactivité pour une liste complète des conditions qui doivent être satisfaites afin de déclencher l'analyse d'inactivité.

Par défaut, l'analyse d'inactivité n'est pas exécutée lorsque l'ordinateur (portable) fonctionne sur batterie. Vous pouvez passer outre ce paramètre en activant la case à cocher en regard de l'option **Exécuter même si l'ordinateur est alimenté sur batterie** dans la configuration avancée.

Activez le bouton bascule **Activer la journalisation** dans la configuration avancée pour enregistrer les sorties d'analyses d'ordinateur dans la section Fichiers journaux (à partir de la fenêtre principale du programme, cliquez sur **Outils** > **Fichiers journaux** et, dans le menu déroulant **Journaliser**, sélectionnez **Analyse de l'ordinateur**).

La détection en cas d'inactivité s'exécute lorsque les états de votre ordinateur sont les suivants :

- Économiseur d'écran
- Ordinateur verrouillé
- Utilisateur déconnecté

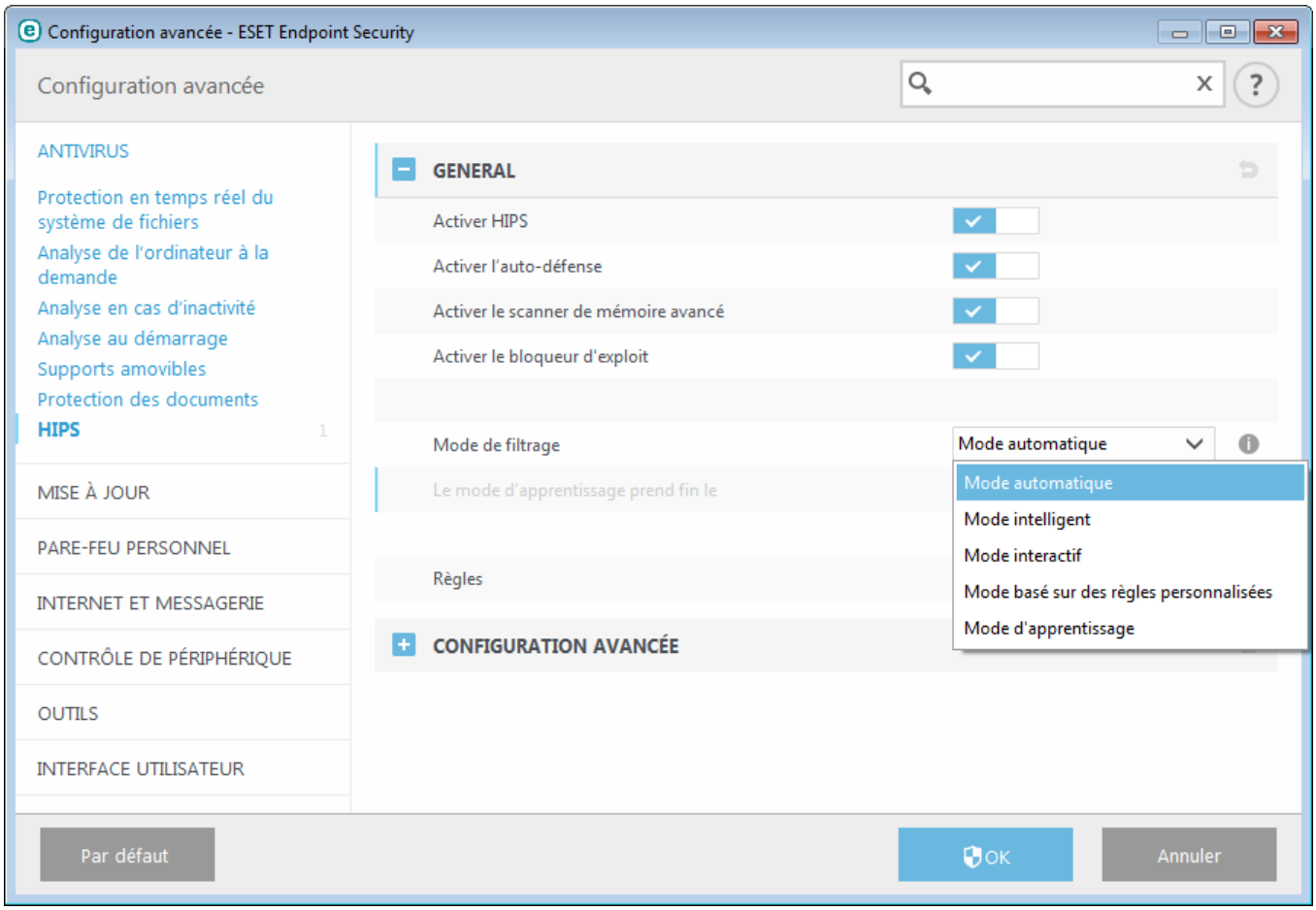
Cliquez sur Configuration des paramètres du moteur ThreatSense pour modifier les paramètres d'analyse (par exemple les méthodes de détection) pour l'analyse en cas d'inactivité.

3.8.1.8 Système HIPS

Les modifications apportées aux paramètres HIPS ne doivent être effectuées que par un utilisateur expérimenté. Une configuration incorrecte des paramètres HIPS peut en effet entraîner une instabilité du système.

Le **système HIPS (Host Intrusion Prevention System)** protège votre système des logiciels malveillants et de toute activité non souhaitée qui pourrait avoir une incidence sur votre ordinateur. Il utilise l'analyse avancée des comportements, associée aux fonctionnalités de détection du filtre réseau qui surveille les processus en cours, les fichiers et les clés de registre. Le système HIPS diffère de la protection en temps réel du système de fichiers et ce n'est pas un pare-feu. Il surveille uniquement les processus en cours d'exécution au sein du système d'exploitation.

Les paramètres HIPS sont disponibles dans **Configuration avancée** (F5) > **Antivirus** > **HIPS** > **Général**. L'état du système HIPS (activé/désactivé) est indiqué dans la fenêtre principale du programme ESET Endpoint Security, dans la section **Configuration** > **Ordinateur**.



ESET Endpoint Security utilise la technologie Auto-défense intégrée pour empêcher les logiciels malveillants d'endommager ou de désactiver la protection antivirus et antispyware ; vous avez la garantie que votre système est protégé en permanence. Il est nécessaire de redémarrer Windows pour désactiver le système HIPS ou Auto-défense.

Le **scanner de mémoire avancé** fonctionne avec le bloqueur d'exploit afin de renforcer la protection contre les logiciels malveillants qui ne sont pas détectés par les produits anti-logiciels malveillants grâce à l'obscurcissement ou au chiffrement. Le scanner de mémoire avancé est désactivé par défaut. Pour en savoir plus sur ce type de protection, consultez le glossaire.

Le **bloqueur d'exploit** est conçu pour renforcer les types d'applications connues pour être très vulnérables aux exploits (navigateurs, lecteurs de fichiers PDF, clients de messagerie et composants MS Office). Le bloqueur d'exploit est désactivé par défaut. Pour en savoir plus sur ce type de protection, consultez le glossaire.

Le filtrage peut être effectué dans l'un des quatre modes :

Mode automatique - Les opérations sont autorisées, à l'exception de celles bloquées par des règles prédéfinies qui

protègent votre système.

Mode interactif - L'utilisateur est invité à confirmer les opérations.

Mode basé sur des règles personnalisées - Les opérations sont bloquées.

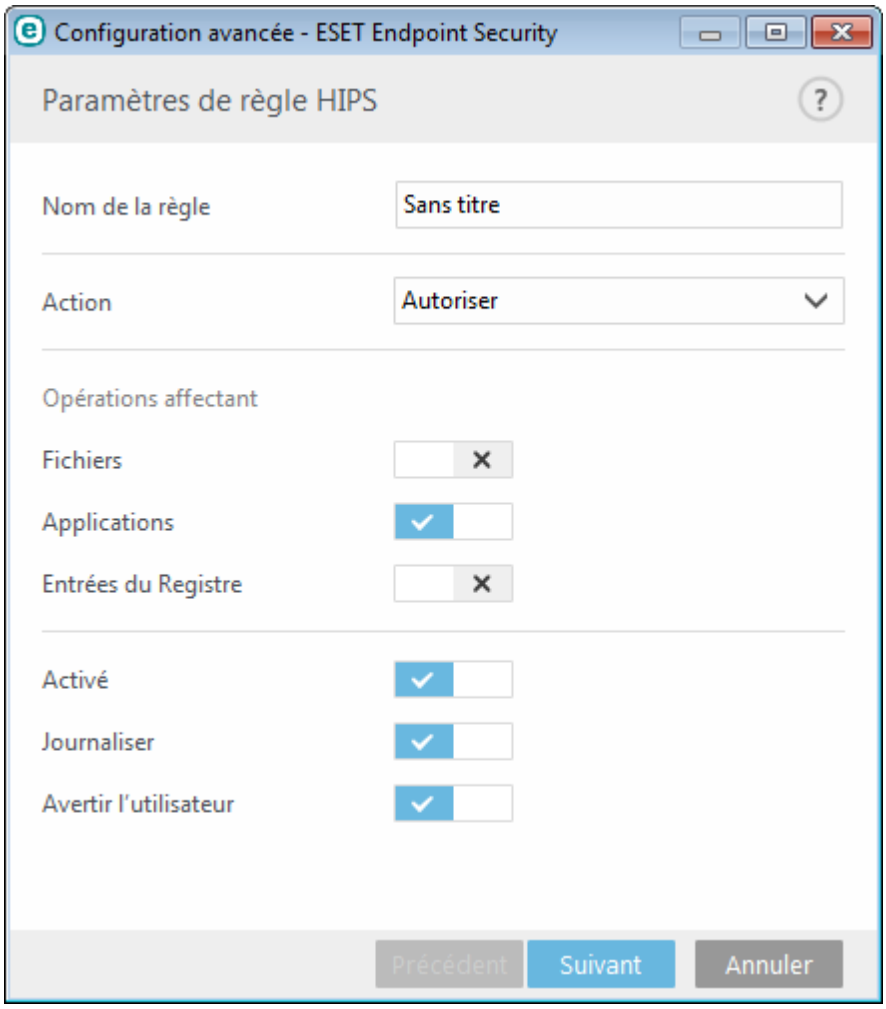
Mode d'apprentissage - Les opérations sont autorisées et une règle est créée après chaque opération. Les règles créées dans ce mode peuvent être affichées dans l'éditeur de règles, mais leur niveau de priorité est inférieur à celui des règles créées manuellement ou en mode automatique. Lorsque vous sélectionnez l'option Mode d'apprentissage dans le menu déroulant Mode de filtrage HIPS, le paramètre **Le mode d'apprentissage prend fin le** devient disponible. Sélectionnez la durée du mode d'apprentissage. La durée maximale est de 14 jours. Lorsque la durée spécifiée est arrivée à son terme, vous êtes invité à modifier les règles créées par HIPS en mode d'apprentissage. Vous pouvez également choisir un autre mode de filtrage ou continuer à utiliser le mode d'apprentissage.

Mode intelligent - L'utilisateur n'est averti que lors d'événements très suspects.

Le système HIPS surveille les événements dans le système d'exploitation et réagit en fonction de règles qui sont semblables à celles utilisées par le pare-feu personnel. Cliquez sur **Modifier** pour ouvrir la fenêtre de gestion des règles HIPS. Cette fenêtre vous permet de sélectionner, de créer, de modifier ou de supprimer des règles.

Dans l'exemple suivant, nous allons montrer comment limiter le comportement indésirable des applications :

1. Nommez la règle et sélectionnez **Bloquer** dans le menu déroulant **Action**.
2. Activez le bouton bascule **Avertir l'utilisateur** pour afficher une notification à chaque fois qu'une règle est appliquée.
3. Sélectionnez au moins une opération pour laquelle la règle sera appliquée. Dans la fenêtre **Applications source**, sélectionnez **Toutes les applications** dans le menu déroulant pour appliquer la nouvelle règle à toutes les applications qui tentent d'effectuer les opérations sélectionnées sur les applications spécifiées.
4. Sélectionnez **Modifier l'état d'une autre application**(toutes les opérations sont décrites dans l'aide du produit disponible en appuyant sur la touche F1)..
5. Sélectionnez **Applications spécifiques** dans le menu déroulant, puis **ajoutez** une ou plusieurs applications à protéger.
6. Cliquez sur **Terminer** pour enregistrer la nouvelle règle.



3.8.1.8.1 Configuration avancée

Les options suivantes sont utiles au débogage et à l'analyse d'un comportement d'application :

Pilotes dont le chargement est toujours autorisé - Le chargement des pilotes sélectionnés est toujours autorisé, quel que soit le mode de filtrage configuré, excepté en cas de blocage explicite par une règle utilisateur.

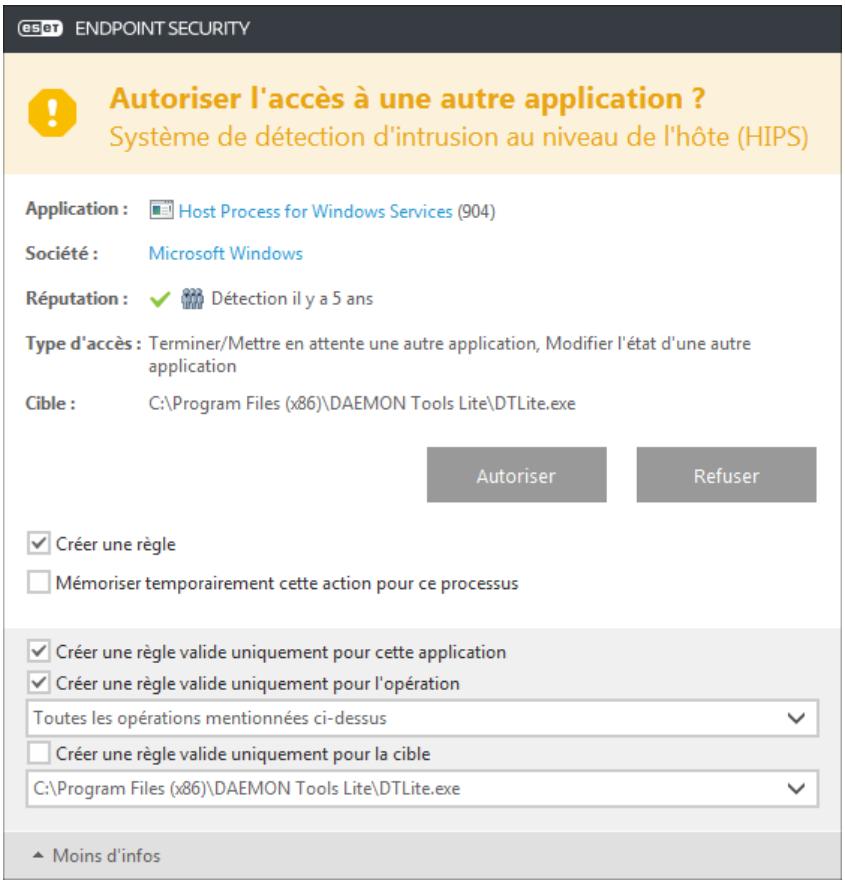
Consigner toutes les opérations bloquées - Toutes les opérations bloquées sont inscrites dans le journal HIPS.

Avertir en cas de changements dans les applications de démarrage : affiche une notification sur le Bureau chaque fois qu'une application est ajoutée au démarrage du système ou en est supprimée.

Veuillez vous reporter à notre base de connaissance pour une version mise à jour de cette page d'aide.

3.8.1.8.2 Fenêtre interactive HIPS

Si l'action par défaut d'une règle est définie sur **Demander**, une boîte de dialogue apparaît à chaque déclenchement de la règle. Vous pouvez choisir de **refuser** ou **autoriser** l'opération. Si vous ne choisissez aucune action dans la période donnée, une nouvelle action est sélectionnée en fonction des règles.



La boîte de dialogue permet de créer une règle en fonction de toute nouvelle action détectée par le système HIPS, puis de définir les conditions dans lesquelles autoriser ou refuser cette action. Pour définir les paramètres exacts, cliquez sur **Plus d'infos**. Les règles créées de cette manière sont équivalentes aux règles créées manuellement ; la règle créée à partir d'une boîte de dialogue peut être moins spécifique que celle qui a déclenché l'affichage de la boîte de dialogue. En d'autres termes, après la création d'une règle, la même opération peut déclencher la même fenêtre.

Mémoriser temporairement cette action pour ce processus entraîne la mémorisation de l'action (**Autoriser/Refuser**) à utiliser jusqu'à la modification des règles ou du mode de filtrage, une mise à jour du module HIPS ou le redémarrage du système. À l'issue de l'une de ces trois actions, les règles temporaires seront supprimées.

3.8.1.9 Mode de présentation

Le mode de présentation est une fonctionnalité destinée aux utilisateurs qui ne veulent pas être interrompus lors de l'utilisation de leur logiciel. Ils ne souhaitent pas être dérangés par des fenêtres contextuelles et veulent réduire les contraintes sur l'UC. Il peut également être utilisé au cours de présentations qui ne peuvent pas être interrompues par l'activité antivirus. Lorsqu'il est activé, toutes les fenêtres contextuelles sont désactivées et les tâches planifiées ne sont pas exécutées. La protection du système continue à fonctionner en arrière-plan, mais n'exige aucune interaction de la part de l'utilisateur.

Cliquez sur **Configuration** > **Ordinateur**, puis sur le bouton bascule en regard de l'option **Mode de présentation** pour activer manuellement le mode de présentation. Dans **Configuration avancée** (F5), cliquez sur **Outils** > **Mode de présentation**, puis sur le bouton bascule en regarde de l'option **Activer le mode de présentation automatiquement lors de l'exécution d'applications en mode plein écran** pour qu'ESET Endpoint Security active automatiquement le mode de présentation lorsque les applications sont exécutées en mode plein écran. L'activation du mode de présentation constitue un risque potentiel pour la sécurité. C'est la raison pour laquelle l'icône d'état de la protection située dans la barre des tâches devient orange et affiche un symbole d'avertissement. Ce symbole

apparaît également dans la fenêtre principale du programme, où **Mode de présentation activé** apparaît en orange.

Lorsque l'option **Activer le mode de présentation automatiquement lors de l'exécution d'applications en mode plein écran** est activée, le mode de présentation démarre lorsque vous lancez une application en mode plein écran et s'arrête automatiquement lorsque vous quittez l'application. Cette option est particulièrement utile, car elle permet de démarrer le mode de présentation immédiatement après le démarrage d'un jeu, l'ouverture d'une application en mode plein écran ou le démarrage d'une présentation.

Vous pouvez également sélectionner **Désactiver automatiquement le mode de présentation après** pour définir une durée en minutes après laquelle le mode de présentation est automatiquement désactivé.

REMARQUE : si le pare-feu personnel est en mode interactif et que le mode de présentation est activé, vous risquez de rencontrer des difficultés pour vous connecter à Internet. Cela peut être problématique si vous démarrez un jeu qui se connecte à Internet. Dans un tel cas, vous devriez normalement recevoir une demande de confirmation de cette action (si aucune règle de communication ni exception n'a été définie), mais l'interaction utilisateur est désactivée en mode de présentation. La solution consiste à définir une règle de communication pour chaque application pouvant entrer en conflit avec ce comportement. Il est également possible d'utiliser un autre mode de filtrage dans le pare-feu personnel. Notez que si le mode de présentation est activé, et que vous accédez à une page Web ou à une application qui peut constituer un risque pour la sécurité, cette page peut être bloquée. En revanche, vous ne recevez aucune explication ni avertissement, car l'interaction utilisateur est désactivée.

3.8.1.10 Analyse au démarrage

Par défaut, la vérification automatique des fichiers au démarrage est effectuée au démarrage du système et lors des mises à jour de la base des signatures de virus. Cette analyse dépend de la configuration et des tâches du Planificateur.

Les options d'analyse au démarrage font partie de la tâche planifiée **Contrôle des fichiers de démarrage du système**. Pour modifier les paramètres d'analyse au démarrage, accédez à **Outils** > **Planificateur**, cliquez sur **Vérification automatique des fichiers de démarrage**, puis sur **Modifier**. À la dernière étape, la fenêtre Vérification des fichiers de démarrage s'affichera (reportez-vous à la section suivante pour plus de détails).

Pour des instructions détaillées sur la création et à la gestion de tâches planifiées, voir Création de nouvelles tâches.

3.8.1.10.1 Vérification automatique des fichiers de démarrage

Lorsque vous créez une tâche planifiée de contrôle des fichiers au démarrage du système, plusieurs options s'offrent à vous pour définir les paramètres suivants :

Le menu déroulant **Fichiers couramment utilisés** définit la profondeur d'analyse pour les fichiers qui s'exécutent au démarrage du système selon un algorithme sophistiqué secret. Les fichiers sont organisés par ordre décroissant suivant ces critères :

- **Tous les fichiers enregistrés** (la plupart des fichiers sont analysés)
- **Fichiers rarement utilisés**
- **Fichiers couramment utilisés**
- **Fichiers fréquemment utilisés**
- **Seulement les fichiers utilisés fréquemment** (nombre minimum de fichiers analysés)

Il existe en outre deux groupes spécifiques :

- **Fichiers exécutés avant la connexion de l'utilisateur** - Contient des fichiers situés à des emplacements accessibles sans qu'une session ait été ouverte par l'utilisateur (englobe pratiquement tous les emplacements de démarrage tels que services, objets Application d'assistance du navigateur, notification Winlogon, entrées de planificateur Windows, DLL connues, etc.).
- **Fichiers exécutés après la connexion de l'utilisateur** - Contient des fichiers situés à des emplacements accessibles uniquement après l'ouverture d'une session par l'utilisateur (englobe des fichiers qui ne sont exécutés que pour un utilisateur spécifique, généralement les fichiers de *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*)

Les listes des fichiers à analyser sont fixes pour chaque groupe précité.

Priorité d'analyse - Niveau de priorité servant à déterminer le démarrage d'une analyse :

- **En période d'inactivité** - la tâche n'est exécutée que lorsque le système est inactif,
- **La plus faible** - lorsque la charge du système est la plus faible possible,
- **Faible** - lorsque le système est faiblement chargé,
- **Normale** - lorsque le système est moyennement chargé.

3.8.1.11 Protection des documents

La fonctionnalité de protection des documents analyse les documents Microsoft Office avant leur ouverture, ainsi que les fichiers téléchargés automatiquement par Internet Explorer, tels que des éléments Microsoft ActiveX. La protection des documents fournit une couche de protection supplémentaire qui vient s'ajouter à la protection en temps réel du système de fichiers. Elle peut être désactivée pour améliorer la performance des systèmes qui ne sont pas exposés à un grand nombre de documents Microsoft Office.

Intégration du système active le système de protection. Pour modifier cette option, appuyez sur F5 pour ouvrir la fenêtre Configuration avancée et cliquez sur **Antivirus** > **Protection des documents** dans l'arborescence de la configuration avancée.

Cette fonctionnalité est activée par des applications utilisant Microsoft Antivirus API (par exemple Microsoft Office 2000 et versions ultérieures, ou Microsoft Internet Explorer 5.0 et versions ultérieures).

3.8.1.12 Exclusions

Les exclusions permettent d'exclure des fichiers et dossiers de l'analyse. Pour que la détection des menaces s'appliquent bien à tous les objets, il est recommandé de ne créer des exclusions que lorsque cela s'avère absolument nécessaire. Certaines situations justifient l'exclusion d'un objet. Par exemple, lorsque les entrées de bases de données volumineuses risquent de ralentir l'ordinateur pendant l'analyse ou lorsqu'il peut y avoir conflit entre le logiciel et l'analyse (par exemple, logiciel de sauvegarde).

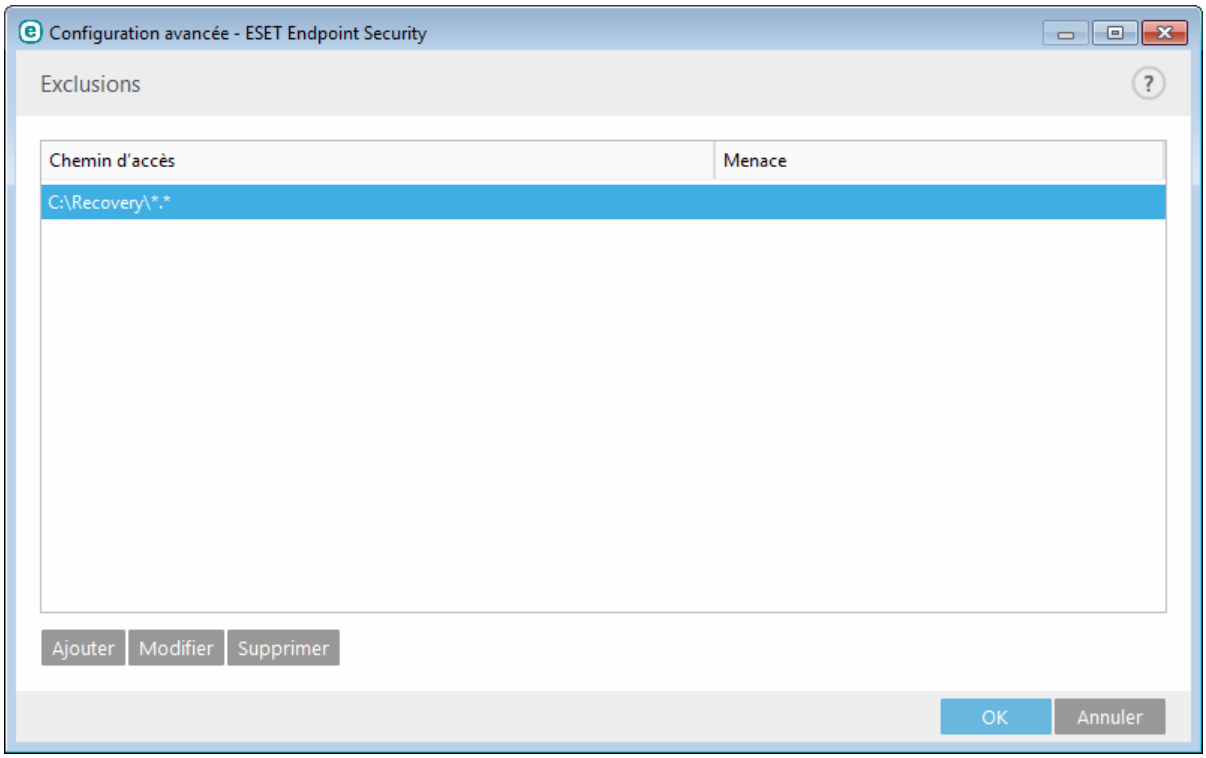
Pour exclure un objet de l'analyse :

1. Cliquez sur **Ajouter**.
2. Entrez le chemin d'un objet ou sélectionnez-le dans l'arborescence.

Vous pouvez utiliser des caractères génériques pour indiquer un groupe de fichiers. Un point d'interrogation (?) représente un seul caractère variable tandis qu'un astérisque (*) représente une chaîne variable de zéro caractère ou plus.

Exemples

- Si vous souhaitez exclure tous les fichiers d'un dossier, tapez le chemin d'accès au dossier et utilisez le masque « *.* ».
- Pour exclure un disque complet avec tous ses fichiers et sous-dossiers, utilisez le masque « D:\ ».
- Si vous ne souhaitez exclure que les fichiers doc, utilisez le masque « *.doc ».
- Si le nom d'un fichier exécutable comporte un certain nombre de caractères variables dont vous ne connaissez que le premier (par exemple « D »), utilisez le format suivant : « D????.exe ». Les points d'interrogation remplacent les caractères manquants (inconnus).



REMARQUE : une menace présente dans un fichier n'est pas détectée par le module de protection du système de fichiers en temps réel ou par le module d'analyse de l'ordinateur si le fichier en question répond aux critères d'exclusion de l'analyse.

Colonnes

Chemin - Chemin d'accès aux fichiers et dossiers exclus.

Menace - Si le nom d'une menace est affiché en regard d'un fichier exclu, cela signifie que ce fichier n'est exclu que pour cette menace. Si le fichier est infecté ultérieurement par un autre logiciel malveillant, il est détecté par le module antivirus. Ce type d'exclusion ne peut être utilisé que pour certains types d'infiltrations. Il peut être créé soit dans la fenêtre des alertes de menaces qui signale l'infiltration (cliquez sur **Afficher les options avancées** et sélectionnez **Exclure de la détection**), soit en cliquant sur **Configuration** > **Quarantaine** à l'aide d'un clic droit sur le fichier placé en quarantaine et en sélectionnant **Restaurer et exclure de la détection** dans le menu contextuel.

Éléments de commande

Ajouter - Exclut les objets de la détection.

Modifier - Permet de modifier des entrées sélectionnées.

Supprimer - Supprime les entrées sélectionnées.

3.8.1.13 Configuration des paramètres du moteur ThreatSense

ThreatSense est une technologie constituée de nombreuses méthodes complexes de détection de menaces. C'est une technologie proactive : elle fournit une protection dès le début de la propagation d'une nouvelle menace. Elle utilise une combinaison d'analyse de code, d'émulation de code, de signatures génériques et de signatures de virus qui se conjuguent pour améliorer sensiblement la sécurité du système. Ce moteur d'analyse est capable de contrôler plusieurs flux de données simultanément, ce qui maximise l'efficacité et le taux de détection. La technologie ThreatSense élimine avec succès les rootkits.

Les options de configuration du moteur ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

- les types de fichiers et les extensions à analyser ;
- la combinaison de plusieurs méthodes de détection ;
- les niveaux de nettoyage, etc.

Pour ouvrir la fenêtre de configuration, cliquez sur **Configuration des paramètres du moteur ThreatSense** dans la fenêtre de configuration avancée de chaque module utilisant la technologie ThreatSense (reportez-vous aux informations ci-dessous). Chaque scénario de sécurité peut exiger une configuration différente. ThreatSense est configurable individuellement pour les modules de protection suivants :

- protection en temps réel du système de fichiers ;
- analyse en cas d'inactivité ;
- analyse au démarrage ;
- protection des documents ;
- protection du client de messagerie ;
- protection de l'accès au Web ;
- analyse de l'ordinateur.

Les paramètres ThreatSense sont spécifiquement optimisés pour chaque module et leur modification peut avoir une incidence significative sur le fonctionnement du système. Par exemple, en modifiant les paramètres pour toujours analyser les Fichiers exécutables compressés par un compresseur d'exécutables ou pour autoriser l'heuristique avancée dans la protection en temps réel du système de fichiers, vous pouvez dégrader les performances du système (normalement, seuls les fichiers nouvellement créés sont analysés par ces méthodes). Il est donc recommandé de ne pas modifier les paramètres par défaut de ThreatSense pour tous les modules, à l'exception du module Analyse de l'ordinateur.

Objets à analyser

Cette section permet de définir les fichiers et les composants de l'ordinateur qui vont faire l'objet d'une analyse visant à rechercher les éventuelles infiltrations.

Mémoire vive - Lance une analyse visant à rechercher les menaces qui attaquent la mémoire vive du système.

Secteurs d'amorçage - Analyse les secteurs d'amorçage afin de détecter la présence éventuelle de virus dans l'enregistrement d'amorçage principal.

Fichiers des courriers électroniques - Le programme prend en charge les extensions suivantes : DBX (Outlook Express) et EML.

Archives - Le programme prend en charge les extensions suivantes : ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE et de nombreuses autres extensions.

Archives auto-extractibles - Les archives auto-extractibles (SFX) n'ont pas besoin de programmes spécialisés pour être décompressées.

Fichiers exécutables compressés - Contrairement aux archiveurs standard, ces fichiers se décompressent en mémoire. Outre les compacteurs statiques standard (UPX, yoda, ASPack, FSG, etc.), l'analyseur peut reconnaître plusieurs autres types de compacteurs via l'utilisation de l'émulation de code.

Options d'analyse

Sélectionnez les méthodes à utiliser lors de la recherche d'infiltrations dans le système. Les options disponibles sont les suivantes :

Heuristique - La méthode heuristique utilise un algorithme d'analyse de l'activité (malveillante) des programmes. Elle présente l'avantage d'identifier un code malveillant qui n'existait pas ou qui n'était pas connu par la base de signatures de virus antérieure. Cette méthode présente néanmoins l'inconvénient d'une probabilité (très faible) de fausses alarmes.

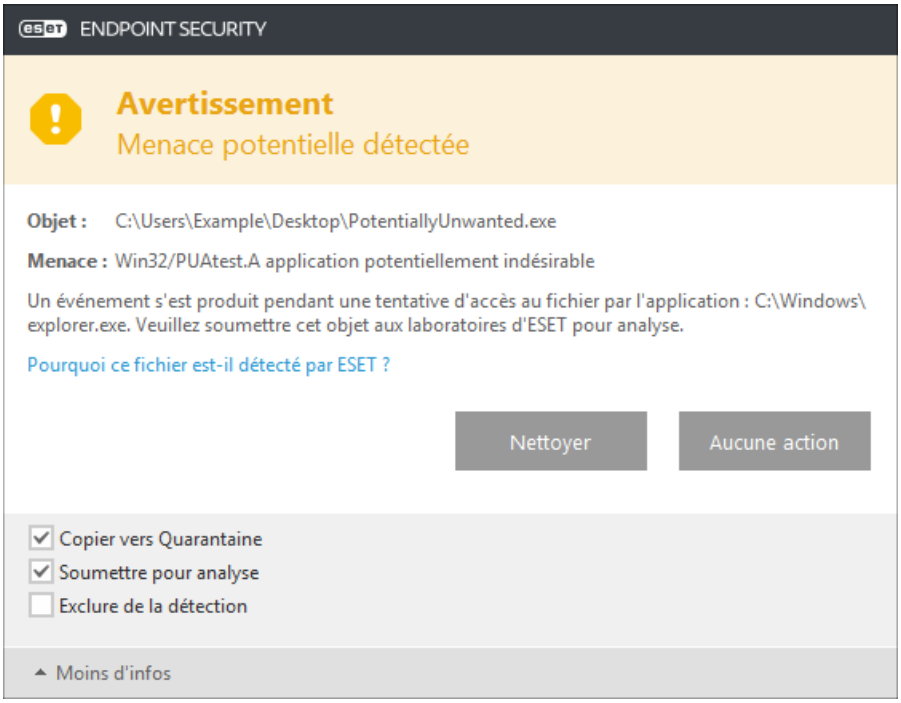
Heuristique avancée/ADN/Signatures intelligentes - La méthode heuristique avancée utilise un algorithme heuristique développé par ESET, optimisé pour la détection des vers d'ordinateur et des chevaux de Troie, et écrit dans un langage de programmation de haut niveau. L'utilisation de la méthode heuristique avancée accroît de manière significative les possibilités de détection des menaces des produits ESET. Les signatures peuvent détecter et identifier les virus avec grande efficacité. Grâce au système de mise à jour automatique, les nouvelles signatures peuvent être disponibles dans les quelques heures qui suivent la détection des menaces. L'inconvénient des signatures est qu'elles ne détectent que les virus qu'elles connaissent (ou leurs versions légèrement modifiées).

Une application potentiellement indésirable est un programme qui contient un logiciel publicitaire, qui installe des barres d'outils ou dont les objectifs ne sont pas clairs. Dans certains cas, un utilisateur peut estimer que les avantages offerts par une application potentiellement 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 (chevaux de Troie ou vers, par exemple).

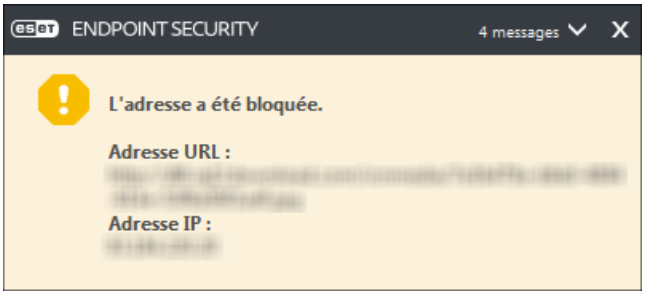
Avertissement - Menace potentielle détectée

Lorsqu'une application potentiellement indésirable est détectée, vous pouvez choisir l'action à exécuter :

1. **Nettoyer/Déconnecter** : cette option met fin à l'action et empêche la menace potentielle de pénétrer dans le système.
2. **Aucune action** : cette option permet à une menace potentielle de pénétrer dans le système.
3. Pour permettre l'exécution future de l'application sur votre ordinateur sans interruption, cliquez sur **Plus d'infos/ Afficher les options avancées**, puis cochez la case en regard de l'option **Exclure de la détection**.

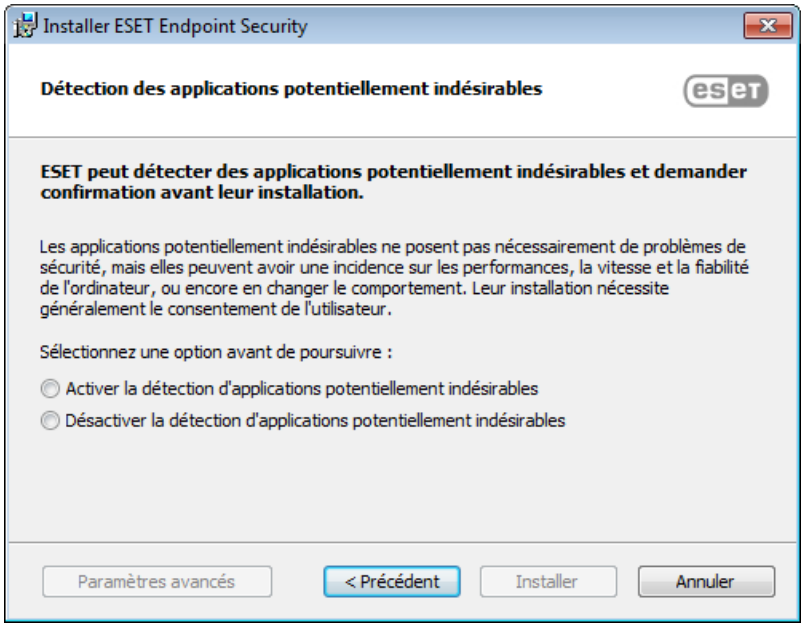


Lorsqu'une application potentiellement indésirable est détectée et qu'il n'est pas possible de procéder au nettoyage, la fenêtre de notification **L'adresse a été bloquée** s'affiche dans le coin inférieur droit de l'écran. Pour obtenir plus d'informations sur cet événement, accédez à **Outils** > **Fichiers journaux** > **Sites Web filtrés** à partir du menu principal.



Applications potentiellement indésirables - Paramètres

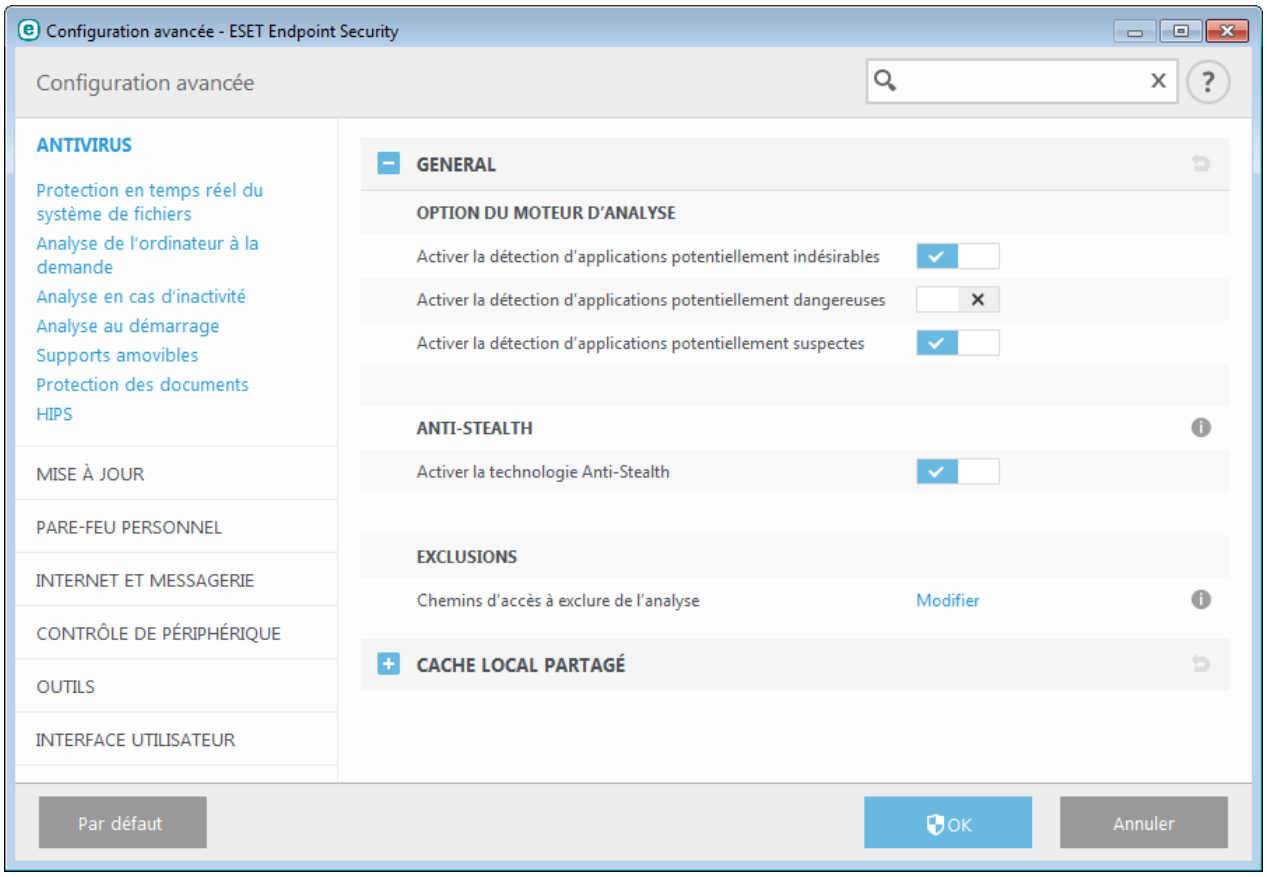
Lorsque vous installez votre produit ESET, vous pouvez choisir d'activer ou non la détection des applications potentiellement indésirables, comme illustré ci-dessous.



Les applications potentiellement indésirables peuvent installer des logiciels publicitaires et des barres d'outils ou contenir d'autres fonctionnalités indésirables ou dangereuses.

Ces paramètres peuvent être modifiés à tout moment dans les paramètres du programme. Pour activer ou désactiver la détection des applications potentiellement indésirables, dangereuses ou suspectes, procédez comme suit :

1. Ouvrez votre produit ESET. Comment ouvrir mon produit ESET ?
2. Appuyez sur la touche **F5** pour accéder à **Configuration avancée**.
3. Cliquez sur **Antivirus**, puis activez ou désactivez les options **Activer la détection des applications potentiellement indésirables**, **Activer la détection d'applications potentiellement dangereuses** et **Activer la détection d'applications potentiellement suspectes**, selon vos préférences. Cliquez ensuite sur **OK** pour confirmer.



Applications potentiellement indésirables - Wrappers logiciels

Un wrapper logiciel est un type spécial de modification d'application qui est utilisé par certains sites Web d'hébergement de fichiers. Il s'agit d'un outil tiers qui installe le programme que vous avez téléchargé tout en ajoutant d'autres logiciels comme des barres d'outils ou des logiciels publicitaires. Les autres logiciels peuvent également apporter des modifications à la page d'accueil de votre navigateur Web et aux paramètres de recherche. De plus, les sites Web d'hébergement de fichiers n'avertissent pas l'éditeur ou le destinataire du téléchargement que des modifications ont été apportées et ne permettent pas de les annuler facilement. Pour ces raisons, ESET classe les wrappers logiciels comme un type d'application potentiellement indésirable afin que les utilisateurs puissent accepter ou non de les télécharger.

Consultez cet article de la base de données ESET pour une version mise à jour de cette page d'aide.

Applications potentiellement dangereuses - Applications potentiellement dangereuses correspond à la classification utilisée pour les logiciels commerciaux légitimes, tels que les programmes d'accès à distance, les applications de résolution de mot de passe ou les keyloggers ((programmes qui enregistrent chaque frappe au clavier de l'utilisateur). Cette option est désactivée par défaut.

ESET Live Grid - Grâce à la technologie de réputation d'ESET, les informations sur les fichiers analysés sont comparées aux données issues du système ESET Live Grid basé sur le cloud computing. Cette comparaison permet d'améliorer la détection tout en accélérant l'analyse.

Nettoyage

Les paramètres de nettoyage déterminent le comportement de l'analyseur lors du nettoyage des fichiers infectés. Trois niveaux de nettoyage sont possibles :

Pas de nettoyage - Les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche alors une fenêtre d'avertissement et laisse l'utilisateur choisir une action. Ce niveau est conçu pour les utilisateurs expérimentés qui connaissent les actions à entreprendre en cas d'infiltration.

Nettoyage normal - Le programme tente de nettoyer ou de supprimer automatiquement tout fichier sur la base d'une action prédéfinie (dépendant du type d'infiltration). La détection et la suppression d'un fichier infecté sont signalées par une notification affichée dans l'angle inférieur droit de l'écran. S'il n'est pas possible de sélectionner automatiquement l'action correcte, le programme propose plusieurs actions de suivi. C'est le cas également si une

action prédéfinie ne peut pas être menée à bien.

Nettoyage strict - Le programme nettoie ou supprime tous les fichiers infectés. Les seules exceptions sont les fichiers système. S'il n'est pas possible de les nettoyer, l'utilisateur est invité à sélectionner une action dans une fenêtre d'avertissement.

Avertissement : si une archive contient un ou plusieurs fichiers infectés, elle peut être traitée de deux façons différentes. En mode standard (Nettoyage standard), toute l'archive est supprimée si tous ses fichiers sont infectés. En mode de **nettoyage strict**, l'archive est supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

Exclusions

L'extension est la partie du nom de fichier située après le point. Elle définit le type et le contenu du fichier. Cette section de la configuration des paramètres ThreatSense vous permet de définir les types de fichiers à analyser.

Autre

Lorsque vous configurez les paramètres du moteur ThreatSense pour l'analyse à la demande d'un ordinateur, vous disposez également des options de la section **Autre** suivantes :

Analyser les flux de données alternatifs (ADS) - Les flux de données alternatifs (ADS) utilisés par le système de fichiers NTFS sont des associations de fichiers et de dossiers que les techniques d'analyse ordinaires ne permettent pas de détecter. De nombreuses infiltrations tentent d'éviter la détection en se faisant passer pour des flux de données alternatifs.

Exécuter les analyses en arrière-plan avec une priorité faible - Toute séquence d'analyse consomme une certaine quantité de ressources système. Si vous utilisez des programmes qui exigent une grande quantité de ressources système, vous pouvez activer l'analyse en arrière-plan à faible priorité de manière à réserver des ressources pour vos applications.

Journaliser tous les objets - Si cette option est sélectionnée, le fichier journal affiche tous les fichiers analysés, même ceux qui ne sont pas infectés. Par exemple, si une infiltration est détectée dans une archive, le journal répertorie également les fichiers nettoyés contenus dans l'archive.

Activer l'optimisation intelligente - Lorsque cette option est sélectionnée, les paramètres optimaux sont utilisés de manière à garantir le niveau d'analyse le plus efficace tout en conservant la meilleure vitesse d'analyse. Les différents modules de protection proposent une analyse intelligente en utilisant différentes méthodes et en les appliquant à des types de fichiers spécifiques. Si l'option Activer l'optimisation intelligente est désactivée, seuls les paramètres définis par l'utilisateur dans le noyau ThreatSense des différents modules sont appliqués lors de la réalisation d'une analyse.

Conserver la date et l'heure du dernier accès - Sélectionnez cette option pour conserver l'heure d'accès d'origine des fichiers analysés au lieu de les mise à jour (par exemple, pour les utiliser avec des systèmes de sauvegarde de données).

Limites

La section Limites permet de spécifier la taille maximale des objets et les niveaux d'imbrication des archives à analyser :

Paramètres d'objet

Taille maximale d'objet - Définit la taille maximale des objets à analyser. Le module antivirus n'analyse que les objets d'une taille inférieure à celle spécifiée. Cette option ne doit être modifiée que par des utilisateurs expérimentés et qui ont des raisons particulières d'exclure de l'analyse des objets de plus grande taille. Valeur par défaut : *illimité*.

Durée d'analyse maximale pour l'objet (s) - Définit la durée maximum attribuée à l'analyse d'un objet. Si la valeur de ce champ a été définie par l'utilisateur, le module antivirus cesse d'analyser un objet une fois ce temps écoulé, que l'analyse soit terminée ou non. Valeur par défaut : *illimité*.

Configuration de l'analyse d'archive

Niveau d'imbrication des archives - Spécifie la profondeur maximale d'analyse des archives. Valeur par défaut : *10*.

Taille maximale de fichier dans l'archive - Cette option permet de spécifier la taille maximale des fichiers (après extraction) à analyser contenus dans les archives. Valeur par défaut : *illimité*.

REMARQUE : il n'est pas recommandé de modifier les valeurs par défaut. Dans des circonstances normales, il n'y a aucune raison de le faire.

3.8.1.13.1 Exclusions

L'extension est la partie du nom de fichier située après le point. Elle définit le type et le contenu du fichier. Cette section de la configuration des paramètres ThreatSense vous permet de définir les types de fichiers à analyser.

Par défaut, tous les fichiers sont analysés. Toutes les extensions peuvent être ajoutées à la liste des fichiers exclus de l'analyse.

L'exclusion de fichiers peut être utile si l'analyse de certains types de fichiers provoque un dysfonctionnement de l'application utilisant certaines extensions. Par exemple, il peut être judicieux d'exclure les extensions .edb, .eml et .tmp si vous utilisez le serveur Microsoft Exchange.

Les boutons **Ajouter** et **Supprimer** permettent d'activer ou d'empêcher l'analyse des fichiers portant certaines extensions. Pour ajouter une nouvelle extension à la liste, cliquez sur **Ajouter**, tapez l'extension dans le champ correspondant, puis cliquez sur **OK**. Lorsque vous sélectionnez **Entrer plusieurs valeurs**, vous pouvez ajouter plusieurs extensions de fichier en les séparant par des lignes, des virgules ou des points-virgules. Lorsque la sélection multiple est activée, les extensions s'affichent dans la liste. Sélectionnez une extension dans la liste, puis cliquez sur **Supprimer** pour la supprimer de la liste. Si vous souhaitez modifier une extension sélectionnée, cliquez sur **Modifier**.

Vous pouvez utiliser les symboles spéciaux « * » (astérisque) et « ? » (point d'interrogation). L'astérisque représente n'importe quelle chaîne de caractères, tandis que le point d'interrogation symbolise n'importe quel caractère.

3.8.2 Réseau

Le pare-feu personnel contrôle tout le trafic réseau entrant et sortant du système. Il autorise ou refuse les différentes connexions réseau en se basant sur vos règles de filtrage. Il fournit une protection contre les attaques en provenance d'ordinateurs distants et permet de bloquer certains services potentiellement dangereux. Le pare-feu personnel offre également la fonctionnalité IDS/IPS en inspectant le contenu du trafic réseau autorisé et en bloquant le trafic réputé pour être potentiellement nuisible.

La configuration du **pare-feu personnel** est disponible dans le volet **Configuration**, sous **Réseau**. Dans cette section, vous pouvez régler le mode de filtrage pour le pare-feu personnel ESET. Vous pouvez également accéder à des paramètres plus détaillés en cliquant sur l'engrenage > **Configurer** en regard du **Pare-feu personnel** ou en appuyant sur **F5** pour accéder à Configuration avancée.

Protection contre les attaques réseau (IDS) - Analyse le contenu du trafic réseau et protège contre les attaques réseau. Tout trafic considéré comme nuisible sera bloqué. Vous pouvez désactiver la protection contre les attaques réseau pendant une période spécifique en cliquant sur .

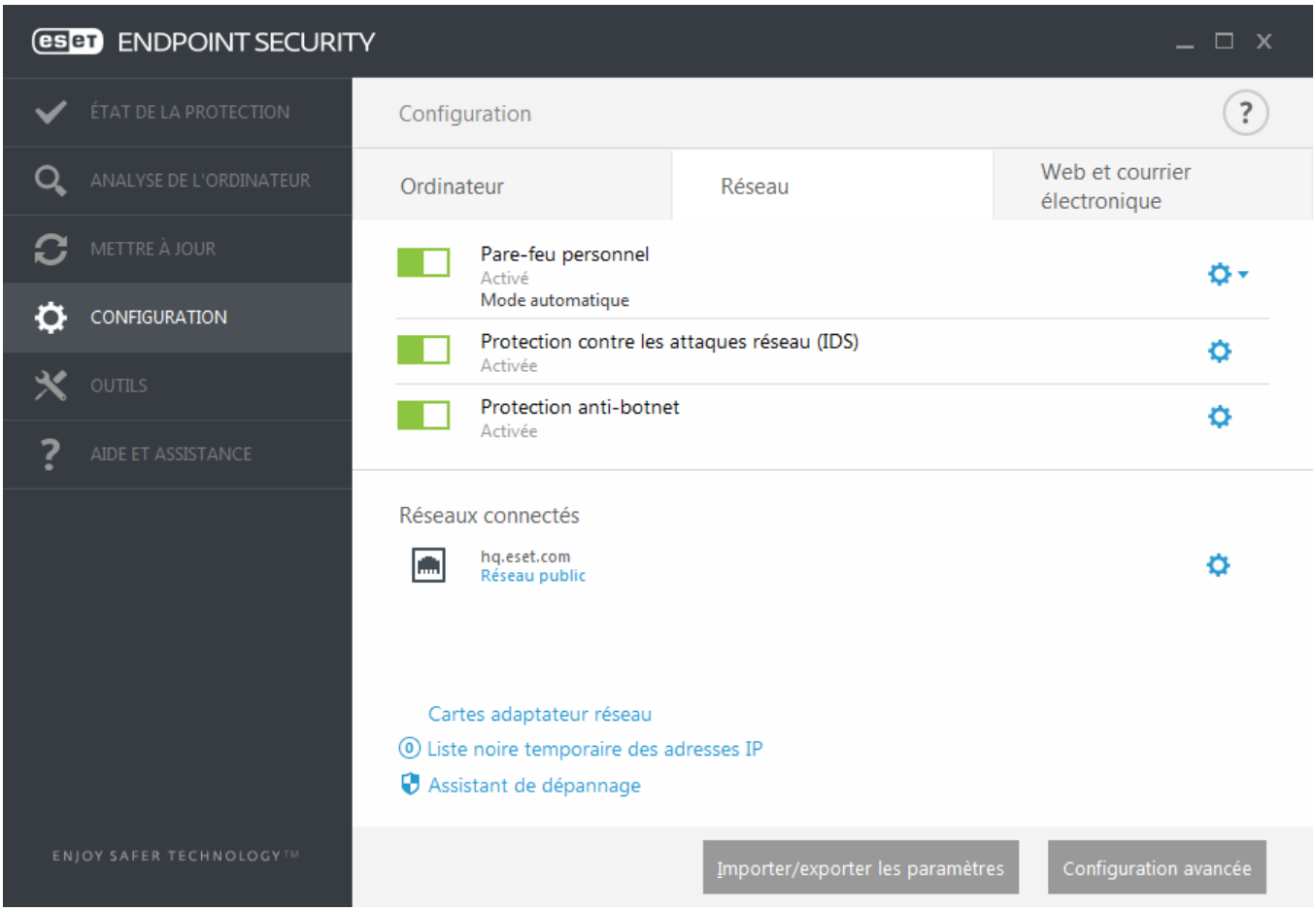
Protection anti-botnet - Détecte rapidement et précisément les logiciels malveillants sur le système. Vous pouvez désactiver la protection anti-botnet pendant une période spécifique en cliquant sur .

Réseaux connectés : indique les réseaux auxquels les cartes réseau sont connectées. Lorsque vous cliquez sur l'engrenage, vous êtes invité à sélectionner un type de protection pour le réseau auquel vous être connecté via votre carte réseau.

Cartes réseau - Affiche chaque carte réseau avec la zone Fiable et le profil de pare-feu attribués. Pour plus d'informations, reportez-vous à la section Cartes réseau.

Liste noire temporaire des adresses IP : affichez la liste des adresses IP qui ont été détectées comme source d'attaques et ajoutées à la liste noire pour bloquer les connexions pendant une certaine période. Pour obtenir plus d'informations, cliquez sur cette option et appuyez sur F1.

Assistant de dépannage permet de résoudre les problèmes de connectivité liés au pare-feu personnel ESET. Pour plus d'informations, reportez-vous à la section Assistant de dépannage.



Cliquez sur l'engrenage ⚙ en regard de **Pare-feu personnel** pour accéder aux paramètres suivants :

Configurer... : ouvre la fenêtre Pare-feu personnel dans Configuration avancée. Elle permet de configurer la gestion des communications réseau par le pare-feu.

Bloquer tout le trafic : toutes les communications entrantes et sortantes sont bloquées par le pare-feu personnel. N'utilisez cette option qu'en cas de soupçon de risque critique de sécurité qui nécessite la déconnexion du système du réseau. Lorsque le filtrage du trafic réseau est en mode **Bloquer tout le trafic**, cliquez sur **Arrêter le blocage de l'intégralité du trafic** pour rétablir le fonctionnement normal du pare-feu.

Interrompre le pare-feu (autoriser l'intégralité du trafic) : opposé du blocage de tout le trafic réseau. Si cette option est activée, toutes les options de filtrage du pare-feu personnel sont désactivées et toutes les connexions entrantes et sortantes sont autorisées. Lorsque le filtrage du trafic réseau est dans ce mode, cliquez sur **Activer le pare-feu** pour réactiver le pare-feu.

Mode automatique (lorsqu'un autre mode de filtrage est activé) : cliquez sur cette option pour changer le mode de filtrage en mode de filtrage automatique (avec règles définies par l'utilisateur).

Mode interactif (lorsqu'un autre mode de filtrage est activé) : cliquez sur cette option pour changer le mode de filtrage en mode de filtrage interactif.

3.8.2.1 Pare-feu personnel

Le pare-feu personnel contrôle tout le trafic réseau entrant et sortant du système. Il autorise ou refuse les différentes connexions réseau en se basant sur les règles de filtrage spécifiées. Il offre une protection contre les attaques provenant d'ordinateurs distants et permet de bloquer certains services. Il assure aussi une protection antivirus pour les protocoles HTTP, POP3 et IMAP. Cette fonctionnalité représente un élément important de la sécurité d'un ordinateur.

Activer la protection contre les attaques réseau (IDS) - Analyse le contenu du trafic réseau et protège contre les attaques réseau. Tout trafic considéré comme nuisible sera bloqué.

Activer la protection anti-botnet - Détecte et bloque les communications avec des serveurs de contrôle et de commande malveillants selon les modèles classqiues lorsque l'ordinateur est infecté et qu'un robot tente de communiquer.

Quatre modes de filtrage sont disponibles pour le pare-feu personnel d'ESET Endpoint Security. Les modes de filtrage sont disponibles dans **Configuration avancée** (F5) en cliquant sur **Pare-feu personnel**. Le comportement du pare-feu change en fonction du mode de filtrage. Les modes de filtrage affectent également le niveau d'interaction de l'utilisateur.

Le filtrage peut être effectué dans l'un des quatre modes :

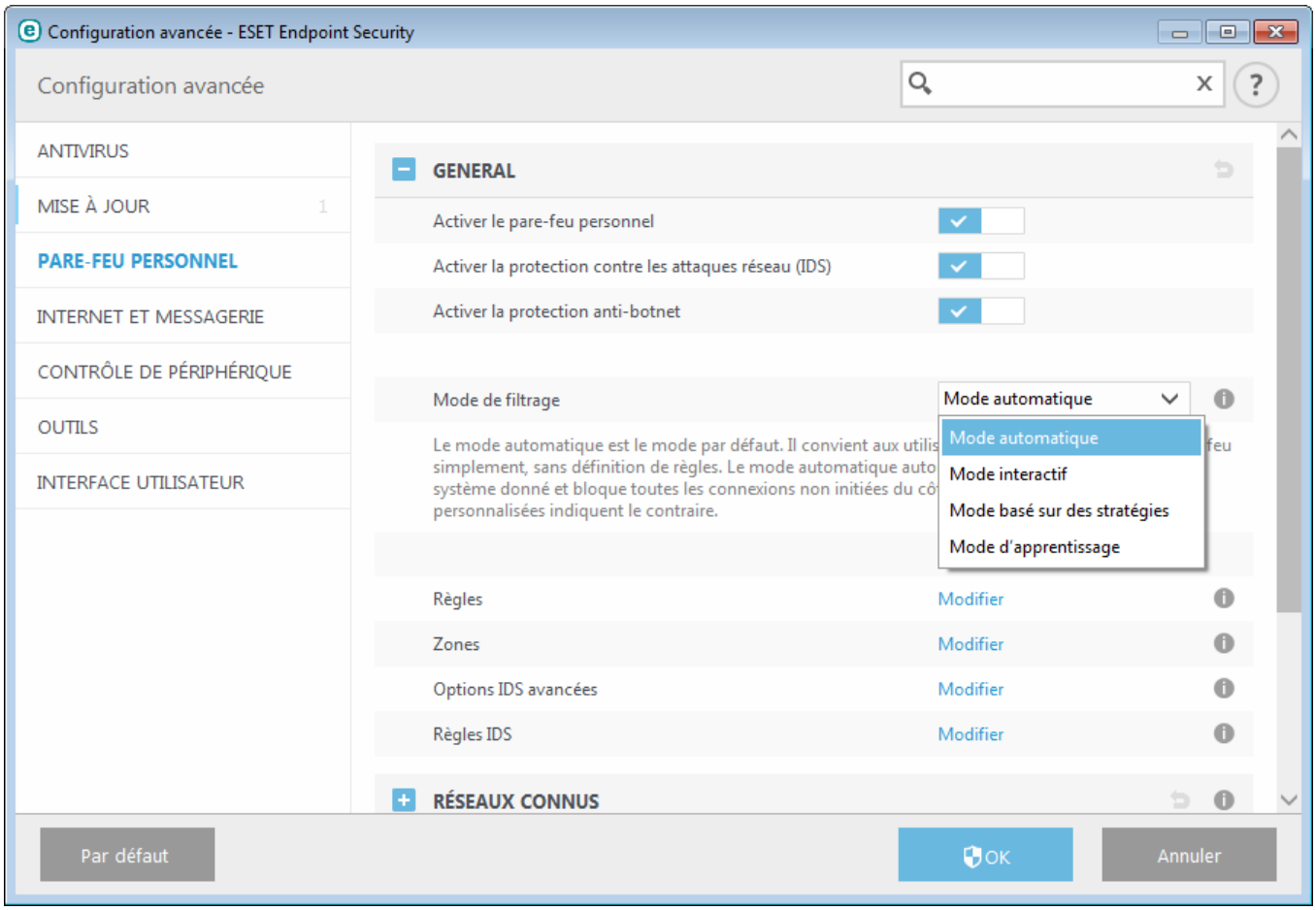
Mode automatique - Mode par défaut. Ce mode convient aux utilisateurs qui préfèrent utiliser le pare-feu simplement, sans définition de règles. Des règles personnalisées définies par l'utilisateur peuvent être créées, mais ne sont nécessaires en mode automatique. Le mode automatique autorise tout trafic sortant du système donné et bloque la plupart du trafic entrant (à l'exception du trafic à partir de la zone Fiable, comme autorisé dans Options IDS avancées/Services autorisés et du trafic entrant répondant à une communication récente du même site distant).

Mode interactif - Vous permet d'élaborer une configuration personnalisée pour votre pare-feu personnel. Lors de la détection d'une communication à laquelle aucune règle ne s'applique, une boîte de dialogue s'affiche pour signaler une connexion inconnue. Cette boîte de dialogue permet d'autoriser ou de refuser la communication, cette décision pouvant être enregistrée comme nouvelle règle pour le pare-feu personnel. Si vous choisissez de créer une règle, toutes les connexions ultérieures de ce type sont autorisées ou refusées, conformément à la règle.

Mode basé sur des règles personnalisées - Le mode basé sur des règles personnalisées bloque toute connexion ne faisant pas l'objet d'une règle spécifique l'autorisant. Ce mode permet aux utilisateurs expérimentés de définir des règles qui n'autorisent que des connexions souhaitées et sûres. Toutes les autres connexions spécifiées sont bloquées par le pare-feu personnel.

Mode d'apprentissage - Crée et enregistre automatiquement les règles ; ce mode convient à la configuration initiale du pare-feu personnel. Aucune intervention de l'utilisateur n'est requise, car ESET Endpoint Security enregistre les règles conformément aux paramètres prédéfinis. Le mode d'apprentissage n'étant pas sécurisé, il est recommandé de ne l'utiliser que jusqu'à ce que toutes les règles aient été créées pour les communications requises.

Des profils peuvent être utilisés pour personnaliser le comportement du pare-feu personnel d'ESET Endpoint Security en spécifiant différents jeux de règles dans des situations différentes.



Règles - Vous pouvez ajouter ici des règles et définir comment le pare-feu personnel gère le trafic réseau.

Zones - Vous pouvez créer ici des zones composées de plusieurs adresses IP.

Options IDS avancées - Permet de configurer des options de filtrage avancées et la fonctionnalité IDS (utilisée pour détecter plusieurs types d'attaques et d'exploits).

Règles IDS - Permet d'ajouter des exceptions IDS et de personnaliser les réactions face aux activités malveillantes.

3.8.2.1.1 Mode d'apprentissage

Le mode d'apprentissage crée et enregistre automatiquement une règle pour chaque communication établie dans le système. Aucune intervention de l'utilisateur n'est requise, car ESET Endpoint Security enregistre les règles conformément aux paramètres prédéfinis.

Ce mode pouvant exposer votre système à des risques, son utilisation n'est recommandée que pour la configuration initiale du pare-feu personnel.

Activez le mode d'apprentissage dans **Configuration avancée** (F5) > **Pare-feu personnel** > **Paramètres du mode d'apprentissage** pour afficher les options relatives à celui-ci. Cette section comprend les éléments suivants :

Avertissement : en mode d'apprentissage, le pare-feu personnel ne filtre pas les communications. Toutes les communications entrantes et sortantes sont autorisées. Dans ce mode, le pare-feu personnel ne protège pas totalement l'ordinateur.

Type de communication - Sélectionnez des paramètres spécifiques de création de règle pour chaque type de communication. Il existe quatre types de communication :

Trafic entrant à partir de la zone Fiable - Un ordinateur distant dans la zone Fiable tentant d'établir une communication avec une application locale s'exécutant sur votre ordinateur est un exemple de connexion entrante avec la zone Fiable.

Trafic sortant vers la zone Fiable - Une application locale tente d'établir une connexion avec un autre ordinateur se trouvant dans le réseau local ou dans un réseau situé à l'intérieur de la zone Fiable.

Trafic Internet entrant - Un ordinateur distant tente de communiquer avec une application s'exécutant sur cet ordinateur.

Trafic Internet sortant - Une application locale tente d'établir la connexion avec un autre ordinateur.

Chaque section permet de définir des paramètres à ajouter aux règles nouvellement créées :

Ajouter un port local - Inclut le numéro de port local des communications réseau. Pour les communications sortantes, les numéros générés sont généralement aléatoires. C'est pourquoi il est recommandé de n'activer cette option que pour les communications entrantes.

Ajouter une application - Inclut le nom de l'application locale. Cette option ne convient que pour les règles de niveau application (règles définissant la communication pour une application entière) futures. Par exemple, vous pouvez n'activer la communication que pour un navigateur ou un client de messagerie.

Ajouter un port distant - Inclut le numéro de port distant des communications réseau. Par exemple, vous pouvez autoriser ou refuser un service spécifique associé à un numéro de port standard (HTTP - 80, POP3 - 110, etc.).

Ajouter une adresse IP distante/Zone fiable - Vous pouvez utiliser une zone ou une adresse IP distante comme paramètre pour les nouvelles règles définissant toutes les connexions réseau entre le système local et cette adresse ou zone. Cette option convient si vous voulez définir des actions pour un ordinateur ou un groupe d'ordinateurs en réseau.

Nombre maximum de règles différentes pour une application : si une application communique, via plusieurs ports, avec diverses adresses IP, etc., le pare-feu en mode d'apprentissage crée un nombre de règles approprié pour cette application. Cette option permet de limiter le nombre de règles pouvant être créées pour une application.

3.8.2.2 Profils du pare-feu

Des profils peuvent être utilisés pour contrôler le comportement du pare-feu personnel d'ESET Endpoint Security. Lorsque vous créez ou modifiez une règle de pare-feu personnel, vous pouvez l'attribuer à un profil spécifique ou l'appliquer à tous les profils. Lorsqu'un profil est actif sur une interface réseau, seules les règles globales (sans aucun profil indiqué) et les règles attribuées à ce profil sont appliquées. Vous pouvez créer plusieurs profils avec différentes règles attribuées aux cartes réseau ou aux réseaux pour modifier facilement le comportement du pare-feu personnel.

Cliquez sur **Modifier** en regard de l'option **Liste des profils** pour ouvrir la fenêtre **Profils du pare-feu** dans laquelle vous pouvez modifier les profils.

Une carte réseau peut être configurée pour utiliser un profil configuré pour un réseau spécifique lorsqu'elle est connectée à ce dernier. Vous pouvez également attribuer un profil spécifique à utiliser sur un réseau donné dans **Configuration avancée** (F5) > **Pare-feu personnel** > **Réseaux connus**. Dans la liste **Réseaux connus**, sélectionnez un réseau, puis cliquez sur **Modifier** pour attribuer un profil de pare-feu à celui-ci dans le menu déroulant **Profil de pare-feu**. Si aucun profil n'est attribué à ce réseau, le profil par défaut de la carte est utilisé. Si la carte est configurée pour ne pas utiliser le profil du réseau, son profil par défaut est utilisé, quel que soit le réseau auquel elle est connectée. S'il n'existe aucun profil pour la configuration de la carte ou du réseau, le profil par défaut global est utilisé. Pour attribuer un profil à une carte réseau, sélectionnez cette dernière, cliquez sur **Modifier** en regard de l'option **Profils attribués aux cartes réseau**, sélectionnez le profil dans le menu déroulant **Profil de pare-feu par défaut**, puis cliquez sur **Enregistrer**.

Lorsque le pare-feu personnel bascule vers un autre profil, une notification apparaît dans l'angle inférieur droit, à côté de l'horloge système.

3.8.2.2.1 Profils attribués aux cartes réseau

En changeant de profils, vous pouvez rapidement effectuer plusieurs modifications au comportement du pare-feu. Des règles personnalisées peuvent être définies et appliquées pour des profils spécifiques. Les entrées de toutes les cartes réseau présentes sur l'ordinateur sont automatiquement ajoutées à la liste **Cartes réseau**.

Colonnes

Nom : nom de la carte réseau.

Profil de pare-feu par défaut : le profil par défaut est utilisé lorsque le réseau auquel vous êtes connecté ne dispose pas de profil configuré ou que la carte réseau n'est pas définie pour utiliser un profil réseau.

Préférer le profil du réseau : lorsque l'option **Préférer le profil de pare-feu du réseau connecté** est activée, la carte réseau utilise le profil de pare-feu attribué à un réseau connecté lorsque cela est possible.

Éléments de commande

Ajouter : permet d'ajouter une nouvelle carte réseau.

Modifier : permet de modifier une carte réseau existante.

Supprimer : sélectionnez une carte réseau, puis cliquez sur **Supprimer** si vous souhaitez la supprimer de la liste.

OK/Annuler : cliquez sur **OK** si vous souhaitez enregistrer les modifications. Sinon, cliquez sur **Annuler**.

3.8.2.3 Configuration et utilisation des règles

Les règles représentent un ensemble de conditions utilisées pour tester toutes les connexions réseau, ainsi que toutes les actions affectées à ces conditions. À l'aide des règles de pare-feu personnel, vous pouvez définir l'action à entreprendre si une connexion réseau (de différents types) est établie. Pour accéder à la configuration des règles de filtrage, accédez à **Configuration avancée** (F5) > **Pare-feu personnel** > **Général**. Certaines des règles prédéfinies sont liées aux cases à cocher des **services autorisés** (Options IDS avancées) et ne peuvent pas être directement désactivées. Vous pouvez utiliser ces cases à cocher associées pour les désactiver.

Contrairement à la version précédente d'ESET Endpoint Security, les règles sont évaluées du haut vers le bas. L'action de la première règle correspondante est utilisée pour chaque connexion réseau évaluée. Il s'agit d'une modification de comportement importante par rapport à la version précédente, dans laquelle la priorité des règles était automatique et les règles plus spécifiques avaient une priorité plus élevée que celles plus générales.

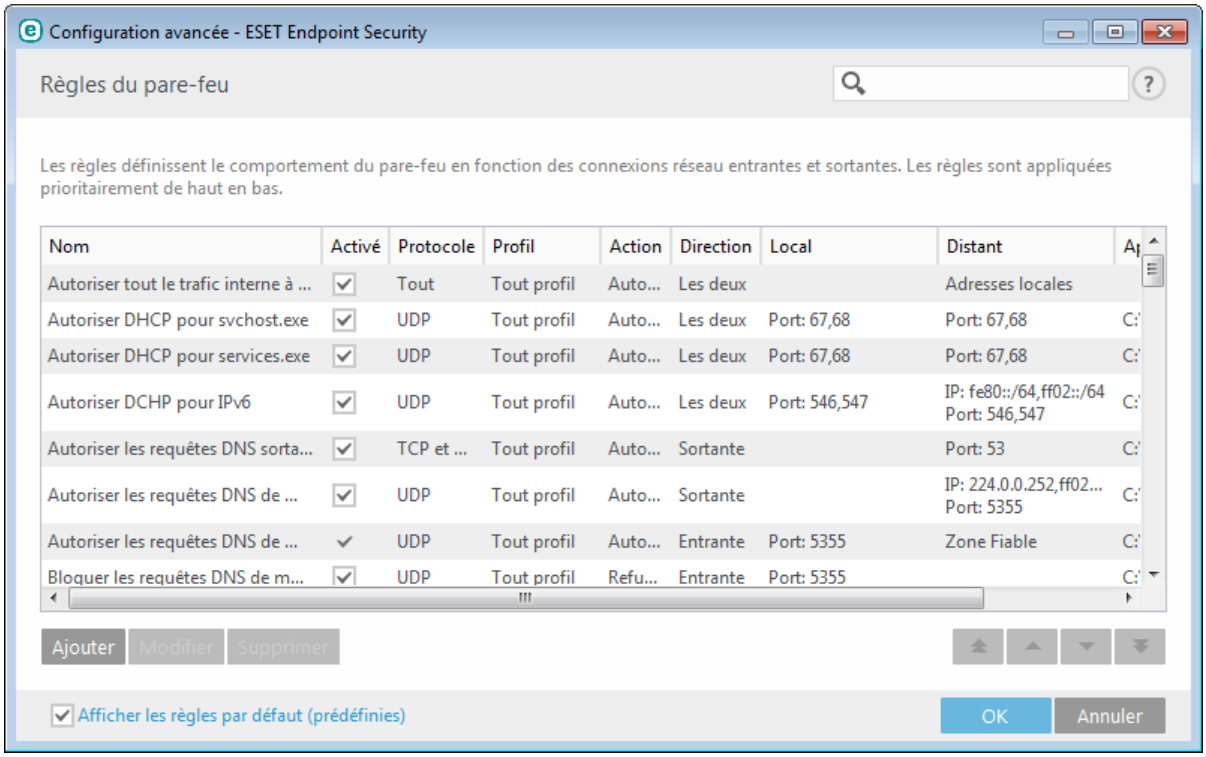
Les connexions peuvent être divisées en connexions entrantes et sortantes. Les connexions entrantes sont initiées par un ordinateur distant qui tente d'établir une connexion avec le système local. Les connexions sortantes fonctionnent dans le sens opposé : le système local contacte l'ordinateur distant.

Si une nouvelle communication inconnue est détectée, la décision de l'autoriser ou de la refuser doit être prise avec prudence. Les connexions non sollicitées, non sécurisées ou inconnues posent un risque de sécurité au système. Si une telle connexion est établie, il est recommandé de faire très attention au côté distant et aux applications qui tentent de se connecter à votre ordinateur. De nombreuses infiltrations essaient d'obtenir et d'envoyer des données personnelles ou de télécharger d'autres applications malveillantes aux postes de travail hôtes. Le pare-feu personnel permet à l'utilisateur de détecter et de mettre fin à de telles connexions.

3.8.2.3.1 Configuration des règles

Cliquez sur **Modifier** en regard de **Règles** dans la section de l'onglet **Général** pour afficher la fenêtre **Règles du pare-feu** qui contient la liste de toutes les règles. Les options **Ajouter**, **Modifier** et **Supprimer** vous permettent d'ajouter, de configurer ou de supprimer des règles. Pour définir le niveau de priorité d'une règle, sélectionnez-la, puis cliquez sur **Haut/Monter/Bas/Descendre**.

CONSEIL : vous pouvez utiliser le champ **Rechercher** pour rechercher des règles par nom, protocole ou port.



Colonnes

Activé : indique si les règles sont activées ou désactivées. Vous devez activer la case à cocher correspondant à une règle pour l'activer.

Nom :nom de la règle.

Protocole : protocole pour lequel cette règle est valide.

Profil : indique pour quel profil de pare-feu cette règle est valide.

Action : indique l'état de la communication (bloquer/autoriser/demander).

Direction : sens de la communication (entrante/sortante/les deux).

Local : adresse IP et port de l'ordinateur local.

Distant : adresse IP et port de l'ordinateur distant.

Application : application à laquelle la règle s'applique.

Éléments de commande

Ajouter : permet de créer une règle.

Modifier : permet de modifier les règles existantes.

Supprimer : permet de supprimer les règles existantes.

Afficher les règles par défaut (prédéfinies) : règles prédéfinies par ESET Endpoint Security qui autorisent ou refusent des communications spécifiques. Vous pouvez désactiver ces règles, mais vous ne pouvez pas les supprimer.

Haut/Monter/Bas/Descendre : permet d'ajuster le niveau de priorité des règles (les règles sont exécutées du haut vers le bas).

3.8.2.3.2 Utilisation de règles

Une modification s'impose chaque fois que des paramètres de contrôle changent. Si les modifications apportées empêchent une règle de remplir les conditions et que l'action spécifiée ne peut pas être appliquée, la connexion donnée peut être refusée. Cela peut entraîner des problèmes de fonctionnement pour l'application affectée par une règle. Un exemple est le changement d'adresse ou le numéro de port du côté distant.

La partie supérieure de la fenêtre contient trois onglets :

- **Général** - Indiquez un nom de règle, le sens de la connexion, l'action (**Autoriser**, **Refuser**, **Demander**), le protocole et le profil auquel la règle s'applique.
- **Local** - Affiche les informations concernant la partie locale de la connexion, notamment le numéro du port local ou la plage des ports, ainsi que le nom de l'application communicante. Cet onglet permet également d'ajouter une zone prédéfinie ou créée avec une plage d'adresses IP en cliquant sur **Ajouter**.
- **Distant** - Cet onglet comprend des informations concernant le port distant (plage de ports). Il vous permet également de définir la liste des adresses IP ou zones distantes pour la règle en question. Vous pouvez également y ajouter une zone prédéfinie ou créée avec une plage d'adresses IP en cliquant sur **Ajouter**.

Lorsque vous créez une règle, vous devez entrer son nom dans le champ **Nom**. Sélectionnez le sens dans lequel la règle s'applique dans le menu déroulant **Direction** et l'action à exécuter lorsqu'une communication répond à la règle, à partir du menu déroulant **Action**.

Protocole représente le protocole de transfert utilisée par la règle. Dans le menu déroulant, sélectionnez le protocole à utiliser pour une règle donnée.

Le **type/code ICMP** représente un message ICMP identifié par un nombre (0 représente « réponse d'écho », par exemple).

Par défaut, toutes les règles sont activées pour **Tout profil**. Vous pouvez également sélectionner un profil de pare-feu personnalisé à l'aide du menu déroulant **Profils**.

Si vous activez l'option **Journaliser**, l'activité liée à la règle est enregistrée dans un journal. **Notifier l'utilisateur** affiche une notification lorsque la règle est appliquée.

Vous trouverez ci-dessous un exemple dans lequel une nouvelle règle permet d'autoriser le navigateur Web à accéder au réseau. Dans cet exemple, la configuration doit être effectuée comme suit :

- Dans l'onglet **Général**, activez les communications sortantes via les protocoles TCP et UDP.
- Ajoutez le navigateur (pour Internet Explorer, iexplore.exe) dans l'onglet **Local**.
- Dans l'onglet **Distant**, activez le port numéro 80 pour autoriser la navigation Internet standard.

REMARQUE : notez que la modification des règles prédéfinies est limitée.

3.8.2.4 Zone Fiable

La zone Fiable représente un groupe d'adresses réseau pour lesquelles le pare-feu personnel autorise du trafic entrant à l'aide de paramètres par défaut. Les paramètres des fonctionnalités telles que le partage de fichiers et Bureau à distance à l'intérieur de la zone Fiable sont déterminés dans Options IDS avancées.

La zone Fiable actuelle est calculée dynamiquement de manière séparée pour chaque carte réseau selon le réseau auquel est actuellement connecté l'ordinateur. Les adresses définies comme à l'intérieur de la zone Fiable dans l'Éditeur de zones sont toujours approuvées. Si une carte réseau est connectée à un réseau connu, les **autres adresses fiables** configurées pour ce dernier sont ajoutées à la zone Fiable de la carte. Si un réseau est associé au type de protection Domicile/professionnel, tous les sous-réseaux directement connectés sont inclus dans la zone Fiable. La zone Fiable actuelle de chaque carte réseau peut être affichée dans la fenêtre **Configuration**, sous **Réseau** > **Cartes réseau**.

REMARQUE : la zone Fiable par interface n'est pas prise en charge sur les systèmes d'exploitation Windows XP. Pour ces systèmes d'exploitation, toutes les cartes disposent de la même zone Fiable, ce qui est visible dans la page Cartes réseau.

3.8.2.5 Configuration des zones

Les zones sont des groupes d'adresses IP qui s'avèrent utiles lorsque vous devez réutiliser un même ensemble d'adresses dans plusieurs règles. Vous pouvez configurer des zones dans **Configuration avancée** > **Pare-feu personnel** > **Général**, en cliquant sur le bouton **Modifier** en regard de **Zones**. Pour ajouter une nouvelle zone, cliquez sur **Ajouter**, entrez un **nom** et une **description** pour la zone, puis ajoutez une adresse IP distante dans le champ **Adresse de l'ordinateur distant (IPv4, IPv6, plage, masque)**.

Dans la fenêtre de configuration **Zones de pare-feu**, vous pouvez indiquer un nom de zone, une description et une liste d'adresses réseau (voir aussi Éditeur de réseaux connus).

3.8.2.6 Réseaux connus

Lorsque vous utilisez un ordinateur qui se connecte fréquemment à des réseaux publics ou des réseaux en dehors de votre réseau professionnel normal, il est recommandé de vérifier la fiabilité du réseau auquel vous vous connectez. Une fois les réseaux définis, ESET Endpoint Security peut reconnaître les réseaux (domestiques/professionnels) fiables à l'aide de divers paramètres réseau configurés dans **Identification du réseau**. Les ordinateurs se connectent souvent à des réseaux avec des adresses IP semblables à celle du réseau fiable. Dans ces cas, ESET Endpoint Security peut considérer un réseau inconnu comme étant fiable (domestique/professionnel). Il est recommandé d'utiliser l'option **Authentification réseau** pour éviter ce type de situation.

Lorsqu'une carte réseau est connectée à un réseau ou que ses paramètres réseau sont reconfigurés, ESET Endpoint Security recherche une entrée correspondant au nouveau réseau dans la liste des réseaux connus. Si les options **Identification du réseau** et **Authentification réseau** (facultatifs) correspondent, le réseau est indiqué comme connecté dans cette interface. Lorsqu'aucun réseau connu n'est trouvé, un réseau est créé avec la configuration d'identification du réseau définie afin d'identifier le réseau à la prochaine connexion. Par défaut, la nouvelle connexion réseau utilise le type de protection **Public**. La boîte de dialogue **Nouvelle connexion réseau détectée** vous invite à choisir le type de protection **Public** ou **Domestique/professionnel**. Si une carte réseau est connectée à un réseau connu et si ce réseau est indiqué comme **Domestique/professionnel**, les sous-réseaux locaux de la carte sont ajoutés à la zone Fiable.

REMARQUE : lorsque vous sélectionnez **Marquer automatiquement les nouveaux réseaux comme publics**, la boîte de dialogue **Nouvelle connexion détectée** ne s'affiche pas, et le réseau auquel vous êtes connecté est automatiquement marqué comme public. De ce fait, certaines fonctionnalités (comme le partage de fichiers et Bureau à distance) deviennent inaccessibles à partir des nouveaux réseaux.

Les réseaux connus peuvent être manuellement configurés dans la fenêtre Éditeur de réseaux connus.

3.8.2.6.1 Éditeur de réseaux connus

Les réseaux connus peuvent être configurés manuellement en cliquant sur **Modifier** dans **Configuration avancée** > **Pare-feu personnel** > **Réseaux connus**.

Colonnes

Nom : nom du réseau connu.

Type de protection : indique si le réseau est défini sur **Domestique/professionnel** ou **Public**.

Profil de pare-feu : sélectionnez un profil à partir du menu déroulant **Afficher les règles utilisées dans le profil** pour afficher le filtre des règles du profil.

Éléments de commande

Ajouter : permet de créer un réseau connu.

Modifier : cliquez sur cette option pour modifier un réseau connu existant.

Supprimer : sélectionnez un réseau, puis cliquez sur **Supprimer** pour le supprimer de la liste des réseaux connus.

Haut/Monter/Bas/Descendre : permet d'ajuster le niveau de priorité des réseaux connus (les réseaux sont évalués du haut vers le bas).

Les paramètres de configuration réseau sont répartis dans les onglets suivants :

Réseau

Vous pouvez définir sous cet onglet le nom du réseau et sélectionner le type de protection (**Public** ou **Domestique/professionnel**) du réseau. Utilisez le menu déroulant **Profil de pare-feu** pour sélectionner le profil de ce réseau. Si le réseau utilise le type de protection **Domestique/professionnel**, tous les sous-réseaux directement connectés sont considérés comme fiables. Par exemple, si une carte réseau est connectée à ce réseau avec l'adresse IP 192.168.1.5 et le masque de sous-réseau 255.255.255.0, le sous-réseau 192.168.1.0/24 est ajouté à la zone Fiable de cette carte. Si la carte possède plusieurs adresses/sous-réseaux, ces derniers sont tous fiables, indépendamment de la configuration de l'**identification du réseau** du réseau connu.

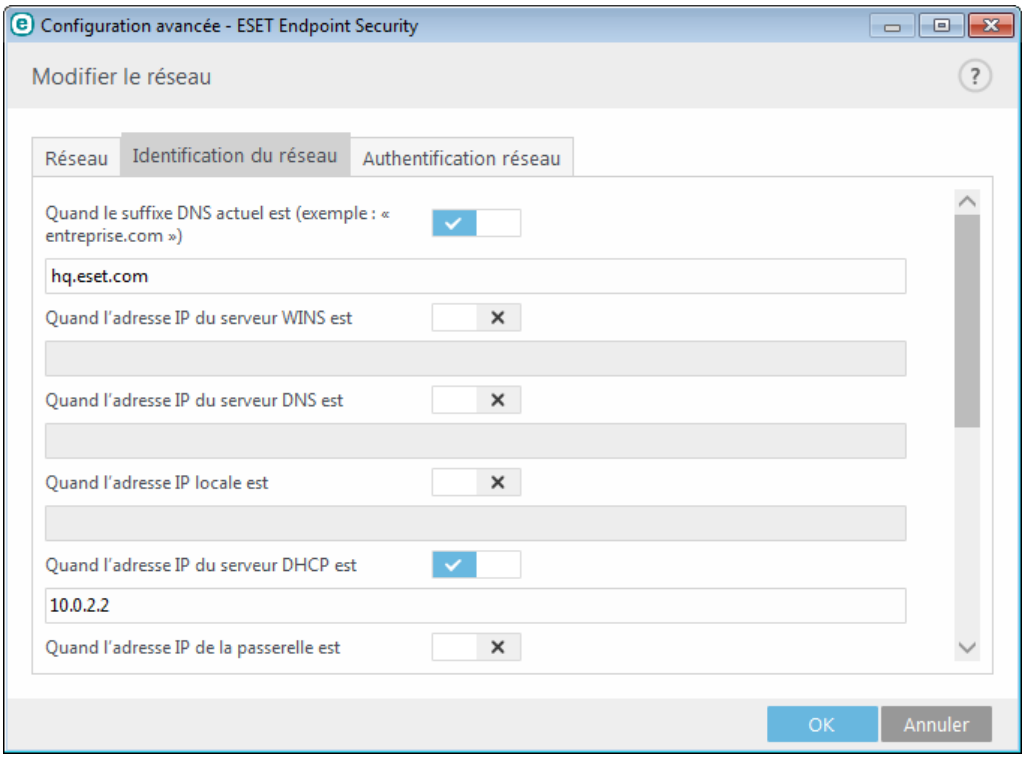
De plus, les adresses ajoutées sous **Autres adresses fiables** sont toujours ajoutées à la zone Fiable des cartes connectées à ce réseau (quel que soit le type de protection du réseau).

Pour qu'un réseau soit indiqué comme connecté dans la liste des réseaux connectés, les conditions suivantes doivent être remplies :

- Identification du réseau : tous les paramètres renseignés doivent correspondre aux paramètres de connexion active.
- Authentification réseau : si le serveur d'authentification est sélectionné, une authentification réussie doit être effectuée avec ESET Authentication Server.
- Restrictions réseau (Windows XP uniquement) : toutes les restrictions globales sélectionnées doivent être respectées.

Identification du réseau

L'identification du réseau est effectuée en fonction des paramètres de la carte de réseau local. Tous les paramètres sélectionnés sont comparés aux paramètres actuels des connections réseau actives. Les adresses IPv4 et IPv6 sont autorisées.



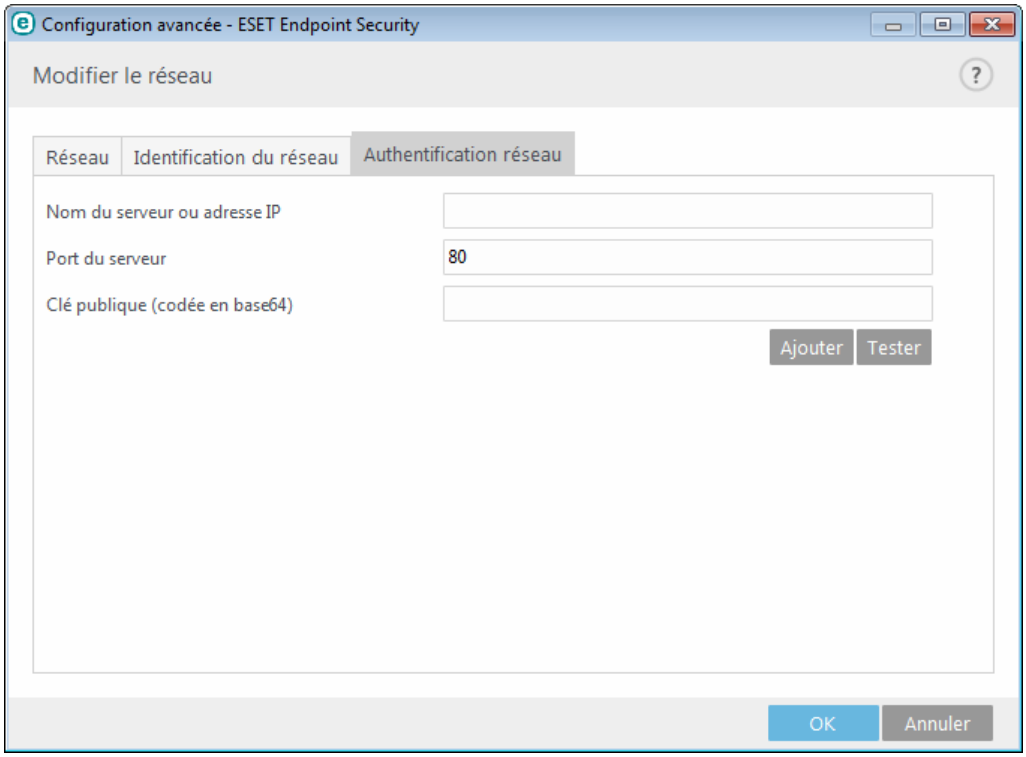
Authentification réseau

L'authentification réseau recherche un serveur spécifique sur le réseau et utilise le chiffrement asymétrique (algorithme RSA) pour authentifier le serveur. Le nom du réseau en cours d'authentification doit correspondre au

nom de la zone défini dans les paramètres du serveur d'authentification. Le nom respecte la casse. Indiquez un nom de serveur, un port d'écoute de serveur et une clé publique correspondant à la clé privée du serveur (reportez-vous à la section Authentification réseau - Configuration du serveur). Le nom du serveur peut être saisi sous la forme d'une adresse IP, d'un nom DNS ou NetBios et suivi d'un chemin indiquant l'emplacement de la clé sur le serveur (par exemple, nom_serveur_/répertoire1/répertoire2/authentication). Vous pouvez indiquer d'autres serveurs à utiliser en les ajoutant au chemin, en les séparant par des points-virgules.

La clé publique peut être importées à l'aide d'un des types de fichier suivants :

- Clé publique chiffrée PEM (.pem) : cette clé peut être générée à l'aide d'ESET Authentication Server (reportez-vous à Authentification réseau - Configuration du serveur).
- Clé publique chiffrée
- Certificat de clé publique (.crt)



Cliquez sur **Tester** pour tester vos paramètres. Si l'authentification aboutit, *Authentification de serveur réussie* s'affiche. Si l'authentification n'est pas configurée correctement, l'un des messages d'erreur suivants s'affiche :

Authentification de serveur échouée. Signature non valide ou non correspondante.
La signature du serveur ne correspond pas à la clé publique saisie.

Authentification de serveur échouée. Le nom du réseau ne correspond pas.
Le nom du réseau configuré ne correspond pas au nom de la zone du serveur d'authentification. Vérifiez les deux noms et assurez-vous qu'ils soient identiques.

Authentification de serveur échouée. Réponse non valide ou inexistante du serveur.
Aucune réponse n'est reçue si le serveur n'est pas en cours d'exécution ou accessible. Une réponse non valide peut être reçue si un autre serveur HTTP s'exécute sur l'adresse spécifiée.

Clé publique non valide.
Vérifiez que le fichier de clé publique n'est pas endommagé.

Restrictions réseau (pour Windows XP uniquement)

Sur les systèmes d'exploitation modernes (Windows Vista et versions ultérieures), chaque carte réseau possède sa propre zone Fiable et un profil de pare-feu actif. Sur Windows XP, cette disposition n'est pas prise en charge. Par conséquent, toutes les cartes réseau partagent toujours les mêmes zone Fiable et profil de pare-feu actif. Cela entraîne un risque de sécurité potentiel lorsque l'ordinateur est connecté simultanément à plusieurs réseaux. Dans de tels cas, le trafic du réseau non fiable peut être évalué à l'aide de la zone Fiable et du profil de pare-feu configurés pour l'autre réseau connecté. Pour limiter tout risque de sécurité, vous pouvez utiliser les restrictions ci-

après pour éviter d'appliquer globalement une configuration réseau alors qu'un autre réseau (éventuellement non fiable) est connecté.

Sur Windows XP, les paramètres des réseaux connectés (zone Fiable et profil de pare-feu) sont appliqués globalement à moins que l'une de ces restrictions soient activées et non respectées :

a. Seule une connexion est active.
b. Aucune connexion sans fil n'est établie.
c. Aucune connexion sans fil non sécurisée n'est établie.

3.8.2.6.2 Authentification réseau - Configuration du serveur

Le processus d'authentification peut être exécuté par tout ordinateur/serveur connecté au réseau et qui doit être authentifié. L'application ESET Authentication Server doit être installée sur un ordinateur/serveur qui est toujours accessible pour l'authentification dès qu'un client tente de se connecter au réseau. Le fichier d'installation de l'application ESET Authentication Server est téléchargeable depuis le site ESET.

Après l'installation de l'application ESET Authentication Server, une boîte de dialogue apparaît (vous pouvez accéder à l'application à tout moment en cliquant sur **Démarrer** > **Programmes** > **ESET** > **ESET Authentication Server**).

Pour configurer le serveur d'authentification, saisissez le nom du réseau d'authentification, le port d'écoute du serveur (il s'agit par défaut du port 80), ainsi que l'emplacement de stockage de la paire clé publique-clé privée. Générez ensuite la clé publique et la clé privée qui seront utilisées dans l'authentification. La clé privée reste sur le serveur, tandis que la clé publique doit être importée sur le client, dans la section d'authentification réseau, lors de la configuration d'un réseau de la configuration du pare-feu.

3.8.2.7 Journalisation

Le pare-feu personnel ESET Endpoint Security enregistre tous les événements importants dans un journal, accessible directement à partir du menu du programme. Cliquez sur **Outils** > **Fichiers journaux**, puis sélectionnez **Pare-feu personnel** dans le menu déroulant **Journaliser**. Pour activer la consignation du pare-feu personnel, accédez à **Configuration avancée** > **Outils** > **Fichiers journaux**, puis définissez la verbosité minimale des journaux sur **Diagnostic**. Toutes les connexions refusées seront enregistrées.

Les fichiers journaux peuvent servir à détecter des erreurs et à révéler des intrusions dans le système. Les journaux du pare-feu personnel d'ESET contiennent les données suivantes :

- **Heure** : date et heure de l'événement.
- **Événement** : nom de l'événement.
- **Source** : adresse réseau source.
- **Cible** : adresse réseau cible.
- **Protocole** : protocole de communication réseau.
- **Nom de règle/virus** : règle appliquée ou nom du ver s'il est identifié.
- **Application** : application concernée.
- **Utilisateur** : nom de l'utilisateur connecté au moment où l'infiltration a été détectée.

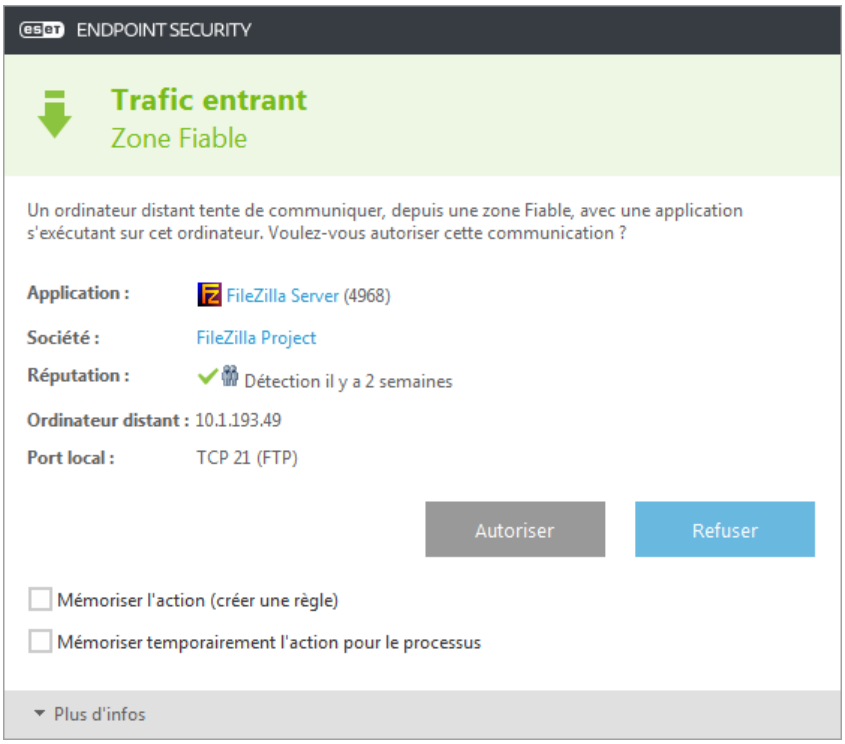
Une analyse approfondie de ces données peut contribuer à détecter les tentatives qui risquent de compromettre la sécurité du système. Beaucoup d'autres facteurs peuvent informer l'utilisateur sur les risques potentiels de sécurité et l'aident à minimiser leur effet. Voici quelques exemples d'indicateurs de menace potentielle : trop de connexions en provenance de sites inconnus, plusieurs tentatives d'établissement de connexions, communications issues d'applications inconnues, utilisation de numéros de ports inhabituels.

3.8.2.8 Établissement d'une connexion - détection

Le pare-feu personnel détecte toute nouvelle connexion au réseau. Le mode pare-feu actif détermine les actions à exécuter pour la nouvelle connexion. Si l'option **Mode automatique** ou **Mode basé sur des règles personnalisées** est activée, le pare-feu personnel exécutera les actions prédéfinies sans intervention de l'utilisateur.

Le mode interactif affiche une fenêtre d'information qui signale la détection d'une nouvelle connexion réseau et donne des informations détaillées sur la connexion. Vous pouvez choisir d'autoriser la connexion ou de la refuser (la bloquer). Si vous autorisez toujours la même connexion dans la boîte de dialogue, il est recommandé de créer une nouvelle règle pour la connexion. Pour ce faire, sélectionnez **Mémoriser l'action (créer une règle)** et sauvegardez l'action comme une nouvelle règle pour le pare-feu personnel. Si le pare-feu personnel reconnaît ultérieurement cette connexion, il applique la règle existante sans intervention de l'utilisateur.

Mémoriser temporairement cette action pour ce processus entraîne la mémorisation de l'action (**Autoriser/ Refuser**) à utiliser jusqu'à la modification des règles ou des modes de filtrage, une mise à jour du module Pare-feu, le redémarrage du système ou de l'application. À l'issue de l'une de ces actions, les règles temporaires sont supprimées.



Soyez très attentif lors de la création de nouvelles règles. Pensez également à n'autoriser que les connexions que vous savez sécurisées. Si toutes les connexions sont autorisées, le pare-feu personnel n'a aucune raison d'exister. Voici les paramètres importants pour les connexions :

- **Côté distant** - Autorise uniquement les connexions aux adresses fiables et connues.
- **Application locale** - Il n'est pas conseillé d'autoriser la connexion d'applications et processus inconnus.
- **Numéro de port** - Les communications via les ports communs (le port 80 pour le trafic Internet, par exemple) doivent toujours être autorisées en situation normale.

Pour proliférer, les infiltrations dans les ordinateurs utilisent souvent des connexions masquées et Internet pour infecter les systèmes distants. Si les règles sont correctement configurées, le pare-feu personnel devient un important outil de protection contre les diverses attaques répétées des codes malveillants.

3.8.2.9 Résolution des problèmes liés au pare-feu personnel ESET

Si vous rencontrez des problèmes de connectivité depuis l'installation d'ESET Endpoint Security, il existe plusieurs méthodes pour déterminer si ces problèmes sont liés au pare-feu personnel ESET. De plus, le pare-feu personnel ESET peut vous aider à créer des règles ou des exceptions pour résoudre les problèmes de connectivité.

Pour obtenir de l'aide pour la résolution des problèmes liés au pare-feu personnel ESET, consultez les rubriques suivantes :

- Assistant de dépannage
- Consignation et création de règles ou d'exceptions à partir du journal
- Création d'exceptions à partir des notifications du pare-feu
- Journalisation PCAP avancée
- Résolution des problèmes liés au filtrage des protocoles

3.8.2.9.1 Assistant de dépannage

L'assistant de dépannage surveille en silence toutes les connexions bloquées et vous guide tout au long du processus de dépannage des problèmes de pare-feu avec des périphériques ou des applications spécifiques. L'assistant propose ensuite un nouvel ensemble de règles à appliquer s'il est approuvé. L'**assistant de dépannage** est accessible dans le menu principal, sous **Configuration** > **Réseau**.

3.8.2.9.2 Consignation et création de règles ou d'exceptions à partir du journal

Par défaut, le pare-feu personnel ESET ne consigne pas toutes les connexions bloquées. Si vous voulez examiner les éléments bloqués par le pare-feu personnel, activez la consignation dans la section **Dépannage** de **Configuration avancée**, sous **Pare-feu personnel** > **Options IDS avancées**. Si vous voyez dans le journal un élément que vous ne voulez pas que le pare-feu personnel bloque, vous pouvez créer une règle ou une exception IDS pour celui-ci en cliquant avec le bouton droit dessus et en sélectionnant **Ne pas bloquer les événements similaires à l'avenir**. Notez que le journal de toutes les connexions bloquées peut contenir des milliers d'éléments. Il peut donc être difficile de trouver une connexion spécifique dans le journal. Vous pouvez désactiver la consignation une fois le problème résolu.

Pour plus d'informations sur le journal, reportez-vous à la section Fichiers journaux.

Remarque : utilisez la consignation pour déterminer l'ordre dans lequel le pare-feu personnel a bloqué des connexions spécifiques. La création de règles à partir du journal vous permet en outre de créer des règles qui effectuent les actions que vous voulez.

3.8.2.9.2.1 Créer une règle à partir du journal

La nouvelle version d'ESET Endpoint Security permet de créer une règle à partir du journal. Dans le menu principal, cliquez sur **Outils** > **Fichiers journaux**. Dans le menu déroulant, sélectionnez **Pare-feu personnel**, cliquez avec le bouton droit sur l'entrée de journal souhaitée, puis sélectionnez **Ne pas bloquer les événements similaires à l'avenir** dans le menu déroulant. Une fenêtre de notification affiche la nouvelle règle.

Pour permettre la création d'autres règles à partir du journal, ESET Endpoint Security doit être configuré avec les paramètres suivants :

- définition de la verbosité minimale des journaux sur **Diagnostic** dans **Configuration avancée** (F5) > **Outils** > **Fichiers journaux**,
- activation de **Afficher également des notifications pour les attaques entrantes contre les trous de sécurité** dans **Configuration avancée** (F5) > **Pare-feu personnel** > **Options IDS avancées** > **Détection d'intrusion**.

3.8.2.9.3 Création d'exceptions à partir des notifications du pare-feu personnel

Lorsque le pare-feu personnel ESET détecte une activité réseau malveillante, une fenêtre de notification décrivant l'événement s'affiche. Cette notification contient un lien qui vous permet d'en savoir plus sur l'événement et de configurer une exception pour celui-ci.

REMARQUE : si un périphérique ou une application réseau ne met pas en œuvre les normes réseau correctement, il ou elle peut déclencher des notifications IDS de pare-feu répétitives. Vous pouvez créer une exception directement dans la notification pour empêcher le pare-feu personnel ESET de détecter cette application ou ce périphérique.

3.8.2.9.4 Journalisation PCAP avancée

Cette fonctionnalité est destinée à fournir des fichiers journaux plus complexes au service client ESET. Utilisez-la uniquement lorsque le service client ESET vous le demande, car elle peut générer un fichier journal très volumineux et ralentir votre ordinateur.

1. Accédez à **Configuration avancée** > **Pare-feu personnel** > **Options IDS avancées** > **Dépannage**, puis activez l'option **Activer la journalisation PCAP avancée**.
2. Essayez de reproduire le problème que vous rencontrez.
3. Désactivez la journalisation PCAP avancée.
4. Le fichier journal PCAP se trouve dans le même répertoire où sont générés les fichiers d'image mémoire de diagnostic :

- Microsoft Windows Vista ou version ultérieure

  C:\ProgramData\ESET\ESET Smart Security\Diagnostics

- Microsoft Windows XP

  C:\Documents and Settings\All Users\...

3.8.2.9.5 Résolution des problèmes liés au filtrage des protocoles

Si vous rencontrez des problèmes avec votre navigateur ou votre client de messagerie, vous devez d'abord déterminer si le filtrage des protocoles en est la cause. Pour ce faire, désactivez temporairement le filtrage des protocoles d'application dans la configuration avancée (pensez à le réactiver une fois que vous avez terminé, sinon votre navigateur et votre client de messagerie ne seront pas protégés). Si le problème ne se reproduit plus après la désactivation, vous trouverez ci-dessous la liste des problèmes courants et les solutions pour les résoudre :

Problèmes liés aux mises à jour ou à la sécurité des communications

Si votre application n'est pas en mesure d'être mise à jour ou si un canal de communication n'est pas sécurisé :

- Si le filtrage du protocole SSL est activé, essayez de le désactiver temporairement. Vous pouvez conserver le filtrage SSL et effectuer la mise à jour en excluant la communication qui pose problème :
  Changez le mode de filtrage du protocole SSL en mode interactif. Réexécutez la mise à jour. Une boîte de dialogue doit s'afficher pour vous fournir des informations sur le trafic réseau chiffré. Vérifiez que l'application correspond à celle que vous dépannez et que le certificat semble provenir du serveur à partir duquel il effectue la mise à jour. Choisissez ensuite de mémoriser l'action pour ce certificat et cliquez sur Ignorer. Si aucune boîte de dialogue ne s'affiche, vous pouvez rechanger le mode de filtrage en mode automatique. Le problème doit être résolu.
- Si l'application concernée ne correspond pas à un navigateur ou un client de messagerie, vous pouvez complètement l'exclure du filtrage des protocoles (procéder ainsi avec un navigateur ou un client de messagerie expose votre ordinateur à des risques). Les applications dont les communications ont déjà été filtrées doivent figurer dans la liste fournie lors de l'ajout de l'exception. Il n'est donc pas nécessaire d'ajouter une application manuellement.

Problème d'accès à un périphérique sur le réseau

Si vous ne parvenez pas à utiliser les fonctionnalités d'un périphérique sur le réseau (ouvrir une page Web de la

webcam ou lire une vidéo sur un lecteur multimédia domestique, par exemple), essayez d'ajouter ses adresses Pv4 et IPv6 à la liste des adresses exclues.

Problème lié à un site Web spécifique

Vous pouvez exclure des sites Web spécifiques du filtrage des protocoles à l'aide de la gestion des adresses URL. Par exemple, si vous ne parvenez pas à accéder au site https://www.gmail.com/intl/fr/mail/help/about.html, ajoutez *gmail.com* à la liste des adresses exclues.

Erreur « Certaines applications aptes à importer un certificat racine sont toujours en cours d'utilisation »

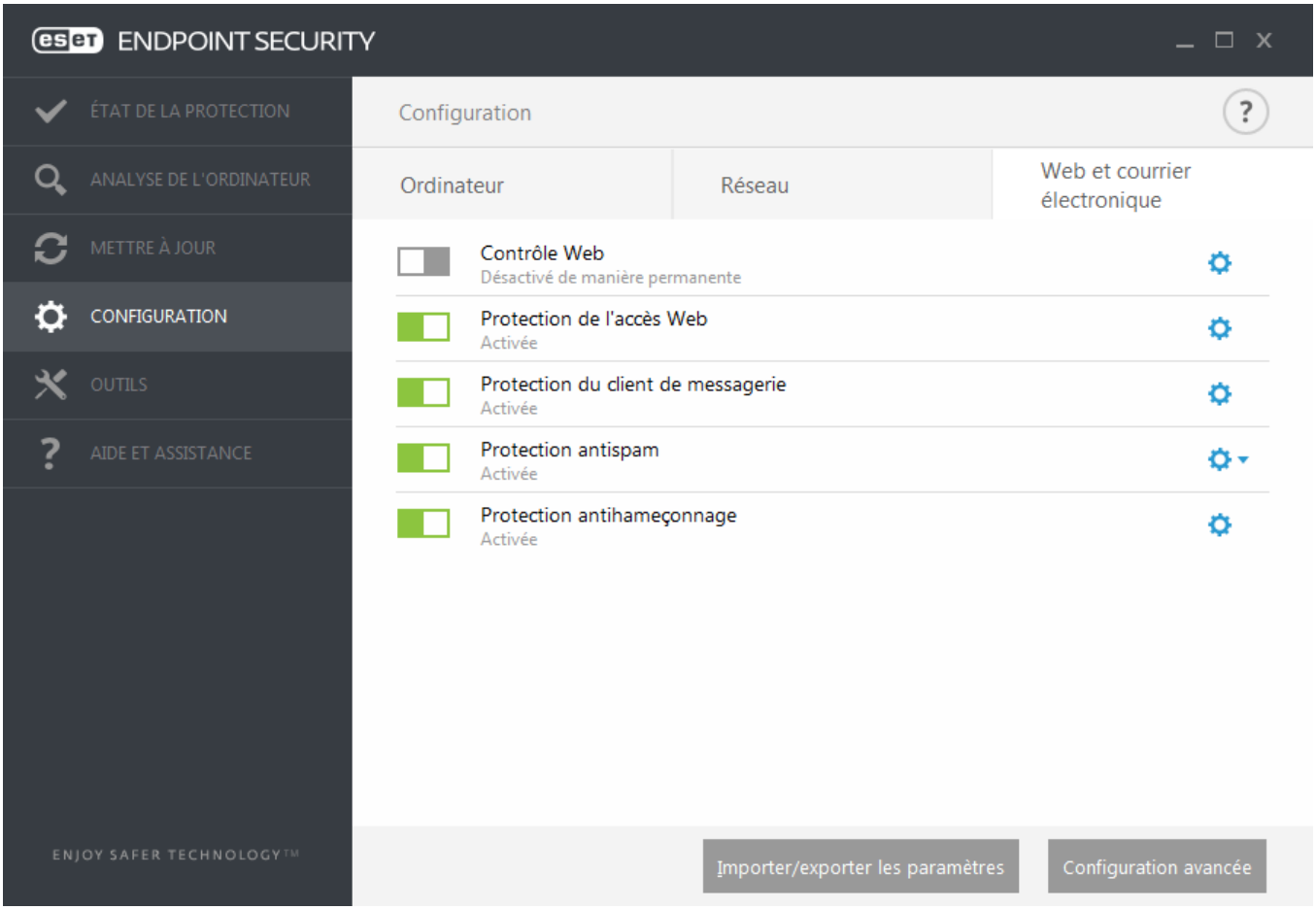
Lorsque vous activez le filtrage du protocole SSL, ESET Endpoint Security vérifie que les applications installées approuvent le filtrage du protocole SSL en important un certificat dans leur magasin de certificats. Cette opération n'est pas possible lorsque certaines applications sont en cours d'exécution. C'est le cas de Firefox et Opera. Vérifiez qu'aucune de ces applications n'est en cours d'exécution (la méthode la plus simple pour effectuer cette vérification consiste à ouvrir le Gestionnaire des tâches et s'assurer que les fichiers firefox.exe ou opera.exe ne figurent pas sous l'onglet Processus).

Erreur liée à un émetteur non approuvé ou une signature non valide

Cette erreur indique probablement que l'importation décrite ci-dessus a échoué. Vérifiez tout d'abord qu'aucune des applications mentionnées n'est en cours d'exécution. Désactivez ensuite le filtrage du protocole SSL et réactivez-le. L'importation est réexécutée.

3.8.3 Internet et messagerie

La configuration d'Internet et messagerie est accessible sous **Configuration** > **Internet et messagerie**. Elle permet d'accéder à des paramètres plus détaillés du programme.



Le module **Filtrage Internet** permet de configurer les paramètres qui fournissent aux administrateurs des outils automatisés qui protègent les postes de travail et définissent des restrictions de navigation Internet. L'objectif de la fonctionnalité Filtrage Internet est d'empêcher l'accès à des pages dont le contenu est inapproprié ou nuisible. Pour plus d'informations, reportez-vous à la section Filtrage Internet.

La connectivité Internet est une fonctionnalité standard des ordinateurs personnels. Elle est malheureusement devenue le principal mode de transfert des codes malveillants. Il est donc essentiel de surveiller de près la **protection de l'accès Web**.

La **protection du client de messagerie** permet de contrôler les communications par courrier électronique reçues via les protocoles POP3 et IMAP. ESET Endpoint Security utilise le plugin de votre client de messagerie pour contrôler toutes les communications concernant le client de messagerie (POP3, IMAP, HTTP, MAPI).

Protection antispam filtre les messages non sollicités.

Lorsque vous cliquez sur l'engrenage en regard de **Protection antispam**, les options suivantes sont disponibles :

Configurer... : affiche les paramètres avancés de la protection antispam du client de messagerie.

Liste blanche/Liste noire/Liste d'exceptions de l'utilisateur : ouvre une boîte de dialogue permettant d'ajouter, de modifier ou de supprimer des adresses électroniques considérées comme étant sûres ou non. Selon les règles définies ici, le courrier électronique provenant de ces adresses n'est pas analysé ou est traité comme courrier indésirable. Cliquez sur Liste d'exceptions de l'utilisateur pour ouvrir une boîte de dialogue permettant d'ajouter, de modifier ou de supprimer des adresses électroniques qui peuvent être usurpées et utilisées pour l'envoi de courrier indésirable. Les messages provenant des adresses répertoriées dans la liste d'exceptions sont toujours inclus à l'analyse visant à identifier le courrier indésirable.

La **protection antihameçonnage** offre une autre couche de protection qui protège des tentatives d'acquisition de mots de passe ou d'autres informations sensibles par des sites Web non légitimes. Elle est accessible dans le volet **Configuration**, sous **Internet et messagerie**. Pour plus d'informations, reportez-vous à la section Protection antihameçonnage.

Désactiver ; cliquez sur le bouton bascule pour désactiver la protection Internet/messagerie/antispam pour les navigateurs Web et les clients de messagerie .

3.8.3.1 Filtrage des protocoles

La protection antivirus des protocoles d'application est fournie par le moteur d'analyse ThreatSense qui intègre en toute transparence toutes les techniques avancées d'analyse des logiciels malveillants. Le filtrage des protocoles fonctionne automatiquement, indépendamment du navigateur Internet ou du client de messagerie utilisés. Pour modifier les paramètres chiffrés (SSL), accédez à **Internet et messagerie** > **Contrôle de protocole SSL**.

Activer le filtrage du contenu des protocoles d'application : cette option peut être utilisée pour désactiver le filtrage des protocoles. Notez que la plupart des composants d'ESET Endpoint Security (protection de l'accès Web, protection des protocoles de messagerie, protection antihameçonnage, filtrage Internet) dépendent de ce filtrage et ne fonctionneront pas sans celui-ci.

Applications exclues : permet d'exclure des applications spécifiques du filtrage des protocoles. Cette option s'avère utile lorsque le filtrage des protocoles entraîne des problèmes de compatibilité.

Adresses IP exclues : permet d'exclure des adresses distantes spécifiques du filtrage des protocoles. Cette option s'avère utile lorsque le filtrage des protocoles entraîne des problèmes de compatibilité.

Web et clients de messagerie : utilisée uniquement sur les systèmes d'exploitation Windows XP, cette option permet de sélectionner les applications pour lesquelles tout le trafic est filtré par le filtrage des protocoles, indépendamment des ports utilisés.

Enregistrer les informations nécessaires pour que l'assistance ESET puisse diagnostiquer les problèmes de filtrage des protocoles : active la journalisation avancée des données de diagnostic. Utilisez cette option uniquement lorsque cela est demandé par l'assistance ESET.

3.8.3.1.1 Web et clients de messagerie

REMARQUE : depuis Windows Vista Service Pack 1 et Windows Server 2008, la nouvelle architecture de plateforme de filtrage Windows permet de vérifier les communications réseau. Étant donné que la technologie WFP utilise des techniques de surveillance spéciales, la section **Web et clients de messagerie** est indisponible.

À cause du nombre considérable de codes malveillants circulant sur Internet, la sécurisation de la navigation sur Internet est un aspect très important de la protection des ordinateurs. Les vulnérabilités des navigateurs Internet et les liens frauduleux contribuent à faciliter l'accès imperceptible au système par des codes malveillants. C'est pourquoi ESET Endpoint Security se concentre sur la sécurité des navigateurs Internet. Chaque application accédant au réseau peut être marquée comme étant un navigateur Internet. Les applications qui ont déjà utilisé des protocoles pour les communications ou l'application du chemin d'accès sélectionné peuvent être ajoutées à la liste Web et clients de messagerie.

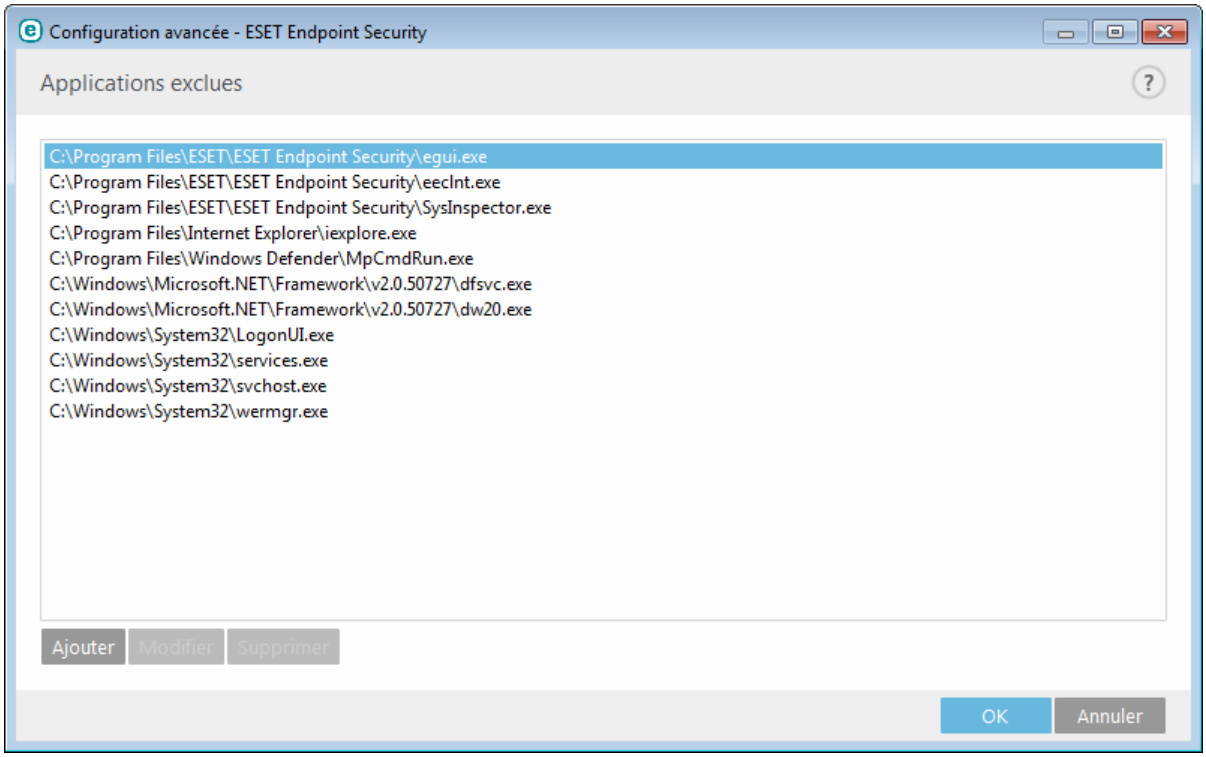
3.8.3.1.2 Applications exclues

Pour exclure du filtrage des protocoles les communications de certaines applications sensibles au réseau, ajoutez-les à la liste. Les communications HTTP/POP3/IMAP des applications sélectionnées ne font pas l'objet d'une détection des menaces. Il est recommandé d'utiliser uniquement cette technique si les applications ne fonctionnent pas correctement lorsque le filtrage des protocoles est activé.

Les applications et les services qui ont déjà été affectés par le filtrage des protocoles sont automatiquement affichés après avoir cliqué sur **Ajouter**.

Modifier - Modifie les entrées sélectionnées de la liste.

Supprimer - Supprime les entrées sélectionnées de la liste.



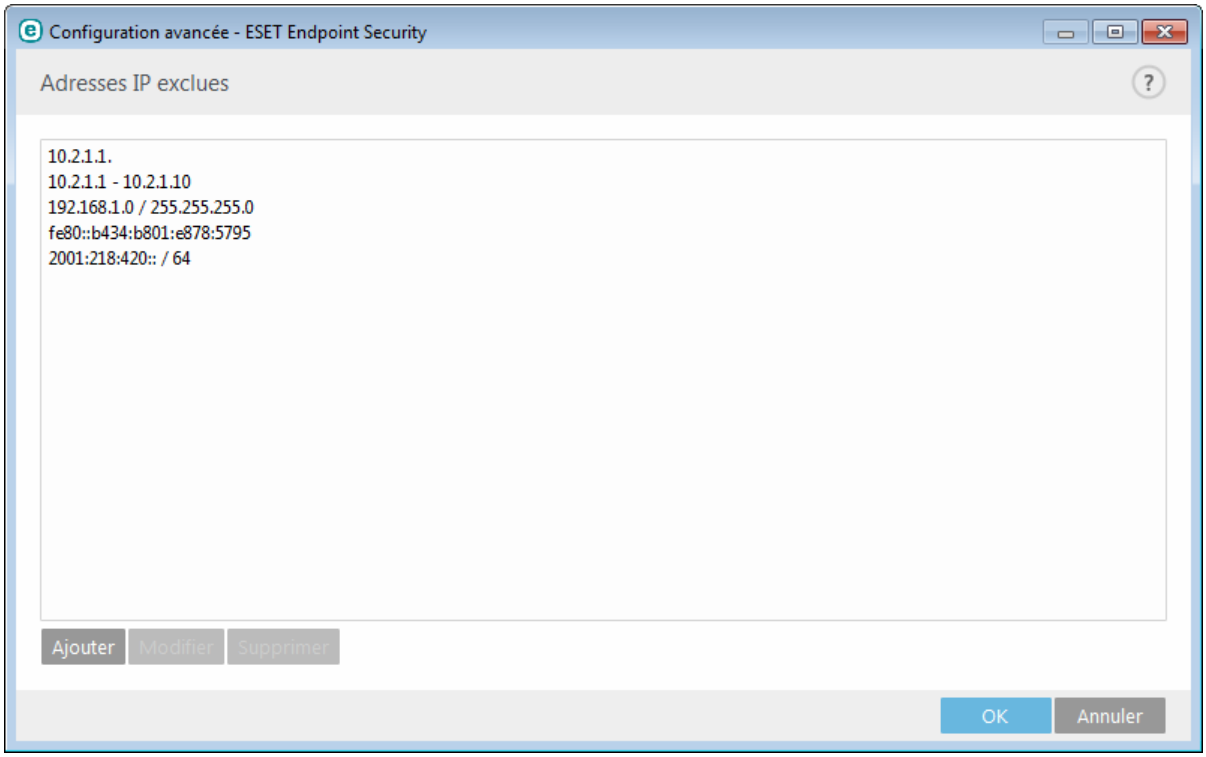
3.8.3.1.3 Adresses IP exclues

Les adresses IP contenues dans cette liste sont exclues du filtrage du contenu des protocoles. Les communications HTTP/POP3/IMAP liées aux adresses sélectionnées ne font pas l'objet d'une détection des menaces. Il est recommandé d'utiliser cette option uniquement pour les adresses que vous savez être fiables.

Ajouter - Cliquez pour ajouter une adresse/une plage d'adresses/un sous-réseau IP d'un point distant auquel une règle est appliquée.

Modifier - Modifie les entrées sélectionnées de la liste.

Supprimer - Supprime les entrées sélectionnées de la liste.



3.8.3.1.4 Contrôle de protocole SSL

ESET Endpoint Security est capable de rechercher les menaces dans les communications qui utilisent le protocole SSL. Vous pouvez utiliser plusieurs modes d'analyse pour examiner les communications SSL protégées à l'aide de certificats approuvés, de certificats inconnus ou de certificats exclus de la vérification des communications SSL protégées.

Activer le filtrage du protocole SSL : si le filtrage des protocoles est désactivé, le programme n'analyse pas les communications sur le protocole SSL.

Le **mode de filtrage de protocole SSL** est disponible dans les options suivantes :

Mode automatique : sélectionnez cette option pour analyser toutes les communications SSL protégées, à l'exception des communications protégées par des certificats exclus de la vérification. Si une nouvelle communication utilisant un certificat signé inconnu est établie, vous n'êtes pas informé et la communication est automatiquement filtrée. Lorsque vous accédez à un serveur disposant d'un certificat non approuvé indiqué comme (il figure dans la liste des certificats approuvés), la communication vers le serveur est autorisée et le contenu du canal de communication est filtré.

Mode interactif : si vous entrez un nouveau site protégé par SSL (avec un certificat inconnu), une boîte de dialogue de sélection d'action s'affiche. Ce mode vous permet de créer la liste des certificats SSL qui seront exclus de l'analyse.

Bloquer les communications chiffrées à l'aide du protocole obsolète SSL v2 : les communications utilisant la version antérieure du protocole SSL sont automatiquement bloquées.

Certificat racine

Certificat racine : pour que la communication SSL fonctionne correctement dans les navigateurs/clients de messagerie, il est essentiel d'ajouter le certificat racine pour ESET à la liste des certificats racines connus (éditeurs). **Ajouter le certificat racine aux navigateurs connus** doit être activé. Sélectionnez cette option pour ajouter automatiquement le certificat racine d'ESET aux navigateurs connus (Opera et Firefox par exemple). Pour les navigateurs utilisant le magasin de certification système, le certificat est ajouté automatiquement (Internet Explorer par exemple).

Pour appliquer le certificat à des navigateurs non pris en charge, cliquez sur **Afficher le certificat** > **Détails** > **Copier dans un fichier...**, puis importez-le manuellement dans le navigateur.

Validité du certificat

S'il est impossible de vérifier le certificat à l'aide du magasin de certificats TRCA : dans certains cas, il est impossible de vérifier le certificat d'un site Web à l'aide du magasin d'Autorités de certification racine de confiance. Cela signifie que le certificat est signé par un utilisateur (l'administrateur d'un serveur Web ou une petite entreprise, par exemple) et que le fait de le considérer comme fiable n'est pas toujours un risque. La plupart des grandes entreprises (les banques par exemple) utilisent un certificat signé par TRCA. Si **Interroger sur la validité du certificat** est activé (sélectionné par défaut), l'utilisateur est invité à sélectionner une action à entreprendre lorsque la communication chiffrée est établie. Vous pouvez sélectionner **Bloquer toute communication utilisant le certificat** pour mettre toujours fin aux connexions chiffrées aux sites avec des certificats non vérifiés.

Si le certificat n'est pas valide ou est endommagé : cela signifie qu'il est arrivé à expiration ou que sa signature est incorrecte. Dans ce cas, il est recommandé de conserver l'option **Bloquer toute communication utilisant le certificat** activée.

La **liste des certificats connus** permet de personnaliser le comportement d'ESET Endpoint Security pour des certificats SSL spécifiques.

3.8.3.1.4.1 Communication SSL chiffrée

Si votre système est configuré pour utiliser l'analyse du protocole SSL, une boîte de dialogue vous invitant à choisir une action peut s'afficher dans les deux cas suivants :

Lorsqu'un site Web utilise un certificat non valide ou ne pouvant pas être vérifié et qu'ESET Endpoint Security est configuré pour demander à l'utilisateur l'action à effectuer dans ce cas (par défaut, oui pour les certificats ne pouvant pas être vérifiés, non pour les certificats non valides), une boîte de dialogue s'affiche pour **autoriser** ou **bloquer** la connexion.

Lorsque l'option **Mode de filtrage du protocole SSL** est définie sur **Mode interactif**, une boîte de dialogue demande pour chaque site Web d'**analyser** ou d'**ignorer** le trafic. Certaines applications vérifient que le trafic SSL n'est ni modifié ni inspecté par quelqu'un. Dans ce cas, ESET Endpoint Security doit **ignorer** ce trafic pour que les applications continuent de fonctionner.

Dans les deux cas, l'utilisateur peut choisir de mémoriser l'action sélectionnée. Les actions enregistrées sont stockées dans la **liste des certificats connus**.

3.8.3.1.4.2 Liste des certificats connus

La **liste des certificats connus** peut être utilisée pour personnaliser le comportement d'ESET Endpoint Security pour des certificats SSL spécifiques et mémoriser les actions choisies en cas de sélection de l'option **Mode interactif** dans **Mode de filtrage de protocole SSL**. La liste peut être affichée et modifiée dans **Configuration avancée** (F5) > **Internet et messagerie** > **Contrôle de protocole SSL** > **Liste des certificats connus**.

La fenêtre **Liste des certificats connus** contient les éléments suivants :

Colonnes

Nom : nom du certificat.

Émetteur du certificat : nom du créateur du certificat.

Objet du certificat : le champ d'objet identifie l'entité associée à la clé publique stockée dans le champ d'objet de la clé publique.

Accès : sélectionnez **Autoriser** ou **Bloquer** comme **Action d'accès** pour autoriser/bloquer les communications sécurisées par ce certificat indépendamment de sa fiabilité. Sélectionnez **Automatique** pour autoriser les certificats approuvés et demander quelle action effectuer pour les certificats non approuvés. Sélectionnez **Demander** pour demander toujours à l'utilisateur quelle action effectuer.

Analyser : sélectionnez **Analyser** ou **Ignorer** comme **Action d'analyse** pour analyser ou ignorer les communications sécurisées par ce certificat. Sélectionnez **Automatique** pour effectuer une analyse en mode automatique et demander quelle action entreprendre en mode interactif. Sélectionnez **Demander** pour demander toujours à l'utilisateur quelle action effectuer.

Éléments de commande

Modifier : sélectionnez le certificat à configurer, puis cliquez sur **Modifier**.

Supprimer : sélectionnez le certificat à supprimer, puis cliquez sur **Supprimer**.

OK/Annuler : **cliquez sur** OK **si vous souhaitez enregistrer les modifications. Sinon, cliquez sur** Annuler.

3.8.3.2 Protection du client de messagerie

3.8.3.2.1 Clients de messagerie

L'intégration d'ESET Endpoint Security aux clients de messagerie augmente le niveau de protection active contre les codes malveillants dans les messages électroniques. Si votre client de messagerie est pris en charge, l'intégration peut être activée dans ESET Endpoint Security. Lorsque l'intégration est activée, la barre d'outils d'ESET Endpoint Security est insérée directement dans le client de messagerie (la barre d'outils pour les nouvelles versions de Windows Live Mail n'est pas insérée), ce qui permet une protection plus efficace des messages. Les paramètres d'intégration sont situés sous **Configuration** > **Configuration avancée** > **Internet et messagerie** > **Protection du client de messagerie** > **Clients de messagerie**.

Intégration aux clients de messagerie

Les clients de messagerie actuellement pris en charge sont Microsoft Outlook, Outlook Express, Windows Mail et Windows Live Mail. Ce module fonctionne comme un plugin pour ces programmes. L'avantage principal du plugin réside dans le fait qu'il est indépendant du protocole utilisé. Lorsqu'un client de messagerie reçoit un message chiffré, il le déchiffre et l'envoie au scanner de virus. Pour obtenir la liste complète des clients de messagerie pris en charge, avec leur version, reportez-vous à cet article de la base de connaissances ESET.

Même si l'intégration n'est pas activée, les communications par messagerie demeurent protégées par le module de protection du client de messagerie (POP3, IMAP).

Activez l'option **Désactiver la vérification au changement de contenu de la boîte aux lettres** si vous constatez un ralentissement du système lors de l'utilisation du client de messagerie (MS Outlook uniquement). Ce cas de figure peut survenir lors de la récupération d'un courrier électronique à partir du magasin Kerio Outlook Connector.

Courrier électronique à analyser

Courrier reçu - Active/désactive la vérification des messages reçus.
Courrier envoyé - Active/désactive la vérification des messages envoyés.
Courrier lu - Active/désactive la vérification des messages lus.

Action à exécuter sur le courrier électronique infecté

Aucune action - Si cette option est activée, le programme identifie les pièces jointes infectées, mais n'entreprend aucune action sur les messages concernés.
Supprimer les courriers - Le programme avertit l'utilisateur à propos d'une infiltration et supprime le message.
Déplacer les courriers vers le dossier Éléments supprimés - Les courriers infectés sont automatiquement placés dans le dossier Éléments supprimés.
Déplacer les courriers vers le dossier - Les courriers infectés sont automatiquement placés dans le dossier spécifié.

Dossier - Spécifiez le dossier personnalisé vers lequel les messages infectés doivent être déplacés lorsqu'ils sont détectés.

Répéter l'analyse après mise à jour - Active/désactive la répétition de l'analyse après la mise à jour de la base des signatures de virus.

Accepter les résultats d'analyse d'autres modules - Si cette option est activée, le module de protection de messages accepte les résultats d'analyse d'autres modules de protection (analyse des protocoles IMAP, POP3).

3.8.3.2.2 Protocoles de messagerie

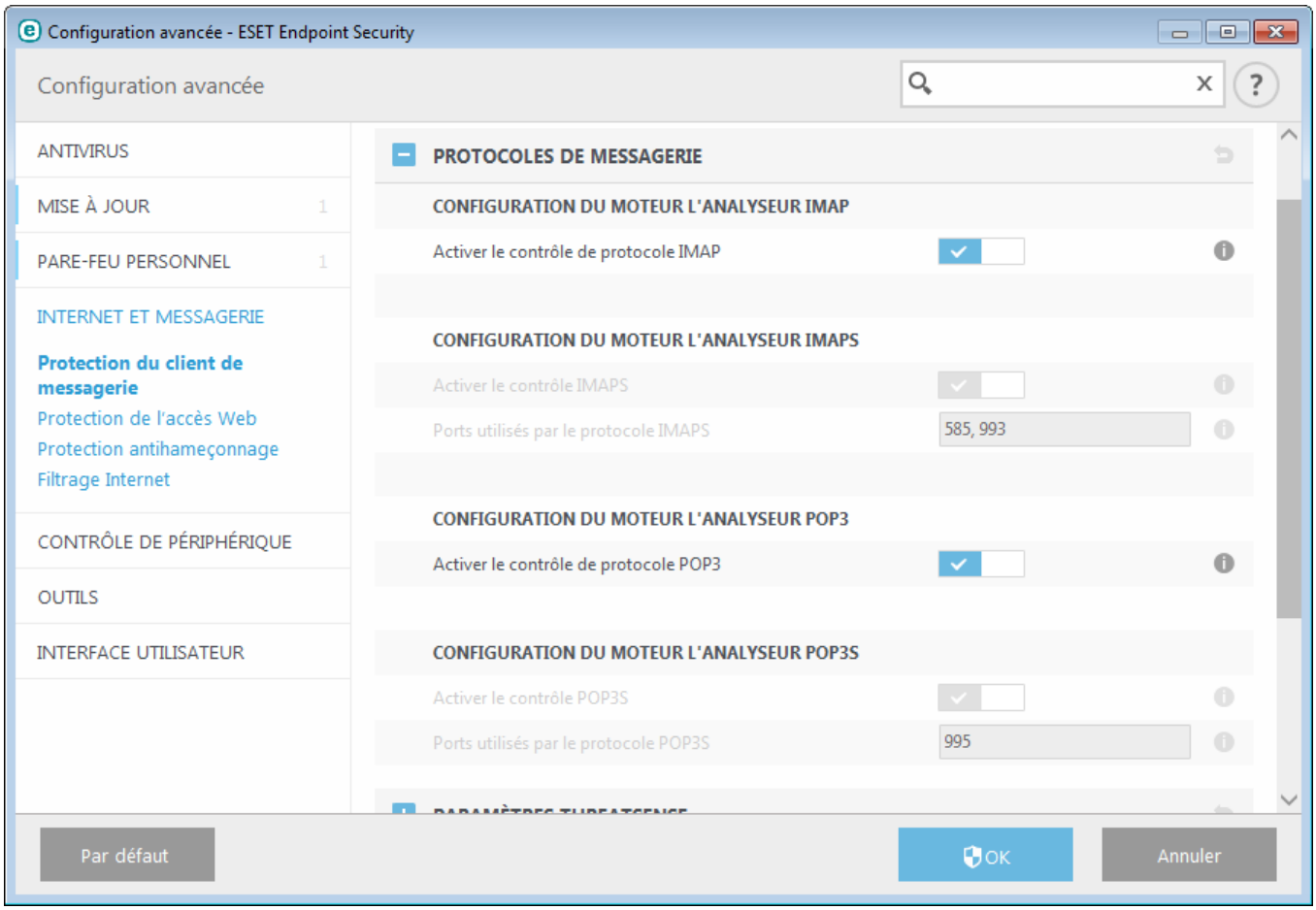
Les protocoles IMAP et POP3 sont les protocoles les plus répandus pour la réception de messages dans un client de messagerie. ESET Endpoint Security protège ces protocoles, quel que soit le client de messagerie utilisé, sans avoir à reconfigurer le client de messagerie.

Vous pouvez configurer le contrôle des protocoles IMAP/IMAPS et POP3/POP3S dans la configuration avancée. Pour accéder à ce paramètre, développez **Internet et messagerie** > **Protection du client de messagerie** > **Protocoles de messagerie**.

Dans Windows Vista et version ultérieure, les protocoles IMAP et POP3 sont automatiquement détectés et analysés sur tous les ports. Dans Windows XP, seuls les **ports utilisés par le protocole POP3** configurés sont analysés pour toutes les applications. Tous les ports sont analysés pour les applications signalées en tant que Web et clients de messagerie.

ESET Endpoint Security prend également en charge l'analyse des protocoles IMAPS et POP3S qui utilisent un canal chiffré pour transférer des informations entre un serveur et un client. ESET Endpoint Security contrôle la communication à l'aide des protocoles SSL (Secure Socket Layer) et TLS (Transport Layer Security). Le programme analyse uniquement le trafic sur les ports définis dans **Ports utilisés par le protocole IMAPS/POP3S**, quelle que soit la version du système d'exploitation.

Les communications chiffrées ne sont pas analysées lorsque les paramètres par défaut sont utilisés. Pour activer l'analyse des communications chiffrées, accédez à l'option Contrôle de protocole SSL dans la configuration avancée, cliquez sur **Internet et messagerie** > **Contrôle de protocole SSL**, puis sélectionnez **Activer le filtrage du protocole SSL**.



3.8.3.2.3 Alertes et notifications

La protection de la messagerie permet de contrôler les communications reçues via les protocoles POP3 et IMAP. ESET Endpoint Security utilise le plugin pour Microsoft Outlook et d'autres clients de messagerie pour contrôler toutes les communications impliquant le client de messagerie (POP3, MAPI, IMAP, HTTP). Lorsqu'il examine les messages entrants, le programme utilise toutes les méthodes d'analyse avancées comprises dans le moteur d'analyse ThreatSense. Autrement dit, la détection des programmes malveillants s'effectue avant la comparaison avec la base des signatures de virus. L'analyse des communications via le protocole POP3 et IMAP est indépendante du client de messagerie utilisé.

Les options de cette fonctionnalité sont disponibles dans **Configuration avancée** sous **Internet et messagerie** > **Protection du client de messagerie** > **Alertes et notifications**.

Configuration des paramètres du moteur ThreatSense - La configuration avancée de l'analyseur de virus permet de configurer les cibles à analyser, les méthodes de détection, etc. Cliquez sur cette option pour afficher la fenêtre de configuration détaillée de l'analyseur de virus.

Après la vérification d'un courrier, une notification avec le résultat de l'analyse peut être ajoutée au message. Vous pouvez sélectionner **Ajouter une notification aux messages reçus et lus, Ajouter une note à l'objet des messages infectés reçus et lus** ou **Ajouter une notification aux messages envoyés**. Gardez à l'esprit qu'en de rares occasions, les notifications peuvent être omises en cas de messages HTML problématiques ou de messages élaborés par un logiciel malveillant. Les notifications peuvent être ajoutées aux messages reçus et lus, aux messages envoyés, ou aux deux catégories. Les options disponibles sont les suivantes :

- **Jamais** - Aucune notification n'est ajoutée.
- **Aux e-mails infectés seulement** - Seuls les messages contenant un code malveillant sont marqués comme contrôlés (valeur par défaut).
- **Aux e-mails infectés seulement** - Le programme ajoute des messages à tout courrier analysé.

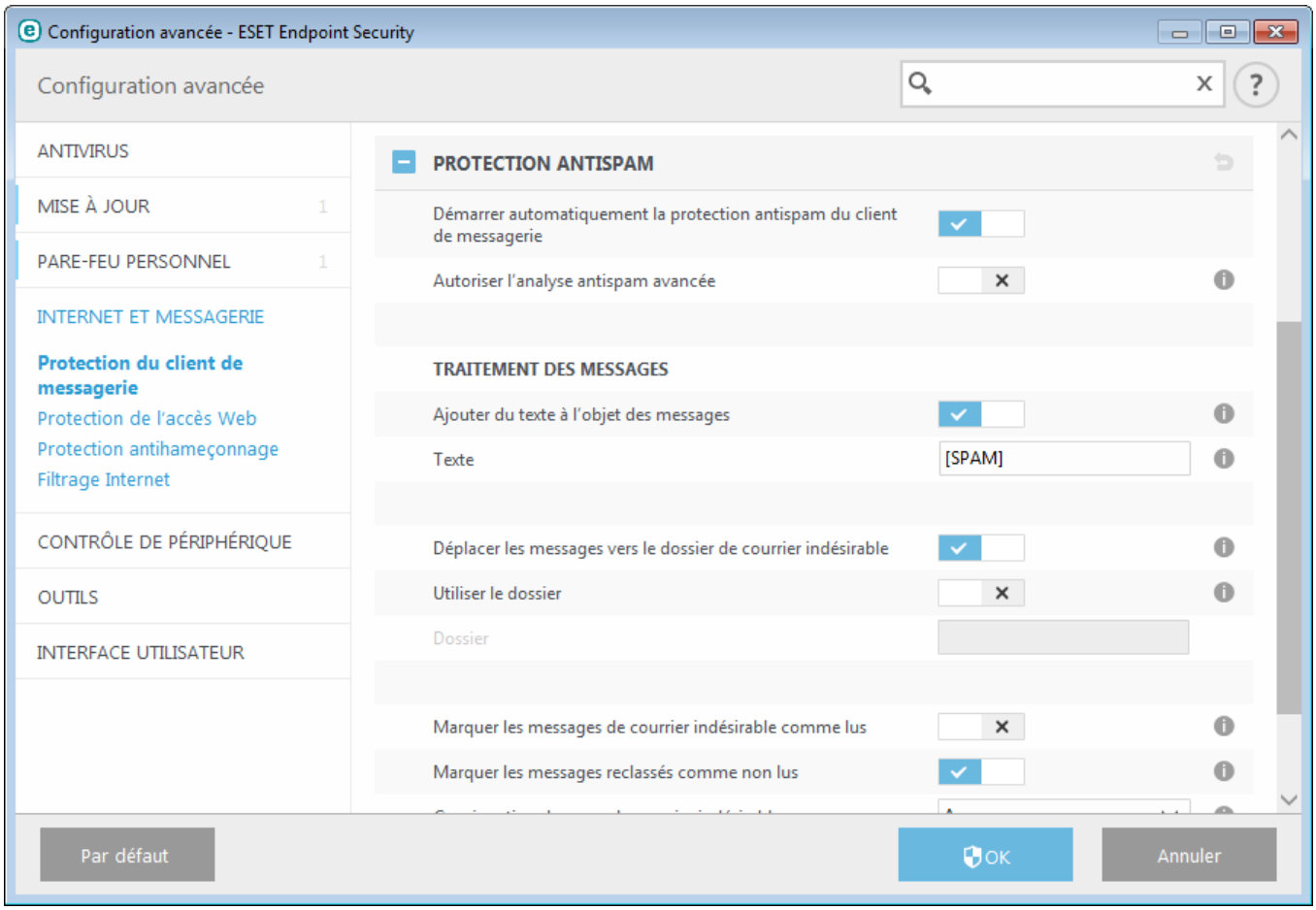
Ajouter une note à l'objet des messages infectés envoyés - Désactivez cette option si vous ne souhaitez pas que la protection de la messagerie ajoute un avertissement de virus dans l'objet d'un message infecté. Cette fonctionnalité permet tout simplement de filtrer les courriers infectés en fonction de son objet (s'il est pris en

charge par le programme de messagerie). Elle augmente également la crédibilité du destinataire et, en cas de détection d'une infiltration, fournit des informations précieuses sur le niveau de menace d'un message ou d'un expéditeur.

Texte ajouté à l'objet des messages infectés - Modifiez ce texte si vous souhaitez modifier le format du préfixe de l'objet d'un courrier infecté. Cette fonction remplace l'objet du message *"Bonjour"* par le préfixe *"[virus]"* au format suivant : *"[virus] Bonjour"*. La variable *%VIRUSNAME%* représente la menace détectée.

3.8.3.2.4 Protection antispam

Le courrier non sollicité, ou spam, constitue l'un des plus grands problèmes liés à la communication électronique. Le spam représente jusqu'à 80 % de toutes les communications par messagerie électronique. La protection antispam sert à vous prémunir de ce problème. En combinant plusieurs principes de sécurité de messagerie, le module antispam garantit un meilleur filtrage pour que votre boîte de réception reste saine.



La détection de spam reconnaît le courrier non sollicité d'après des listes prédéfinies d'adresses fiables (liste blanche) et de spam (liste noire). Toutes les adresses de votre liste de contacts sont automatiquement ajoutées à la liste blanche, ainsi que toutes les autres adresses que vous désignez comme sûres.

La principale méthode utilisée pour détecter du courrier indésirable est l'analyse des propriétés des messages. Les messages reçus sont analysés selon des critères antispam de base (définitions de messages, heuristique statistique, algorithmes de reconnaissance et autres méthodes uniques). L'indice qui en résulte détermine si un message est du spam ou non.

Démarrer la protection antispam de client de messagerie automatiquement : lorsque cette option est activée, la protection antispam est automatiquement activée au démarrage du système.

Autoriser l'analyse antispam avancée - Des données antispam supplémentaires sont régulièrement téléchargées, augmentant ainsi les possibilités antispam et produisant de meilleurs résultats.

La protection antispam dans ESET Endpoint Security vous permet de définir différents paramètres à utiliser avec les listes de messagerie. Les options sont les suivantes :

Traitement des messages

Ajouter un texte à l'objet des messages - Permet d'ajouter une chaîne de caractères personnalisée à la ligne de l'objet des messages classés comme courrier indésirable. La valeur par défaut est [SPAM].

Déplacer les messages vers le dossier des courriers indésirables - Lorsque cette option est activée, les messages de courrier indésirable sont déplacés vers le dossier de courrier indésirable par défaut. De plus, les messages reclassés comme n'étant pas du courrier indésirable sont déplacés vers la boîte de réception. Lorsque vous cliquez avec le bouton droit sur un message électronique et que vous sélectionnez ESET Endpoint Security dans le menu contextuel, plusieurs options vous sont proposées.

Utiliser le dossier - Cette option permet le déplacement des messages spam vers un dossier défini par l'utilisateur.

Marquer les messages de courrier indésirable comme lus - Activez cette option pour marquer automatiquement le courrier indésirable comme lu. Vous pouvez ainsi vous concentrer sur les messages « propres ».

Marquer les messages reclassés comme non lus - Les messages classés au départ comme courrier indésirable, mais marqués ultérieurement comme « propres », sont affichés comme non lus.

Consignation du score définissant un message comme étant du courrier indésirable - Le moteur antispam ESET Endpoint Security attribue à chaque message analysé un score de courrier indésirable. Le message est enregistré dans le journal du courrier indésirable (**ESET Endpoint Security** > **Outils** > **Fichiers journaux** > **Protection antispam**).

- **Aucune** - Le score de l'analyse antispam n'est pas consigné.
- **Reclassé comme courrier indésirable** - Sélectionnez cette option si vous souhaitez enregistrer un score de courrier indésirable pour les messages marqués comme étant du courrier indésirable.
- **Tous** - Tous les messages sont enregistrés dans le journal avec un score de courrier indésirable.

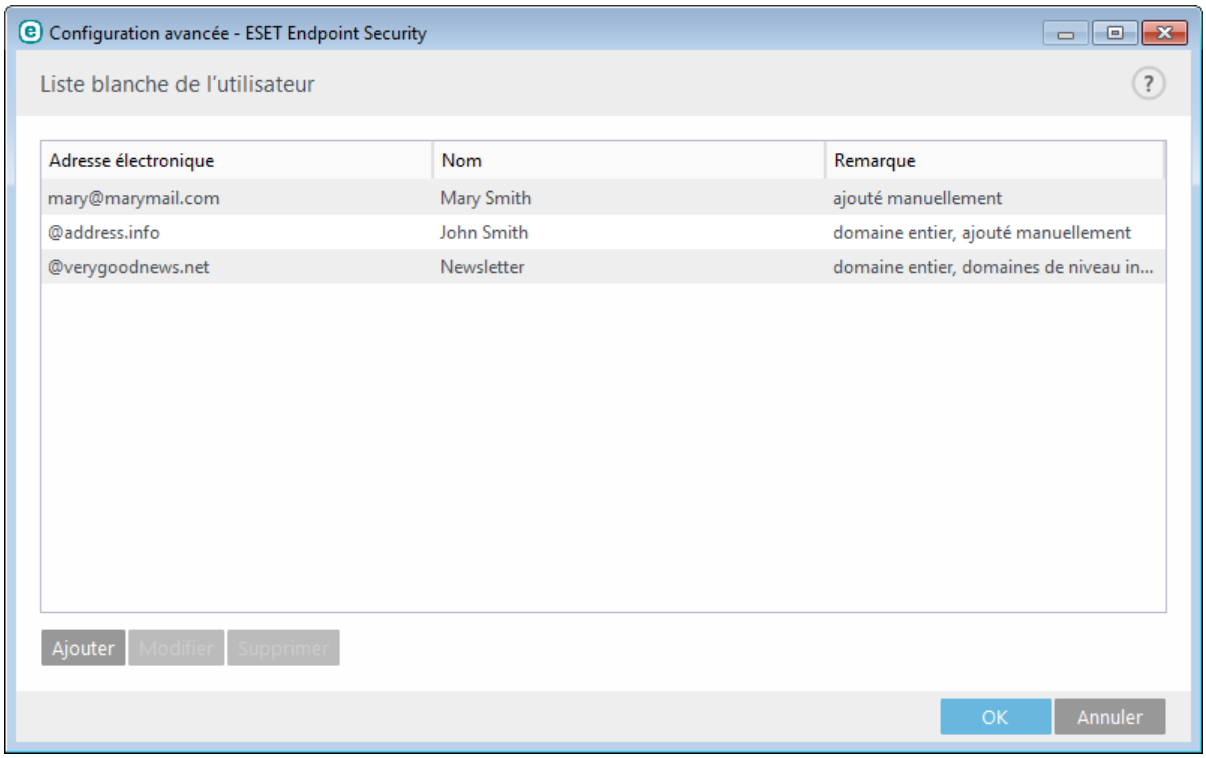
REMARQUE : lorsque vous cliquez sur un message dans le dossier de courrier indésirable, vous pouvez sélectionner **Reclassifier les messages comme NON-courrier indésirable** pour le déplacer vers la boîte de réception. Lorsque vous cliquez sur un message que vous identifiez comme étant du courrier indésirable dans la boîte de réception, sélectionnez **Reclassifier les messages comme courrier indésirable** pour le déplacer vers le dossier de courrier indésirable. Vous pouvez sélectionner plusieurs messages et leur appliquer simultanément la même action.

REMARQUE : ESET Endpoint Security prend en charge la protection antispam pour Microsoft Outlook, Outlook Express, Windows Mail et Windows Live Mail.

3.8.3.2.4.1 Liste noire/Liste blanche/Liste d'exceptions

Pour vous protéger contre les messages non sollicités, ESET Endpoint Security permet de classer des adresses électroniques à l'aide de listes spécialisées. La liste blanche contient les adresses électroniques que vous jugez sûres. Les messages d'utilisateurs figurant dans la liste blanche vont directement dans le dossier du courrier entrant. La liste noire contient les adresses classées comme sources de courrier indésirable. Tous les messages provenant d'expéditeurs qui y figurent sont marqués comme tels. La liste d'exceptions contient les adresses de messagerie qui font toujours l'objet d'une recherche de courrier indésirable. Elle peut également contenir des adresses d'expéditeurs de messages non sollicités ressemblant à des messages de type non-courrier indésirable.

Toutes les listes peuvent être modifiées dans la fenêtre principale du programme ESET Endpoint Security. Pour ce faire, dans **Configuration avancée** > **Internet et messagerie** > **Protection du client de messagerie** > **Carnets d'adresses antispam**, cliquez sur les boutons Ajouter, Modifier et Supprimer de la boîte de dialogue de chaque liste (ou dans **Configuration** > **Internet et messagerie** après avoir cliqué sur l'engrenage ⚙ en regard de **Protection antispam**).



Par défaut, ESET Endpoint Security ajoute toutes les adresses du carnet d'adresses des clients de messagerie pris en charge à la liste blanche. Par défaut, la liste noire est vide. La liste d'exceptions ne contient par défaut que les propres adresses de l'utilisateur.

3.8.3.2.4.2 Ajout d'adresses à la liste blanche et à la liste noire

Les adresses de messagerie des personnes avec lesquelles vous communiquez régulièrement peuvent être ajoutées à la liste blanche. Ainsi, les messages provenant d'adresses figurant dans la liste blanche ne sont jamais classés comme courrier indésirable. Les adresses connues pour envoyer du courrier indésirable peuvent être ajoutées à la liste noire et sont toujours classées comme émettant du courrier indésirable. Pour ajouter une adresse à la liste blanche ou à la liste noire, cliquez avec le bouton droit sur le courrier électronique et sélectionnez **ESET Endpoint Security** > **Ajouter à la liste blanche** ou **Ajouter à la liste noire**, ou cliquez sur le bouton **Adresse fiable** ou **Adresse de courrier indésirable** dans la barre d'outils Antispam ESET Endpoint Security du programme de messagerie.

De façon similaire, le même processus s'applique également aux adresses émettant du courrier indésirable. Si une adresse figure dans la liste noire, tous les messages provenant de cette adresse sont classifiés comme du spam.

3.8.3.2.4.3 Marquage de messages comme courrier indésirable ou non

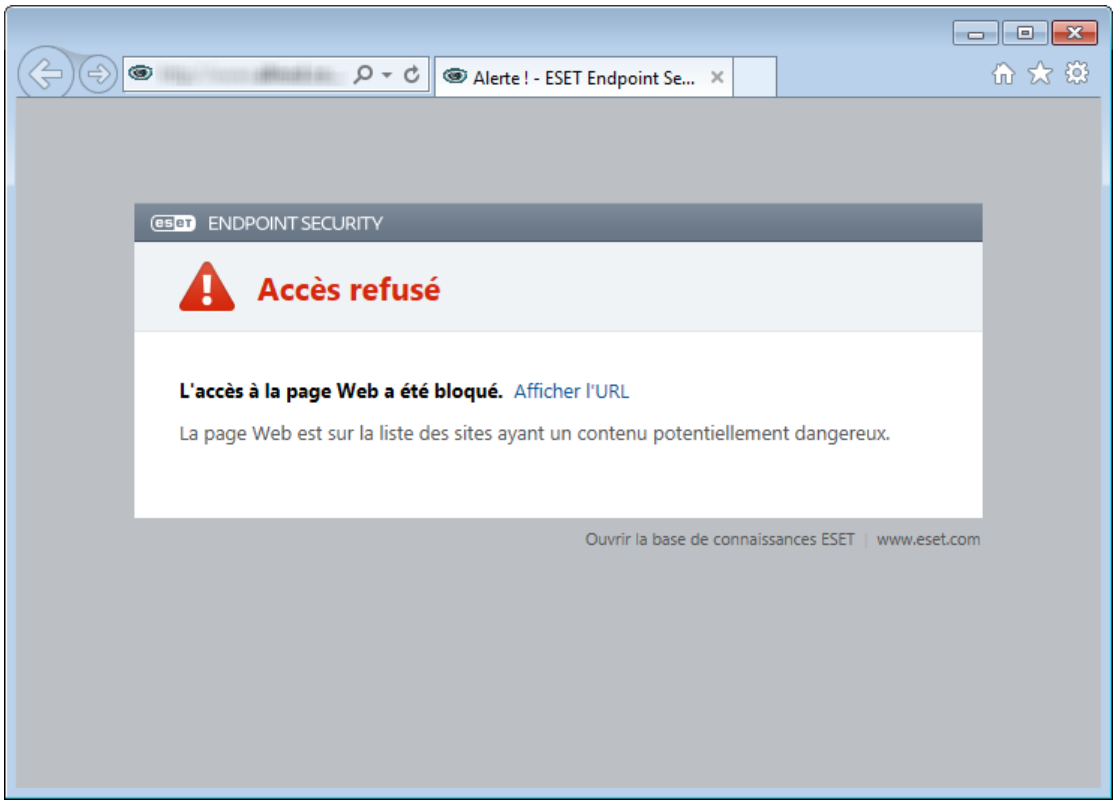
Tout message affiché dans votre client de messagerie peut être marqué comme du courrier indésirable. Pour ce faire, cliquez avec le bouton droit sur le message et cliquez sur **ESET Endpoint Security** > **Reclassifier les messages sélectionnés comme courrier indésirable** ou sur **Courrier indésirable** dans la barre d'outils Antispam ESET Endpoint Security située dans la partie supérieure du client de messagerie.

Les messages reclassés sont automatiquement déplacés vers le dossier COURRIER INDÉSIRABLE, mais l'adresse de l'expéditeur n'est pas ajoutée à la **liste noire**. De même, les messages peuvent être reclassifiés comme « non-courrier indésirable » en cliquant sur **ESET Endpoint Security** > **Reclassifier les messages sélectionnés comme NON-courrier indésirable** ou sur **Non-courrier indésirable** dans la barre d'outils Antispam ESET Endpoint Security située dans la partie supérieure du client de messagerie. Si des messages du dossier « **Junk E-mail** » sont classés comme non-courrier indésirable, ils sont déplacés dans le dossier **Boîte de réception**. Lorsqu'un message est marqué comme non-courrier indésirable, l'adresse de l'expéditeur est automatiquement ajoutée à la **liste blanche**.

3.8.3.3 Protection de l'accès Web

La connectivité Internet est une fonctionnalité standard sur la plupart des ordinateurs personnels. Elle est malheureusement devenue le principal mode de transfert des codes malveillants. La protection de l'accès au Web opère par surveillance des communications entre les navigateurs Internet et les serveurs distants, conformément aux règles des protocoles HTTP et HTTPS (communications chiffrées).

L'accès aux pages Web connues pour comporter du contenu malveillant est bloqué avant le téléchargement du contenu. Toutes les autres pages Web sont analysées par le moteur d'analyse ThreatSense lors de leur chargement et sont bloquées en cas de détection de contenu malveillant. La protection de l'accès Web offre deux niveaux de protection : un blocage par liste noire et un blocage par contenu.



Il est vivement recommandé de conserver l'option de protection de l'accès Web activée. Cette option est accessible à partir de la fenêtre principale de ESET Endpoint Security en accédant à **Configuration** > **Internet et messagerie** > **Protection de l'accès Web**.

Les options suivantes sont disponibles dans **Configuration avancée** (F5) > **Internet et messagerie** > **Protection de l'accès Web** :

- **Protocoles Web** : permet de configurer le contrôle de ces protocoles standard qui sont utilisés par la plupart des navigateurs Internet.
- **Gestion des adresses URL** : permet de spécifier des listes d'adresses HTTP qui seront bloquées, autorisées ou exclues de la vérification.
- **Configuration des paramètres du moteur ThreatSense** : la configuration avancée de l'analyseur de virus permet de configurer des paramètres tels que les types d'objet à analyser (courriers électroniques, archives, etc.), les méthodes de détection pour la protection de l'accès Web, etc.

3.8.3.3.1 Protocoles Web

Par défaut, ESET Endpoint Security est configuré pour contrôler le protocole HTTP utilisé par la plupart des navigateurs Internet.

Dans Windows Vista et version ultérieure, le trafic HTTP est toujours contrôlé sur tous les ports pour toutes les applications. Dans Windows XP, vous pouvez modifier les **ports utilisés par le protocole HTTP** dans **Configuration avancée** (F5) > **Internet et messagerie** > **Protection de l'accès Web** > **Protocoles Web** > **Configuration de l'analyseur HTTP**. Le trafic HTTP est contrôlé sur les ports spécifiés pour toutes les applications et sur tous les ports des applications signalées comme Web et clients de messagerie.

ESET Endpoint Security prend également en charge le contrôle de protocole HTTPS. Les communications HTTPS utilisent un canal chiffré pour transférer des informations entre un serveur et un client. ESET Endpoint Security contrôle les communications à l'aide des protocoles SSL (Secure Socket Layer) et TLS (Transport Layer Security). Le programme analyse uniquement le trafic sur les ports définis dans **Ports utilisés par le protocole HTTPS**, quelle que soit la version du système d'exploitation.

Les communications chiffrées ne sont pas analysées lorsque les paramètres par défaut sont utilisés. Pour activer l'analyse des communications chiffrées, accédez à l'option Contrôle de protocole SSL dans la configuration avancée, cliquez sur **Internet et messagerie** > **Contrôle de protocole SSL**, puis sélectionnez **Activer le filtrage du protocole SSL**.

3.8.3.3.2 Gestion d'adresse URL

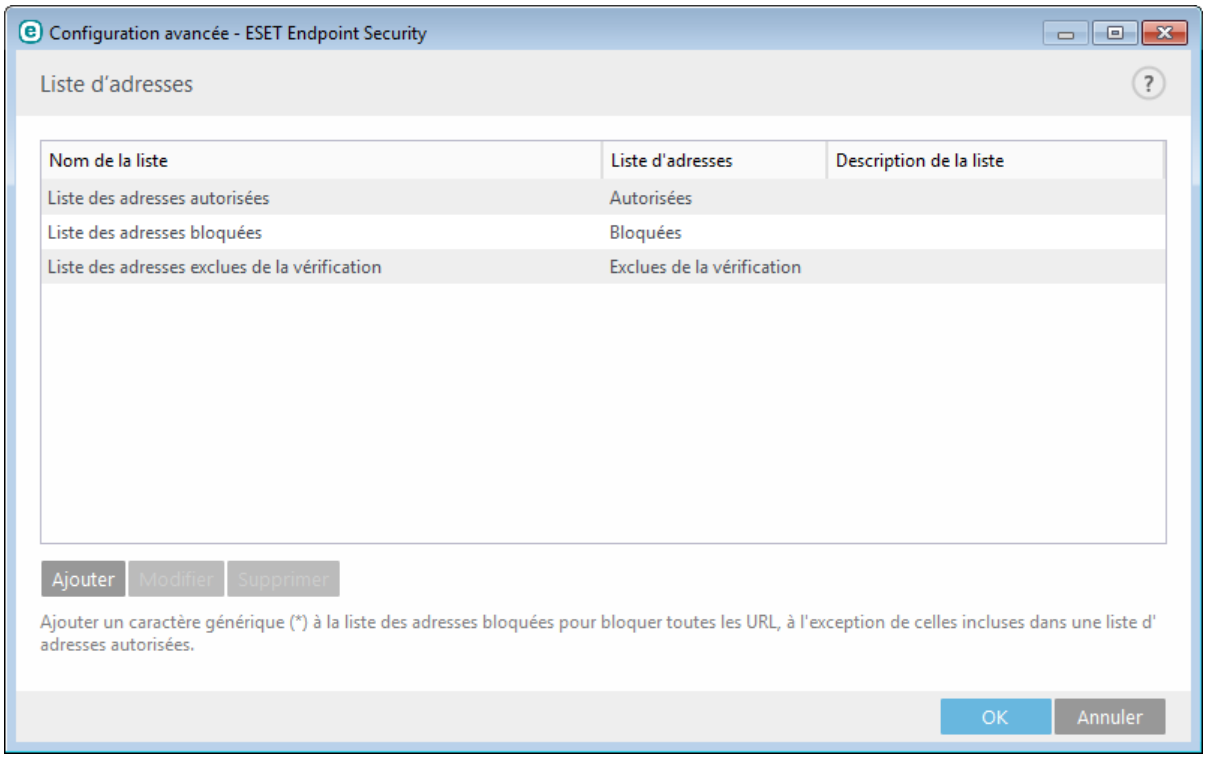
La section Gestion d'adresse URL permet de spécifier des listes d'adresses HTTP qui seront bloquées, autorisées ou exclues de la vérification.

Les sites Web qui figurent dans la **liste des adresses bloquées** ne sont pas accessibles, sauf s'ils sont également inclus dans la **liste des adresses autorisées**. Les sites Web qui se trouvent dans la **liste des adresses exclues de la vérification** ne font pas l'objet d'une analyse de code malveillant lors de leur accès.

L'option **Activer le filtrage du protocole SSL** doit être sélectionnée si vous souhaitez filtrer les adresses HTTPS en plus des pages Web HTTP. Sinon, seuls les domaines des sites HTTPS que vous avez visités sont ajoutés et non l'URL complète.

Dans toutes les listes, vous pouvez utiliser les symboles spéciaux « * » (astérisque) et « ? » (point d'interrogation). L'astérisque représente n'importe quel chiffre ou caractère, alors que le point d'interrogation symbolise n'importe quel caractère. Un soin particulier doit être apporté à la spécification des adresses exclues, car la liste ne doit contenir que des adresses sûres et fiables. De la même manière, veillez à employer correctement les symboles « * » et « ? » dans cette liste. Reportez-vous à Ajout d'un masque de domaine/d'adresse HTTP pour déterminer comment faire correspondre un domaine complet avec tous ses sous-domaines en toute sécurité. Pour activer une liste, activez l'option **Liste active**. Si vous souhaitez être averti lors de la saisie d'une adresse figurant dans la liste actuelle, sélectionnez l'option **Notifier lors de l'application**.

Si vous souhaitez bloquer toutes les adresses HTTP, à l'exception des adresses figurant dans la **liste des adresses autorisées** active, ajoutez un astérisque (*) à la **liste des adresses bloquées** active.



Ajouter : permet de créer une liste en plus des listes prédéfinies. Cela peut s'avérer utile si vous souhaitez diviser de manière logique des groupes différents d'adresses. Par exemple, une liste d'adresses bloquées peut contenir les adresses d'une liste noire publique externe et une autre liste peut comporter votre propre liste noire, ce qui simplifie la mise à jour de la liste externe tout en conservant la vôtre intacte.

Modifier : permet de modifier les listes existantes. Utilisez cette option pour ajouter ou supprimer des adresses des listes.

Supprimer : permet de supprimer une liste existante. Il est possible uniquement de supprimer les listes créées à l'aide de l'option **Ajouter** et non les listes par défaut.

3.8.3.4 Protection antihameçonnage

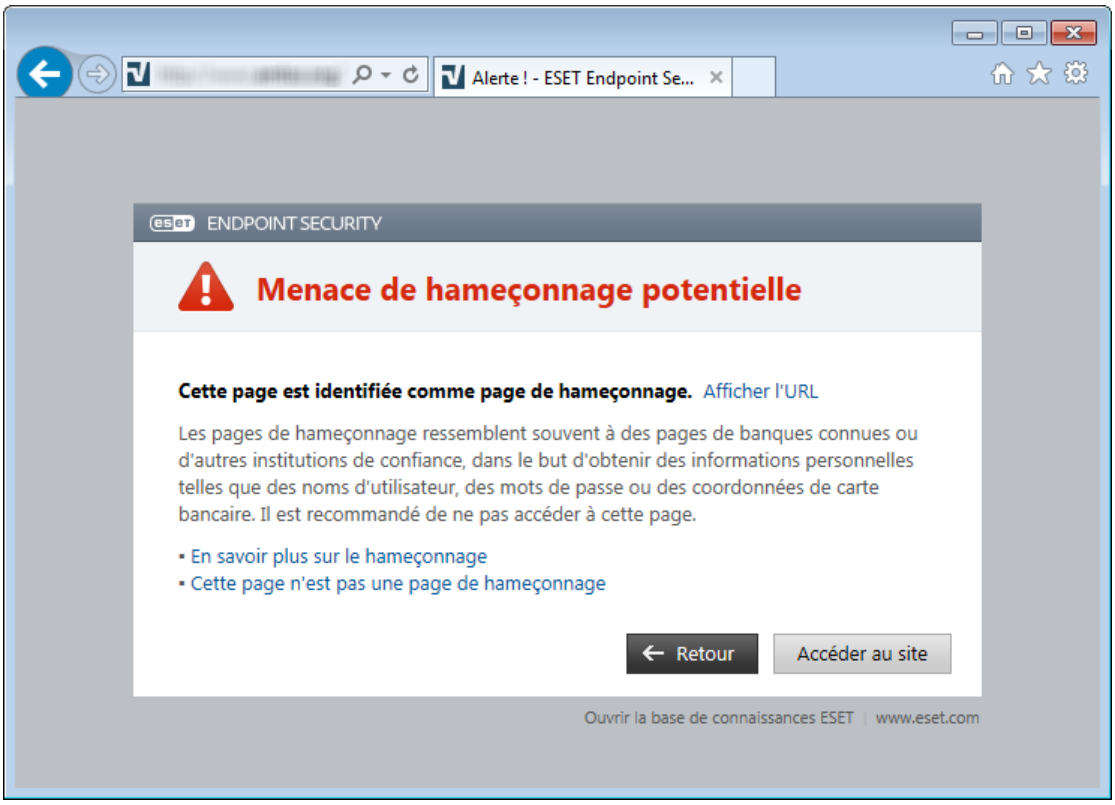
Le terme d'hameçonnage (phishing en anglais) désigne une activité frauduleuse utilisant des techniques de piratage psychologique qui consistent à manipuler les utilisateurs pour obtenir des informations confidentielles. L'hameçonnage est souvent utilisé pour accéder à des données sensibles, telles que numéros de comptes bancaires, codes secrets, etc. Pour en savoir plus sur cette activité, reportez-vous au glossaire. ESET Endpoint Security assure une protection antihameçonnage qui permet de bloquer les pages Web connues qui présentent ce type de contenu.

Nous vous recommandons fortement d'activer l'antihameçonnage dans ESET Endpoint Security. Pour ce faire, accédez à **Configuration avancée** (F5), puis à **Internet et messagerie** > **Protection antihameçonnage**.

Pour plus d'informations sur la protection antihameçonnage d'ESET Endpoint Security, consultez notre article de la base de connaissances.

Accès à un site Web d'hameçonnage

Lorsque vous accédez à un site Web d'hameçonnage reconnu, la boîte de dialogue suivante s'affiche dans votre navigateur Web. Si vous souhaitez toujours accéder au site Web, cliquez sur **Accéder au site** (non recommandé).



REMARQUE : Par défaut, les sites Web d'hameçonnage potentiels que vous avez ajoutés à la liste blanche expirent plusieurs heures après. Pour autoriser un site Web de manière permanente, utilisez l'outil Gestion des adresses URL. Dans **Configuration avancée** (F5), développez **Internet et messagerie** > **Protection de l'accès Web** > **Gestion des adresses URL** > **Liste d'adresses**, cliquez sur **Modifier**, puis ajoutez le site Web à modifier à cette liste.

Signalement d'un site de hameçonnage

Le lien Signaler vous permet de signaler un site Web de hameçonnage/malveillant à ESET pour analyse.

REMARQUE : Avant de soumettre un site Web à ESET, assurez-vous qu'il répond à au moins l'un des critères suivants :

- le site Web n'est pas du tout détecté,
- le site Web est, à tort, détecté comme une menace. Dans ce cas, vous pouvez Signaler un site faux positif de hameçonnage.

Vous pouvez également soumettre le site Web par e-mail. Envoyez votre message à l'adresse samples@eset.com. Veillez à utiliser un objet descriptif et indiquez le plus d'informations possible sur le site Web (notez, par exemple, le site Web référant, comment vous avez appris l'existence du site Web, etc.).

3.8.4 Filtrage Internet

La section Filtrage Internet permet de configurer des paramètres qui contribuent à protéger votre entreprise contre les responsabilités juridiques. Le filtrage Internet peut réglementer l'accès aux sites Web qui enfreignent les droits de propriété intellectuelle. L'objectif est d'empêcher les employés d'accéder à des pages au contenu inapproprié ou nuisible ou qui sont susceptibles d'avoir une incidence négative sur leur productivité.

Le filtrage Internet permet de bloquer les pages Web dont le contenu peut être choquant. En outre, les employés ou les administrateurs système peuvent interdire l'accès à plus de 27 catégories de sites Web prédéfinies et à plus de 140 sous-catégories.

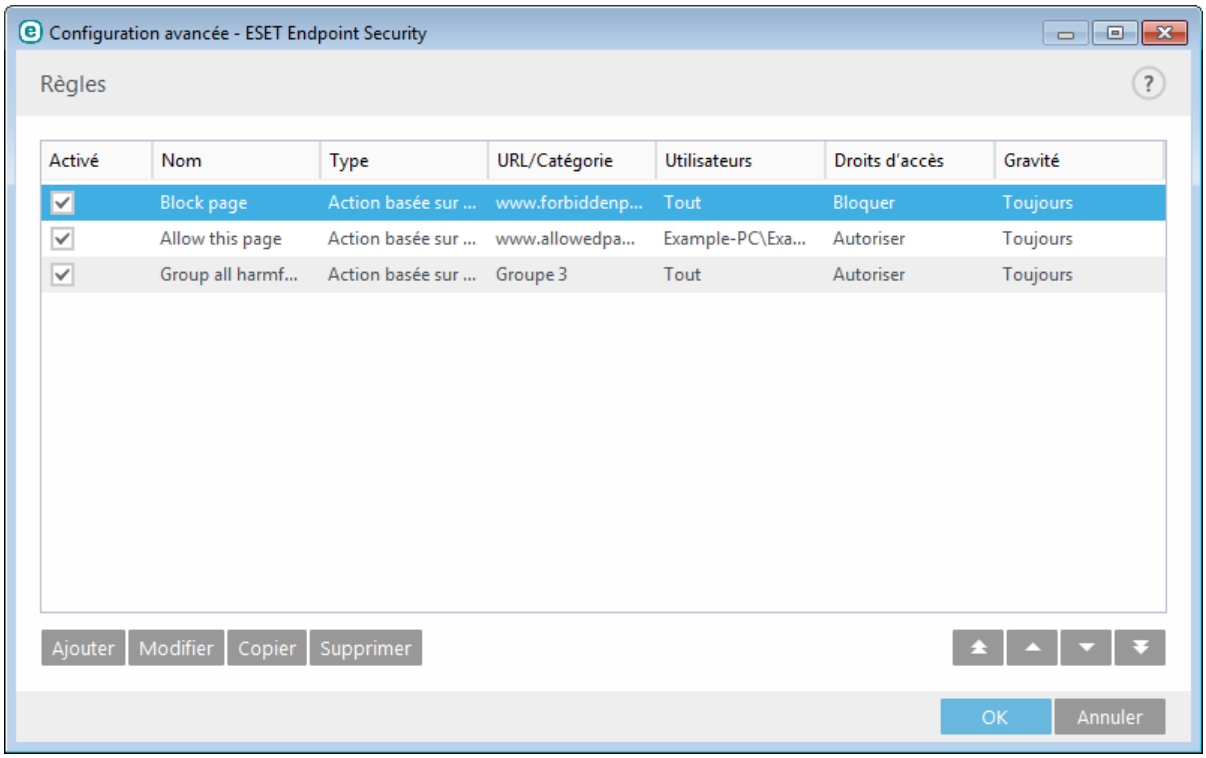
Par défaut, le filtrage Internet est désactivé. Pour l'activer, appuyez sur F5 pour accéder à **Configuration avancée**, puis développez **Internet et messagerie** > **Filtrage Internet**. Sélectionnez **Intégrer dans le système** pour activer le filtrage Internet dans ESET Endpoint Security. Cliquez sur **Modifier** en regard de **Règles** pour accéder à la fenêtre Éditeur de règles du filtrage Internet.

Les champs **Message de page Web bloquée** et **Image de page Web bloquée** vous permettent de personnaliser facilement le message affiché lorsqu'un site Web est bloqué.

CONSEIL : voici un exemple de message de page Web bloquée : *La page Web est bloquée car elle est considérée comme inconvenante ou comporte du contenu nuisible. Contactez votre administrateur pour obtenir des informations.* Vous pouvez également saisir une adresse Web ou un chemin réseau avec une image personnalisée (*http://test.com/test.jpg*, par exemple). La taille d'image personnalisée est automatiquement définie sur 90 x 30. Les images seront automatiquement mises à l'échelle, si nécessaire.

3.8.4.1 Règles

La fenêtre d'éditeur **Règles** affiche les règles existantes basées sur l'URL ou la catégorie.



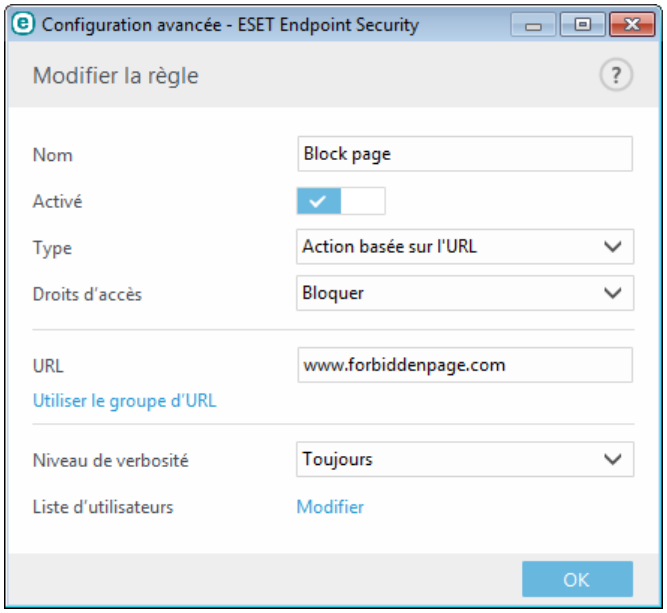
La liste des règles contient plusieurs descriptions des règles, telles que le nom, le type de blocage, l'action à effectuer après l'application d'une règle de filtrage Internet et le niveau de gravité d'après le journal.

Cliquez sur **Ajouter** ou **Modifier** pour gérer une règle. Cliquez sur **Copier** pour créer une règle à l'aide d'options prédéfinies utilisées pour une autre règle sélectionnée. En appuyant sur **Ctrl** et en cliquant, vous pouvez sélectionner plusieurs règles et supprimer toutes les règles sélectionnées. La case à cocher **Activé** permet d'activer ou de désactiver la règle ; elle peut être utile si vous ne voulez pas supprimer la règle de façon définitive en cas de réutilisation ultérieure.

Les règles sont triées selon leur priorité, les règles de priorité supérieure au-dessus. L'évaluation des règles basée sur les URL a toujours une priorité plus élevée que celle basée sur les catégories. Par exemple, si une règle basée sur une URL se trouve en dessous d'une règle basée sur une catégorie dans la liste des règles, la règle basée sur une URL possède une priorité plus élevée et est évaluée en premier.

3.8.4.1.1 Ajout de règles de filtrage Internet

La fenêtre Règles de filtrage Internet permet de créer ou de modifier manuellement une règle de filtrage Internet existante.



Entrez une description de la règle dans le champ **Nom** afin de mieux l'identifier. Cliquez sur le bouton bascule **Activé** pour désactiver ou activer la règle ; cela peut être utile si vous ne souhaitez pas supprimer la règle de façon définitive.

Type d'action

- **Action basée sur l'URL** - Pour les règles qui contrôlent l'accès d'un site Web donné, saisissez l'URL dans le champ **URL**.
- **Action basée sur la catégorie** - Lorsque cette option est sélectionnée, définissez la catégorie de l'action dans le menu déroulant.

Vous ne pouvez pas utiliser les symboles spéciaux « * » (astérisque) et « ? » (point d'interrogation) dans la liste des adresses URL. Lorsque vous créez un groupe d'URL qui contient un site Web avec plusieurs domaines de niveau supérieur, vous devez ajouter séparément chacun d'entre eux. Si vous ajoutez un domaine au groupe, tout le contenu situé dans ce domaine et ses sous-domaines (par exemple *sous.pageexemple.com*) sera bloqué ou autorisé en fonction du choix d'action basée sur l'URL.

Droits d'accès

- **Autoriser** - L'accès à l'adresse URL/catégorie est autorisé.
- **Autoriser et avertir** - Affiche un avertissement concernant l'adresse URL/la catégorie.
- **Bloquer** - Bloque l'adresse URL/la catégorie.

URL ou **Utiliser le groupe d'URL** - Utilise l'URL de lien ou le groupe de liens pour autoriser, bloquer ou afficher un avertissement lors de la détection de l'une de ces URL.

Niveau de verbosité :

- **Toujours** - Consigne toutes les communications en ligne.
- **Diagnostic** - Consigne les informations nécessaires au réglage du programme.
- **Informations** - Enregistre tous les messages d'information, y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissement** - Enregistre les erreurs critiques et les messages d'avertissement.
- **Aucune** - Aucun journal n'est enregistré.

Liste d'utilisateurs

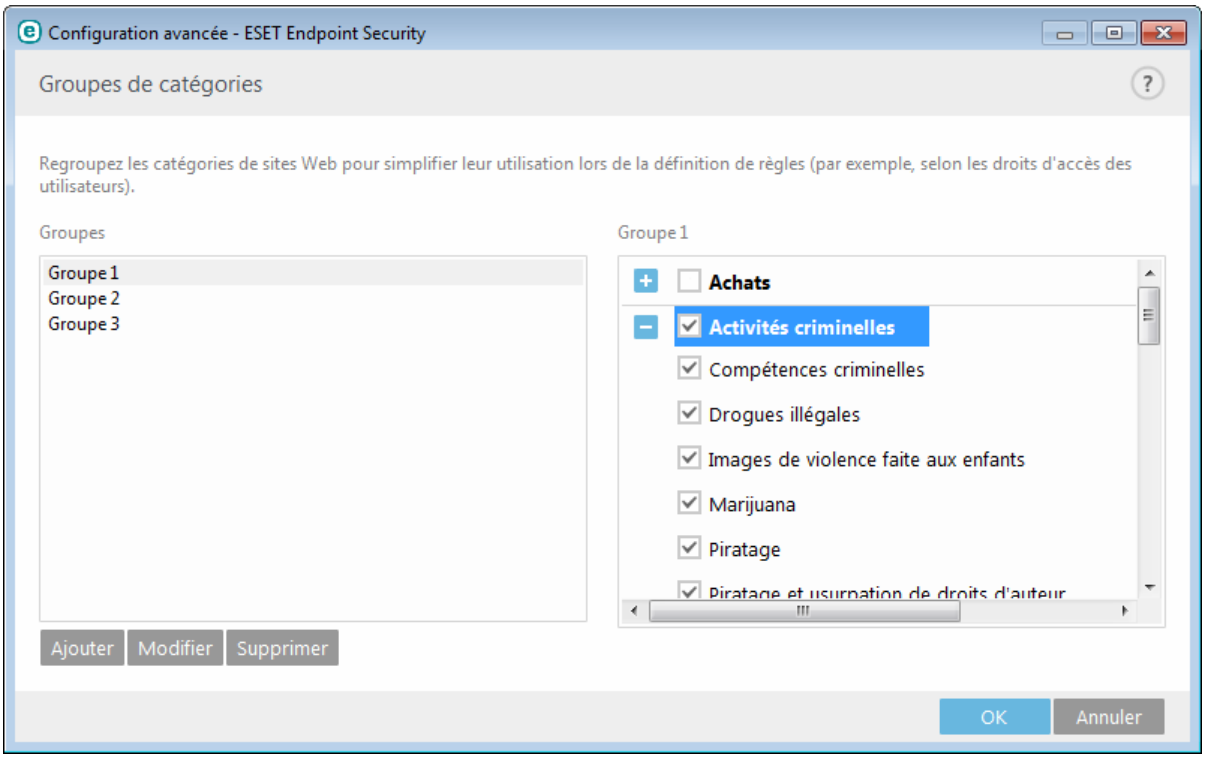
- **Ajouter** - Ouvre la boîte de dialogue **Sélectionner des utilisateurs ou groupes** qui permet de sélectionner les utilisateurs voulus. Lorsqu'aucun utilisateur n'est entré, la règle est appliquée à tous les utilisateurs.
- **Supprimer** - Supprime l'utilisateur sélectionné du filtre.

3.8.4.2 Groupes de catégories

La fenêtre Groupes de catégories se divise en deux parties. La partie droite de la fenêtre contient une liste de catégories et sous-catégories. Sélectionnez une catégorie dans la liste Catégorie pour afficher les sous-catégories correspondantes.

Chaque groupe contient des sous-catégories réservées aux adultes et/ou généralement inappropriées ainsi que des catégories généralement considérées comme acceptables. Lorsque vous ouvrez la fenêtre Groupes de catégories et cliquez sur le premier groupe, vous pouvez ajouter ou supprimer des catégories/sous-catégories de la liste des groupes appropriés (Violence ou Armes, par exemple). Les pages Web comportant du contenu inapproprié peuvent être bloquées ou les utilisateurs peuvent en être informés après la création d'une règle avec des actions prédéfinies.

Activez la case à cocher pour ajouter ou supprimer une sous-catégorie dans un groupe spécifique.



Voici quelques exemples de catégories avec lesquelles les utilisateurs ne sont peut-être pas familiarisés :

Divers - En général, adresses IP privées (locales) comme l'intranet, 192.168.0.0/16, etc. Lorsque vous recevez un code d'erreur 403 ou 404, le site Web en question sera également associé à cette catégorie.
Non résolu - Cette catégorie inclut des pages Web qui ne sont pas résolues en raison d'une erreur de connexion au moteur de base de données du filtrage Internet.
Non classé - Pages Web inconnues non répertoriées dans la base de données du filtrage Internet.
Proxys - Les pages Web comme les sites de navigation anonymes, les redirecteurs ou les serveurs proxy publics peuvent être utilisées pour accéder (de façon anonyme) aux pages Web généralement bloquées par le filtre du filtrage Internet.
Partage de fichier - Ces pages Web contiennent de grandes quantités de données comme des photos, des vidéos ou des livres électroniques. Il existe un risque que le contenu de ces sites soit choquant ou réservé aux adultes.

REMARQUE : une sous-catégorie peut appartenir à n'importe quel groupe. Certaines sous-catégories ne sont pas incluses à des groupes prédéfinis (par exemple, Jeux). Pour qu'une sous-catégorie soit prise en compte comme vous l'entendez lors du filtrage Internet, ajoutez-la au groupe voulu.

3.8.4.3 Groupes d'URL

Les groupes d'URL permettent de créer un groupe contenant plusieurs liens URL pour lesquels vous souhaitez créer une règle (autoriser/refuser un site Web spécifique).

Pour créer un groupe d'URL, cliquez sur **Ajouter**. Sélectionnez un groupe d'URL et cliquez sur **Ajouter** dans la partie inférieure droite de la fenêtre pour ajouter une nouvelle adresse URL à la liste. Vous pouvez également cliquer sur **Importer** pour importer un fichier contenant une liste d'adresses URL (séparez les valeurs par un saut de ligne, par exemple *.txt utilisant le codage UTF-8). Si vous souhaitez définir une action à effectuer pour un groupe d'URL spécifique, ouvrez l'**Éditeur de règles du filtrage Internet**, sélectionnez le groupe d'URL à l'aide du menu déroulant, réglez les autres paramètres, puis cliquez sur **OK**.

REMARQUE : bloquer ou autoriser une page Web spécifique peut s'avérer plus approprié que de bloquer ou autoriser une catégorie complète de pages Web. Soyez vigilant lorsque vous modifiez ces paramètres et ajoutez une catégorie/page Web à la liste.

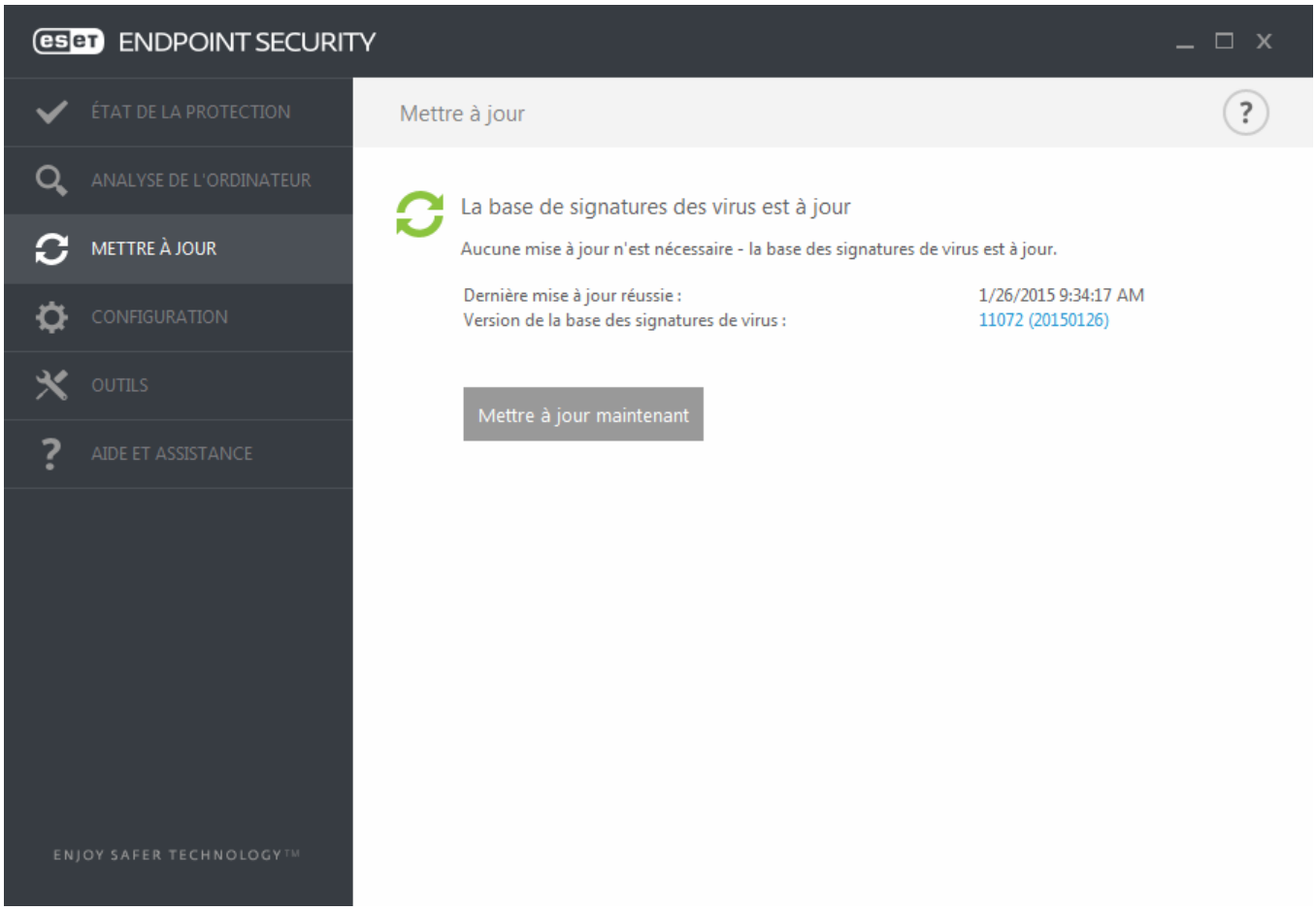
3.8.5 Mise à jour du programme

La mise à jour régulière d'ESET Endpoint Security est la meilleure méthode pour bénéficier du niveau maximum de sécurité de votre ordinateur. Le module de mise à jour veille à ce que le programme soit toujours à jour de deux façons : en mettant à jour la base des signatures de virus et en mettant à jour les composants système.

En cliquant sur **Mettre à jour** dans la fenêtre principale du programme, vous pouvez connaître l'état actuel de la mise à jour, notamment la date et l'heure de la dernière mise à jour. Vous pouvez également savoir si une mise à jour est nécessaire. La fenêtre Mise à jour contient également la version de la base des signatures de virus. Cette indication numérique est un lien actif vers le site Web d'ESET, qui répertorie toutes les signatures ajoutées dans cette mise à jour.

Par ailleurs, il est possible de démarrer manuellement la mise à jour à l'aide de l'option **Mise à jour de la base des signatures de virus**. La mise à jour de la base des signatures de virus et celle des composants du programme sont des opérations importantes de la protection totale contre les attaques des codes malveillants. Il convient donc d'apporter une grande attention à leur configuration et à leur fonctionnement. Si vous n'avez pas saisi les détails de la licence pendant l'installation, vous pouvez entrer votre clé de licence en cliquant sur **Activer le produit** lors de la mise à jour pour accéder aux serveurs de mise à jour ESET.

REMARQUE : la clé de licence est fournie par ESET après l'achat d'ESET Endpoint Security.

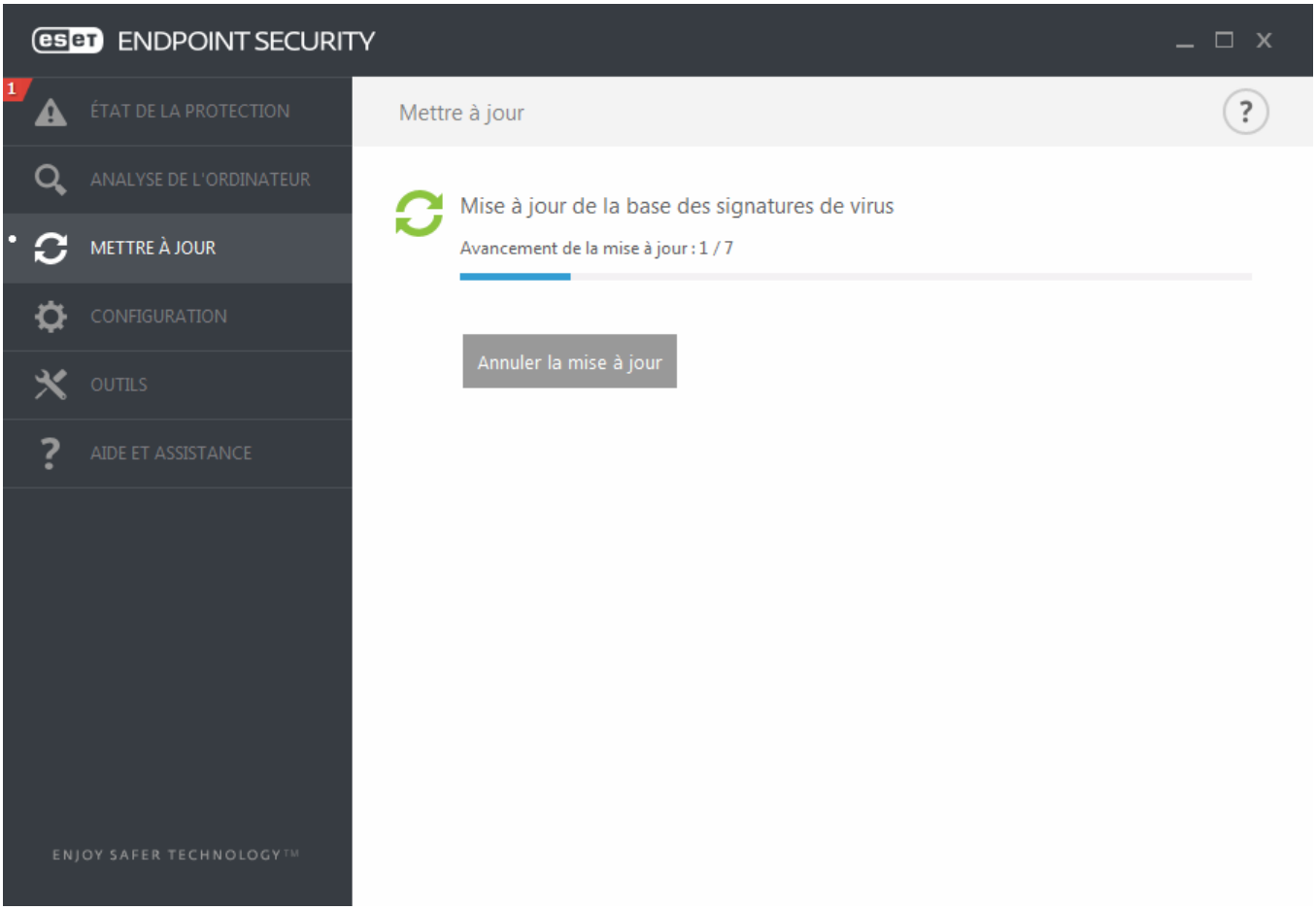


Dernière mise à jour réussie - Date de la dernière mise à jour. Vérifiez qu'il s'agit d'une date récente indiquant que la base des signatures de virus est à jour.

Version de la base des signatures de virus - Numéro de base des signatures de virus ; il s'agit également d'un lien actif vers le site Web d'ESET. Cliquez ici pour afficher la liste de toutes les signatures ajoutées dans la mise à jour.

Processus de mise à jour

Une fois que vous avez cliqué sur **Mise à jour de la base des signatures de virus**, le processus de téléchargement commence. La barre de progression qui s'affiche indique le temps de téléchargement restant. Pour interrompre la mise à jour, cliquez sur **Annuler la mise à jour**.

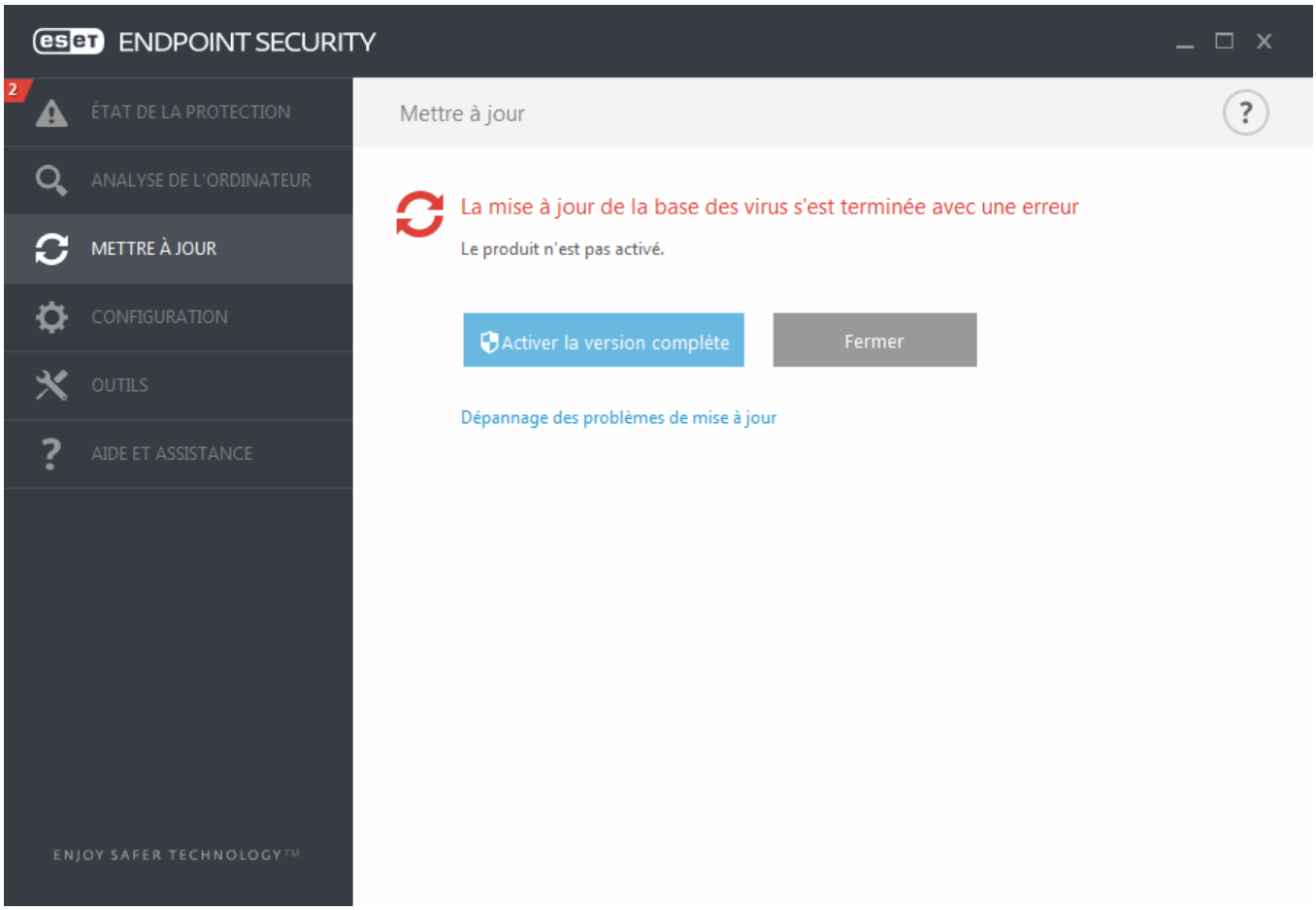


Important : dans des circonstances normales, lorsque les mises à jour sont téléchargées correctement, le message **Mise à jour non nécessaire - la base des signatures de virus installée est à jour** s'affiche dans la fenêtre **Mise à jour**. Si ce n'est pas le cas, le programme n'est pas à jour et le risque d'infection est accru. Veillez à mise à jour la base des signatures de virus dès que possible. Dans d'autres circonstances, l'un des messages d'erreur suivants s'affiche :

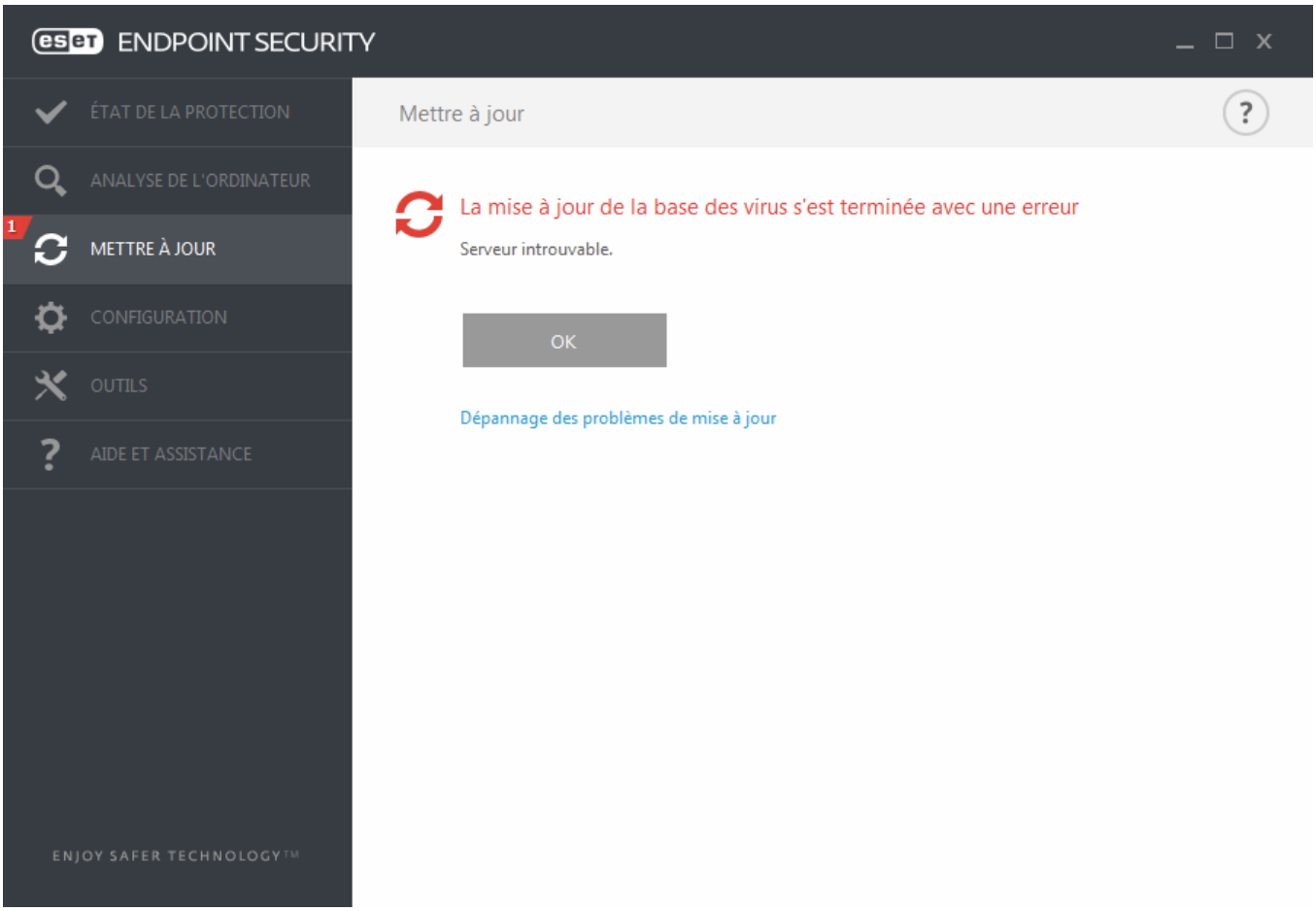
La base des signatures de virus n'est plus à jour - Cette erreur apparaît après plusieurs tentatives infructueuses de mise à jour de la base des signatures de virus. Nous vous conseillons de vérifier les paramètres de mise à jour. Cette erreur provient généralement de l'entrée incorrecte de données d'authentification ou de la configuration incorrecte des paramètres de connexion.

La notification précédente concerne les deux messages **Échec de la mise à jour de la base des signatures de virus** sur les mises à jour infructueuses :

1. **Licence non valide** - La clé de licence n'a pas été correctement saisie lors de la configuration des mises à jour. Nous vous recommandons de vérifier vos données d'authentification. La fenêtre Configuration avancée (cliquez sur **Configuration** dans le menu principal, puis sur **Configuration avancée**, ou appuyez sur la touche F5 de votre clavier) comporte d'autres options de mise à jour. Dans le menu principal, cliquez sur **Aide et assistance** > **Gérer la licence** pour saisir une nouvelle clé de licence.



2. **Une erreur s'est produite pendant le téléchargement des fichiers de mise à jour** - L'erreur peut être due à des paramètres de connexion Internet incorrects. Nous vous recommandons de vérifier votre connectivité à Internet (en ouvrant un site Web dans votre navigateur). Si le site Web ne s'ouvre pas, cela est probablement dû au fait qu'aucune connexion à Internet n'est établie ou que votre ordinateur a des problèmes de connectivité. Consultez votre fournisseur de services Internet si vous n'avez pas de connexion Internet active.



REMARQUE : pour plus d'informations, consultez cet article de la base de connaissances ESET.

3.8.5.1 Configuration des mises à jour

Les options de configuration des mises à jour sont accessibles dans l'arborescence **Configuration avancée** (F5), sous **Mise à jour** > **Général**. Cette section permet de spécifier les informations concernant les sources des mises à jour, telles que les serveurs de mise à jour utilisés et les données d'authentification donnant accès à ces serveurs.

Général

Le profil de mise à jour en cours d'utilisation est affiché dans le menu déroulant **Profil sélectionné**. Pour créer un profil, cliquez sur **Modifier** en regard de **Liste des profils**, saisissez un nom dans **Nom du profil**, puis cliquez sur **Ajouter**.

Si vous rencontrez des problèmes lors du téléchargement des mises à jour de la base des signatures de virus, cliquez sur **Effacer** pour supprimer les fichiers de mise à jour/le cache temporaires.

Alertes de base des signatures de virus obsolète

Définir automatiquement l'âge maximal de la base de signatures de virus- Permet de définir la durée maximale (en jours) au terme de laquelle la base des signatures de virus est signalée comme étant obsolète. La valeur par défaut est 7.

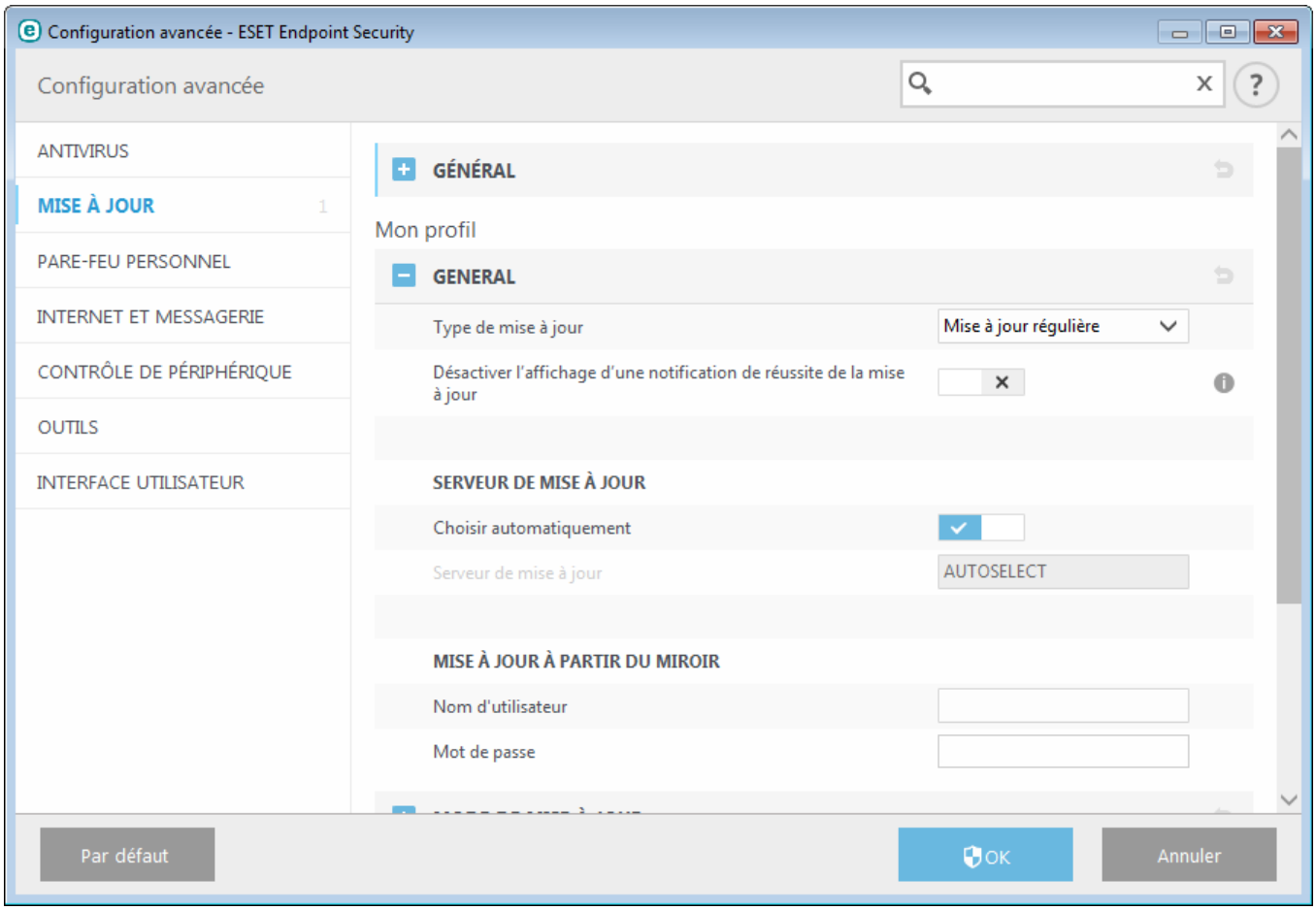
Restaurer

Si vous pensez qu'une mise à jour de la base de virus ou des modules du programme est instable ou corrompue, vous pouvez restaurer la version précédente et désactiver les mises à jour pendant une période donnée. D'un autre

côté, il est aussi possible d'activer les mises à jour précédemment désactivées si vous les avez reportées pour une durée indéterminée.

ESET Endpoint Security enregistre des instantanés de base des signatures de virus et de modules du programme à utiliser avec la fonctionnalité de *restauration*. Pour permettre la création d'instantanés de la base de virus, conservez le bouton bascule **Créer des instantanés des fichiers de mise à jour** activé. Le champ **Nombre d'instantanés stockés localement** définit le nombre d'instantanés de la base de virus stockés.

Si vous cliquez sur **Restaurer** (**Configuration avancée** (F5) > **Mise à jour** > **Général**), vous devez sélectionner une durée dans le menu déroulant qui représente la période durant laquelle les mises à jour de la base des signatures de virus et celles des modules de programme sont interrompues.



Il est essentiel de remplir tous les paramètres de mise à jour avec précision afin de télécharger correctement les mises à jour. Si vous utilisez un pare-feu, vérifiez que le programme ESET est autorisé à accéder à Internet (communication HTTP, par exemple).

Général

Par défaut, l'option **Type de mise à jour** est définie sur **Mise à jour régulière** pour que les fichiers de mise à jour soient téléchargés automatiquement du serveur ESET lorsque le trafic réseau est le moins surchargé. Les mises à jour des versions bêta (option **Mise à jour des versions bêta**) ont subi toutes les phases internes de test et seront disponibles très prochainement pour le grand public. Vous pouvez activer ces versions bêta afin d'accéder aux dernières méthodes de détection et aux derniers correctifs. Toutefois, ces versions ne sont peut-être pas suffisamment stables pour être utilisées en permanence et NE DOIVENT PAS être utilisées sur des serveurs de production et des stations de travail qui exigent les plus grandes disponibilité et stabilité. L'option **Mise à jour retardée** permet d'effectuer la mise à jour à partir de serveurs de mise à jour spéciaux fournissant les nouvelles versions de bases de virus après un délai d'au moins X heures (bases testées dans un environnement réel et donc considérées comme stables).

Désactiver l'affichage d'une notification de réussite de la mise à jour - Désactive les notifications qui apparaissent dans la barre d'état système, dans l'angle inférieur droit de l'écran. Cette option est utile si une application ou un jeu s'exécute en mode plein écran. Veuillez noter que le mode de présentation désactive toutes les notifications.

Le menu **Serveur de mise à jour** est défini par défaut sur SÉLECTION AUTOMATIQUE. Le serveur de mise à jour est l'emplacement où sont stockées les mises à jour. Si vous utilisez un serveur ESET, il est recommandé de conserver l'option par défaut.

Si un serveur local HTTP, appelé également miroir, est utilisé, le serveur de mise à jour doit être configuré comme suit :
http://nom_ordinateur_ou_son_adresse_IP:2221

Si vous utilisez un serveur local HTTP avec SSL, le serveur de mise à jour doit être configuré comme suit :
https://nom_ordinateur_ou_son_adresse_IP:2221

Si vous utilisez un dossier partagé local, le serveur de mise à jour doit être configuré comme suit :
\\nom_ordinateur_ou_son_adresse_IP\dossier_partagé

Mise à jour à partir du miroir

L'authentification des serveurs de mise à jour est basée sur la **clé de licence** générée et qui vous a été envoyée après l'achat. Lors de l'utilisation d'un serveur miroir local, vous pouvez définir des informations d'identification pour les clients afin qu'ils se connectent au serveur miroir avant la réception des mises à jour. Par défaut, aucune vérification n'est exigée, et les champs **Nom d'utilisateur** et **Mot de passe** restent vides.

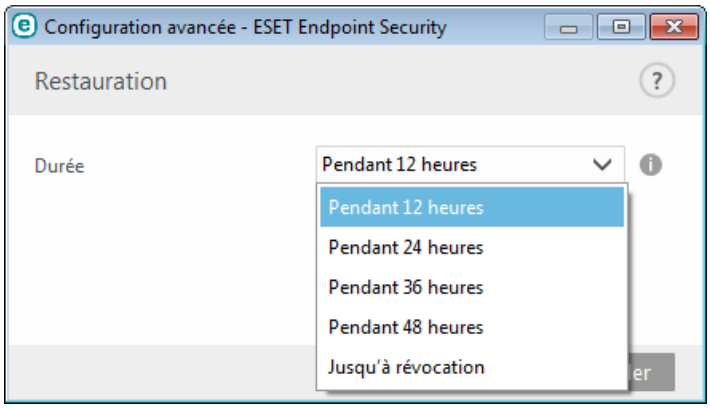
3.8.5.1.1 Profils de mise à jour

Les profils de mise à jour ne peuvent pas être créés pour différentes configurations et tâches de mise à jour. La création de profils de mise à jour est particulièrement utile pour les utilisateurs mobiles qui ont besoin d'un autre profil correspondant aux propriétés de connexion Internet qui changent régulièrement.

Le menu déroulant **Profil sélectionné** affiche le profil actuellement sélectionné, qui est défini par défaut sur **Mon profil**. Pour créer un profil, cliquez sur **Modifier** en regard de **Liste des profils**, saisissez un nom dans **Nom du profil**, puis cliquez sur **Ajouter**.

3.8.5.1.2 Paramètres avancés de mises à jour

Si vous cliquez sur **Restaurer** (**Configuration avancée** (F5) > **Mise à jour** > **Profil**), vous devez sélectionner une durée dans le menu déroulant qui représente la période durant laquelle les mises à jour de la base des signatures de virus et celles des modules de programme sont interrompues.



Sélectionnez **Jusqu'à son retrait** pour différer indéfiniment les mises à jour régulières jusqu'à ce que vous restauriez manuellement cette fonctionnalité. Nous ne recommandons pas de sélectionner cette option qui présente un risque potentiel pour la sécurité de l'ordinateur.

La base des signatures de virus revient à la version la plus ancienne disponible, stockée sous forme d'instantané dans le système de fichiers de l'ordinateur local.

Exemple : admettons que le numéro 10646 correspond à la base des signatures de virus la plus récente. Les bases des signatures de virus 10645 et 10643 sont stockées sous forme d'instantanés. Notez que la base numéro 10644 n'est pas disponible parce que l'ordinateur était éteint et qu'une mise à jour plus récente a été mise à disposition avant que 10644 n'ait été téléchargée, par exemple. Si le champ **Nombre d'instantanés stockés localement** est défini sur 2 et que vous cliquez sur **Restaurer**, la base des signatures de virus (y compris les modules du programme)

sera restaurée à la version numéro 10643. Ce processus peut prendre un certain temps. Vérifiez si la base des signatures de virus est bien retournée à une version antérieure dans la fenêtre principale de ESET Endpoint Security dans la section Mise à jour.

3.8.5.1.3 Mode de mise à jour

L'onglet **Mode de mise à jour** contient les options concernant la mise à jour des composants du programme. Le programme vous permet de prédéfinir son comportement lorsqu'une nouvelle mise à niveau de composant programme est disponible.

Les mises à jour des composants du programme offrent de nouvelles fonctionnalités ou modifient les versions précédentes. Cette mise à jour peut s'effectuer sans intervention de l'utilisateur ou après sa notification. Le redémarrage de l'ordinateur peut être nécessaire après la mise à jour des composants du programme. Dans la section **Mise à jour des composants du programme**, trois options sont disponibles :

- **Demander avant de télécharger les composants du programme** - Option par défaut. Vous êtes invité à confirmer ou à refuser les mises à jour de composants de programme lorsqu'elles sont disponibles.
- **Toujours mise à jour les composants du programme** - Les mises à jour de composants du programme sont téléchargées et installées automatiquement. Notez que le redémarrage du système peut être nécessaire.
- **Ne jamais mise à jour les composants du programme** - Aucune mise à jour des composants du programme n'a lieu. Cette option convient aux serveurs, car ces derniers ne peuvent généralement être redémarrés qu'en cas de maintenance.

REMARQUE : la sélection de l'option la plus appropriée dépend du poste de travail sur lequel les paramètres sont appliqués. Notez qu'il existe des différences entre les postes de travail et les serveurs. Par exemple, le redémarrage automatique d'un serveur après une mise à jour du programme peut causer de sérieux dommages.

Si l'option **Demander avant de télécharger une mise à jour** est activée, une notification s'affiche lorsqu'une nouvelle mise à jour est disponible.

Si la taille du fichier de mise à jour est supérieure à la valeur spécifiée dans le champ **Demander si un fichier de mise à jour a une taille supérieure à (Ko)**, le programme affiche une notification.

3.8.5.1.4 Proxy HTTP

Pour accéder aux options de configuration du serveur proxy pour un profil de mise à jour donné, cliquez sur **Mise à jour** dans l'arborescence **Configuration avancée** (F5), puis sur **Proxy HTTP**. Cliquez sur le menu déroulant **Mode proxy** et sélectionnez l'une des trois options suivantes :

- Ne pas utiliser de serveur proxy
- Connexion via un serveur proxy
- Utiliser les paramètres globaux de serveur proxy

L'option **Utiliser les paramètres globaux de serveur proxy** utilise les options de configuration de serveur proxy déjà indiquées dans la branche **Outils** > **Serveur proxy** de la configuration avancée complète.

Sélectionnez **Ne pas utiliser de serveur proxy** pour indiquer qu'aucun serveur proxy ne sera utilisé pour la mise à jour d'ESET Endpoint Security.

L'option **Connexion via un serveur proxy** doit être sélectionnée si :

- Un serveur proxy doit être utilisé pour mise à jour ESET Endpoint Security et ce serveur doit être différent de celui indiqué dans les paramètres globaux (**Outils** > **Serveur proxy**). Si c'est le cas, des paramètres supplémentaires doivent être spécifiés : l'adresse du **Serveur proxy**, le **Port** de communication (3128 by default), ainsi que le **nom d'utilisateur** et le **mot de passe** du serveur proxy, si nécessaire.
- Les paramètres de serveur proxy n'ont pas été définis globalement, mais ESET Endpoint Security se connecte à un serveur proxy pour les mises à jour.
- Votre ordinateur est connecté à Internet par l'intermédiaire d'un serveur proxy. Les paramètres sont pris dans Internet Explorer pendant l'installation du programme, mais s'ils sont modifiés par la suite (par exemple, en cas de changement de fournisseur de services Internet), vérifiez que les paramètres du proxy HTTP figurant dans la fenêtre sont corrects. Dans le cas contraire, le programme ne pourra pas se connecter aux serveurs de mise à jour.

L'option par défaut pour le serveur proxy est **Utiliser les paramètres globaux de serveur proxy**.

REMARQUE : les données d'authentification telles que **Nom d'utilisateur** et **Mot de passe** permettent d'accéder au serveur proxy. Ne remplissez ces champs que si un nom d'utilisateur et un mot de passe sont requis. Notez que ces champs ne sont pas ceux du mot de passe/nom d'utilisateur d'ESET Endpoint Security et ne doivent être remplis que si vous savez que vous avez besoin d'un mot de passe pour accéder à Internet via un serveur proxy.

3.8.5.1.5 Se connecter au réseau local comme

Lors de mise à jour depuis un serveur local sur un système d'exploitation Windows NT, une authentification est par défaut exigée pour chaque connexion réseau.

Pour configurer un compte de ce type, sélectionnez **Type d'utilisateur local** dans le menu déroulant :

- **Compte système (par défaut)**
- **Utilisateur actuel**
- **Utilisateur spécifié**.

Sélectionnez **Compte système (par défaut)** afin d'utiliser le compte système pour l'authentification. Normalement, aucun traitement d'authentification n'a lieu si les données d'authentification ne sont pas fournies dans la section de configuration des mises à jour.

Pour s'assurer que le programme s'authentifie à l'aide du compte de l'utilisateur connecté, sélectionnez **Utilisateur actuel**. L'inconvénient de cette solution est que le programme ne peut pas se connecter au serveur de mise à jour si aucun utilisateur n'est connecté.

Sélectionnez **Utilisateur spécifié** si vous voulez que le programme utilise un compte utilisateur spécifié pour l'authentification. Utilisez cette méthode si la connexion avec le compte système échoue. Notez que le compte de l'utilisateur spécifié doit avoir accès au dossier des fichiers de mise à jour du serveur local. Dans le cas contraire, le programme ne pourrait pas établir la connexion nécessaire pour télécharger les mises à jour.

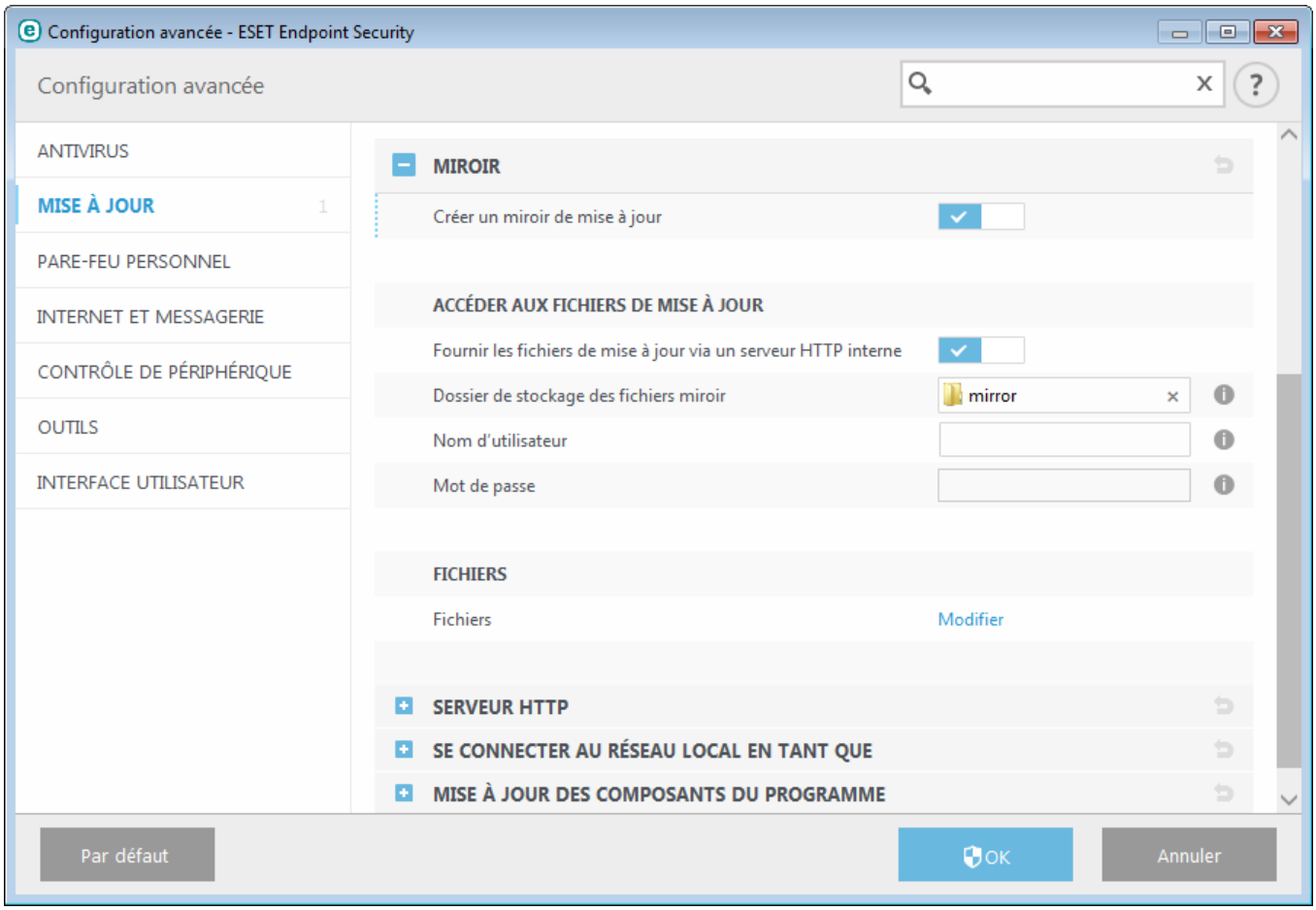
Avertissement : Si l'une des options **Utilisateur actuel** ou **Utilisateur spécifié** est activée, une erreur peut se produire en cas de changement de l'identité du programme pour l'utilisateur souhaité. C'est pour cette raison que nous recommandons d'entrer les données d'authentification du réseau local dans la section de configuration des mises à jour. Dans cette section de configuration des mises à jour, les données d'authentification doivent être entrées comme suit : *nom_de_domaine\utilisateur* (dans le cas d'un groupe de travail, entrez *nom_de_groupe_de_travail\utilisateur*) et le mot de passe. La mise à jour de la version HTTP du serveur local n'exige aucune authentification.

Sélectionnez **Déconnecter du serveur après la mise à jour** pour forcer une déconnexion si la connexion au serveur reste active, même après le téléchargement des mises à jour.

3.8.5.1.6 Miroir

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 postes de travail du réseau. L'utilisation d'un *miroir*, 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 toutes les stations de travail. Les mises à jour sont téléchargées sur le serveur miroir local puis distribuées à toutes les stations de travail pour éviter tout risque de surcharge du réseau. La mise à jour de postes de travail à partir d'un miroir optimise l'équilibre de la charge réseau et libère les bandes passantes des connexions Internet.

Les options de configuration du serveur miroir local figurent dans Configuration avancée, sous **Mise à jour**. Pour accéder à cette section, appuyez sur **F5** (pour ouvrir la fenêtre Configuration avancée), cliquez sur **Mise à jour**, puis sélectionnez l'onglet **Miroir**.



Pour créer un miroir sur un poste de travail client, activez l'option **Créer un miroir de mise à jour**. L'activation de cette option active d'autres options de configuration du miroir, telles que la manière d'accéder aux fichiers de mise à jour et le chemin des fichiers miroir.

Accéder aux fichiers de mise à jour

Fournir les fichiers de mise à jour via un serveur HTTP interne : si cette option est activée, les fichiers de mise à jour sont accessibles via un serveur HTTP. Aucune information d'identification n'est requise.

REMARQUE : Windows XP requiert le Service Pack 2 ou version ultérieure pour utiliser le serveur HTTP.

Les méthodes d'accès au serveur miroir sont décrites en détail dans Mise à jour à partir du miroir. Il existe deux méthodes de base pour accéder au miroir : le dossier des fichiers de mise à jour peut être considéré comme un dossier réseau partagé ou les clients peuvent accéder au miroir situé sur un serveur HTTP.

Le dossier dédié aux fichiers de mise à jour du miroir peut être défini sous **Dossier de stockage des fichiers miroir**. Cliquez sur **Dossier** pour naviguer jusqu'au dossier souhaité sur un ordinateur local ou un dossier réseau partagé. Si une autorisation pour le dossier spécifié est requise, les données d'authentification doivent être entrées dans les champs **Nom d'utilisateur** et **Mot de passe**. Si le dossier destination sélectionné se trouve sur un disque réseau exécutant le système d'exploitation Windows NT/2000/XP, le nom d'utilisateur et le mot de passe spécifiés doivent disposer du droit d'écriture sur ce dossier. Le nom d'utilisateur et le mot de passe doivent être entrés sous le format *Domaine/Utilisateur* ou *Workgroup/Utilisateur*. N'oubliez pas de fournir les mots de passe correspondants.

Fichiers : lors de la configuration du miroir, vous pouvez indiquer les versions linguistiques des mises à jour à télécharger. Les langues sélectionnées doivent être prises en charge par le serveur miroir configuré par l'utilisateur.

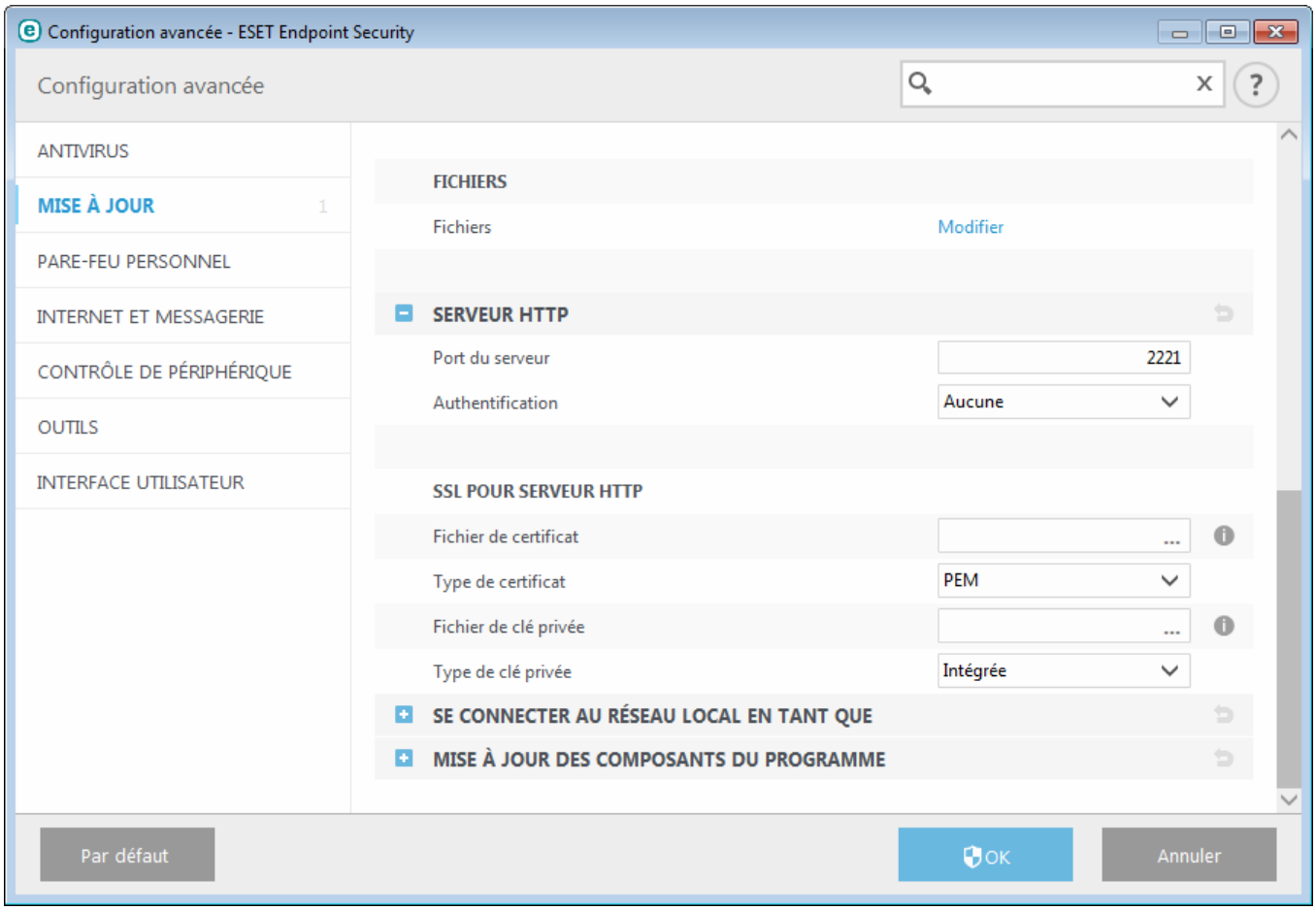
Serveur HTTP

Port du serveur : par défaut, le port su serveur est défini sur 2221.

Authentification : définit la méthode d'authentification utilisée pour accéder aux fichiers de mise à jour. Les options disponibles sont les suivantes : **Aucune**, **Général** et **NTLM**. Sélectionnez **Général** pour utiliser le codage base64 avec l'authentification de base du nom d'utilisateur et mot de passe. L'option **NTLM** fournit un codage utilisant une méthode de codage fiable. L'utilisateur créé sur le poste de travail partageant les fichiers de mise à jour est utilisé

pour l'authentification. L'option par défaut est **Aucune**. Elle autorise l'accès aux fichiers de mise à jour sans exiger d'authentification.

Ajoutez votre **Fichier de chaîne de certificat** ou générez un certificat signé automatiquement si vous souhaitez exécuter le serveur HTTP avec la prise en charge HTTPS (SSL). Les types de certificats suivants sont disponibles : ASN, PEM et PFX. Pour plus de sécurité, vous pouvez utiliser le protocole HTTPS pour télécharger les fichiers de mise à jour. Il est pratiquement impossible d'identifier des transferts de données et des informations de connexion lorsque ce protocole est utilisé. L'option **Type de clé privée** est définie sur **Intégrée** par défaut (ainsi, l'option **Fichier de clé privée** est désactivée par défaut), ce qui signifie que la clé privée fait partie du fichier de chaîne de certificat sélectionné.



Se connecter au réseau local comme

Type d'utilisateur local : les paramètres **Compte système (par défaut)**, **Utilisateur actuel** et **Utilisateur spécifié** s'affichent dans les menus déroulants correspondants. Les paramètres **Nom d'utilisateur** et **Mot de passe** sont facultatifs. Voir Se connecter au réseau local comme.

Sélectionnez **Déconnecter du serveur après la mise à jour** pour forcer une déconnexion si la connexion au serveur reste active, même après le téléchargement des mises à jour.

Mise à jour des composants du programme

Mettre à jour automatiquement les composants : permet l'installation de nouvelles fonctionnalités et de mises à jour des fonctionnalités existantes. Une mise à jour peut s'effectuer sans intervention de l'utilisateur ou après sa notification. Le redémarrage de l'ordinateur peut être nécessaire après la mise à jour des composants du programme.

Mettre à jour les composants maintenant : met à jour les composants du programme avec la nouvelle version.

3.8.5.1.6.1 Mise à jour à partir du miroir

Il existe deux méthodes de base pour configurer un miroir, qui consiste essentiellement en un référentiel dans lequel les clients peuvent télécharger les fichiers de mise à jour. Le dossier des fichiers de mise à jour peut être considéré comme un dossier réseau partagé ou un serveur HTTP.

Accès au miroir au moyen d'un serveur HTTP interne

Cette configuration est l'option par défaut ; elle est indiquée dans la configuration du programme prédéfinie. Pour permettre l'accès au miroir à l'aide du serveur HTTP, accédez à **Configuration avancée** >**Mise à jour** > **Miroir**, puis sélectionnez l'option **Créer un miroir de mise à jour**.

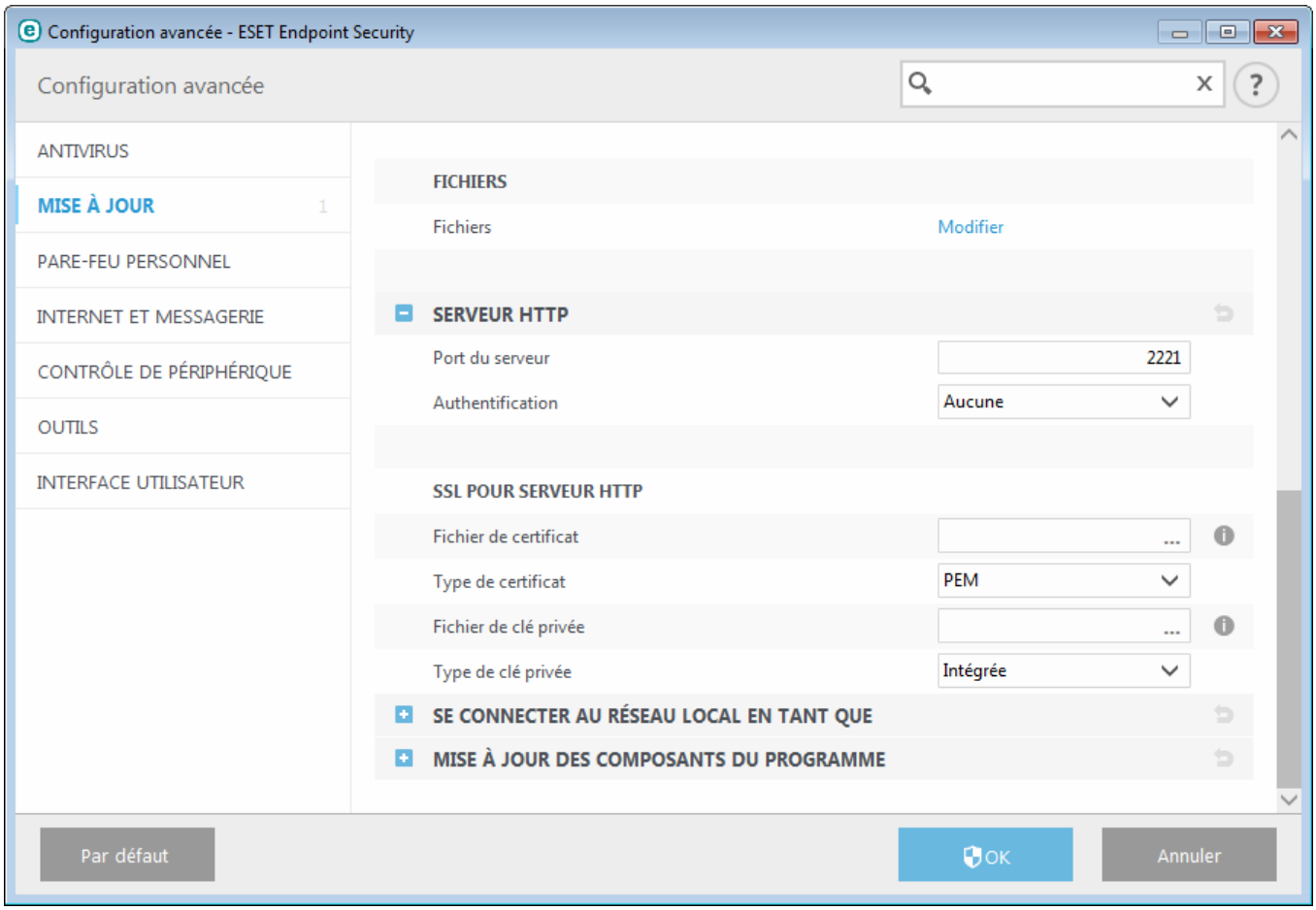
Dans la section **Serveur HTTP** de l'onglet **Miroir**, vous pouvez indiquer le **port du serveur** sur lequel le serveur HTTP écoute, ainsi que le type d'**authentification** utilisé par le serveur HTTP. Par défaut, cette option est configurée sur **2221**. L'option **Authentification** définit la méthode d'authentification utilisée pour accéder aux fichiers de mise à jour. Les options disponibles sont les suivantes : **Aucune**, **Général** et **NTLM**. Sélectionnez **Général** pour utiliser le codage base64 avec l'authentification de base du nom d'utilisateur et mot de passe. L'option **NTLM** fournit un codage utilisant une méthode de codage fiable. L'utilisateur créé sur le poste de travail partageant les fichiers de mise à jour est utilisé pour l'authentification. L'option par défaut est **Aucune**. Elle autorise l'accès aux fichiers des mises à jour sans exiger d'authentification.

Avertissement : l'accès aux fichiers des mises à jour au moyen du serveur HTTP exige que le dossier miroir soit sur le même ordinateur que l'instance ESET Endpoint Security qui l'a créé.

SSL pour serveur HTTP

Ajoutez votre **Fichier de chaîne de certificat** ou générez un certificat signé automatiquement si vous souhaitez exécuter le serveur HTTP avec la prise en charge HTTPS (SSL). Les types de certificats suivants sont disponibles : **PEM, PFX** et **ASN**. Pour plus de sécurité, vous pouvez utiliser le protocole HTTPS pour télécharger les fichiers de mise à jour. Il est pratiquement impossible d'identifier des transferts de données et des informations de connexion lorsque ce protocole est utilisé. **Type de clé privée** est défini sur **Intégrée** par défaut, ce qui signifie que la clé privée fait partie du fichier de chaîne de certificat sélectionné.

REMARQUE : L'erreur **Nom d'utilisateur et/ou mot de passe incorrects** s'affiche dans le volet Mise à jour du menu principal après plusieurs échecs de la mise à jour de la base des signatures de virus à partir du miroir. Il est conseillé d'accéder à **Configuration avancée** > **Mise à jour** > **Miroir** pour vérifier le nom d'utilisateur et le mot de passe. La saisie de données d'authentification incorrectes est raison la plus courante de cette erreur.



Une fois le serveur miroir configuré, vous devez ajouter le nouveau serveur de mise à jour sur les postes de travail clients. Pour ce faire, procédez comme suit :

- Accédez à **Configuration avancée** (F5), puis cliquez sur **Mise à jour** > **Général**.
- Désactivez l'option **Choisir automatiquement**, puis ajoutez un nouveau serveur dans le champ **Serveur de mise à jour** dans l'un des formats suivants :
  http://adresse_IP_de_votre_serveur:2221
  https://adresse_IP_de_votre_serveur:2221 (si vous utilisez SSL)

Accès au miroir via le partage des systèmes

Un dossier partagé doit d'abord être créé sur un lecteur local ou réseau. Lors de la création du dossier pour le miroir, il est nécessaire d'octroyer le droit d'*écriture* à l'utilisateur qui va sauvegarder les fichiers de mise à jour dans le dossier et le droit de *lecture* aux utilisateurs qui vont utiliser le dossier miroir pour la mise à jour de ESET Endpoint Security.

Configurez ensuite l'accès au miroir dans l'onglet **Configuration avancée** > **Mise à jour** > **Miroir** en désactivant l'option **Fournir les fichiers de mise à jour via un serveur HTTP interne**. Cette option est activée par défaut lors de l'installation du programme.

Si le dossier partagé se trouve sur un autre ordinateur du réseau, une authentification est nécessaire pour accéder à l'autre ordinateur. Pour entrer les données d'authentification, ouvrez la **Configuration avancée** (F5) de ESET Endpoint Security et cliquez sur **Mise à jour** > **Se connecter au réseau local comme**. Il s'agit du même paramètre utilisé pour la mise à jour, comme l'indique la section Se connecter au réseau local comme.

Une fois la configuration du miroir terminée, définissez sur les postes de travail clients *\\UNC\CHEMIN* comme serveur de mise à jour en procédant comme suit :

1. Ouvrez la **Configuration avancée** de ESET Endpoint Security et cliquez sur **Mise à jour** > **Général**.
2. Cliquez sur le champ **Serveur de mise à jour** et ajoutez un nouveau serveur à l'aide du format *\\UNC\CHEMIN*.

REMARQUE : pour que les mises à jour fonctionnent correctement, le chemin du dossier miroir doit être spécifié comme un chemin UNC. Les mises à jour à partir de lecteurs mappés peuvent ne pas fonctionner.

La dernière section contrôle les composants du programme. Par défaut, les composants de programme téléchargés sont préparés pour copie sur le miroir local. Si l'option **Mettre à jour les composants du programme** est activée, il n'est pas nécessaire de cliquer sur **Mettre à jour** puisque les fichiers sont copiés automatiquement sur le miroir local lorsqu'ils sont disponibles. Voir Mode de mise à jour pour plus d'informations sur les mises à jour des composants du programme.

3.8.5.1.6.2 Dépannage des problèmes de miroir de mise à jour

Dans la plupart des cas, les problèmes de mise à jour depuis un serveur miroir proviennent des raisons suivantes : mauvaise spécification des options du dossier miroir, données d'authentification incorrectes pour l'accès au dossier miroir, mauvaise configuration des postes de travail qui cherchent à télécharger des fichiers de mise à jour du miroir ou combinaison des raisons citées précédemment. Nous donnons ici un aperçu des problèmes les plus fréquents qui peuvent se produire lors d'une mise à jour depuis le miroir :

ESET Endpoint Security signale une erreur de connexion au serveur miroir - probablement causée par une spécification incorrecte du serveur de mise à jour (chemin réseau du dossier miroir) à partir duquel les postes de travail locaux téléchargent les mises à jour. Pour vérifier le dossier, cliquez sur le menu **Démarrer** de Windows, puis sur **Exécuter**, entrez le nom du dossier et cliquez sur **OK**. Le contenu du dossier doit s'afficher.

ESET Endpoint Security exige un nom d'utilisateur et un mot de passe : l'erreur est probablement causée par l'entrée dans la section mise à jour de données d'authentification incorrectes (Nom d'utilisateur et Mot de passe). Le nom d'utilisateur et le mot de passe donnent accès au serveur de mise à jour, à partir duquel le programme se télécharge. Assurez-vous que les données d'authentification sont correctes et entrées dans le bon format. Par exemple, *Domaine/Nom d'utilisateur* ou *Groupe de travail/Nom d'utilisateur*, en plus des mots de passe correspondants. Si le serveur miroir est accessible à Tous, cela ne veut pas dire que tout utilisateur est autorisé à y accéder. « Tous » ne veut pas dire tout utilisateur non autorisé, cela veut tout simplement dire que le dossier est accessible à tous les utilisateurs du domaine. Par conséquent, si le dossier est accessible à Tous, un nom d'utilisateur du domaine et un mot de passe sont toujours nécessaires et doivent être entrés dans la configuration des mises à jour.

ESET Endpoint Security signale une erreur de connexion au serveur miroir – le port de communication défini pour l'accès au miroir via HTTP est bloqué.

3.8.5.2 Comment créer des tâches de mise à jour

Vous pouvez déclencher les mises à jour manuellement en cliquant sur **Mise à jour la base des signatures de virus** dans la fenêtre principale qui s'affiche lorsque vous cliquez sur **Mise à jour** dans le menu principal.

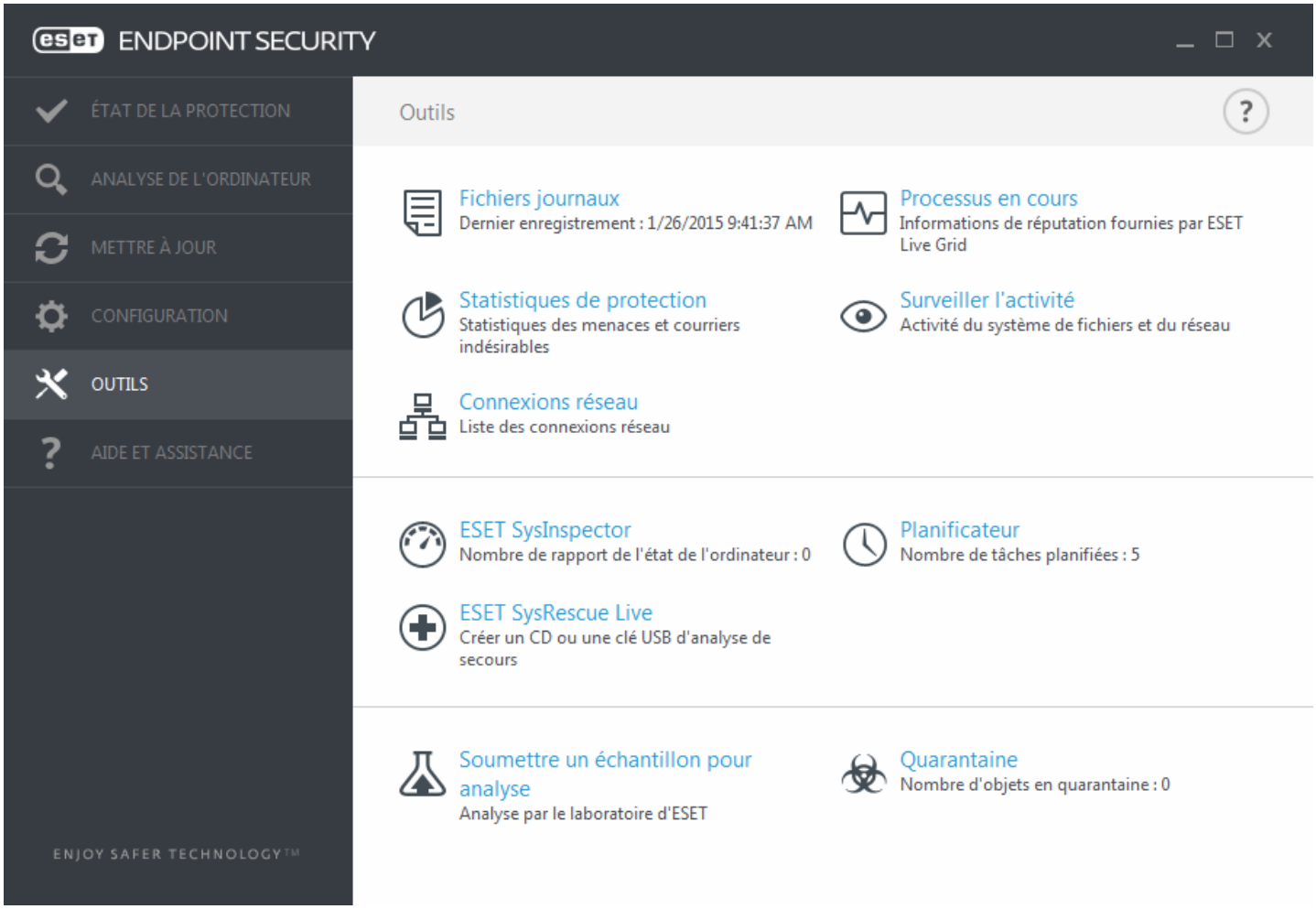
Les mises à jour peuvent également être exécutées sous forme de tâches planifiées. Pour configurer une tâche planifiée, cliquez sur **Outils** > **Planificateur**. Par défaut, les tâches suivantes sont activées dans ESET Endpoint Security :

- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion commutée**
- **Mise à jour automatique après ouverture de session utilisateur**

Chaque tâche de mise à jour peut être modifiée selon les besoins de l'utilisateur. Outre les tâches de mise à jour par défaut, vous pouvez en créer des nouvelles avec vos propres paramètres. Pour plus d'informations sur la création et la configuration des tâches de mise à jour, reportez-vous à Planificateur.

3.8.6 Outils

Le menu **Outils** comprend des modules qui contribuent à simplifier l'administration du programme et offrent des options supplémentaires aux utilisateurs expérimentés.



Ce menu comprend les éléments suivants :

- Fichiers journaux
- Statistiques de protection
- Surveiller l'activité
- Processus en cours d'exécution (si ESET Live Grid est activé dans ESET Endpoint Security)
- Planificateur
- Quarantaine
- Connexions réseau (si le est activé dans ESET Endpoint Security)
- ESET SysInspector

Soumettre un échantillon pour analyse : permet de soumettre un fichier suspect pour analyse aux laboratoires d'ESET. La boîte de dialogue qui s'affiche lorsque vous cliquez sur cette option est décrite dans la section Soumission d'échantillons pour analyse.

ESET SysRescue : vous redirige vers la page ESET SysRescue Live à partir de laquelle vous pouvez télécharger l'image d'ESET SysRescue Live ou Live CD/USB Creator pour les systèmes d'exploitation Microsoft Windows.

3.8.6.1 Fichiers journaux

Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées. Les journaux constituent un outil puissant pour l'analyse système, la détection de menaces et le dépannage. La consignation est toujours active en arrière-plan sans interaction de l'utilisateur. Les informations sont enregistrées en fonction des paramètres de détail actifs. Il est possible de consulter les messages texte et les journaux directement à partir de l'environnement ESET Endpoint Security. Il est aussi possible d'archiver les fichiers journaux.

Vous pouvez accéder aux fichiers journaux depuis la fenêtre principale du programme en cliquant sur **Outils** > **Fichiers journaux**. Sélectionnez le type de journal à partir du menu déroulant **Journaliser**. Les journaux suivants sont disponibles :

- **Menaces détectées** - Le journal des menaces contient des informations sur les infiltrations détectées par les modules ESET Endpoint Security. Ces informations comprennent l'heure de détection, le nom de l'infiltration, l'emplacement, l'action exécutée et le nom de l'utilisateur connecté au moment où l'infiltration a été détectée. Double-cliquez sur une entrée du journal pour afficher son contenu dans une fenêtre distincte.
- **Événements** - Toutes les actions importantes exécutées par ESET Endpoint Security sont enregistrées dans le journal des événements. Le journal des événements contient des informations sur les événements qui se sont produits dans le programme. Il permet aux administrateurs système et aux utilisateurs de résoudre des problèmes. Les informations qu'il contient peuvent aider à trouver une solution à un problème qui s'est produit dans le programme.
- **Analyse de l'ordinateur** - Tous les résultats des analyses sont affichés dans cette fenêtre. Chaque ligne correspond à un seul contrôle d'ordinateur. Double-cliquez sur une entrée pour afficher les détails de l'analyse correspondante.
- **HIPS** - Contient des entrées de règles spécifiques qui sont marquées pour enregistrement. Le protocole affiche l'application qui a appelé l'opération, le résultat (si la règle a été autorisée ou bloquée), ainsi que le nom de la règle créée.
- **Pare-feu personnel** - Le journal du pare-feu contient toutes les attaques distantes détectées par le pare-feu personnel. Il comprend des renseignements sur les attaques subies par votre ordinateur. La colonne *Événement* répertorie les attaques détectées. La colonne *Source* fournit des informations sur l'attaquant. La colonne *Protocole* indique le protocole de communication utilisé pour l'attaque. L'analyse du journal de pare-feu permet de détecter à temps les tentatives d'infiltration du système et d'éviter tout accès non autorisé à votre système. Pour plus de détails sur des attaques réseau spécifiques, voir Options IDS avancées.
- **Sites Web filtrés** - Cette liste est utile pour afficher la liste des sites Web bloqués par la protection de l'accès Web ou le filtrage Internet. Ces journaux permettent de voir l'heure, l'URL, l'utilisateur et l'application ayant ouvert une connexion au site Web en question.
- **Protection antispam** - Contient des entrées relatives aux messages marqués comme spam.
- **Filtrage Internet** - Affiche les adresses URL bloquées ou autorisées et les détails sur leurs catégories. La colonne *Action effectuée* indique comment les règles de filtrage ont été appliquées.
- **Contrôle de périphérique** - Contient des enregistrements des supports amovibles ou périphériques qui ont été connectés à l'ordinateur. Seuls les périphériques auxquels correspond une règle de contrôle de périphérique seront enregistrés dans le fichier journal. Si la règle ne correspond pas à un périphérique connecté, aucune entrée de journal ne sera créée pour un périphérique connecté. Des détails figurent également tels que le type de périphérique, le numéro de série, le nom du fournisseur et la taille du support (le cas échéant).

Dans chaque section, vous pouvez copier les informations affichées dans le Presse-papiers (à l'aide du raccourci clavier **Ctrl + C**) en sélectionnant l'entrée souhaitée, puis en cliquant sur **Copier**. Pour sélectionner plusieurs entrées, vous pouvez utiliser les touches **Ctrl** et **Maj**.

Cliquez sur **Filtrage** pour ouvrir la fenêtre **Filtrage des journaux** dans laquelle vous pouvez définir les critères de filtrage.

Vous pouvez afficher le menu contextuel d'une entrée en cliquant avec le bouton droit sur celle-ci. Le menu contextuel permet d'accéder aux options suivantes :

- **Afficher** - Affiche des détails supplémentaires sur le journal sélectionné dans une nouvelle fenêtre.
- **Filtrer les enregistrements identiques** - Si vous activez ce filtre, vous voyez uniquement les enregistrements du même type (diagnostics, avertissement, etc.).
- **Filtrer.../Rechercher...** - Après avoir cliqué sur cette option, la fenêtre Rechercher dans le journal permet de définir des critères de filtrage pour des entrées de journal spécifiques.
- **Activer le filtre** - Active les paramètres du filtre.
- **Désactiver le filtre** - Supprime tous les paramètres du filtre (comme décrit ci-dessus).
- **Copier/Copier tout** - Copie des informations sur toutes les entrées de la fenêtre.
- **Supprimer/Supprimer tout** - Supprime les entrées sélectionnées ou toutes les entrées affichées. Vous devez disposer des privilèges d'administrateur pour effectuer cette action.
- **Exporter...** - Exporte les informations sur les entrées au format XML.
- **Dérouler le journal** - Laissez cette option activée pour que les anciens journaux défilent automatiquement et pour consulter les journaux actifs dans la fenêtre **Fichiers journaux**.

3.8.6.1.1 Rechercher dans le journal

Les journaux stockent des informations relatives aux événements importants du système. La fonction de filtrage des journaux permet d'afficher les enregistrements propres à un événement en particulier.

Saisissez le mot-clé de recherche dans le champ **Rechercher le texte**. Si vous souhaitez rechercher le mot-clé dans certaines colonnes, changez le filtre dans le menu déroulant **Rechercher dans les colonnes**.

Types d'enregistrements - Choisissez un ou plusieurs types de journal dans le menu déroulant :

- **Diagnostic** - Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** - Enregistre tous les messages d'information, y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissements** - Enregistre les erreurs critiques et les messages d'avertissement.
- **Erreurs** - Enregistre les erreurs du type « Erreur de téléchargement du fichier » et les erreurs critiques.
- **Critique** - Consigne uniquement les erreurs critiques (erreur de démarrage de la protection antivirus, pare-feu intégré, etc...).

Période - Définissez la période pour laquelle vous souhaitez afficher les résultats.

Mot entier - Cochez cette case si vous souhaitez rechercher des mots complets afin d'obtenir des résultats plus précis.

Respecter la casse - Activez cette option s'il est important d'utiliser des majuscules et des minuscules lors du filtrage.

Vers le haut - Les résultats de la recherche qui apparaissent plus haut dans le document sont affichés en premier.

3.8.6.2 Configuration du serveur proxy

Dans les grands réseaux locaux, les communications entre votre ordinateur et Internet peuvent s'effectuer par l'intermédiaire d'un serveur proxy. Lorsque cette configuration est utilisée, les paramètres suivants doivent être définis. Dans le cas contraire, le programme ne pourra pas se mise à jour automatiquement. Dans ESET Endpoint Security, il est possible de configurer le serveur proxy à partir de deux sections différentes de la configuration avancée complète.

Tout d'abord, les paramètres de serveur proxy peuvent être configurés dans **Configuration avancée**, depuis **Outils** > **Serveur proxy**. La spécification du serveur proxy à ce niveau définit les paramètres de serveur proxy globaux pour l'intégralité d'ESET Endpoint Security. Les paramètres définis ici seront utilisés par tous les modules qui requièrent une connexion à Internet.

Pour spécifier des paramètres de serveur proxy à ce niveau, sélectionnez **Utiliser un serveur proxy**, puis entrez l'adresse du serveur proxy dans le champ **Serveur proxy**, ainsi que le numéro de **port** de ce serveur proxy.

Si les communications avec le serveur proxy exigent une authentification, sélectionnez **Le serveur proxy nécessite une authentification** et entrez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants. Cliquez sur **Détecter** pour détecter et renseigner automatiquement les paramètres du serveur proxy. Les paramètres indiqués dans Internet Explorer sont copiés.

REMARQUE : vous devez saisir manuellement votre nom d'utilisateur et votre mot de passe dans les paramètres **Serveur proxy**.

Les paramètres de serveur proxy peuvent également définis dans la configuration avancée des mises à jour (**Configuration avancée** > **Mise à jour** > **Proxy HTTP** en sélectionnant **Connexion via un serveur proxy** dans le menu déroulant **Mode proxy**). Ce paramètre s'applique au profil de mise à jour donné et est recommandé pour les ordinateurs portables, car il permet de recevoir les mises à jour de la base des signatures de virus depuis des emplacements distants. Pour plus d'informations sur ce paramètre, consultez Configuration avancée des mises à jour.

3.8.6.3 Planificateur

Le planificateur gère et lance les tâches planifiées qui ont été préalablement définies et configurées.

Le planificateur est accessible depuis la fenêtre principale de ESET Endpoint Security, dans **Outils** > **Planificateur**. Le **planificateur** contient la liste de toutes les tâches planifiées, des propriétés de configuration telles que la date et l'heure prédéfinies, ainsi que le profil d'analyse utilisé.

Il sert à planifier les tâches suivantes : la mise à jour de la base des signatures de virus, l'analyse, le contrôle des fichiers de démarrage du système et la maintenance des journaux. Vous pouvez ajouter ou supprimer des tâches dans la fenêtre principale du planificateur (cliquez sur **Ajouter une tâche** ou **Supprimer** dans la partie inférieure). Cliquez avec le bouton droit dans la fenêtre du planificateur pour effectuer les actions suivantes : afficher des informations détaillées, exécuter la tâche immédiatement, ajouter une nouvelle tâche et supprimer une tâche existante. Utilisez les cases à cocher au début de chaque entrée pour activer/désactiver les tâches.

Par défaut, les tâches planifiées suivantes sont affichées dans le **planificateur** :

- **Maintenance des journaux**
- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion commutée**
- **Mise à jour automatique après ouverture de session utilisateur**
- **Vérification des fichiers de démarrage** (après l'ouverture de session de l'utilisateur)
- **Vérification automatique des fichiers de démarrage** (après la réussite de la mise à jour de la base des signatures de virus)
- **Première analyse automatique**

Pour modifier la configuration d'une tâche planifiée existante (par défaut ou définie par l'utilisateur), cliquez avec le bouton droit sur la tâche et cliquez sur **Modifier...**. Vous pouvez également sélectionner la tâche à modifier et cliquer sur le bouton **Modifier**.

Ajout d'une nouvelle tâche

1. Cliquez sur **Ajouter une tâche** dans la partie inférieure de la fenêtre.
2. Entrez le nom de la tâche.

3. Sélectionnez la tâche souhaitée dans le menu déroulant :

- **Exécuter une application externe** - Permet de programmer l'exécution d'une application externe.
- **Maintenance des journaux** - Les fichiers journaux contiennent également des éléments provenant d'enregistrements supprimés. Cette tâche optimise régulièrement les entrées des fichiers journaux pour garantir leur efficacité.
- **Contrôle des fichiers de démarrage du système** - Vérifie les fichiers autorisés à s'exécuter au démarrage du système ou lors de l'ouverture de session de l'utilisateur.
- **Analyse de l'ordinateur** - Crée un instantané ESET SysInspector de l'ordinateur et collecte des informations détaillées sur les composants système (pilotes, applications) et évalue le niveau de risque de chacun de ces composants.
- **Analyse de l'ordinateur à la demande** : effectue une analyse des fichiers et des dossiers de votre ordinateur.
- **Première analyse** - par défaut, 20 minutes après une installation ou un redémarrage, une analyse de l'ordinateur sera effectuée en tant que tâche de faible priorité.
- **Mise à jour** - Planifie une tâche de mise à jour en mettant à jour la base des signatures de virus et les modules de l'application.

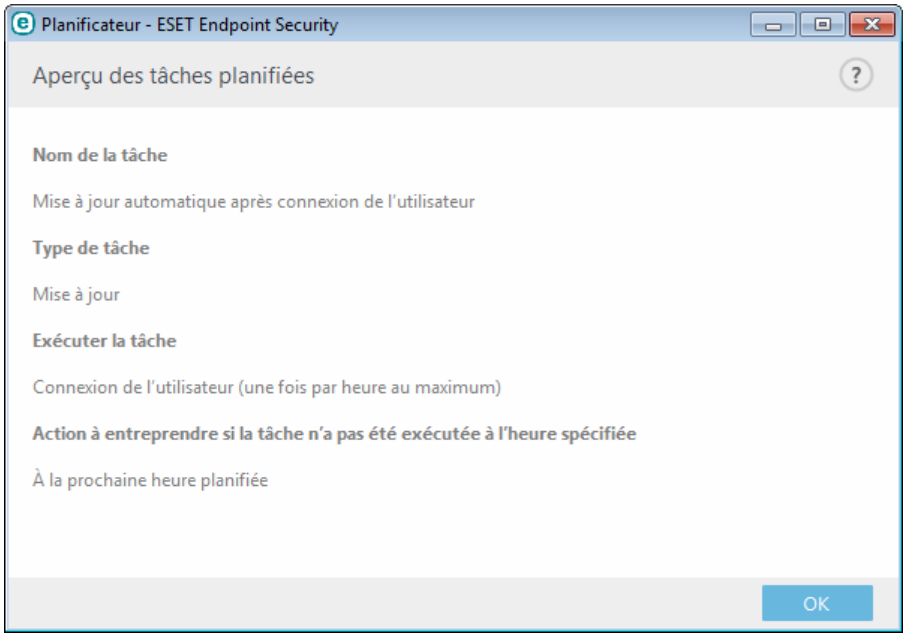
4. Activez le bouton bascule **Activé** si vous souhaitez activer la tâche (vous pouvez le faire ultérieurement en activant/désactivant la case à cocher correspondante dans la liste des tâches planifiées). Cliquez ensuite sur **Suivant** et sélectionnez une des options de planification :

- **Une fois** - La tâche est exécutée à la date et à l'heure prédéfinies.
- **Plusieurs fois** - La tâche est exécutée aux intervalles indiqués.
- **Quotidiennement** - La tâche est exécutée tous les jours à l'heure définie.
- **Chaque semaine** - La tâche est exécutée à l'heure et au jour prédéfinis.
- **Déclenchée par un événement** - La tâche est exécutée après un événement particulier.

5. Sélectionnez **Ignorer la tâche en cas d'alimentation par batterie** pour diminuer les ressources système lorsque l'ordinateur portable fonctionne sur batterie. Cette tâche est exécutée à l'heure et au jour spécifiées dans les champs **Exécution de tâche**. Si la tâche n'a pas pu être exécutée au moment défini, vous pouvez désigner le moment auquel elle doit être réexécutée :

- **À la prochaine heure planifiée**
- **Dès que possible**
- **Immédiatement, si la durée écoulée depuis la dernière exécution dépasse la valeur spécifiée** (l'intervalle peut être spécifié dans la zone de liste déroulante **Durée écoulée depuis la dernière exécution**.)

Pour examiner une tâche planifiée, cliquez sur **Afficher les détails des tâches**.



3.8.6.4 Statistiques de protection

Pour afficher un graphique des données statistiques relatives aux modules de protection d'ESET Endpoint Security, cliquez sur **Outils** > **Statistiques**. Dans le menu déroulant **Statistiques**, sélectionnez le module de protection souhaité pour afficher le graphique et la légende correspondants. Si vous faites glisser le pointeur de la souris sur un élément de la légende, seules les données correspondant à cet élément sont représentées dans le graphique.

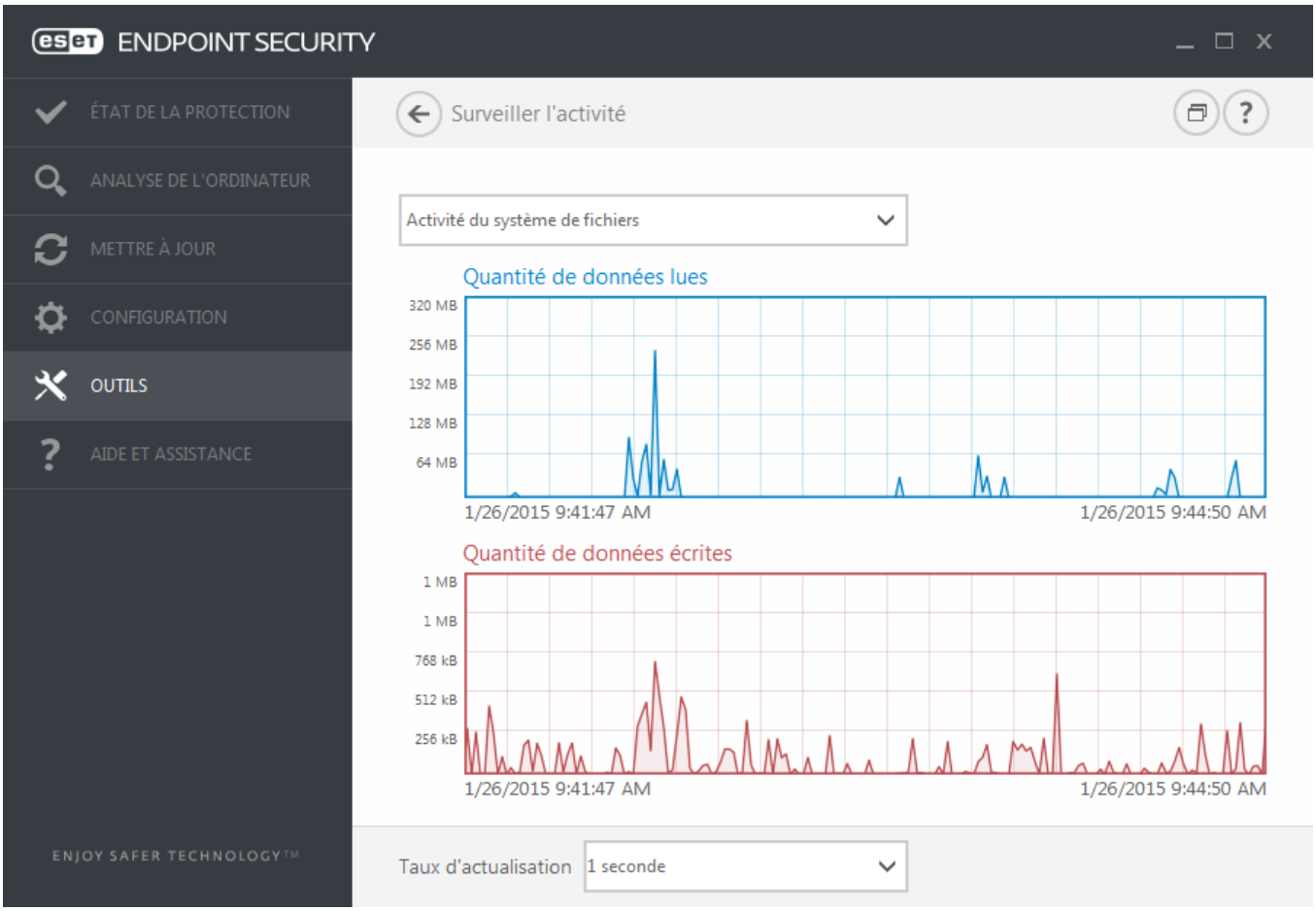
Les graphiques statistiques suivants sont disponibles :

- **Protection antivirus et antispyware** - Affiche le nombre d'objets infectés et nettoyés.
- **Protection du système de fichiers** - Affiche uniquement les objets lus ou écrits dans le système de fichiers.
- **Protection du client de messagerie** - Affiche uniquement les objets envoyés ou reçus par les clients de messagerie.
- **Protection de l'accès au Web et antihameçonnage** - Affiche uniquement les objets téléchargés par des navigateurs Web.
- **Protection antispam du client messagerie** - Affiche l'historique des statistiques de blocage du courrier indésirable depuis le dernier démarrage.

À côté des graphiques statistiques, vous pouvez voir le nombre total d'objets analysés, le nombre d'objets infectés, le nombre d'objets nettoyés et le nombre d'objets propres. Cliquez sur **Réinitialiser** pour effacer les informations de statistiques. Pour effacer et supprimer toutes les données existantes, cliquez sur **Tout réinitialiser**.

3.8.6.5 Surveiller l'activité

Pour voir l'**activité actuelle du système de fichiers** sous forme graphique, cliquez sur **Outils** > **Surveiller l'activité**. Au bas du graphique figure une chronologie qui enregistre en temps réel l'activité du système de fichiers sur la base de l'intervalle sélectionné. Pour modifier l'intervalle, effectuez une sélection dans le menu déroulant **Taux d'actualisation**.



Les options disponibles sont les suivantes :

- **Pas : 1 seconde** - Le graphique est actualisé toutes les secondes et la chronologie couvre les 10 dernières minutes.
- **Pas : 1 minute (24 dernières heures)** - Le graphique est actualisé toutes les secondes et la chronologie couvre les 24 dernières heures.
- **Pas : 1 heure (dernier mois)** - Le graphique est actualisé toutes les heures et la chronologie couvre le dernier mois.
- **Pas : 1 heure (mois sélectionné)** - Le graphique est actualisé toutes les heures et la chronologie couvre les X mois sélectionnés.

L'axe vertical du **Graphique d'activité du système de fichiers** représente les données lues (en bleu) et les données écrites (en rouge). Les deux valeurs sont exprimées en Ko (kilo-octets)/Mo/Go. Si vous faites glisser le curseur de la souris sur les données lues ou écrites dans la légende sous le graphique, celui-ci n'affiche que les données relatives à ce type d'activité.

Vous pouvez également sélectionner **Activité réseau** dans le menu déroulant. L'affichage et les options du graphique pour l'**activité du système de fichiers** et l'**activité du réseau** sont identiques, à la différence près que, pour cette dernière, la quantité de données reçues (en rouge) et envoyées (en bleu) sont présentées.

3.8.6.6 ESET SysInspector

ESET SysInspector est une application qui inspecte méticuleusement votre ordinateur, réunit des informations détaillées sur les composants système, tels que pilotes et applications, connexions réseau ou entrées de registre importantes, puis évalue le niveau de risque de chaque composant. Ces informations peuvent aider à déterminer la cause d'un comportement suspect du système pouvant être dû à une incompatibilité logicielle ou matérielle, ou à une infection par un logiciel malveillant.

La fenêtre SysInspector affiche les informations suivantes relatives aux journaux créés :

- **Heure** - Heure de création du journal.
- **Commentaire** - Bref commentaire.
- **Utilisateur** - Nom de l'utilisateur qui a créé le journal.
- **État** - État de création du journal.

Les actions disponibles sont les suivantes :

- **Ouvrir** - Ouvre le journal créé. Vous pouvez également cliquer avec le bouton droit sur un fichier journal, puis sélectionner **Afficher** dans le menu contextuel.
- **Comparer** - Compare deux journaux existants.
- **Créer...** - Crée un journal. Patientez jusqu'à ce qu'ESET SysInspector ait terminé (l'état du journal s'affiche en tant que créé) avant d'accéder au journal.
- **Supprimer** - Supprime les journaux sélectionnés de la liste.

Les options suivantes sont disponibles dans le menu contextuel lorsqu'un fichier journal ou plusieurs fichiers journaux sont sélectionnés :

- **Afficher** - Ouvre le journal sélectionné dans ESET SysInspector (équivaut à double-cliquer sur un journal).
- **Comparer** - Compare deux journaux existants.
- **Créer...** - Crée un journal. Patientez jusqu'à ce qu'ESET SysInspector ait terminé (l'état du journal s'affiche en tant que créé) avant d'accéder au journal.
- **Supprimer tout** - Supprime tous les journaux.
- **Exporter...** - Exporte le journal dans un fichier *.xml* ou un fichier *.xml* compressé.

3.8.6.7 ESET Live Grid

ESET Live Grid est un système avancé d'avertissement anticipé constitué de plusieurs technologies de cloud. Il contribue à la détection des nouvelles menaces en s'appuyant sur l'évaluation de la réputation et améliore les performances d'analyse par la mise en liste blanche. Les informations sur les nouvelles menaces sont envoyées en continu dans le cloud, ce qui permet aux laboratoires d'ESET de lutte contre les logiciels malveillants d'assurer en permanence une protection à jour et constante. Les utilisateurs peuvent s'informer de la réputation des processus et des fichiers en cours d'exécution depuis l'interface du programme ou à partir d'un menu contextuel comprenant des informations supplémentaires mises à disposition par ESET Live Grid. Lors de l'installation d'ESET Endpoint Security, sélectionnez l'une des options suivantes :

1. Vous pouvez décider de ne pas activer ESET Live Grid. Le logiciel ne perd aucune fonctionnalité, mais ESET Endpoint Security peut répondre dans certains cas plus lentement aux nouvelles menaces que la mise à jour de la base des signatures de virus.
2. Vous pouvez configurer ESET Live Grid afin d'envoyer des informations anonymes qui concernent les nouvelles menaces et indiquent l'endroit où a été détecté le code dangereux. Ce fichier peut être envoyé à ESET pour une analyse détaillée. En étudiant ces menaces, ESET améliore ses capacités à détecter les menaces.

Le système ESET Live Grid collecte sur votre ordinateur des informations concernant les nouvelles menaces détectées. Ces informations comprennent un échantillon ou une copie du fichier dans lequel la menace est apparue, le chemin et le nom du fichier, la date et l'heure, le processus par lequel la menace est apparue sur votre ordinateur et des informations sur le système d'exploitation de votre ordinateur.

Par défaut, ESET Endpoint Security est configuré pour soumettre les fichiers suspects au laboratoire d'ESET pour une analyse détaillée. Les fichiers ayant une extension définie (*.doc* ou *.xls* par exemple) sont toujours exclus. Vous pouvez également ajouter d'autres extensions si vous ou votre entreprise souhaitez éviter d'envoyer certains fichiers.

Le système de réputation ESET Live Grid permet la mise en liste blanche ou noire dans le cloud. Pour accéder aux paramètres d'ESET Live Grid, appuyez sur **F5** pour passer à la configuration avancée, puis développez **Outils** > **ESET Live Grid**.

Activer le système de réputation ESET Live Grid (recommandé) - Le système de réputation ESET Live Grid améliore l'efficacité des solutions de protection contre les logiciels malveillants en comparant les fichiers analysés à une base de données d'éléments mis en liste blanche et noire dans le cloud.

Soumettre des statistiques anonymes - permet à ESET de collecter des informations sur les nouvelles menaces détectées telles que le nom de la menace, la date et l'heure de détection, la méthode de détection et les métadonnées associées, la version du produit et la configuration (informations sur votre système).

Soumettre les fichiers - Les fichiers suspects ressemblant à des menaces et/ou des fichiers aux caractéristiques ou au comportement inhabituels peuvent être envoyés pour analyse à ESET.

Sélectionnez **Activer la journalisation** pour créer un journal d'événements permettant d'enregistrer les soumissions des fichiers et des informations statistiques. Il permettra de consigner les fichiers ou statistiques envoyés dans le Journal des événements.

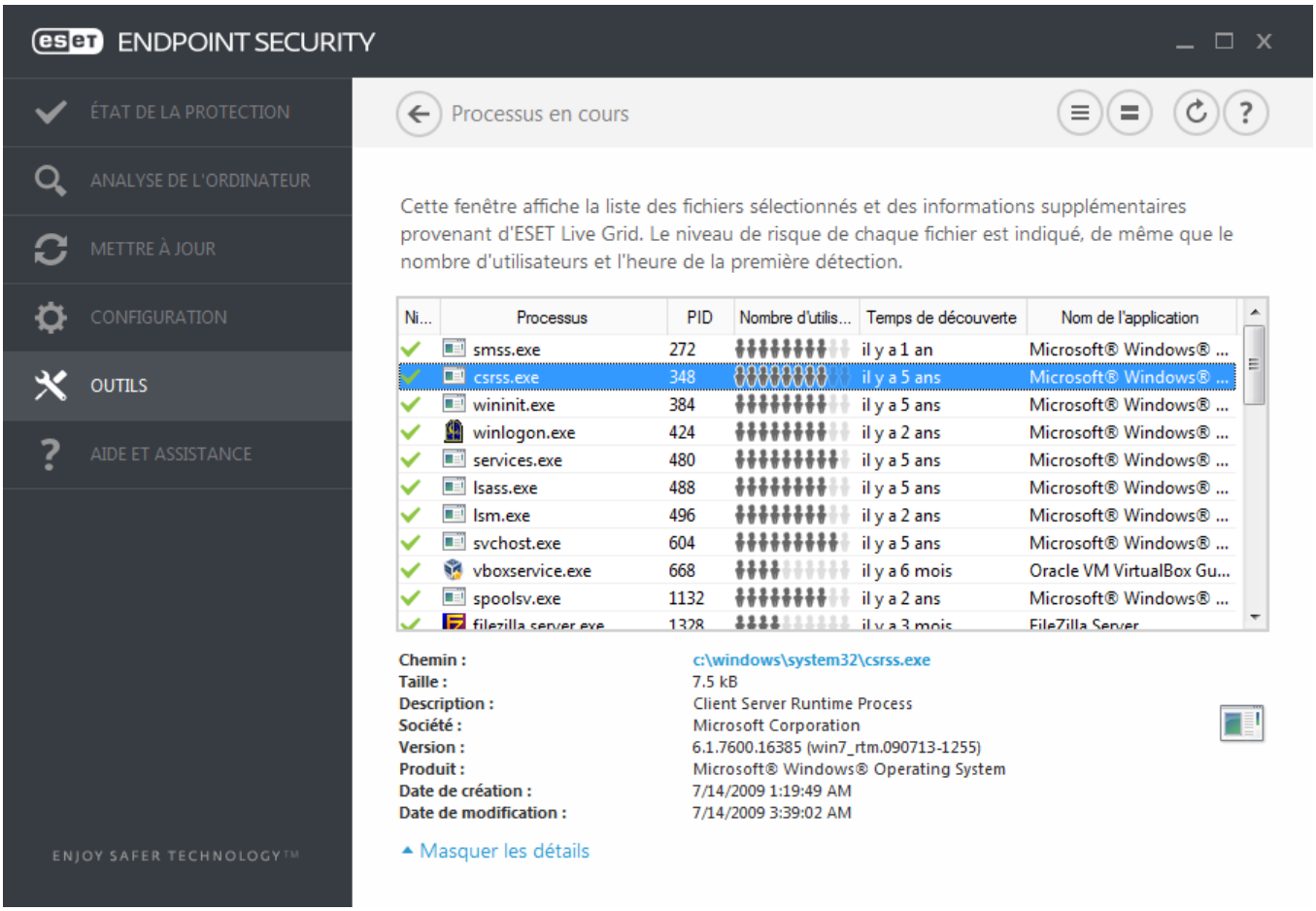
Adresse électronique de contact (facultatif) - Votre adresse électronique peut être incluse avec les fichiers suspects. Nous pourrons l'utiliser pour vous contacter si des informations complémentaires sont nécessaires pour l'analyse. Notez que vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires s'avèrent nécessaires.

Exclusion - Le filtre Exclusion permet d'exclure certains fichiers/dossiers de la soumission (par exemple, il peut être utile d'exclure des fichiers qui peuvent comporter des informations confidentielles, telles que des documents ou des feuilles de calcul). Les fichiers de la liste ne seront jamais envoyés aux laboratoires d'ESET pour analyse, même s'ils contiennent un code suspect. Les fichiers les plus ordinaires sont exclus par défaut (.doc, etc.). Vous pouvez ajouter des fichiers à la liste des fichiers exclus si vous le souhaitez.

Si vous avez déjà utilisé le système ESET Live Grid et l'avez désactivé, il est possible qu'il reste des paquets de données à envoyer. Même après la désactivation, ces paquets sont envoyés à ESET. Une fois toutes les informations actuelles envoyées, plus aucun paquet ne sera créé.

3.8.6.8 Processus en cours

Les processus en cours affichent les programmes ou processus en cours d'exécution sur votre ordinateur et informe ESET immédiatement et en permanence de l'existence de nouvelles infiltrations. ESET Endpoint Security fournit des informations détaillées sur l'exécution des processus afin de protéger les utilisateurs à l'aide de la technologie ESET Live Grid.



Niveau de risque - Dans la majorité des cas, ESET Endpoint Security et la technologie ESET Live Grid attribuent des niveaux de risque aux objets (fichiers, processus, clés de registre, etc.) sur la base d'une série de règles heuristiques qui examinent les caractéristiques de chaque objet, puis qui évaluent le potentiel d'activité malveillante. Cette analyse heuristique attribue aux objets un niveau de risque allant de 1 - OK (vert) à 9 - Risqué (rouge).

Processus - Nom de l'image du programme ou du processus en cours d'exécution sur l'ordinateur. Vous pouvez également utiliser le Gestionnaire de tâches pour afficher tous les processus en cours d'exécution sur votre ordinateur. Vous pouvez ouvrir le Gestionnaire de tâches en cliquant avec le bouton droit de la souris sur une zone vide de la barre des tâches, puis en cliquant sur Gestionnaire de tâches ou en appuyant sur les touches **Ctrl**+**Maj** +**Échap** du clavier.

PID - ID des processus en cours d'exécution dans les systèmes d'exploitation Windows.

REMARQUE : les applications connues marquées OK (vert) sont saines (répertoriées dans la liste blanche) et sont exclues de l'analyse, ce qui améliore la vitesse de l'analyse d'ordinateur à la demande ou de la protection du système en temps réel sur votre ordinateur.

Nombre d'utilisateurs - Nombre d'utilisateurs utilisant une application donnée. Ces informations sont collectées par la technologie ESET Live Grid.

Temps de découverte - Durée écoulée depuis la détection de l'application par la technologie ESET Live Grid.

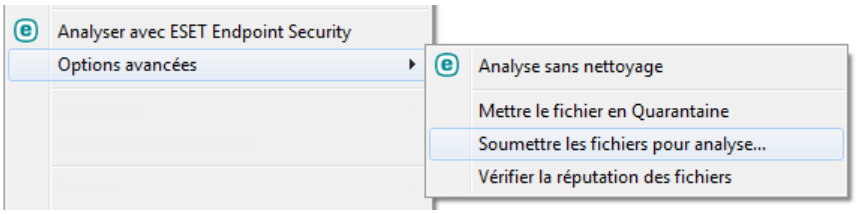
Remarque : Une application marquée avec le niveau de sécurité Inconnu (orange) n'est pas nécessairement un logiciel malveillant. Il s'agit généralement d'une nouvelle application. Vous pouvez soumettre un fichier pour analyse au laboratoire ESET si ce fichier vous semble suspect. Si le fichier s'avère être une application malveillante, sa détection sera ajoutée à l'une des prochaines mises à jour de la base des signatures de virus.

Nom de l'application - Nom d'un programme ou d'un processus.

Lorsque vous cliquez sur une application située au bas de la fenêtre, les informations suivantes apparaissent dans la partie inférieure de la fenêtre :

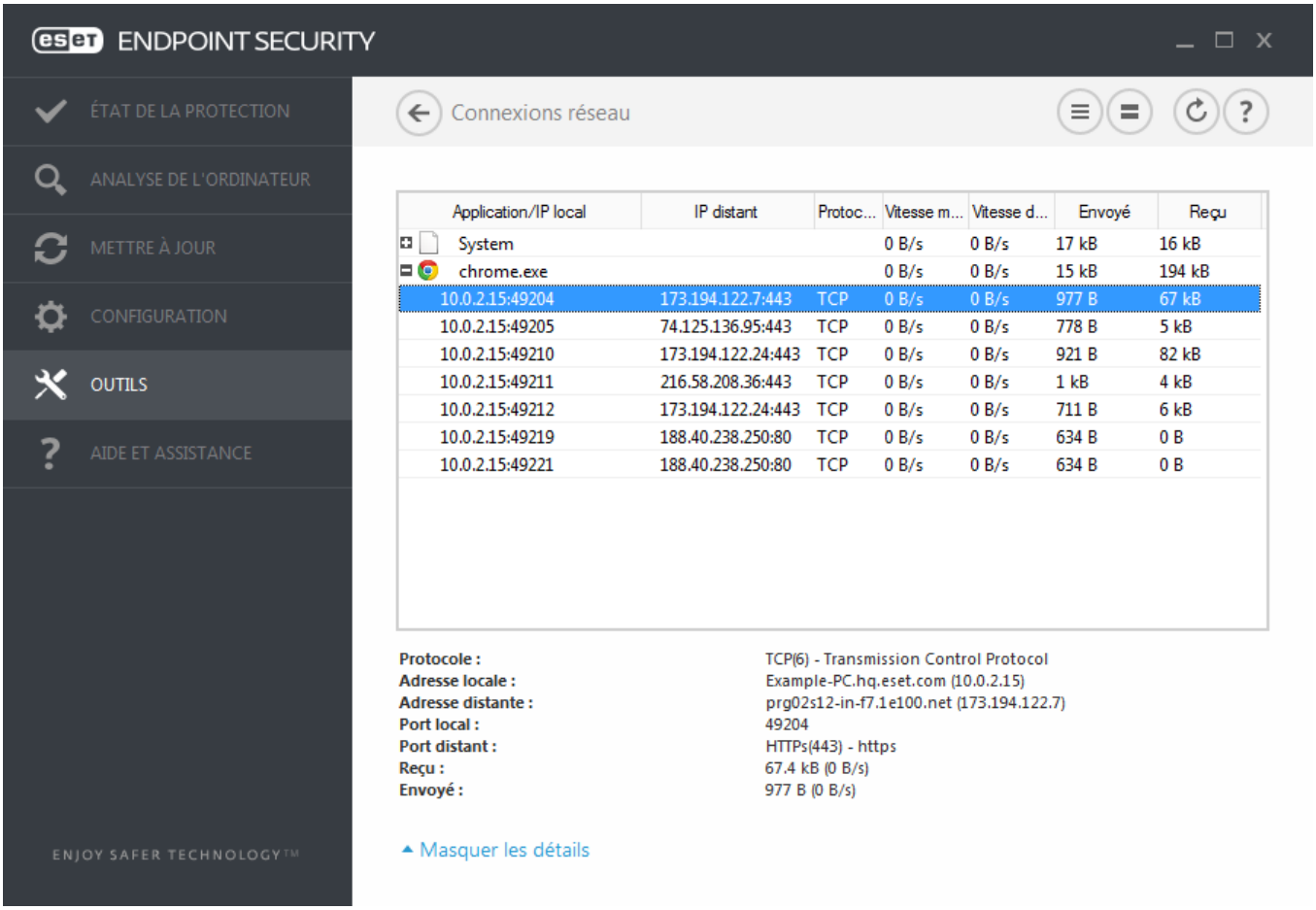
- **Chemin** - Emplacement de l'application sur l'ordinateur.
- **Taille** - Taille du fichier en Ko (kilo-octets) ou Mo (méga-octets).
- **Description** - Caractéristiques du fichier basées sur sa description du système d'exploitation.
- **Réseaux Sociaux** - Nom du fournisseur ou du processus de l'application.
- **Version** - Informations fournies par l'éditeur de l'application.
- **Produit** - Nom de l'application et/ou nom de l'entreprise.
- **Date de création** - Date et heure de création d'une application.
- **Date de modification** - Date et heure de dernière modification d'une application.

REMARQUE : la réputation peut également être vérifiée sur des fichiers qui n'agissent pas en tant que programmes/processus en cours - Marquez les fichiers que vous souhaitez vérifier, cliquez dessus avec le bouton droit et, dans le menu contextuel, sélectionnez **Options avancées** > **Évaluer la réputation des fichiers à l'aide de ESET Live Grid**.



3.8.6.9 Connexions réseau

La section Connexions réseau présente la liste des connexions actives et en attente. Elle vous aide à contrôler toutes les applications qui établissent des connexions sortantes.



La première ligne affiche le nom de l'application et la vitesse de transfert de données. Pour afficher la liste des connexions établies par l'application (ainsi que des informations plus détaillées), cliquez sur **+**.

Colonnes

Application/IP locale - Nom de l'application, adresses IP locales et ports de communication.

Adresse IP distante - Adresse IP et numéro de port d'un ordinateur distant spécifique.

Protocole - Protocole de transfert utilisé.

Vitesse montante/descendante - Vitesse actuelle des données sortantes et entrantes.

Envoyé/Reçu - Quantité de données échangées sur la connexion.

Afficher les détails - Permet d'afficher les informations détaillées de la connexion sélectionnée.

Sélectionnez une application ou une adresse IP dans l'écran Connexions réseau, puis cliquez avec le bouton droit dessus pour afficher un menu contextuel dont la structure est la suivante :

Résoudre les noms - Dans la mesure du possible, toutes les adresses réseau sont affichées dans le format DNS et non dans le format d'adresse IP numérique.

Afficher uniquement les connexions TCP - Cette liste affiche uniquement les connexions appartenant à la suite du protocole TCP.

Afficher les connexions d'écoute - Cette option permet d'afficher uniquement les connexions sans communication actuellement établie, mais pour lesquelles le système a ouvert un port et est en attente de connexion.

Afficher les connexions internes à l'ordinateur - Cette option permet de n'afficher que les connexions où le côté distant est un système local ; ces connexions sont appelées connexions *hôte local*.

Cliquez avec le bouton droit sur une connexion pour afficher les options supplémentaires suivantes :

Refuser la communication pour la connexion - Met fin à la connexion établie. Cette option n'est disponible que lorsque vous cliquez sur une connexion active.

Vitesse de rafraîchissement - Permet de choisir la fréquence de rafraîchissement des connexions actives.

Rafraîchir maintenant - Recharge la fenêtre des connexions réseau.

Les options suivantes ne sont disponibles que lorsque vous cliquez sur une application ou un processus, mais pas sur une connexion active :

Refuser temporairement la communication pour le processus - Rejette les connexions actuelles de l'application. Si une nouvelle connexion est établie, le pare-feu utilise une règle prédéfinie. Les paramètres sont décrits dans la section Règles et zones.

Autoriser temporairement la communication pour le processus - Autorise les connexions actuelles de l'application. Si une nouvelle connexion est établie, le pare-feu utilise une règle prédéfinie. Les paramètres sont décrits dans la section Règles et zones.

3.8.6.10 Soumission d'échantillons pour analyse

La boîte de dialogue de soumission d'échantillons permet d'envoyer un fichier ou un site à ESET pour analyse ; elle est accessible dans **Outils** > **Soumettre un échantillon pour analyse**. Si vous trouvez sur votre ordinateur un fichier dont le comportement est suspect, vous pouvez le soumettre au laboratoire de recherche sur les menaces d'ESET pour analyse. Si le fichier s'avère être une application malveillante, sa détection sera intégrée à une prochaine mise à jour.

Vous pouvez également soumettre le fichier par e-mail. Si vous préférez, compressez le ou les fichiers à l'aide de WinRAR/ZIP, protégez l'archive à l'aide du mot de passe « infected » et envoyez-la à samples@eset.com. Veillez à utiliser un objet descriptif et indiquez le plus d'informations possible sur le fichier (notez par exemple le site Internet à partir duquel vous l'avez téléchargé).

REMARQUE : avant de soumettre un échantillon à ESET, assurez-vous qu'il répond à au moins l'un des critères suivants :

- Le fichier ou le site Web n'est pas du tout détecté.
- Le fichier ou le site Web est détecté à tort comme une menace.

Vous ne recevrez pas de réponse, excepté si des informations complémentaires sont nécessaires à l'analyse.

Sélectionnez dans le menu déroulant **Motif de soumission de l'échantillon** la description correspondant le mieux à votre message :

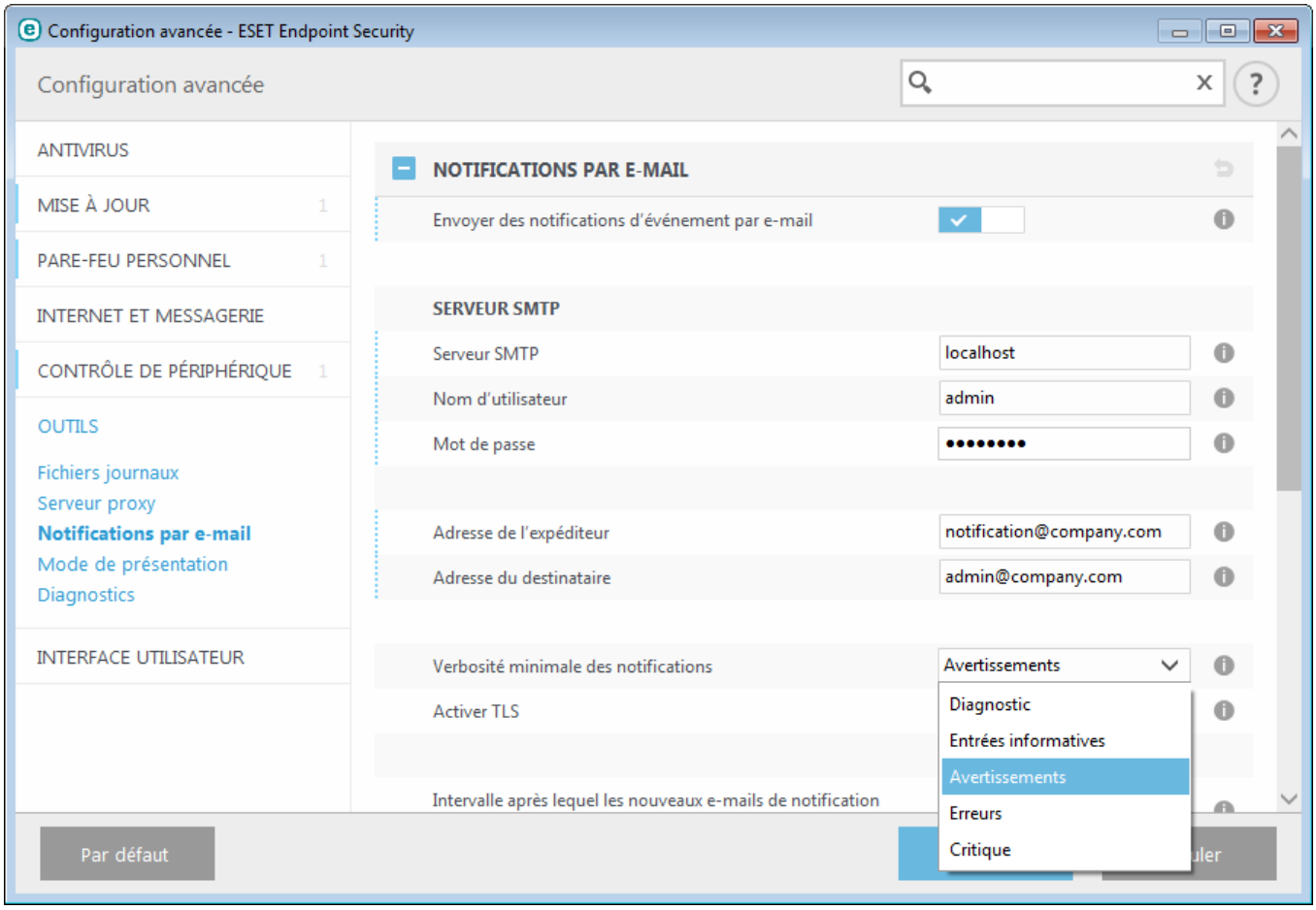
- **Fichier suspect**
- **Site suspect** (site Web infecté par un logiciel malveillant quelconque),
- **Fichier faux positif** (fichier détecté à tort comme infecté),
- **Site faux positif**
- **Autre**

Fichier/Site : le chemin d'accès au fichier ou au site Web que vous souhaitez soumettre.

Adresse de contact - L'adresse de contact est envoyée à ESET avec les fichiers suspects. Elle pourra servir à vous contacter si des informations complémentaires sont nécessaires à l'analyse. La spécification d'une adresse de contact est facultative. Vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires sont nécessaires à l'analyse. Nos serveurs reçoivent, en effet, chaque jour, des dizaines de milliers de fichiers, ce qui ne permet pas de répondre à tous les envois.

3.8.6.11 Notifications par e-mail

ESET Endpoint Security peut automatiquement envoyer des courriers électroniques de notification si un événement avec le niveau de verbosité sélectionné se produit. Activez l'option **Envoyer des notifications d'événement par e-mail** pour activer les notifications par e-mail.



Serveur SMTP

Serveur SMTP - Le serveur SMTP utilisé pour l'envoi de notifications.

REMARQUE : les serveurs SMTP avec chiffrement TLS sont pris en charge par ESET Endpoint Security.

Nom d'utilisateur et **mot de passe** - Si le serveur SMTP exige une authentification, ces champs doivent être remplis avec un nom d'utilisateur et un mot de passe valides donnant accès au serveur SMTP.

Adresse de l'expéditeur - Ce champ spécifie l'adresse de l'expéditeur qui apparaît dans l'en-tête des notifications.

Adresse du destinataire - Ce champ spécifie l'adresse du destinataire qui apparaît dans l'en-tête des notifications.

Dans le menu déroulant **Verbosité minimale des notifications**, vous pouvez sélectionner le niveau de gravité de départ des notifications à envoyer.

- **Diagnostic** - Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** - Enregistre tous les messages d'information (les événements réseau non standard, par exemple), y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissements** - Enregistre les erreurs critiques et les messages d'avertissement (Anti-Stealth ne s'exécute pas correctement ou une mise à jour a échoué).
- **Erreurs** - Enregistre les erreurs (la protection des documents n'a pas démarré) et les erreurs critiques.
- **Critique** - Consigne uniquement les erreurs critiques (erreur de démarrage de la protection antivirus ou système infecté.).

Activer TLS - Permet d'activer l'envoi de messages d'alerte et de notification pris en charge par le chiffrement TLS.

Intervalle après lequel les nouveaux e-mails de notification seront envoyés (min) - Intervalle en minutes après lequel de nouvelles notifications seront envoyées par e-mail. Si vous définissez cette valeur sur 0, les notifications sont envoyées immédiatement.

Envoyer chaque notification dans un e-mail séparé - Lorsque cette option est activée, le destinataire recevra un nouvel e-mail pour chaque notification spécifique. Cela peut se traduire par la réception d'un nombre important d'e-mails dans une courte période de temps.

Format des messages

Format des messages d'événement - Format des messages d'événement qui s'affichent sur les ordinateurs distants.

Format des messages d'avertissement de menace - Messages d'alerte et de notification de menace dont le format par défaut est prédéfini. Il est déconseillé de modifier ce format. Toutefois, dans certaines circonstances (par exemple, si vous avez un système automatisé de traitement des messages), vous serez peut-être amené à modifier le format des messages.

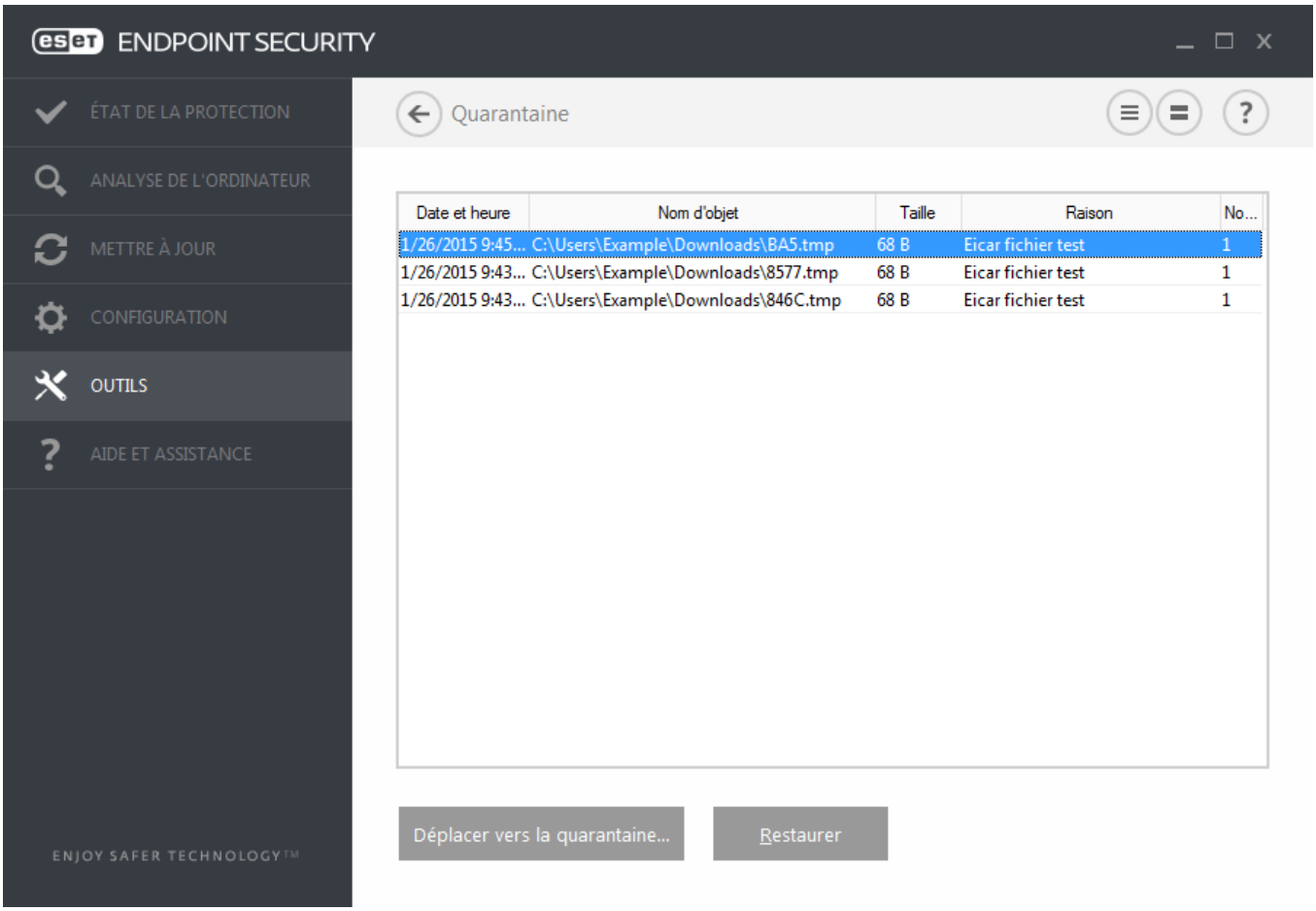
Utiliser les caractères alphabétiques locaux - Convertit le message électronique au codage ANSI sur la base des paramètres régionaux de Windows (par exemple, windows-1250). Si vous ne sélectionnez pas cette option, le message est converti et codé au format ACSII 7 bits (ainsi, « á » est remplacé par « a » et un symbole inconnu par un « ? »).

Utiliser l'encodage des caractères locaux - Le message électronique source est codé au format Quoted-printable (QP) qui utilise les caractères ASCII et peut correctement transmettre les caractères spéciaux par e-mail au format 8 bits (áéíóú).

3.8.6.12 Quarantaine

La principale fonction de la quarantaine est de stocker les fichiers infectés en toute sécurité. 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 Endpoint Security.

Vous pouvez choisir de mettre n'importe quel fichier en quarantaine. Cette action est conseillée si un fichier se comporte de façon suspecte, mais n'a pas été détecté par l'analyseur antivirus. Les fichiers en quarantaine peuvent être soumis pour analyse au laboratoire de recherche d'ESET.



Les fichiers du dossier de quarantaine peuvent être visualisés dans un tableau qui affiche la date et l'heure de mise en quarantaine, le chemin d'accès à l'emplacement d'origine du fichier infecté, sa taille en octets, la raison (par exemple, objet ajouté par l'utilisateur) et le nombre de menaces (s'il s'agit d'une archive contenant plusieurs infiltrations par exemple).

Mise en quarantaine de fichiers

ESET Endpoint Security met automatiquement les fichiers supprimés en quarantaine (si vous n'avez pas désactivé cette option dans la fenêtre d'alerte). Au besoin, vous pouvez mettre manuellement en quarantaine tout fichier suspect en cliquant sur l**Quarantaine**. Le fichier d'origine est supprimé de son emplacement initial. Il est également possible d'utiliser le menu contextuel à cette fin : cliquez avec le bouton droit dans la fenêtre **Quarantaine** et sélectionnez l'option **Quarantaine**.

Restauration depuis la quarantaine

Les fichiers mis en quarantaine peuvent aussi être restaurés à leur emplacement d'origine. Pour restaurer un fichier en quarantaine, cliquez avec le bouton droit dessus dans la fenêtre Quarantaine, puis sélectionnez **Restaurer** dans le menu contextuel. Si un fichier est marqué comme étant une application potentiellement indésirable, l'option **Restaurer et exclure de l'analyse** est également disponible. Le menu contextuel contient également l'option **Restaurer vers...** qui permet de restaurer des fichiers vers un emplacement autre que celui d'origine dont ils ont été supprimés.

Suppression d'un élément en quarantaine : cliquez avec le bouton droit sur un élément donné, puis sélectionnez

Supprimer l'élément en quarantaine. Vous pouvez également sélectionner l'élément à supprimer, puis appuyer sur **Suppr** sur votre clavier. Vous pouvez aussi sélectionner plusieurs éléments et les supprimer simultanément.

REMARQUE : si le programme met en quarantaine, par erreur, un fichier inoffensif, il convient de le restaurer, de l'exclure de l'analyse et de l'envoyer au service client ESET.

Soumission de fichiers mis en quarantaine

Si vous avez mis en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été détecté par erreur comme une menace et placé en quarantaine, envoyez ce fichier au laboratoire d'ESET. Pour soumettre un fichier mis en quarantaine, cliquez avec le bouton droit sur le fichier et sélectionnez l'option **Soumettre le fichier pour analyse** dans le menu contextuel.

3.8.6.13 Microsoft Windows Update

La fonctionnalité Windows Update est un élément important de la protection des utilisateurs contre les logiciels malveillants. C'est pourquoi il est essentiel d'installer les mises à jour de Microsoft Windows dès qu'elles sont disponibles. ESET Endpoint Security vous informe des mises à jour manquantes en fonction du niveau que vous spécifiez. Les niveaux suivants sont disponibles :

- **Pas de mise à jour** - Aucune mise à jour système n'est proposée au téléchargement.
- **Mises à jour optionnelles** - Les mises à jour marquées comme étant faiblement prioritaires et au-dessus sont proposées au téléchargement.
- **Mises à jour recommandées** - Les mises à jour marquées comme étant courantes et au-dessus sont proposées au téléchargement.
- **Mises à jour importantes** - Les mises à jour marquées comme étant importantes et au-dessus sont proposées au téléchargement.
- **Mises à jour critiques** - Seules les mises à jour critiques sont proposées pour le téléchargement.

Cliquez sur **OK** pour enregistrer les modifications. La fenêtre Mises à jour système s'affiche après la vérification de l'état à l'aide du serveur de mise à jour. C'est pourquoi les informations de mise à jour système ne sont peut-être pas immédiatement disponibles après l'enregistrement des modifications.

3.8.7 Interface utilisateur

La section **Interface utilisateur** permet de configurer le comportement de l'interface utilisateur graphique du programme (GUI).

Grâce à l'outil Éléments de l'interface utilisateur, vous pouvez ajuster l'apparence du programme et l'utilisation des effets.

Pour bénéficier de la sécurité maximum de votre logiciel de sécurité, vous pouvez empêcher toute modification non autorisée à l'aide de l'outil Configuration de l’accès.

En configurant Alertes et notifications, vous pouvez modifier le comportement des alertes concernant les menaces détectées et les notifications système. Ces alertes peuvent être personnalisées en fonction de vos besoins.

Si vous choisissez de ne pas afficher certaines notifications, ces dernières apparaissent dans **Éléments de l'interface utilisateur** > **États d'application**. Vous pouvez vérifier dans cette section leur état ou empêcher leur affichage.

L'intégration dans le menu contextuel s'affiche lorsque vous cliquez avec le bouton sur l'objet sélectionné. Utilisez cet outil pour intégrer les options ESET Endpoint Security dans le menu contextuel.

Le mode de présentation est utile pour les utilisateurs qui souhaitent travailler dans une application sans être interrompus par des fenêtres contextuelles, des tâches planifiées et tout autre composant qui pourrait augmenter la charge du processeur et de la mémoire RAM.

3.8.7.1 Éléments de l'interface utilisateur

La configuration de l'interface utilisateur d'ESET Endpoint Security peut être modifiée de manière à adapter l'environnement de travail à vos besoins. Ces options de configuration sont accessibles depuis la branche **Interface utilisateur** > **Éléments de l'interface utilisateur** de l'arborescence de la configuration avancée ESET Endpoint Security.

Dans la section **Éléments de l'interface utilisateur**, vous pouvez ajuster l'environnement de travail. Utilisez le menu déroulant **Mode de démarrage de l'interface utilisateur graphique** pour sélectionner un mode de démarrage de l'interface utilisateur graphique (GUI) parmi les suivants :

Complet - L'intégralité de l'interface utilisateur graphique est affichée.

Minimal - L'interface utilisateur graphique est disponible, mais seules les notifications sont affichées pour l'utilisateur.

Manuel - Aucune notification ni alerte n'est affichée.

Silencieux - L'interface utilisateur graphique, les notifications et les alertes ne sont pas affichées. Ce mode peut s'avérer utilise lorsque vous devez préserver les ressources système. Il peut être uniquement démarré par l'administrateur.

REMARQUE : une fois le mode de démarrage Minimal sélectionné et l'ordinateur redémarré, les notifications s'affichent, mais pas l'interface graphique. Pour rétablir le mode complet, exécutez l'interface utilisateur graphique dans le menu Démarrer, **Tous les programmes** > **ESET** > ESET Endpoint Security (en tant qu'administrateur). Vous pouvez également effectuer cette opération via ESET Remote Administrator à l'aide d'une stratégie.

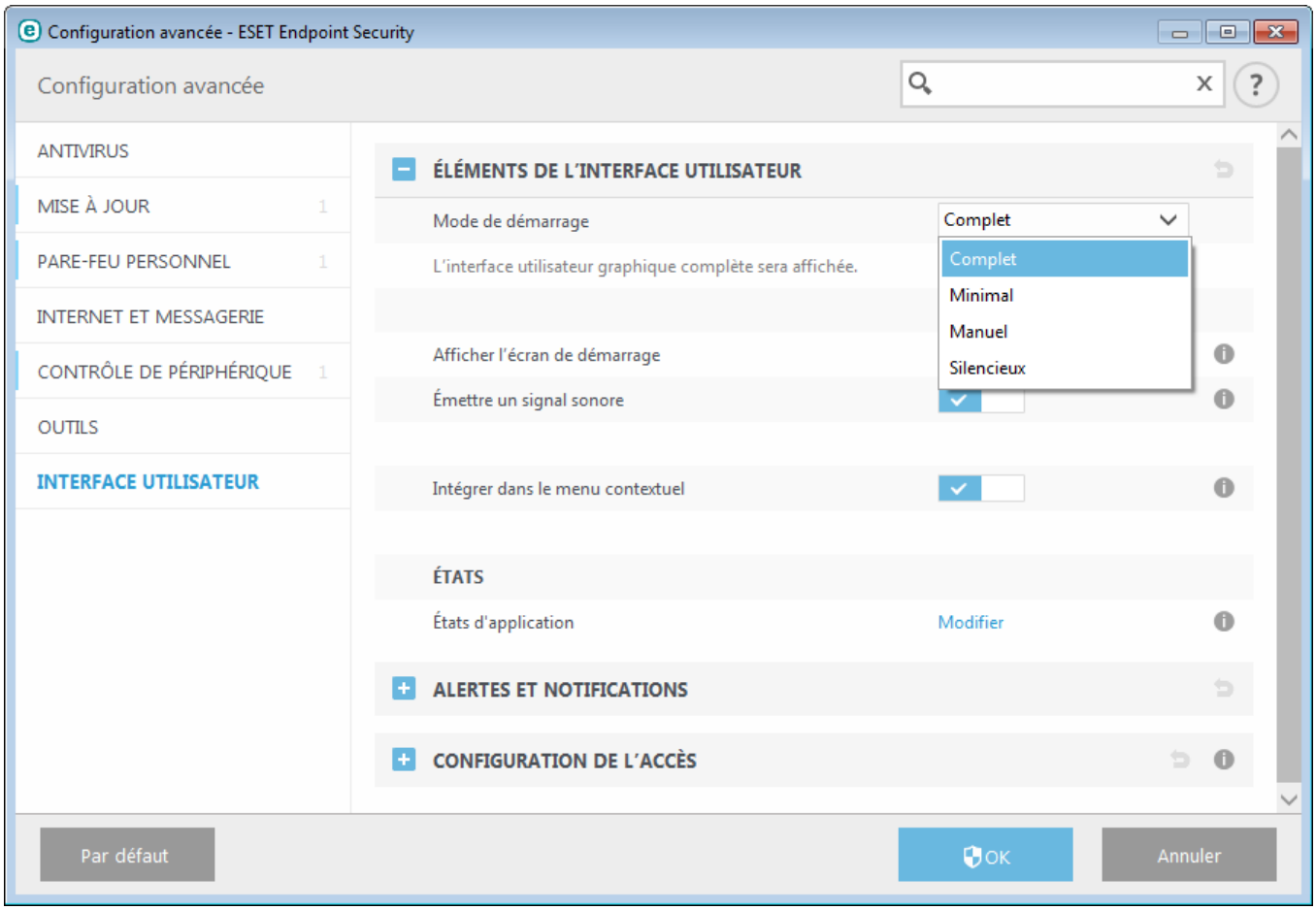
Pour désactiver l'écran de démarrage de ESET Endpoint Security, désactivez **Afficher l'écran de démarrage**.

Pour qu'ESET Endpoint Security émette un signal sonore en cas d'événement important lors d'une analyse, par exemple lorsqu'une menace est découverte ou lorsque l'analyse est terminée, sélectionnez **Utiliser un signal sonore**.

Intégrer dans le menu contextuel - Intègre les options ESET Endpoint Security dans le menu contextuel.

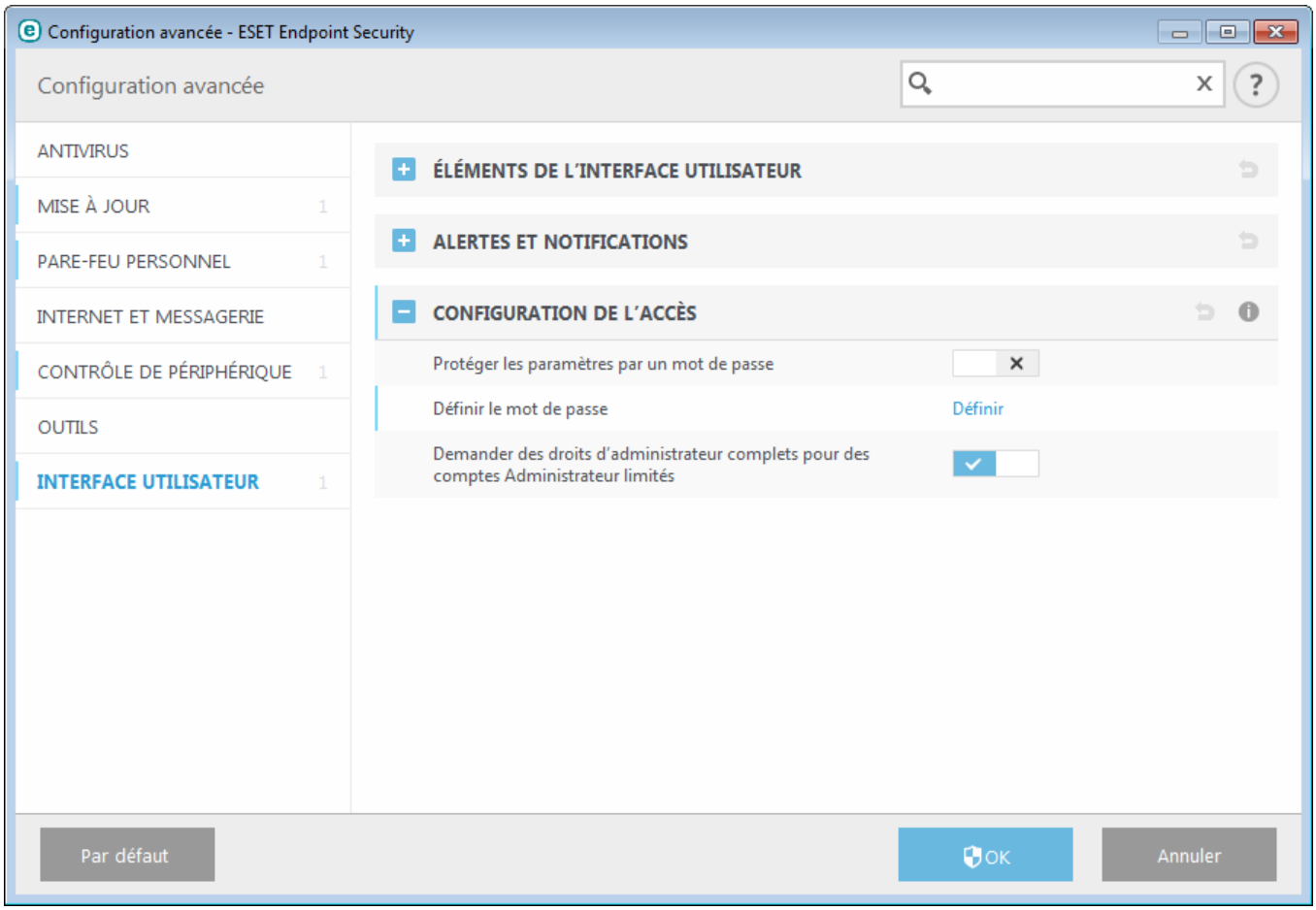
États

États d'application - Cliquez sur le bouton **Modifier** pour gérer (désactiver) les états affichés dans le volet **État de la protection** du menu principal.


Configuration avancée - ESET Endpoint Security
Configuration avancée
ANTIVIRUS
MISE À JOUR 1
PARE-FEU PERSONNEL 1
INTERNET ET MESSAGERIE
CONTRÔLE DE PÉRIPHÉRIQUE 1
OUTILS
INTERFACE UTILISATEUR
ÉLÉMENTS DE L'INTERFACE UTILISATEUR
Mode de démarrage
Complet
L'interface utilisateur graphique complète sera affichée.
Complet
Minimal
Manuel
Silencieux
Afficher l'écran de démarrage
Émettre un signal sonore
Intégrer dans le menu contextuel
ÉTATS
États d'application
Modifier
ALERTES ET NOTIFICATIONS
CONFIGURATION DE L'ACCÈS
Par défaut
OK
Annuler

3.8.7.2 Configuration de l'accès

Il est essentiel que ESET Endpoint Security soit correctement configuré pour garantir la sécurité maximale du système. Tout changement inapproprié peut entraîner la perte de données importantes. Pour éviter des modifications non autorisées, les paramètres de la configuration d'ESET Endpoint Security peuvent être protégés par mot de passe. Les paramètres de configuration pour la protection par mot de passe figurent dans **Configuration avancée** (F5), sous **Configuration de l'accès** > **Interface utilisateur**.



Protéger les paramètres par un mot de passe : indiquez les paramètres du mot de passe. Cliquez sur cette option pour ouvrir la fenêtre Configuration du mot de passe.

Pour définir ou modifier un mot de passe visant à protéger les paramètres de configuration, cliquez sur **Définir**.

Demander des droits d'administrateur complets pour des comptes Administrateur limités - Conservez cette option active pour inviter l'utilisateur actuel (s'il ne possède pas les autorisations d'administrateur) à saisir le nom d'utilisateur et le mot de passe d'administrateur lors de la modification de certains paramètres du système (semblable au contrôle UAC dans Windows Vista). Les modifications comprennent la désactivation des modules de protection ou l'arrêt du pare-feu.

Pour Windows XP uniquement :

Demander des droits d'administrateur (système sans prise en charge UAC) - Activez cette option pour qu'ESET Endpoint Security demande des informations d'identification d'administrateur.

3.8.7.3 Alertes et notifications

La section **Alertes et notifications** sous **Interface utilisateur** vous permet de configurer la manière dont ESET Endpoint Security traite les alertes de menace et les notifications système (par exemple, les messages indiquant une mise à jour réussie). Vous pouvez également configurer l'heure d'affichage et la transparence des notifications dans la barre d'état système (cela ne s'applique qu'aux systèmes prenant en charge ces notifications).

Fenêtres d'alerte

Lorsque l'option **Afficher les alertes** est désactivée, aucune fenêtre d'alerte ne s'affiche, ce qui ne convient qu'à un nombre limité de situations particulières. Nous recommandons à la majorité des utilisateurs de conserver l'option par défaut (activée).

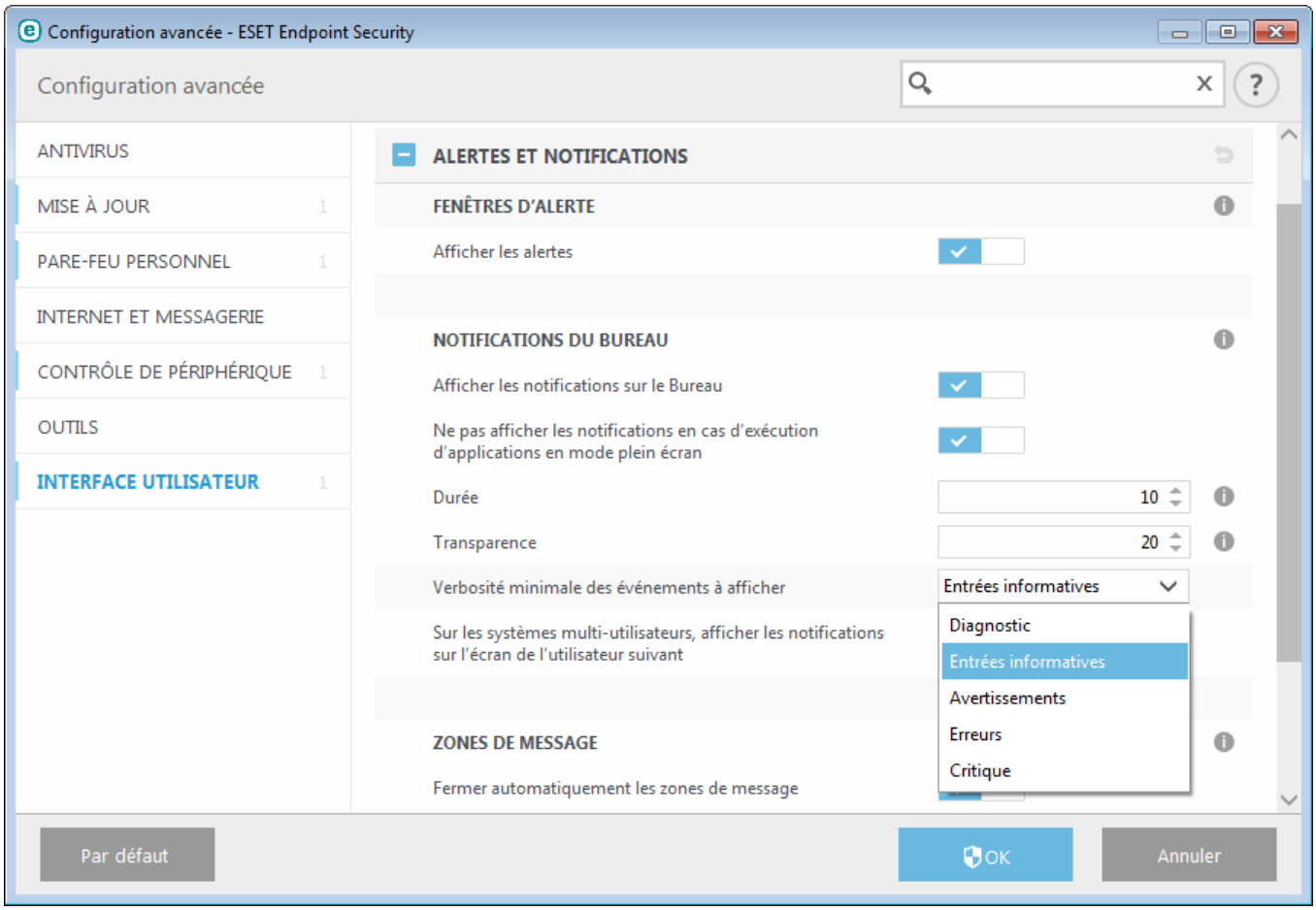
Notifications du Bureau

Les notifications sur le bureau et les info-bulles sont fournies à titre d'information uniquement et n'exigent aucune interaction avec l'utilisateur. Elles s'affichent dans la partie système de la barre d'état, dans l'angle inférieur droit de l'écran. Pour activer l'affichage des notifications sur le bureau, activez l'option **Afficher les notifications sur le bureau**. Activez l'option **Ne pas afficher les notifications en cas d'exécution d'applications en mode plein écran** pour supprimer toutes les notifications non interactives. D'autres options détaillées (la durée d'affichage des notifications et la transparence de la fenêtre) peuvent être modifiées en dessous.

Le menu déroulant **Verbosité minimale des événements à afficher** permet de sélectionner le niveau de gravité des alertes et notifications à afficher. Les options disponibles sont les suivantes :

- **Diagnostic** - Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** - Enregistre tous les messages d'information, y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissements** - Enregistre les erreurs critiques, les erreurs et les messages d'avertissement.
- **Erreurs** - Enregistre les erreurs du type « Erreur de téléchargement du fichier » et les erreurs critiques.
- **Critique** - Consigne uniquement les erreurs critiques (erreur de démarrage de la protection antivirus , pare-feu intégré, etc.).

La dernière fonctionnalité de cette section permet de configurer la destination des notifications dans un environnement multi-utilisateur. Le champ **Sur les systèmes multi-utilisateurs, afficher les notifications sur l'écran de l'utilisateur suivant** indique l'utilisateur qui recevra les notifications système et autres notifications lorsque le système autorise la connexion simultanée de plusieurs utilisateurs. Normalement, il doit s'agir de l'administrateur système ou de l'administrateur réseau. Cette option est particulièrement utile pour les serveurs Terminal Server, à condition que toutes les notifications système soient envoyées à l'administrateur.



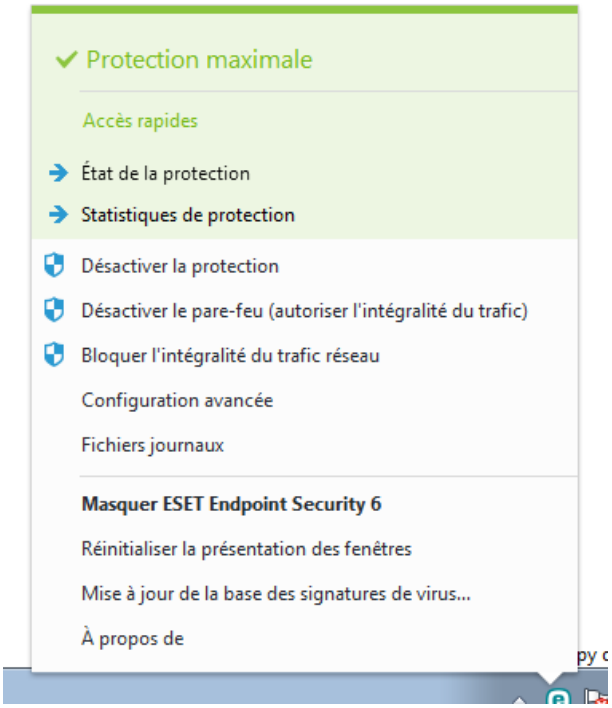
Zones de message

Pour fermer automatiquement les fenêtres d'alerte après un certain délai, sélectionnez **Fermer automatiquement les zones de message**. Si les fenêtres d'alerte ne sont pas fermées manuellement, le système les ferme automatiquement une fois le laps de temps écoulé.

Messages de confirmation - Affiche une liste de messages de confirmation que vous pouvez choisir d'afficher ou non.

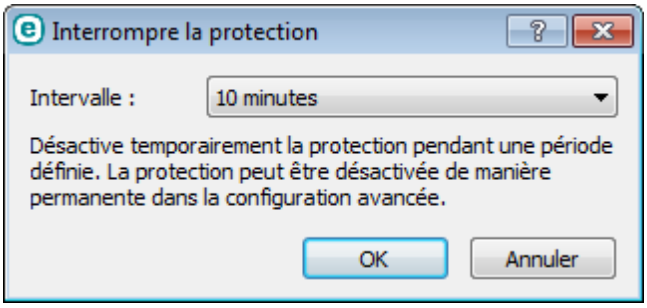
3.8.7.4 Icône dans la partie système de la barre des tâches

Pour accéder à certaines des fonctionnalités et options de configuration les plus importantes, cliquez avec le bouton droit sur l'icône dans la partie système de la barre des tâches.



Bloquer le réseau - Le pare-feu personnel bloque tout le trafic réseau et Internet entrant et sortant.

Désactiver la protection - Affiche la boîte de dialogue de confirmation qui désactive la protection antivirus et antispyware ; cette dernière protège des attaques malveillantes en contrôlant les fichiers et les communications par messagerie et Internet.



Le menu déroulant **Intervalle** indique la durée pendant laquelle la protection antivirus et antispyware est désactivée.

Interrompre le pare-feu (autoriser l'intégralité du trafic) - Le pare-feu passe en mode inactif. Pour plus d'informations, reportez-vous à la section Réseau.

Bloquer tout le trafic réseau - Bloque l'intégralité du trafic réseau. Vous pouvez le réactiver en cliquant sur **Arrêter le blocage de l'intégralité du trafic**.

Configuration avancée - Sélectionnez cette option pour afficher l'arborescence **Configuration avancée**. Vous pouvez également accéder à Configuration avancée en appuyant sur la touche F5 ou en accédant à **Configuration** > **Configuration avancée**.

Fichiers journaux - Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées.

MasquerESET Endpoint Security - Masque la fenêtre ESET Endpoint Security.

Réinitialiser la disposition des fenêtres - Rétablit la taille et la position par défaut de la fenêtre ESET Endpoint Security.

Mise à jour de la base des signatures de virus - Commence la mise à jour de la base des signatures des virus afin de garantir un niveau optimal de protection contre les codes malveillants.

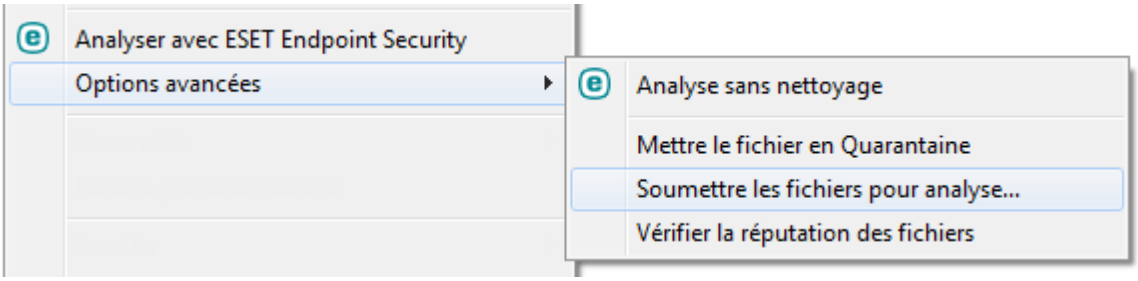
À propos - Les informations système fournissent des détails sur la version installée d'ESET Endpoint Security, sur les modules installés et sur la date d'expiration de votre licence. Des informations sur votre système d'exploitation et les ressources système figurent dans la partie inférieure de la page.

3.8.7.5 Menu contextuel

Le menu contextuel est le menu qui s'affiche lorsque vous cliquez avec le bouton sur un objet (fichier). Il répertorie toutes les actions que vous pouvez effectuer sur un objet.

Il est possible d'intégrer les options ESET Endpoint Security dans le menu contextuel. Les options de configuration de cette fonctionnalité figurent dans l'arborescence de la configuration avancée, sous **Interface utilisateur** > **Éléments de l'interface utilisateur**.

Intégrer dans le menu contextuel - Intègre les options ESET Endpoint Security dans le menu contextuel.



3.9 Utilisateur chevronné

3.9.1 Gestionnaire de profils

Le gestionnaire de profil est utilisé à deux endroits dans ESET Endpoint Security - dans les sections **Analyse de l'ordinateur à la demande** et **Mise à jour**.

Analyse de l'ordinateur à la demande

Vos paramètres d'analyse préférés peuvent être enregistrés pour les prochaines analyses. Il est recommandé de créer autant de profils (avec différentes cibles et méthodes, et d'autres paramètres d'analyse) que d'analyses utilisées régulièrement.

Pour créer un profil, ouvrez la fenêtre Configuration avancée (F5) et cliquez sur **Antivirus** > **Analyse de l'ordinateur à la demande**. Cliquez ensuite sur **Modifier** en regard de **Liste des profils**. Le menu déroulant **Profil sélectionné** répertorie les profils d'analyse existants. Pour plus d'informations sur la création d'un profil d'analyse correspondant à vos besoins, reportez-vous à la section ThreatSenseConfiguration du moteur ; vous y trouverez une description de chaque paramètre de configuration de l'analyse.

Exemple : supposons la situation suivante : vous souhaitez créer votre propre profil d'analyse et la configuration d'analyse intelligente est partiellement adéquate. En revanche, vous ne souhaitez analyser ni les fichiers exécutables compressés par un compresseur d'exécutables, ni les applications potentiellement dangereuses. Vous souhaitez effectuer un **nettoyage strict**. Entrez le nom du nouveau profil dans la fenêtre **Gestionnaire de profils**, puis cliquez sur **Ajouter**. Sélectionnez le nouveau profil dans le menu déroulant **Profil sélectionné** et réglez les paramètres restants selon vos besoin. Cliquez sur **OK** pour enregistrer le nouveau profil.

Mise à jour

L'éditeur de profils de la section de configuration des mises à jour permet aux utilisateurs de créer de nouveaux profils de mise à jour. Il est conseillé de créer et d'utiliser des profils personnalisés (autre que l'option par défaut **Mon profil**) si votre ordinateur utilise plusieurs voies de connexion aux serveurs de mise à jour.

C'est le cas par exemple d'un ordinateur portable qui se connecte normalement à un serveur local (miroir) sur le réseau local, mais qui télécharge les mises à jour directement à partir des serveurs de mise à jour d'ESET lorsqu'il est

déconnecté du réseau local (voyage d'affaires). le premier se connectant au serveur local, le second aux serveurs d'ESET. Une fois ces profils configurés, allez dans **Outils** > **Planificateur** puis modifiez les paramètres de mise à jour de la tâche. Désignez un profil comme principal et l'autre comme secondaire.

Profil sélectionné - Le profil de mise à jour utilisé actuellement. Pour le changer, choisissez un profil dans le menu déroulant.

Liste des profils : permet de créer des profils de mise à jour ou de supprimer ceux existants.

3.9.2 Diagnostics

Le diagnostic fournit un fichier d'image mémoire en cas de défaillance d'une application lors des processus ESET (par exemple *ekrn*). Dès qu'une application présente une défaillance, un fichier d'image mémoire est généré. Ce fichier permet aux développeurs de déboguer et de résoudre différents problèmes ESET Endpoint Security. Cliquez sur le menu déroulant en regard de l'option **Type de fichier d'image mémoire**, puis sélectionnez l'une des trois options disponibles :

- Selectionnez **Désactiver** (valeur par défaut) pour désactiver cette fonctionnalité.
- **Mini** - Enregistre le plus petit ensemble d'informations utiles qui peuvent permettre d'identifier les raisons de l'arrêt inopiné de l'application. Ce type de fichier d'image mémoire peut être utile lorsque l'espace disponible est limité. Toutefois, en raison des informations limitées qui figurent dans ce fichier, les erreurs qui n'étaient pas directement provoquées par la menace, car cette dernière ne s'exécutait pas au moment du problème, risquent de ne pas être détectées par l'analyse de ce fichier.
- **Complet** - Enregistre tout le contenu de la mémoire système en cas d'arrêt inopiné de l'application. Un fichier d'image mémoire complet peut contenir des données provenant des processus en cours au moment de sa collecte.

Répertoire cible - Répertoire dans lequel est généré le fichier d'image mémoire lors de la défaillance.

Ouvrir le dossier de diagnostics - Cliquez sur **Ouvrir** pour ouvrir ce répertoire dans une nouvelle fenêtre de l'*Explorateur Windows*.

3.9.3 Importer et exporter les paramètres

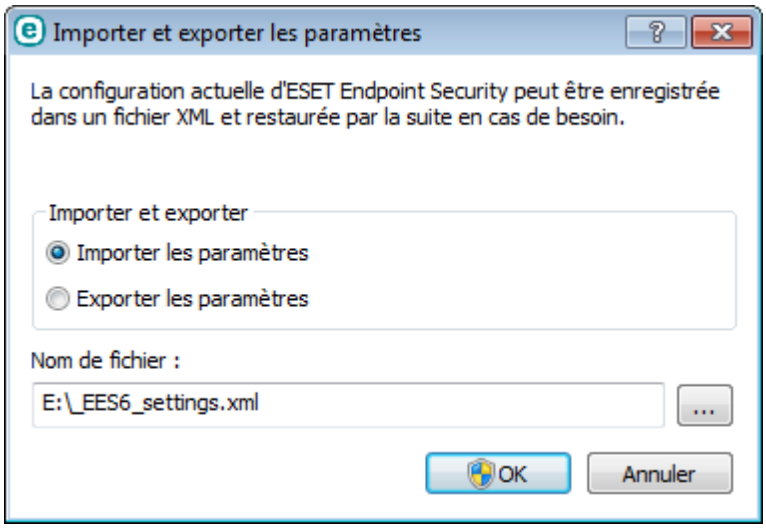
Vous pouvez importer ou exporter votre fichier de configuration .xml ESET Endpoint Security personnalisé à partir du menu **Configuration**.

Ces opérations sont utiles si vous devez sauvegarder la configuration actuelle de ESET Endpoint Security pour l'utiliser ultérieurement. L'option Exporter les paramètres est également pratique pour les utilisateurs qui souhaitent utiliser leur configuration préférée sur plusieurs systèmes. Il leur suffit d'importer un fichier *.xml* pour transférer ces paramètres.

L'importation d'une configuration est très facile. Dans la fenêtre principale du programme, cliquez sur **Configuration** > **Importer/exporter les paramètres**, puis sélectionnez **Importer les paramètres**. Saisissez le nom du fichier de configuration ou cliquez sur le bouton **...** pour accéder au fichier de configuration à importer.

La procédure d'exportation d'une configuration est très semblable. Dans la fenêtre principale du programme, cliquez sur **Configuration** > **Importer/exporter les paramètres**. Sélectionnez **Exporter les paramètres** et saisissez le nom de fichier du fichier de configuration (par exemple, *export.xml*). Utilisez le navigateur pour sélectionner un emplacement de votre ordinateur pour enregistrer le fichier de configuration.

REMARQUE : Vous pouvez rencontrer une erreur lors de l'exportation des paramètres si vous ne disposez pas de suffisamment de droits pour écrire le fichier exporté dans le répertoire spécifié.



3.9.4 Ligne de commande

Le module antivirus d'ESET Endpoint Security peut être lancé depuis la ligne de commande, manuellement (avec la commande « ecls ») ou au moyen d'un fichier de traitement par lots (« bat »). Module d'interface à ligne de commande ESET :

```
ecls [OPTIONS..] FILES..
```

Les paramètres suivants peuvent être utilisés lors de l'exécution de l'analyseur à la demande, à partir de la ligne de commande :

Options

/base-dir=FOLDER	charger les modules depuis le DOSSIER
/quar-dir=FOLDER	DOSSIER de quarantaine
/exclude=MASK	exclure les fichiers correspondant à MASQUE de l'analyse
/subdir	analyser les sous-dossiers (valeur par défaut)
/no-subdir	ne pas analyser les sous-dossiers
/max-subdir-level=LEVEL	sous-niveau maximal de sous-dossiers dans les dossiers à analyser
/symlink	suivre les liens symboliques (valeur par défaut)
/no-symlink	ignorer les liens symboliques
/ads	analyser ADS (valeur par défaut)
/no-ads	ne pas analyser ADS
/log-file=FILE	journaliser les résultats dans un FICHIER
/log-rewrite	écraser le fichier de résultats (valeur par défaut - ajouter)
/log-console	journaliser les résultats sur la console (valeur par défaut)
/no-log-console	ne pas journaliser les résultats sur la console
/log-all	journaliser également les fichiers nettoyés
/no-log-all	ne pas journaliser les fichiers nettoyés (valeur par défaut)
/aind	afficher l'indicateur d'activité
/auto	analyser et nettoyer automatiquement tous les disques locaux

Options de l'analyseur

/files	analyser les fichiers (valeur par défaut)
/no-files	ne pas analyser les fichiers
/memory	analyser la mémoire

/boots	analyser les secteurs d'amorçage
/no-boots	ne pas analyser les secteurs d'amorçage (valeur par défaut)
/arch	analyser les archives (valeur par défaut)
/no-arch	ne pas analyser les archives
/max-obj-size=SIZE	analyser uniquement les fichiers plus petits que TAILLE Mo (valeur par défaut 0 = illimité)
/max-arch-level=LEVEL	sous-niveau maximal d'archives à analyser dans les archives (archives imbriquées)
/scan-timeout=LIMIT	analyser les archives pendant un maximum de LIMITE secondes
/max-arch-size=SIZE	n'analyser les fichiers contenus dans une archive que s'ils sont plus petits que TAILLE (valeur par défaut 0 = illimité)
/max-sfx-size=SIZE	n'analyser les fichiers d'une archive auto-extractible que s'ils sont plus petits que TAILLE Mo (valeur par défaut 0 = illimité)
/mail	analyser les fichiers des courriers électroniques (valeur par défaut)
/no-mail	ne pas analyser les fichiers des courriers électroniques
/mailbox	analyser les boîtes aux lettres (valeur par défaut)
/no-mailbox	ne pas analyser les boîtes aux lettres
/sfx	analyser les archives auto-extractibles (valeur par défaut)
/no-sfx	ne pas analyser les archives auto-extractibles
/rtp	analyser les fichiers exécutables compressés par un compresseur d'exécutables (valeur par défaut)
/no-rtp	ne pas analyser les fichiers exécutables compressés
/unsafe	rechercher les applications potentiellement dangereuses
/no-unsafe	ne pas rechercher les applications potentiellement dangereuses (valeur par défaut)
/unwanted	rechercher les applications potentiellement indésirables
/no-unwanted	ne pas rechercher les applications potentiellement indésirables (valeur par défaut)
/suspicious	rechercher les applications suspectes (valeur par défaut)
/no-suspicious	ne pas rechercher les applications suspectes
/pattern	utiliser les signatures (valeur par défaut)
/no-pattern	ne pas utiliser les signatures
/heur	activer l'heuristique (valeur par défaut)
/no-heur	désactiver l'heuristique
/adv-heur	activer l'heuristique avancée (valeur par défaut)
/no-adv-heur	désactiver l'heuristique avancée
/ext=EXTENSIONS	analyser uniquement les EXTENSIONS délimitées par deux-points
/ext-exclude=EXTENSIONS	exclure de l'analyse les EXTENSIONS délimitées par deux-points
/clean-mode=MODE	utiliser le MODE de nettoyage pour les objets infectés Les options disponibles sont les suivantes : • aucun nettoyage - Aucun nettoyage automatique ne se produit. • nettoyage standard (valeur par défaul) - ecls.exe tente automatiquement de nettoyer ou de supprimer les fichiers infectés. • nettoyage strict - ecls.exe tente automatiquement de nettoyer ou de supprimer les fichiers infectés sans intervention de l'utilisateur (vous ne recevez pas d'invite avant la suppression des fichiers). • nettoyage rigoureux - ecls.exe supprime les fichiers sans tenter de les nettoyer, quel que soit leur type. • suppression - ecls.exe supprime les fichiers sans tenter de les nettoyer, mais s'abstient de supprimer les fichiers sensibles tels que les fichiers système de Windows.
/quarantine	copier les fichiers infectés (si nettoyés) vers Quarantaine (complète l'action effectuée lors du nettoyage)
/no-quarantine	ne pas copier les fichiers infectés vers Quarantaine

Options générales

/help	afficher l'aide et quitter
/version	afficher les informations de version et quitter
/preserve-time	conserver la date et l'heure du dernier accès

Codes de sortie

0	aucune menace détectée
1	menace détectée et nettoyée
10	certains fichiers n'ont pas pu être analysés (peuvent être des menaces)
50	menace détectée
100	erreur

REMARQUE : un code sortie supérieur à 100 signale un fichier non analysé qui est potentiellement infecté.

3.9.5 Détection en cas d'inactivité

Les paramètres de détection en cas d'inactivité peuvent être configurés dans **Configuration avancée**, sous **Antivirus** > **Analyse en cas d'inactivité** > **Détection en cas d'inactivité**. Ces paramètres spécifient un déclencheur pour l'Analyse en cas d'inactivité, quand :

- l'économiseur d'écran est en cours d'exécution,
- l'ordinateur est verrouillé,
- un utilisateur se déconnecte de sa session.

Utilisez les boutons bascules pour chaque état respectif, afin d'activer ou désactiver les différents déclencheurs de détection d'état inactif.

3.9.6 ESET SysInspector

3.9.6.1 Introduction à ESET SysInspector

ESET SysInspector est une application qui inspecte votre ordinateur en profondeur et qui affiche en détail toutes les données obtenues. Des informations telles que les pilotes et applications installés, les connexions réseau ou les entrées de registre importantes peuvent vous aider à élucider un comportement suspect du système, qu'il soit dû à une incompatibilité logicielle ou matérielle, ou à une infection par logiciel malveillant.

Vous pouvez accéder à ESET SysInspector de deux manières : depuis la version intégrée dans les solutions ESET Security ou en téléchargeant gratuitement la version autonome (SysInspector.exe) depuis le site Internet d'ESET. Les deux versions sont identiques en matière de fonctionnalités et disposent des mêmes contrôles de programme. La seule différence réside dans la façon dont les résultats sont gérés. Les versions téléchargées et intégrées vous permettent d'exporter des instantanés du système dans un fichier *.xml* et de les enregistrer sur le disque. Toutefois, la version intégrée vous permet également de stocker les instantanés du système directement dans **Outils** > **ESET SysInspector** (à l'exception de ESET Remote Administrator). Pour plus d'informations, reportez-vous à la section ESET SysInspector comme composant de ESET Endpoint Security.

Veuillez patienter pendant qu'ESET SysInspector analyse votre ordinateur. L'analyse peut prendre entre 10 secondes et quelques minutes, en fonction de la configuration de votre matériel, du système d'exploitation et du nombre d'applications installées sur votre ordinateur.

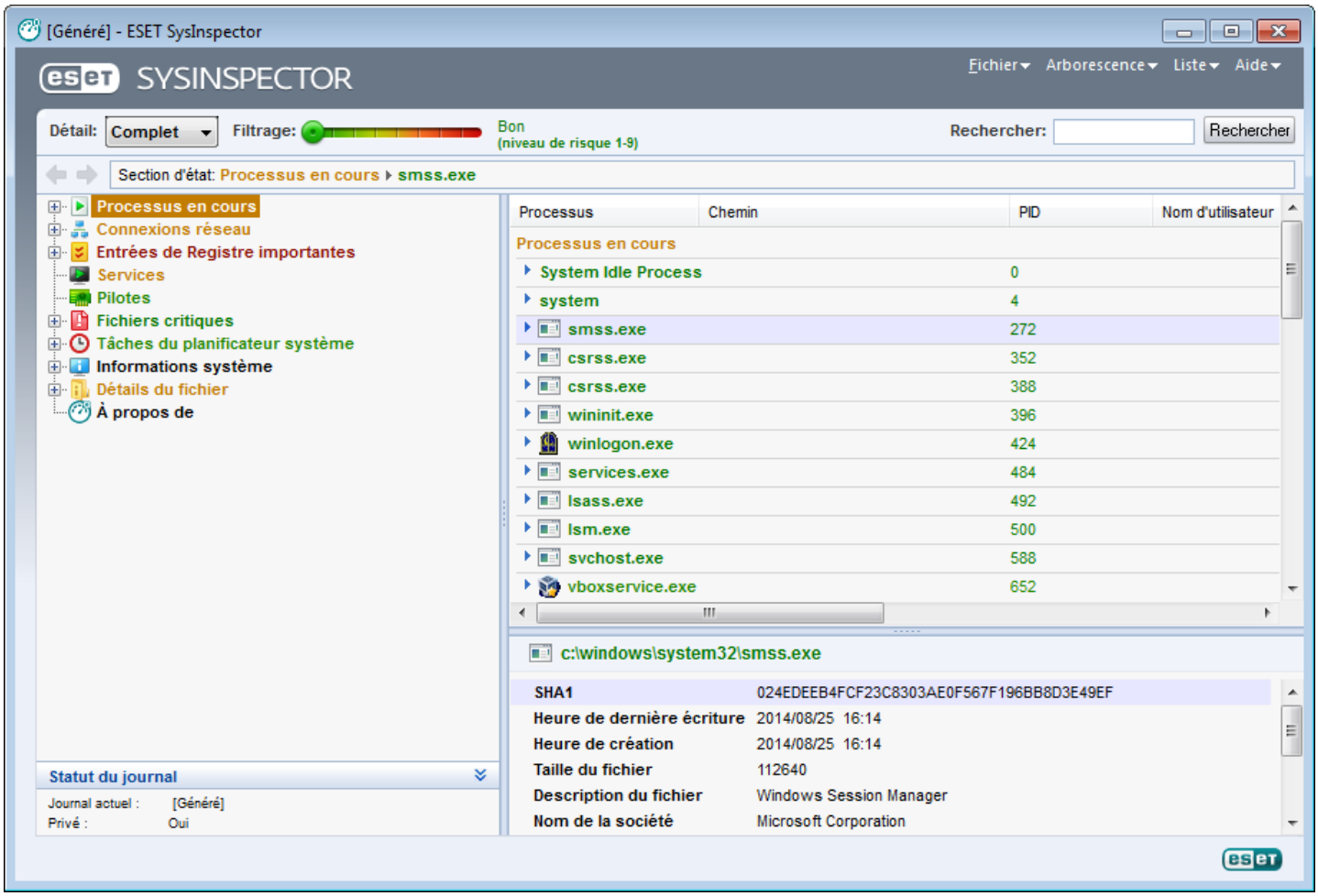
3.9.6.1.1 Démarrage d'ESET SysInspector

Pour démarrer ESET SysInspector, il suffit de lancer le fichier exécutable *SysInspector.exe* téléchargé depuis le site Web d'ESET. Si vous avez déjà installé une des solutions ESET Security, vous pouvez exécuter ESET SysInspector directement à partir du menu Démarrer (cliquez sur **Programmes** > **ESET** > **ESET Endpoint Security**).

Patientez pendant que l'application vérifie le système. Cette opération peut prendre plusieurs minutes.

3.9.6.2 Interface utilisateur et utilisation de l'application

Pour des raisons de clarté, la fenêtre principale du programme est divisée en quatre principales sections : la section des Contrôles du programme en haut, la fenêtre Navigation à gauche, la fenêtre Description à droite au centre et la fenêtre Détails au bas. La section État du journal énumère les paramètres de base d'un journal (utilisation des filtres, type de filtre, journal résultat d'une comparaison, etc.).



3.9.6.2.1 Contrôles du programme

Cette section contient la description de tous les contrôles du programme disponible dans ESET SysInspector.

Fichier

En cliquant sur l'option **Fichier**, vous pouvez enregistrer l'état actuel du système en vue d'une enquête ultérieure ou ouvrir un journal déjà enregistré. Pour la publication, il est conseillé de créer un journal **approprié pour envoi**. Sous cette forme, le journal omet les informations sensibles (nom d'utilisateur, nom d'ordinateur, nom de domaine, privilèges actuels de l'utilisateur, variables d'environnement, etc.).

REMARQUE : vous pouvez ouvrir des rapports enregistrés ESET SysInspector en les faisant glisser et en les déposant dans la fenêtre principale.

Arborescence

Permet de développer ou de réduire tous les nœuds et d'exporter les sections sélectionnées dans le script de service.

Liste

Contient des fonctions qui simplifient la navigation dans le programme, ainsi que d'autres fonctionnalités comme l'obtention d'informations en ligne.

Aide

Contient des informations sur l'application et ses fonctions.

Détails

Ce paramètre conditionne les informations affichées dans la fenêtre principale, ce qui simplifie leur utilisation. En mode de base, vous avez accès aux informations utilisées pour trouver les solutions aux problèmes communs dans votre système. En mode Moyen, le programme affiche moins de détails. En mode Complet, ESET SysInspector affiche toutes les informations nécessaires pour résoudre des problèmes très précis.

Filtrage

Le filtrage des éléments est particulièrement adapté à la recherche de fichiers suspects ou d'entrées de registre dans le système. En déplaçant le curseur, vous pouvez filtrer les éléments en fonction de leur niveau de risque. Quand le curseur est en position maximale vers la gauche (niveau de risque 1), tous les éléments sont affichés. En déplaçant le curseur vers la droite, l'application filtre tous les éléments dont le risque est inférieur au niveau de risque actuel et affiche uniquement les éléments plus suspects (dont le niveau est plus élevé que celui affiché). Si le curseur est en position maximale à droite, le programme affiche uniquement les éléments nuisibles connus.

Tous les éléments portant le niveau de risque 6 à 9 peuvent poser un risque pour la sécurité. Si vous n'utilisez pas de solution de sécurité d'ESET, nous vous conseillons d'analyser votre système à l'aide d'ESET Online Scanner si ESET SysInspector a détecté un élément de ce genre. ESET Online Scanner est un service gratuit.

REMARQUE : le niveau de risque d'un élément peut être rapidement déterminé grâce à la couleur que prend le curseur pour indiquer le niveau de risque.

Comparer

Lors de la comparaison de deux journaux, vous pouvez choisir d'afficher tous les éléments, uniquement les éléments ajoutés, uniquement les éléments supprimés ou uniquement les éléments remplacés.

Rechercher

La fonction de recherche permet de trouver rapidement un élément sur la base de son nom ou d'une partie de son nom. Les résultats de la recherche sont affichés dans la fenêtre Description.

Retour

En cliquant sur la flèche arrière ou avant, vous pouvez revenir aux informations affichées précédemment dans la fenêtre Description. Vous pouvez utiliser la touche de retour arrière et la barre d'espace au lieu de cliquer sur la flèche arrière ou avant.

Section d'état

Affiche le nœud actuel dans la fenêtre Navigation.

Important : les éléments surlignés en rouge sont inconnus et c'est la raison pour laquelle l'application les marque comme potentiellement dangereux. Si un élément est rouge, cela ne signifie pas automatiquement que vous pouvez supprimer le fichier. Avant de le supprimer, assurez-vous que les fichiers sont bel et bien dangereux ou qu'ils ne sont pas nécessaires.

3.9.6.2.2 Navigation dans ESET SysInspector

ESET SysInspector répartit divers types d'informations en plusieurs sections principales appelées nœuds. Le cas échéant, vous pouvez obtenir des détails complémentaires en développant chaque nœud afin d'afficher les sous-nœuds. Pour développer ou réduire un nœud, il suffit de double-cliquer sur son nom ou de cliquer sur ⊞ ou sur ⊟ en regard du nom du nœud. Quand vous parcourez l'arborescence des nœuds et des sous-nœuds dans la fenêtre de navigation, vous pouvez voir différents détails pour chaque nœud dans la fenêtre Description. Si vous parcourez les éléments de la fenêtre Description, des détails supplémentaires pour chaque élément peuvent être affichés dans la fenêtre Détails.

Voici les descriptions des principaux nœuds de la fenêtre Navigation et des informations qui s'y rapportent dans les fenêtres Description et Détails.

Processus en cours

Ce nœud comprend les informations sur les applications et les processus en cours d'exécution au moment de la création du journal. La fenêtre Détails comprend des détails complémentaires pour chaque processus tels que les bibliothèques dynamiques utilisées par les processus et leur emplacement dans le système, le nom de l'éditeur de l'application et le niveau de risque du fichier.

La fenêtre Détails contient des informations complémentaires sur les éléments sélectionnés dans la fenêtre Description telles que la taille du fichier ou son hachage.

REMARQUE : un système d'exploitation contient plusieurs noyaux importants qui fonctionnent en permanence et qui assurent des fonctions élémentaires et vitales pour d'autres applications utilisateur. Dans certains cas, ces processus sont repris dans l'outil ESET SysInspector avec un chemin d'accès au fichier commençant par \??\. Ces symboles garantissent l'optimisation préalable au lancement de ces processus ; ils ne présentent aucun danger pour le système.

Connexions réseau

La fenêtre Description contient la liste des processus et des applications qui communiquent via le réseau à l'aide du protocole sélectionné dans la fenêtre navigation (TCP ou UDP), ainsi que l'adresse distante à laquelle l'application est connectée. Vous pouvez également vérifier les adresses IP des serveurs DNS.

La fenêtre Détails contient des informations complémentaires sur les éléments sélectionnés dans la fenêtre Description telles que la taille du fichier ou son hachage.

Entrées de registre importantes

Contient la liste des entrées de registre sélectionnées qui sont souvent liées à des problèmes système. Il s'agit des entrées qui indiquent les applications de démarrage, les objets d'application d'assistance du navigateur, etc.

La fenêtre Description peut indiquer les fichiers en rapport avec les entrées de registre particulières. Vous pouvez voir des détails complémentaires dans la fenêtre Détails.

Services

La fenêtre Description contient la liste des fichiers enregistrés en tant que services Windows. Vous pouvez consulter la manière dont le service doit démarrer avec des détails spécifiques sur le fichier dans la fenêtre Détails.

Pilotes

Liste des pilotes installés sur le système.

Fichiers critiques

La fenêtre Description affiche le contenu des fichiers critiques liés au système d'exploitation Microsoft Windows.

Tâches du planificateur système

Contient une liste des tâches déclenchées par le planificateur de tâches Windows à une heure/un intervalle défini.

Informations système

Contient des informations détaillées sur le matériel et le logiciel, ainsi que des informations sur les variables d'environnement, les droits d'utilisateur et les journaux d'événements système définis.

Détails du fichier

Liste des fichiers système importants et des fichiers du dossier Program Files. Des informations complémentaires spécifiques sur les fichiers sont disponibles dans les fenêtres Description et Détails.

À propos de

Informations relatives à la version d'ESET SysInspector et liste des modules du programme.

3.9.6.2.2.1 Raccourcis clavier

Voici les raccourcis clavier disponibles dans ESET SysInspector :

Fichier

Ctrl+O	ouvre un journal existant
Ctrl+S	enregistre les journaux créés

Générer

Ctrl+G	génère un instantané standard du statut de l'ordinateur
Ctrl+H	génère un instantané du statut de l'ordinateur qui est susceptible de contenir des informations sensibles

Filtrage des éléments

1, O	affiche les éléments de niveau de risque 1 à 9 (acceptable)
2	affiche les éléments de niveau de risque 2 à 9 (acceptable)
3	affiche les éléments de niveau de risque 3 à 9 (acceptable)
4, U	affiche les éléments de niveau de risque 4 à 9 (inconnu)
5	affiche les éléments de niveau de risque 5 à 9 (inconnu)
6	affiche les éléments de niveau de risque 6 à 9 (inconnu)
7, B	affiche les éléments de niveau de risque 7 à 9 (risqué)
8	affiche les éléments de niveau de risque 8 à 9 (risqué)
9	affiche les éléments de niveau de risque 9 (risqué)
-	diminue le niveau de risque
+	augmente le niveau de risque
Ctrl+9	mode de filtrage, niveau égal ou supérieur
Ctrl+0	mode de filtrage, niveau égal uniquement

Afficher

Ctrl+5	afficher par éditeur, tous les éditeurs
Ctrl+6	afficher par éditeur, uniquement Microsoft
Ctrl+7	afficher par éditeur, tous les autres éditeurs
Ctrl+3	afficher tous les détails
Ctrl+2	afficher les détails de précision moyenne
Ctrl+1	affichage de base
Retour arrière	revient une étape en arrière
Barre d'espace	avance d'une étape
Ctrl+W	développe l'arborescence
Ctrl+Q	réduit l'arborescence

Autres commandes

Ctrl+T	accède à l'emplacement d'origine de l'élément après la sélection dans les résultats de recherche
Ctrl+P	affiche des informations élémentaires sur un élément
Ctrl+A	affiche des informations complètes sur un élément
Ctrl+C	copie l'arborescence de l'élément
Ctrl+X	copie les éléments
Ctrl+B	trouve des informations sur les fichiers sélectionnés sur Internet
Ctrl+L	ouvre le dossier où se trouve le fichier sélectionné.
Ctrl+R	ouvre l'entrée correspondante dans l'éditeur de registre
Ctrl+Z	copie un chemin d'accès à un fichier (si l'élément est lié à un fichier)
Ctrl+F	passe au champ de recherche
Ctrl+D	ferme les résultats de la recherche
Ctrl+E	exécute le script de service

Comparaison

Ctrl+Alt+O	ouvre le journal d'origine/de comparaison
Ctrl+Alt+R	annule la comparaison
Ctrl+Alt+1	affiche tous les éléments
Ctrl+Alt+2	affiche uniquement les éléments ajoutés ; le journal indique les éléments présents dans le journal actuel
Ctrl+Alt+3	affiche uniquement les éléments supprimés ; le journal indique les éléments présents dans le journal précédent
Ctrl+Alt+4	affiche uniquement les éléments remplacés (fichiers inclus)
Ctrl+Alt+5	affiche uniquement les différences entre les journaux
Ctrl+Alt+C	affiche la comparaison
Ctrl+Alt+N	affiche le journal actuel
Ctrl+Alt+P	ouvre le journal précédent

Divers

F1	afficher l'aide
Alt+F4	quitter l'application
Alt+Maj+F4	quitter l'application sans demander
Ctrl+I	statistiques du journal

3.9.6.2.3 Comparer

La fonctionnalité Comparer permet de comparer deux journaux. Cette fonctionnalité met en évidence les éléments qui ne sont pas communs aux deux journaux. Ce procédé est utile si vous souhaitez assurer le suivi des modifications dans le système. Vous pourrez peut-être ainsi détecter l'activité d'un code malveillant.

Après son lancement, l'application crée un journal qui apparaît dans une nouvelle fenêtre. Cliquez sur **Fichier** > **Enregistrer le journal** pour enregistrer le journal dans un fichier. Les fichiers journaux peuvent être ouverts et consultés ultérieurement. Pour ouvrir un journal existant, cliquez sur **Fichier** > **Ouvrir le journal**. Dans la fenêtre principale de l'application, ESET SysInspector affiche toujours un journal à la fois.

Le fait de comparer deux journaux permet d'afficher le journal actif et un journal enregistré dans un fichier. Pour comparer des journaux, cliquez sur **Fichier** > **Comparer les journaux**, puis choisissez **Sélectionner un fichier**. Le journal sélectionné est comparé au journal actif dans les fenêtres principales de l'application. Le journal résultant, appelé journal des comparaisons, affiche uniquement les différences entre les deux journaux.

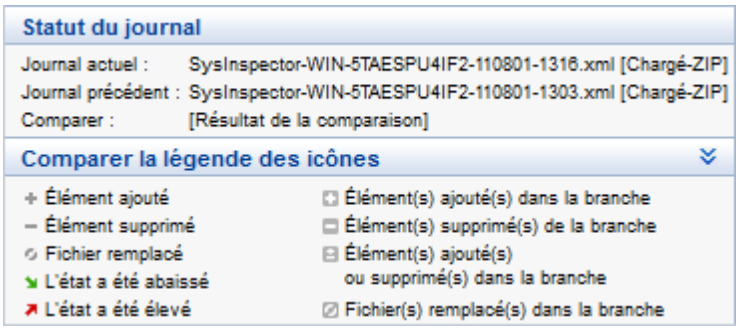
REMARQUE : si vous comparez deux fichiers journaux, cliquez sur **Fichier** > **Enregistrer le journal** et enregistrez-le dans un fichier ZIP. Les deux fichiers sont enregistrés. Si vous ouvrez ce fichier ultérieurement, les journaux qu'il contient seront comparés automatiquement.

En regard des éléments affichés, ESET SysInspector ajoute des symboles qui identifient les différences entre les journaux comparés.

Description de tous les symboles qui peuvent être affichés à côté des éléments :

- + nouvelle valeur, absente du journal précédent.
- cette section de l'arborescence contient de nouvelles valeurs.
- – valeur supprimée, présente uniquement dans le journal précédent.
- cette section de l'arborescence contient des valeurs supprimées.
- valeur/fichier modifié.
- cette section de l'arborescence contient des valeurs/fichiers modifiés.
- le niveau de risque a diminué/était supérieur dans le journal précédent.
- le niveau de risque a augmenté/il était inférieur dans le journal précédent.

La section d'explication affichée dans le coin inférieur gauche décrit tous les symboles et affiche le nom des journaux comparés.



Les journaux de comparaison peuvent être enregistrés dans un fichier et ouverts ultérieurement :

Exemple

Créez un journal reprenant les informations d'origine du système et enregistrez-le dans un fichier appelé précédent.xml. Après avoir modifié le système, ouvrez ESET SysInspector pour qu'il crée un nouveau journal. Enregistrez ce journal sous le nom *actuel.xml*.

Pour voir les différences entre ces deux journaux, cliquez sur **Fichier** > **Comparer les journaux**. Le programme crée un journal de comparaison qui indique les différences entre les journaux.

Un résultat identique peut être obtenu si vous utilisez l'option de ligne de commande suivante :

SysIsnpector.exe actuel.xml précédent.xml

3.9.6.3 Paramètres de la ligne de commande

ESET SysInspector prend en charge la création de rapports via la ligne de commande à l'aide de ces paramètres :

/gen	générer le journal directement à partir de la ligne de commande sans exécuter la GUI
/privacy	générer le journal en omettant les informations sensibles
/zip	enregistrer le journal des résultats dans une archive compressée au format zip
/silent	supprimer la fenêtre de progression durant la génération du journal à partir de la ligne de commande
/blank	lance ESET SysInspector sans générer/charger de journal

Exemples

Utilisation :

```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

Pour charger un journal en particulier directement dans le navigateur, saisissez : *SysInspector.exe .\clientlog.xml*
Pour générer le journal depuis la ligne de commande, saisissez : *SysInspector.exe /gen=.\mynewlog.xml*
Pour générer un journal qui exclut les informations sensibles directement dans un fichier compressé, saisissez : *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Pour comparer deux fichiers journaux et parcourir leurs différences, saisissez : *SysInspector.exe new.xml old.xml*

REMARQUE : si le nom du fichier/dossier contient un espace, saisissez-le entre guillemets.

3.9.6.4 Script de service

Le script de service supprime très facilement les objets indésirables du système et offre une aide aux clients qui utilisent ESET SysInspector.

Le script de service permet à l'utilisateur d'exporter l'ensemble du journal ESET SysInspector ou certaines parties sélectionnées. Après l'exportation, vous pouvez marquer les objets non souhaités pour la suppression. Vous pouvez ensuite exécuter le journal modifié pour supprimer les objets marqués.

Le script de service convient aux utilisateurs expérimentés qui connaissent les problèmes des systèmes de diagnostic. Des modifications erronées pourraient endommager le système d'exploitation.

Exemple

Si vous pensez que votre ordinateur est infecté par un virus qui n'est pas détecté par votre logiciel antivirus, suivez les instructions ci-après :

1. Exécutez ESET SysInspector pour obtenir un nouvel instantané du système.
2. Sélectionnez le premier élément de la section à gauche (dans l'arborescence), appuyez sur la touche Maj et maintenez-la enfoncée, puis sélectionnez le dernier élément afin de marquer tous les éléments.
3. Cliquez à l'aide du bouton droit sur les objets sélectionnés et sélectionnez **Exporter les sections sélectionnées dans un script de service**.
4. Les objets sélectionnés sont exportés dans un nouveau journal.
5. Il s'agit de l'étape la plus importante de toute la procédure : ouvrez le nouveau journal et remplacez l'attribut - par + pour tous les objets que vous souhaitez supprimer. Assurez-vous que vous n'avez sélectionné aucun objet/fichier important pour le système d'exploitation.
6. Ouvrez ESET SysInspector, cliquez sur **Fichier** > **Exécuter le script de services** et entrez le chemin d'accès au script.
7. Cliquez sur **OK** pour lancer le script.

3.9.6.4.1 Création d'un script de service

Pour créer un script, cliquez avec le bouton droit de la souris sur n'importe quel élément de l'arborescence de menus (dans le volet de gauche) dans la fenêtre principale de ESET SysInspector. Dans le menu contextuel, choisissez l'option **Exporter toutes les sections dans un script de service** ou **Exporter les sections sélectionnées dans un script de service**.

REMARQUE : il est impossible d'exporter le script de service lorsque deux journaux sont comparés.

3.9.6.4.2 Structure du script de service

La première ligne de l'en-tête du script reprend des informations sur la version du moteur (ev), la version de l'interface utilisateur graphique (gv) et la version du journal (lv). Ces données permettent d'identifier d'éventuelles modifications dans le fichier .xml qui génère le script et d'éviter toute incohérence durant l'exécution. Cette partie du script ne peut pas être modifiée.

Le reste du fichier est scindé en sections dont les éléments peuvent être modifiés (elles indiquent les éléments qui sont traités par le script). Pour marquer un élément à traiter, remplacez le caractère « - » qui le précède par « + ». Les sections du script sont séparées par une ligne vide. Chaque section possède un numéro et un titre.

01) Running processes (processus en cours)

Cette section contient la liste de tous les processus en cours d'exécution dans le système. Chaque processus est identifié par son chemin UNC, puis par son code de hachage CRC16 entre astérisques (*).

Exemple :

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Dans cet exemple, un processus, à savoir module32.exe, a été sélectionné (marqué par le caractère « + ») ; le

processus s'arrête à l'exécution du script.

02) Loaded modules (modules chargés)

Cette section répertorie la liste des modules système en cours d'utilisation :

Exemple :

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Dans cet exemple, le module khbekhb.dll a été marqué par un « + ». Quand le script est exécuté, il reconnaît les processus qui utilisent ce module et les arrête.

03) TCP connections (connexions TCP)

Cette section contient des informations sur les connexions TCP existantes.

Exemple :

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Lorsque le script est exécuté, il localise le propriétaire du socket dans les connexions TCP marquées et arrête le socket, ce qui libère des ressources système.

04) UDP endpoints (points de terminaison UDP)

Cette section contient des informations sur les points de terminaison UDP existants.

Exemple :

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Lorsque le script est exécuté, il isole le propriétaire du socket aux points de terminaison UDP marqués et arrête le socket.

05) DNS server entries (entrées du serveur DNS)

Cette section contient des informations sur la configuration actuelle du serveur DNS.

Exemple :

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Les entrées du serveur DNS marquées sont supprimées à l'exécution du script.

06) Important registry entries (entrées de registre importantes)

Cette section contient des informations relatives aux entrées de registre importantes.

Exemple :

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Les entrées marquées sont supprimées, réduites à des valeurs de 0 octet ou réinitialisées sur leur valeur par défaut lors de l'exécution du script. L'action à appliquer sur chaque entrée dépend de la catégorie de l'entrée et de la valeur de la clé dans ce registre.

07) Services (services)

Cette section répertorie les services enregistrés dans le système.

Exemple :

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Les services marqués et les services dépendants sont arrêtés et désinstallés après l'exécution du script.

08) Drivers (pilotes)

Cette section répertorie les pilotes installés.

Exemple :

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Lorsque vous exécutez le script, les pilotes sélectionnés sont arrêtés. Notez que certains pilotes ne se laisseront pas arrêter.

09) Critical files (fichiers critiques)

Cette section contient des informations sur les fichiers essentiels au bon fonctionnement du système d'exploitation.

Exemple :

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Les éléments sélectionnés sont soit supprimés, soit restaurés sur leur valeur d'origine.

3.9.6.4.3 Exécution des scripts de services

Marquez tous les éléments souhaités, puis enregistrez et fermez le script. Exécutez le script modifié directement depuis la fenêtre principale ESET SysInspector en choisissant l'option **Exécuter le script de services** dans le menu Fichier. Lorsque vous ouvrez un script, le programme affiche le message suivant : **Voulez-vous vraiment exécuter le script de service « %Scriptname% » ??** Une fois que vous avez confirmé votre sélection, un autre avertissement peut apparaître pour vous indiquer que le script de service que vous essayez d'exécuter n'a pas été signé. Cliquez sur **Exécuter** pour lancer le script.

Une boîte de dialogue confirme l'exécution correcte du script.

Si le script n'a pu être traité que partiellement, une boîte de dialogue avec le message suivant apparaît : **Le script de service n'a été exécuté que partiellement. Voulez-vous afficher le rapport d'erreurs ?** Choisissez **Oui** pour afficher un rapport des erreurs complexe qui répertorie les opérations qui n'ont pas été exécutées.

Si le script n'a pas été reconnu, une boîte de dialogue apparaît avec le message suivant : **Le script de service sélectionné n'est pas signé. L'exécution de scripts non signés et inconnus peut endommager gravement les données de votre ordinateur. Voulez-vous vraiment exécuter le script et ses actions ?** Ceci peut être le résultat d'incohérences au sein du script (en-tête ou titre de section endommagé, ligne vide manquante entre les sections, etc.). Vous pouvez soit rouvrir le fichier de script et corriger les erreurs qu'il contient, soit créer un autre script de service.

3.9.6.5 FAQ

L'exécution d'ESET SysInspector requiert-elle des privilèges d'administrateur ?

Bien qu'ESET SysInspector puisse être exécuté sans privilèges d'administrateur, certaines des informations qu'il recueille peuvent être consultées uniquement via un compte administrateur. Une exécution en tant qu'utilisateur standard ou utilisateur disposant d'un accès restreint entraîne la collecte d'un volume inférieur d'informations sur l'environnement d'exploitation.

ESET SysInspector crée-t-il un fichier journal ?

ESET SysInspector peut créer un fichier journal sur la configuration de votre ordinateur. Pour en enregistrer un, dans la fenêtre principale du programme, cliquez sur **Fichier** > **Enregistrer le journal**. Les journaux sont enregistrés au format XML. Par défaut, les fichiers sont enregistrés dans le répertoire *%USERPROFILE%\Mes documents*, conformément à la convention de dénomination de fichier « SysInpsector-%COMPUTERNAME%-AAMMJJ-HHMM.XML ». Vous pouvez changer l'emplacement et le nom du fichier avant de l'enregistrer si vous le souhaitez.

Comment puis-je consulter le fichier journal d'ESET SysInspector ?

Pour consulter un fichier journal créé par ESET SysInspector, exécutez le programme et choisissez **Fichier** > **Ouvrir le journal** dans la fenêtre principale du programme. Vous pouvez également faire glisser les fichiers journaux et les déposer sur l'application ESET SysInspector. Si vous devez consulter fréquemment les fichiers journaux ESET

SysInspector, il est conseillé de créer un raccourci vers le fichier SYSINSPECTOR.exe sur le Bureau ; vous pourrez ensuite faire glisser les fichiers et les déposer sur ce raccourci. Pour des raisons de sécurité, Windows Vista/7 peuvent désactiver la fonction glisser-déposer entre des fenêtres dont les autorisations diffèrent.

Existe-t-il une spécification pour le format de fichier journal ? Existe-t-il un kit de développement logiciel (SDK) ?

Pour l'instant, il n'existe ni spécifications pour le fichier journal ni SDK, car le programme est toujours au stade du développement. Après la sortie du programme, nous fournirons ces éléments sur la base des commentaires et des demandes des clients.

Comment ESET SysInspector évalue-t-il le risque que pose un objet en particulier ?

Dans la majorité des cas, ESET SysInspector attribue des niveaux de risque aux objets (fichiers, processus, clés de registre, etc.) sur la base d'une série de règles heuristiques qui examinent les caractéristiques de chaque objet, puis qui évaluent le potentiel d'activité malveillante. Cette analyse heuristique attribue aux objets un niveau de risque allant de 1 - OK (vert) à 9 - Risqué (rouge). Dans le volet de navigation gauche, la couleur des sections est définie par le niveau de risque le plus élevé d'un des objets qu'elles contiennent.

Un niveau de risque « 6 - Inconnu (rouge) » signifie-t-il que l'objet est dangereux ?

Les évaluations d'ESET SysInspector ne garantissent pas qu'un objet est malveillant. Cette réponse doit être apportée par l'expert en sécurité. ESET SysInspector a été développé pour fournir aux experts en sécurité une évaluation rapide afin qu'ils puissent identifier les objets d'un système qui devront faire l'objet d'un examen plus approfondi en cas de comportement étrange.

Pourquoi ESET SysInspector se connecte-t-il à Internet ?

À l'instar de nombreuses applications, ESET SysInspector possède un « certificat » avec signature numérique qui permet de garantir que le logiciel a bien été diffusé par ESET et qu'il n'a pas été modifié. Afin de vérifier le certificat, le système d'exploitation contacte une autorité de certification pour confirmer l'identité de l'éditeur de logiciels. Il s'agit d'un comportement normal pour tous les programmes avec signature numérique sous Microsoft Windows.

Qu'est-ce que la technologie Anti-Stealth ?

La technologie Anti-Stealth permet de détecter avec efficacité les rootkits.

Quand un système est attaqué par un code malveillant qui se comporte comme un rootkit, l'utlisateur risque de voir ses données endommagées ou volées. Sans outil spécial de lutte contre les rootkits, il est pratiquement impossible de les détecter.

Pourquoi y a-t-il parfois des fichiers marqués comme « Signé par MS » avec une valeur différente dans le champ « Nom de la société » ?

Lorsqu'ESET SysInspector tente d'identifier la signature numérique d'un fichier exécutable, il vérifie d'abord si une signature numérique est intégrée au fichier. Si c'est le cas, le fichier est validé avec ces informations. Si le fichier ne contient pas de signature numérique, ESI lance la recherche du fichier CAT correspondant (Catalogue de sécurité - *%systemroot%\system32\catroot*) qui contient des informations sur le fichier exécutable traité. Si le fichier CAT pertinent est trouvé, sa signature numérique est appliquée dans la procédure de validation du fichier exécutable.

Voilà pourquoi des fichiers sont parfois marqués « Signé par MS » mais ont un « Nom de la société » différent.

3.9.6.6 ESET SysInspector en tant que composant de ESET Endpoint Security

Pour ouvrir la section ESET SysInspector dans ESET Endpoint Security, cliquez sur **Outils** > **ESET SysInspector**. Le système de gestion disponible dans la fenêtre ESET SysInspector est semblable à celui des journaux d'analyse des ordinateurs ou des tâches planifiées. Toutes les opérations effectuées avec des instantanés système (création, affichage, comparaison, suppression et exportation) sont accessibles en un ou deux clics.

La fenêtre ESET SysInspector contient les informations élémentaires concernant les instantanés créés : heure de création, bref commentaire, nom de l'utilisateur auteur de l'instantané et statut de l'instantané.

Pour comparer, créer ou supprimer des instantanés, utilisez les boutons correspondants situés en dessous de la liste des instantanés dans la fenêtre ESET SysInspector. Ces options sont également disponibles dans le menu contextuel. Pour afficher l'instantané du système sélectionné, sélectionnez l'option **Afficher** dans le menu contextuel. Pour exporter l'instantané sélectionné dans un fichier, cliquez dessus avec le bouton droit de la souris et sélectionnez **Exporter...**

Voici la description détaillée des options disponibles :

- La fonctionnalité **Comparer** permet de comparer deux journaux. Elle est particulièrement adaptée si vous souhaitez effectuer le suivi des modifications entre le journal actuel et un ancien journal. Pour que cette option entre en vigueur, vous devez sélectionner deux instantanés à comparer.
- **Créer...** - Crée un enregistrement. Vous devez d'abord saisir un bref commentaire concernant l'enregistrement. Pour consulter le pourcentage de progression de la création de l'instantané en cours, consultez la colonne **État**. Tous les instantanés générés présentent l'état **Créé**.
- **Supprimer/Supprimer tout** - Supprime les entrées de la liste.
- **Exporter...** - Cette option enregistre l'entrée sélectionnée dans un fichier XML (également dans une version compressée).

3.10 Glossaire

3.10.1 Types de menaces

Une infiltration est un élément de logiciel malveillant qui tente de s'introduire dans l'ordinateur d'un utilisateur et/ou de l'endommager.

3.10.1.1 Virus

Un virus d'ordinateur est un fragment de code malveillant qui est ajouté à des fichiers qui sont sur votre ordinateur. Les virus informatiques sont comparables aux virus biologiques parce qu'ils utilisent des techniques similaires pour se propager d'un ordinateur à l'autre. Le terme « virus » est quant à lui souvent utilisé de manière abusive pour décrire tout type de menace. On tend à le remplacer progressivement par le terme « logiciel malveillant » ou « malware » en anglais.

Les virus informatiques attaquent principalement les fichiers et documents exécutables. En bref, un virus informatique fonctionne de la manière suivante : après l'exécution d'un fichier infecté, le code malveillant est appelé et exécuté avant l'exécution de l'application originale. Un virus peut infecter tous les fichiers pour lesquels l'utilisateur a des droits d'écriture.

Les virus peuvent varier en fonction de leur gravité et de leur cible. Certains sont extrêmement dangereux parce qu'ils ont la capacité de supprimer délibérément des fichiers du disque dur. D'autres, en revanche, ne causent pas de réels dommages : ils ne servent qu'à gêner l'utilisateur et à démontrer les compétences techniques de leurs auteurs.

Si votre ordinateur est infecté par un virus et qu'il est impossible de le nettoyer, soumettez-le au laboratoire d'ESET pour examen. Dans certains cas, les fichiers infectés peuvent avoir subi des modifications telles, qu'il est impossible de les nettoyer. Il faut alors les remplacer par une copie propre.

3.10.1.2 Vers

Un ver est un programme contenant un code malveillant qui attaque les ordinateurs hôtes et se propage via un réseau. La différence fondamentale entre les virus et les vers réside dans le fait que les vers ont la capacité de se propager par eux-mêmes. Ils ne dépendent pas des fichiers hôtes (ou des secteurs d'amorçage). Les vers se propagent par l'intermédiaire des adresses de messagerie de votre liste de contacts ou exploitent les vulnérabilités de sécurité des applications réseau.

Les vers sont ainsi susceptibles de vivre beaucoup plus longtemps que les virus. Par le biais d'Internet, ils peuvent se propager à travers le monde en quelques heures seulement et parfois en quelques minutes. Leur capacité à se répliquer indépendamment et rapidement les rend plus dangereux que les autres types de programmes malveillants.

Un ver activé dans un système peut être à l'origine de plusieurs dérèglements : il peut supprimer des fichiers, dégrader les performances du système ou même désactiver certains programmes. Par nature, il peut servir de « moyen de transport » à d'autres types d'infiltrations.

Si votre ordinateur est infecté par un ver, il est recommandé de supprimer les fichiers infectés, car ils contiennent probablement du code malveillant.

3.10.1.3 Chevaux de Troie

Les chevaux de Troie ont été définis comme une catégorie de menaces dont la particularité est de se présenter comme des programmes utiles pour duper ensuite les utilisateurs qui acceptent de les exécuter.

La catégorie étant très vaste, elle est souvent divisée en plusieurs sous-catégories :

- **Téléchargeur** - Programmes malveillants qui sont en mesure de télécharger d'autres menaces sur Internet.
- **Dropper** - Programmes malveillants qui sont en mesure de déposer d'autres types de logiciels malveillants sur des ordinateurs infectés.
- **Backdoor** - Programmes malveillants qui communiquent avec des attaquants distants, leur permettant d'accéder à l'ordinateur et d'en prendre le contrôle.
- **Keylogger** - Programme qui enregistre chaque touche sur laquelle tape l'utilisateur et envoie les informations aux pirates.
- **Composeur** - Programmes malveillants destinés à se connecter à des numéros surtaxés au lieu du fournisseur de services Internet de l'utilisateur. Il est presque impossible qu'un utilisateur remarque la création d'une nouvelle connexion. Les composeurs ne peuvent porter préjudice qu'aux utilisateurs ayant des modems par ligne commutée, qui sont de moins en moins utilisés.

Si un fichier est identifié comme cheval de Troie sur votre ordinateur, il est recommandé de le supprimer, car il est fort probable qu'il ne contienne rien d'autre que du code malveillant.

3.10.1.4 Rootkits

Les rootkits sont des programmes malveillants qui procurent aux pirates un accès illimité à un système tout en dissimulant leur présence. Après avoir accédé au système (généralement en exploitant une faille), les rootkits utilisent des fonctions du système d'exploitation pour se protéger des logiciels antivirus : ils dissimulent des processus, des fichiers et des données de la base de registre Windows. Pour cette raison, il est presque impossible de les détecter à l'aide des techniques de test ordinaires.

Il existe deux niveaux de détection permettant d'éviter les rootkits :

1. Lorsqu'ils essaient d'accéder au système : Ils ne sont pas encore installés et donc inactifs. La plupart des antivirus sont en mesure d'éliminer les rootkits à ce niveau (en supposant qu'ils détectent effectivement les fichiers comme infectés).

2. Lorsqu'ils sont inaccessibles aux tests habituels : Les utilisateurs ESET Endpoint Security bénéficient de la technologie Anti-Stealth qui permet de détecter et d'éliminer les rootkits en activité.

3.10.1.5 Logiciels publicitaires

Le terme anglais « adware » désigne les logiciels soutenus par la publicité. Les programmes qui affichent des publicités entrent donc dans cette catégorie. Les logiciels publicitaires ouvrent généralement une nouvelle fenêtre contextuelle automatiquement dans un navigateur Internet. Cette fenêtre contient de la publicité ou modifie la page de démarrage du navigateur. Ils sont généralement associés à des programmes gratuits et permettent aux développeurs de couvrir les frais de développement de leurs applications (souvent utiles).

Les logiciels publicitaires en tant que tels ne sont pas dangereux ; ils dérangent simplement les utilisateurs en affichant des publicités. Le danger réside dans le fait qu'ils peuvent également avoir des fonctions d'espionnage (comme les logiciels espions).

Si vous décidez d'utiliser un logiciel gratuit, soyez particulièrement attentif au programme d'installation. La plupart des programmes d'installation vous avertissent en effet qu'ils installent également un programme publicitaire. Dans la plupart des cas, vous pourrez désactiver cette installation supplémentaire et installer le programme sans logiciel publicitaire.

Certains programmes refusent de s'installer sans leur logiciel publicitaire ou voient leurs fonctionnalités limitées. Cela signifie que les logiciels publicitaires accèdent souvent au système de manière « légale », dans la mesure où les utilisateurs l'ont accepté. Dans ce cas, il est préférable de procéder avec prudence. Si un logiciel publicitaire est détecté sur votre ordinateur, il est conseillé de le supprimer, car il est fort probable qu'il contienne du code malveillant.

3.10.1.6 Logiciels espions

Cette catégorie englobe toutes les applications qui envoient des informations confidentielles sans le consentement des utilisateurs et à leur insu. Les logiciels espions utilisent des fonctions de traçage pour envoyer diverses données statistiques telles que la liste des sites Web visités, les adresses e-mail de la liste de contacts de l'utilisateur ou la liste des touches du clavier utilisées.

Les auteurs de ces logiciels espions affirment que ces techniques ont pour but d'en savoir plus sur les besoins et intérêts des utilisateurs afin de mieux cibler les offres publicitaires. Le problème est qu'il n'y a pas de distinction claire entre les applications utiles et les applications malveillantes, et que personne ne peut garantir que les informations récupérées ne sont pas utilisées à des fins frauduleuses. Les données récupérées par les logiciels espions peuvent être des codes de sécurité, des codes secrets, des numéros de compte bancaire, etc. Les logiciels espions sont souvent intégrés aux versions gratuites d'un programme dans le but de générer des gains ou d'inciter à l'achat du logiciel. Les utilisateurs sont souvent informés de la présence d'un logiciel espion au cours de l'installation d'un programme qui vise à les inciter à acquérir la version payante qui en est dépourvue.

Parmi les produits logiciels gratuits bien connus qui contiennent des logiciels espions, on trouve les applications clients de réseaux P2P (poste à poste). Spyfalcon ou Spy Sheriff (et beaucoup d'autres) appartiennent à une sous-catégorie spécifique de logiciels espions : ils semblent être des programmes antispyware alors qu'ils sont en réalité eux-mêmes des logiciels espions.

Si un fichier est détecté comme logiciel espion sur votre ordinateur, il est préférable de le supprimer, car il est fort probable qu'il contienne du code malveillant.

3.10.1.7 Compresseurs

Le compresseur est un fichier exécutable auto-extractible qui regroupe plusieurs genres de programmes malveillants dans un seul package.

Les compresseurs les plus courants sont UPX, PE_Compact, PKLite et ASPack. Le même programme malveillant peut être détecté différemment lorsqu'il est compressé à l'aide d'un compresseur différent. Les compresseurs sont capables de faire muter leur « signature » au fil du temps, les programmes malveillants deviennent ainsi plus difficiles à détecter et à supprimer.

3.10.1.8 Applications potentiellement dangereuses

Il existe de nombreux programmes authentiques qui permettent de simplifier l'administration des ordinateurs en réseau. Toutefois, s'ils tombent entre de mauvaises mains, ces programmes sont susceptibles d'être utilisés à des fins malveillantes. ESET Endpoint Security permet de détecter ces menaces.

Applications potentiellement dangereuses est la classification utilisée pour les logiciels commerciaux légitimes. Cette classification comprend les programmes d'accès à distance, les applications de résolution de mot de passe ou les keyloggers (programmes qui enregistrent chaque frappe au clavier de l'utilisateur).

Si vous découvrez qu'une application potentiellement dangereuse est présente et fonctionne sur votre ordinateur (sans que vous ne l'ayez installée), consultez l'administrateur réseau ou supprimez l'application.

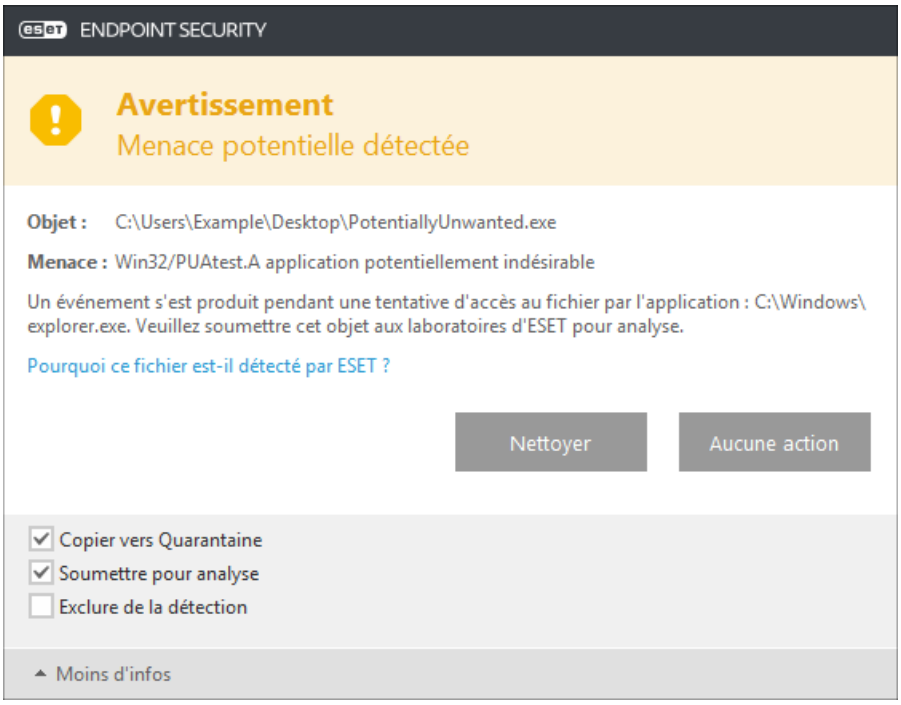
3.10.1.9 Applications potentiellement indésirables

Une application potentiellement indésirable est un programme qui contient un logiciel publicitaire, qui installe des barres d'outils ou dont les objectifs ne sont pas clairs. Dans certains cas, un utilisateur peut estimer que les avantages offerts par une application potentiellement 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 (chevaux de Troie ou vers, par exemple).

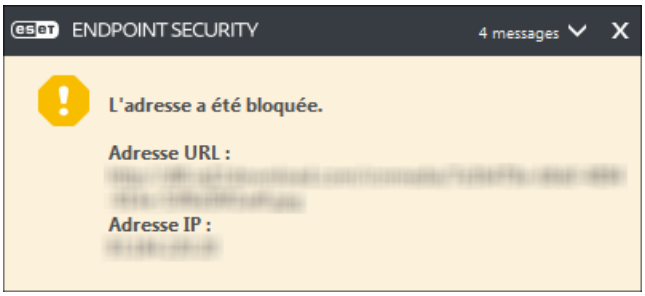
Avertissement - Menace potentielle détectée

Lorsqu'une application potentiellement indésirable est détectée, vous pouvez choisir l'action à exécuter :

1. **Nettoyer/Déconnecter** : cette option met fin à l'action et empêche la menace potentielle de pénétrer dans le système.
2. **Aucune action** : cette option permet à une menace potentielle de pénétrer dans le système.
3. Pour permettre l'exécution future de l'application sur votre ordinateur sans interruption, cliquez sur **Plus d'infos/Afficher les options avancées**, puis cochez la case en regard de l'option **Exclure de la détection**.

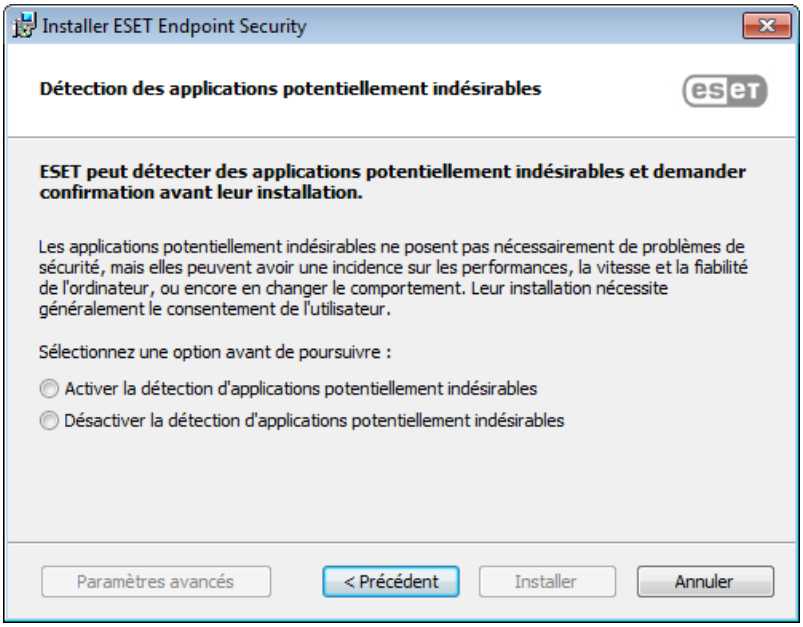


Lorsqu'une application potentiellement indésirable est détectée et qu'il n'est pas possible de procéder au nettoyage, la fenêtre de notification **L'adresse a été bloquée** s'affiche dans le coin inférieur droit de l'écran. Pour obtenir plus d'informations sur cet événement, accédez à **Outils** > **Fichiers journaux** > **Sites Web filtrés** à partir du menu principal.



Applications potentiellement indésirables - Paramètres

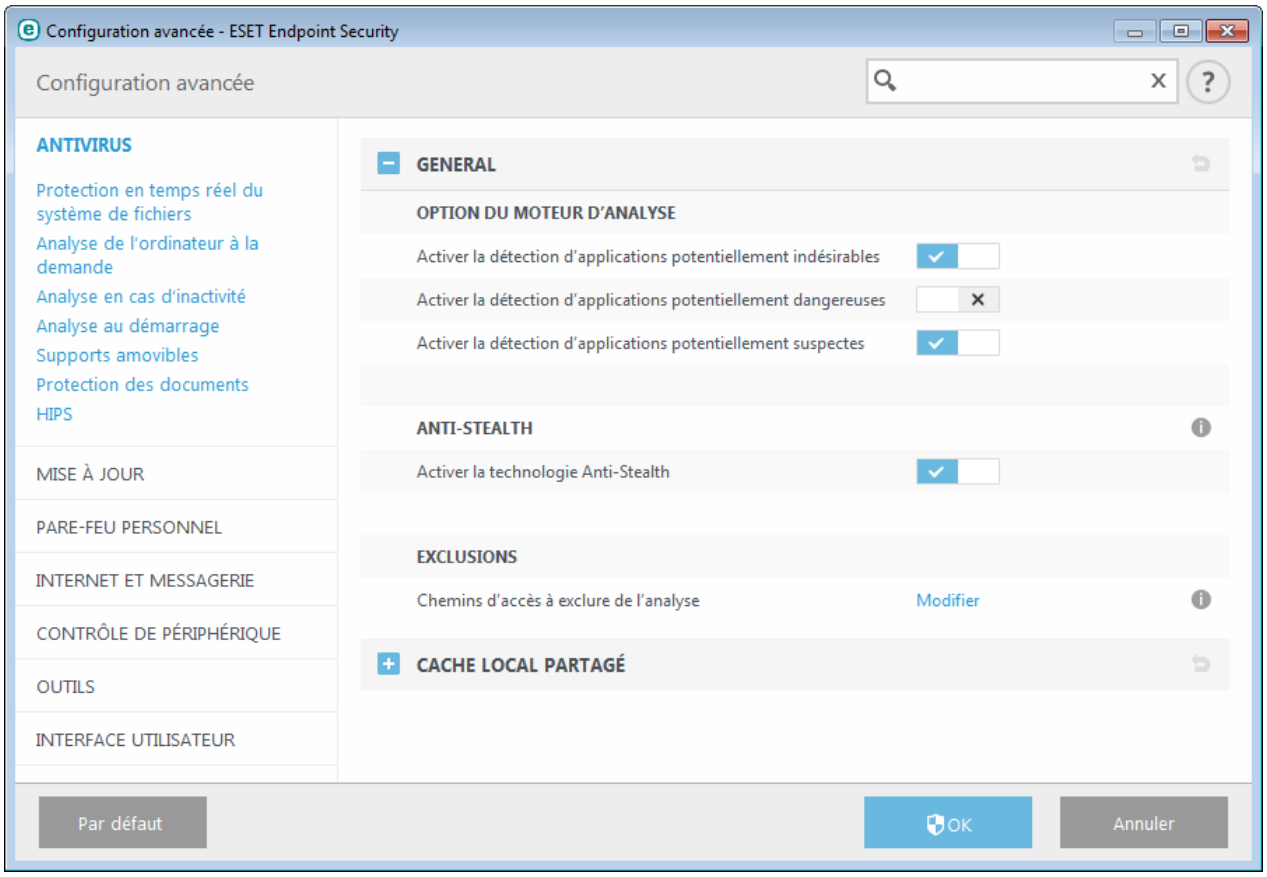
Lorsque vous installez votre produit ESET, vous pouvez choisir d'activer ou non la détection des applications potentiellement indésirables, comme illustré ci-dessous.



Les applications potentiellement indésirables peuvent installer des logiciels publicitaires et des barres d'outils ou contenir d'autres fonctionnalités indésirables ou dangereuses.

Ces paramètres peuvent être modifiés à tout moment dans les paramètres du programme. Pour activer ou désactiver la détection des applications potentiellement indésirables, dangereuses ou suspectes, procédez comme suit :

1. Ouvrez votre produit ESET. Comment ouvrir mon produit ESET ?
2. Appuyez sur la touche **F5** pour accéder à **Configuration avancée**.
3. Cliquez sur **Antivirus**, puis activez ou désactivez les options **Activer la détection des applications potentiellement indésirables**, **Activer la détection d'applications potentiellement dangereuses** et **Activer la détection d'applications potentiellement suspectes**, selon vos préférences. Cliquez ensuite sur **OK** pour confirmer.



Applications potentiellement indésirables - Wrappers logiciels

Un wrapper logiciel est un type spécial de modification d'application qui est utilisé par certains sites Web d'hébergement de fichiers. Il s'agit d'un outil tiers qui installe le programme que vous avez téléchargé tout en ajoutant d'autres logiciels comme des barres d'outils ou des logiciels publicitaires. Les autres logiciels peuvent également apporter des modifications à la page d'accueil de votre navigateur Web et aux paramètres de recherche. De plus, les sites Web d'hébergement de fichiers n'avertissent pas l'éditeur ou le destinataire du téléchargement que des modifications ont été apportées et ne permettent pas de les annuler facilement. Pour ces raisons, ESET classe les wrappers logiciels comme un type d'application potentiellement indésirable afin que les utilisateurs puissent accepter ou non de les télécharger.

Consultez cet article de la base de données ESET pour une version mise à jour de cette page d'aide.

3.10.1.10 Botnet

Un bot ou robot Web est un programme malveillant automatisé qui analyse des blocs d'adresses réseau et infecte les ordinateurs vulnérables. Ce type de programme permet aux pirates de prendre le contrôle de nombreux ordinateurs simultanément et de les transformer en bots (également appelés zombies). Les pirates utilisent généralement des bots pour infecter un grand nombre d'ordinateurs. Ce grand groupe d'ordinateurs infectés est appelé botnet. Si votre ordinateur est infecté et devient membre d'un botnet, il peut être utilisé dans des attaques par déni de service distribué (DDoS) ainsi qu'exploité pour exécuter des tâches automatiques sur Internet, à votre insu (par exemple l'envoi de courrier indésirable, de virus ou le vol d'informations personnelles et privées, telles que des informations d'identification bancaires ou des numéros de carte de crédit).

3.10.2 Types d'attaques distantes

Il existe diverses techniques permettant à des pirates de mettre en péril des systèmes distants. Elles se divisent en plusieurs catégories.

3.10.2.1 Attaques de vers

Un ver est un programme contenant un code malveillant qui attaque les ordinateurs hôtes et se propage via un réseau. Les vers de réseau exploitent les failles de sécurité de diverses applications. Par le biais d'Internet, ils peuvent se propager à travers le monde en quelques heures seulement

La plupart des attaques de vers peuvent être évitées à l'aide des paramètres de sécurité par défaut du pare-feu. Il est également important de choisir le type de protection **Réseau public** dans les réseaux publics et de garder vos programmes et système d'exploitation à jour avec les correctifs de sécurité les plus récents.

3.10.2.2 Attaques DoS

L'attaque DoS, ou attaque par *déni de service*, vise à rendre un ordinateur ou un réseau indisponible pour ses utilisateurs. La communication entre les utilisateurs affectés est obstruée et ne peut plus continuer normalement. Les ordinateurs qui ont subi une attaque DoS doivent généralement redémarrer pour fonctionner correctement.

Dans la plupart des cas, le déni de service cible les serveurs Web et cherche à les rendre inutilisables pendant un certain temps.

3.10.2.3 Balayage de ports

Le balayage de ports permet de déterminer les ports ouverts sur un ordinateur ou un hôte du réseau. Le logiciel utilisé à cette fin s'appelle scanneur de ports.

Le port d'un ordinateur est un point virtuel qui traite les données entrantes et sortantes. C'est un point crucial pour la sécurité. Sur un réseau de grande taille, les informations collectées par le scanneur de ports peuvent permettre d'identifier les failles potentielles. Cette utilisation est bien sûr tout à fait légale.

Néanmoins, le balayage de ports est souvent utilisé par les pirates qui tentent de compromettre la sécurité. Ils envoient d'abord des paquets à chaque port. En fonction du type de réponse, ils parviennent à déterminer les ports qui sont utilisés. Si le balayage lui-même ne cause aucun dommage, cette activité peut révéler les failles potentielles et permettre aux pirates de prendre le contrôle d'ordinateurs distants.

Nous conseillons aux administrateurs du réseau de bloquer tous les ports non utilisés et de protéger ceux qui sont utilisés des accès non autorisés.

3.10.2.4 Empoisonnement DNS

En utilisant l'empoisonnement DNS, les pirates peuvent faire croire au serveur DNS de tout ordinateur que les fausses données qui leur sont transmises sont légitimes et authentiques. Ces fausses informations sont ensuite mises en cache pendant un certain temps, ce qui permet aux attaquants de réécrire les réponses DNS des adresses IP. De cette manière, les utilisateurs qui tentent d'accéder à des sites internet téléchargeront des virus ou des vers au lieu du contenu original de ces sites.

3.10.3 Courrier électronique

Le courrier électronique est une forme de communication moderne qui offre beaucoup d'avantages. Adaptable, rapide et direct, il a joué un rôle crucial dans l'expansion d'Internet au début des années 90.

Malheureusement, le grand anonymat des courriers électroniques et Internet a laissé libre champ aux activités illégales telles que le « spamming » (le fait d'envoyer des messages indésirables à un grand nombre de personnes). Les courriers indésirables comprennent les publicités indésirables, les canulars et les logiciels malveillants. Les désagréments et le danger augmentent, car l'envoi de tels messages ne coûte rien et les auteurs de courrier indésirable disposent de nombreux outils qui leur permettent de se procurer facilement de nouvelles adresses de messagerie. Par ailleurs, le volume et la variété du courrier indésirable ne facilitent pas la réglementation. Plus vous utilisez votre adresse de messagerie, plus vous augmentez la possibilité d'aboutir dans un moteur de base de données de courrier indésirable. Voici quelques conseils de prévention :

- Évitez de publier votre adresse de messagerie sur Internet.
- Ne donnez votre adresse de messagerie qu'à des personnes fiables.
- Évitez d'utiliser des pseudonymes communs : un pseudonyme compliqué est moins susceptible d'être traqué.
- Ne répondez pas au courrier indésirable qui est arrivé dans votre boîte de réception.
- Faites attention lorsque vous remplissez des formulaires sur Internet : soyez particulièrement attentif aux options du type « Oui, je voudrais recevoir des informations concernant... ».
- Utilisez des adresses de messagerie « spécialisées », par exemple une adresse pour votre travail, une autre pour communiquer avec vos amis, etc.
- Changez vos adresses de messagerie de temps en temps.
- Utilisez une solution antispam.

3.10.3.1 Publicités

La publicité via Internet est une des formes de publicité les plus en vogue. D'un point de vue marketing, la publicité présente plusieurs avantages : ses coûts sont minimes, elle est très directe et les messages sont transmis presque immédiatement. De nombreuses entreprises utilisent des outils de marketing par courrier électronique pour communiquer de manière efficace avec leurs clients et prospects.

Ce mode de publicité est légitime, car vous pourriez être intéressé par la réception d'informations commerciales sur certains produits. Toutefois, de nombreuses entreprises envoient des masses de messages commerciaux non sollicités. La publicité par e-mail dépasse alors les limites et devient du courrier indésirable, ou spam.

La quantité de messages publicitaires non sollicités est devenue un réel problème, car elle ne montre aucun signe de ralentissement. Les auteurs de messages non sollicités tentent souvent de déguiser le courrier indésirable sous des dehors de messages légitimes.

3.10.3.2 Canulars

Un canular (ou hoax) est un message propagé sur Internet. Il est envoyé généralement avec le courrier et parfois par des outils de communication tels que ICQ et Skype. Le message est souvent une blague ou une légende urbaine.

Les canulars essaient de provoquer chez les destinataires de la peur, de l'incertitude et du doute, les amenant à croire qu'un « virus indétectable » supprime tous les fichiers et récupère les mots de passe, ou effectue une activité nuisible sur leur système.

Certains canulars demandent aux destinataires de transmettre des messages à leurs contacts, ce qui a pour conséquence de propager les canulars. Même les téléphones portables reçoivent des canulars et des demandes d'aide (des personnes proposant par exemple de vous envoyer de l'argent depuis l'étranger). Il est souvent impossible de déterminer l'intention du créateur.

Si un message vous demande de le faire suivre à toutes vos connaissances, il peut très bien s'agir d'un canular. Sur Internet, de nombreux sites spécialisés peuvent vérifier la légitimité d'un courrier. Avant de retransmettre un message que vous soupçonnez d'être un canular, faites d'abord une recherche sur Internet à son sujet.

3.10.3.3 Hameçonnage

Le terme d'hameçonnage (phishing en anglais) désigne une activité frauduleuse utilisant des techniques de piratage psychologique qui consistent à manipuler les utilisateurs pour obtenir des informations confidentielles. Son but est d'accéder à des données sensibles, telles que numéros de comptes bancaires, codes secrets, etc.

La technique consiste généralement à envoyer un message électronique en se faisant passer pour une personne ou une entreprise digne de confiance (institution financière, compagnie d'assurance par exemple). Le message peut sembler tout à fait authentique et contenir des graphiques et contenus qui proviennent véritablement de la source dont il se réclame. Vous êtes invité à entrer, sous divers prétextes (vérification de données, opérations financières), certaines de vos données personnelles : numéros de compte en banque ou noms d'utilisateur et mots de passe. Toutes ces données, si elles sont soumises, peuvent facilement être volées et utilisées à des fins illégales.

Les banques, compagnies d'assurance et autres sociétés légales ne demandent jamais de noms d'utilisateur et de mots de passe dans un message non sollicité.

3.10.3.4 Reconnaissance du courrier indésirable

Généralement, peu d'indicateurs contribuent à identifier le courrier indésirable (messages non sollicités) dans une boîte à lettres. Si un message remplit au moins l'un des critères suivants, il s'agit probablement de courrier indésirable.

- L'adresse de l'expéditeur ne figure pas dans la liste de vos contacts.
- Le contenu du message concerne une grosse somme d'argent qui vous est offerte. Pour toucher cette somme, vous devez néanmoins fournir au préalable une petite somme.
- Vous devez entrer, sous divers prétextes (vérification de données, opérations financières), certaines de vos données personnelles : numéros de compte en banque ou noms d'utilisateur et mots de passe.
- Le message est écrit dans une langue étrangère.
- Le message vous demande d'acheter un produit qui ne vous intéresse pas. Si vous décidez d'acheter le produit, vérifiez que l'expéditeur du message est un vendeur sérieux (consultez le fabricant original du produit).
- Quelques mots sont mal écrits pour pouvoir passer à travers le filtre de courrier indésirable. Par exemple, « vaigra » au lieu de « viagra », etc.

3.10.3.4.1 Règles

Dans le contexte des solutions de protection antispam et des clients de messagerie, les règles sont des outils permettant de manipuler les fonctions de messagerie. Elles se composent de deux parties logiques :

1. La condition (par exemple, un message entrant provenant d'une certaine adresse)
2. l'action (par exemple, la suppression du message ou son déplacement vers un dossier spécifique).

Le nombre de règles et leurs combinaisons varient en fonction de la solution de protection antispam. Ces règles servent de protection antispam (messages non sollicités). Exemples caractéristiques :

- 1. Condition : un message entrant contient des mots habituellement utilisés dans le courrier indésirable.
  2. Action : supprimer le message.
- 1. Condition : un message entrant contient une pièce jointe comportant l'extension .exe.
  2. Action : supprimer la pièce jointe et livrer le message dans la boîte aux lettres.
- 1. Condition : un message entrant arrive de votre employeur.
  2. Action : déplacer le message dans le dossier Travail.

Nous vous recommandons d'utiliser une combinaison de règles des programmes de programme antispam afin de faciliter l'administration et d'améliorer le filtrage du courrier indésirable.

3.10.3.4.2 Liste blanche

En général, une liste blanche est une liste de personnes ou d'éléments qui ont été acceptés ou ont obtenu une autorisation d'accès. Le terme « liste blanche de messagerie » définit la liste de contacts dont l'utilisateur souhaite recevoir les messages. Ces listes blanches sont basées sur des mots-clés recherchés dans une adresse électronique, des noms de domaines ou des adresses IP.

Si une liste blanche fonctionne en « mode exclusif », les messages de toutes les autres adresses, domaines ou adresses IP sont écartés. Si elle fonctionne en mode non exclusif, ces messages ne sont pas supprimés, mais filtrés d'une autre façon.

Une liste blanche fonctionne sur le principe opposé de la liste noire. Les listes blanches sont relativement faciles à maintenir, plus que les listes noires. Pour un meilleur filtrage du courrier indésirable, nous vous recommandons d'utiliser des listes blanches et des listes noires.

3.10.3.4.3 Liste noire

En général, une liste noire répertorie les personnes ou les éléments non acceptés ou interdits. Dans le monde virtuel, c'est une technique qui permet d'accepter des messages de tous les utilisateurs qui ne figurent pas sur cette liste.

Il existe deux types de listes noires : les listes créées par les utilisateurs dans l'application de protection antispam et les listes professionnelles mises à jour régulièrement. Ces dernières sont créées par des institutions spécialisées et sont disponibles sur Internet.

Il est essentiel d'utiliser les listes noires pour bloquer le courrier indésirable, mais elles sont très difficiles à tenir à jour, car de nouveaux éléments à bloquer apparaissent tous les jours. Nous recommandons d'utiliser à la fois une liste blanche et une liste noire pour mieux filtrer le courrier indésirable.

3.10.3.4.4 Liste d'exceptions

La liste d'exceptions contient généralement des adresses électroniques qui peuvent être usurpées et utilisées pour l'envoi de courrier indésirable. Les messages provenant des adresses répertoriées dans la liste d'exceptions sont toujours inclus à l'analyse visant à identifier le courrier indésirable. Par défaut, la liste d'exceptions contient les adresses électroniques figurant dans vos comptes de client de messagerie existants.

3.10.3.4.5 Contrôle côté serveur

Le contrôle côté serveur est une technique permettant d'identifier le courrier indésirable de masse d'après le nombre de messages reçus et les réactions des utilisateurs. Chaque message laisse une empreinte numérique unique en fonction de son contenu. Le numéro d'identification unique ne donne aucune information sur le contenu du message. Deux messages identiques ont une empreinte identique, tandis que des messages différents ont une empreinte différente.

Si un message est marqué comme courrier indésirable, son empreinte est envoyée au serveur. Si le serveur reçoit plusieurs empreintes identiques (correspondant à un certain message de courrier indésirable), cette empreinte est stockée dans la base des empreintes de courrier indésirable. Lorsqu'il analyse des messages entrants, le programme envoie les empreintes de ces messages au serveur. Le serveur renvoie des informations indiquant les empreintes qui correspondent à des messages déjà identifiés comme courrier indésirable par d'autres utilisateurs.

3.10.4 Technologie ESET

3.10.4.1 Bloqueur d'exploit

Le bloqueur d'exploit est conçu pour renforcer les applications connues pour être très vulnérables aux exploits (navigateurs Web, lecteurs de fichiers PDF, clients de messagerie et composants MS Office). Il surveille le comportement des processus et recherche toute activité suspecte pouvant indiquer un exploit. Il offre une couche de protection supplémentaire, plus proche des pirates, à l'aide d'une technologie complètement différente par rapport aux techniques axées uniquement sur la détection des fichiers malveillants.

Lorsqu'il identifie un processus suspect, le bloqueur d'exploit peut arrêter ce processus immédiatement. Il enregistre les données concernant la menace et les envoie au système ESET Live Grid dans le cloud. Ces données sont traitées par le laboratoire d'ESET et permettent de mieux protéger tous les utilisateurs contre les menaces inconnues et les attaques immédiates (logiciels malveillants très récents n'ayant encore aucun remède préconfiguré).

3.10.4.2 Scanner de mémoire avancé

Le scanner de mémoire avancé fonctionne avec le bloqueur d'exploit pour offrir une meilleure protection contre les logiciels malveillants qui ne sont pas détectés par les produits anti-logiciels malveillants grâce à l'obscurcissement et/ou au chiffrement. Dans les cas où l'émulation ou l'heuristique classique ne détecte pas la menace, le scanner de mémoire avancé est en mesure d'identifier le comportement suspect et il analyse les menaces lorsqu'elles apparaissent dans la mémoire système. Cette solution est efficace même sur les logiciels malveillants fortement obscurcis. Contrairement au bloqueur d'exploit, il s'agit d'une méthode ultérieure à l'exécution. Cela signifie que des activités malveillantes ont pu avoir le temps de s'exécuter avant que cette menace soit détectée. Toutefois, si les autres techniques de détection ont échoué, il apporte une couche supplémentaire de sécurité.

3.10.4.3 ESET Live Grid

Conçu sur le système d'avertissement anticipé de ThreatSense.Net®, ESET Live Grid collecte les données soumises par les utilisateurs ESET du monde entier avant de les envoyer au laboratoire d'ESET. En fournissant des métadonnées et des exemples suspects, ESET Live Grid nous permet de réagir immédiatement aux besoins de nos clients et de faire en sorte qu'ESET réponde aux dernières menaces. Les chercheurs ESET spécialisés dans les logiciels malveillants utilisent ces informations pour concevoir un instantané précis de la nature et de l'ampleur des menaces. Nous pouvons alors nous concentrer sur les cibles pertinentes. Les données ESET Live Grid jouent un rôle important dans la configuration des priorités de notre traitement automatisé.

Par ailleurs, elles permettent de mettre en œuvre un système de réputation qui améliore l'efficacité globale de nos solutions anti-logiciels malveillants. Lorsqu'une archive ou un fichier exécutable est inspecté sur le système d'un ordinateur, son hash tag est d'abord comparé à une base de données d'éléments répertoriés sur une liste noire et une liste blanche. S'il figure dans la liste blanche, le fichier inspecté est considéré comme étant nettoyé et il est identifié de manière à être exclu des prochaines analyses. S'il figure dans la liste noire, les mesures appropriées sont prises en fonction de la nature de la menace. Si aucune correspondance n'est trouvée, le fichier est analysé intégralement. En fonction des résultats de cette analyse, les fichiers sont classés comme menaces ou non-menaces. Cette approche améliore considérablement les performances des analyses.

Ce système de réputation améliore l'efficacité de la détection des exemples de logiciels malveillants, avant même que leur signature ne soit distribuée aux utilisateurs par l'intermédiaire des mises à jour de la base des signatures de virus plusieurs fois par jour.

3.10.4.4 Protection anti-botnet

La protection anti-botnet découvre les logiciels malveillants par l'analyse de ses protocoles de communication réseau. Les logiciels malveillants botnet changent fréquemment, contrairement aux protocoles réseau qui n'ont pas changé ces dernières années. Cette nouvelle technologie permet à ESET de vaincre des logiciels malveillants qui essaient de connecter votre ordinateur à un réseau botnet.

3.10.4.5 Bloqueur d'exploit Java

Le Bloqueur d'exploit Java est une extension de la protection du Bloqueur d'exploit ESET existant. Il surveille Java et recherche les comportements de type exploit. Les échantillons bloqués peuvent être signalés aux analystes de logiciels malveillants pour leur permettre de créer des signatures afin de bloquer les tentatives d'exploit Java sur différentes couches (blocage d'URL, téléchargements de fichiers, etc.).