ESET Internet Security

Guide de l'utilisateur

Cliquez ici pour consulter la version de l'aide en ligne de ce document

Digital Security
Progress. Protected.

ESET Internet Security a été développé par ESET, spol. s r.o.

Pour plus d’informations, visitez le site https://www.eset.com.

Assistance technique : https://support.eset.com

REV. 2024-04-12

ESET Internet Security

ESET Internet Security constitue une nouvelle approche de la sécurité informatique véritablement intégrée. La version la plus récente du moteur d'analyse d'ESET LiveGrid® de pair avec notre pare-feu et nos modules antipourriel personnalisés, misent sur la rapidité et la précision pour assurer la protection de votre ordinateur. Il en résulte un système intelligent qui est constamment à l'affût des attaques et des logiciels malveillants qui pourraient représenter une menace pour votre ordinateur.

ESET Internet Security est une solution de sécurité complète qui allie protection maximale et encombrement minimal. Nos technologies avancées utilisent l'intelligence artificielle pour prévenir les infiltrations de virus, de logiciels espions, de chevaux de Troie, de vers, de logiciels publicitaires, de rootkits et autres attaques, sans atténuer les performances ni perturber votre ordinateur.

Fonctionnalités et avantages

Interface utilisateur renouvelée	L'interface utilisateur de cette version a été considérablement renouvelée et simplifiée en fonction des résultats des tests effectués sur sa convivialité. Tous les termes et notifications IUG ont été examinés attentivement et l'interface prend désormais en charge les langues s'écrivant de droite à gauche comme l'hébreu et l'arabe. L'assistance en ligne est désormais intégrée dans ESET Internet Security et offre un contenu d'assistance mis à jour dynamiquement.
Mode sombre	Une extension qui vous aide à basculer rapidement l'écran vers un thème sombre. Vous pouvez choisir votre jeu de couleurs préféré dans Éléments de l'interface utilisateur.
Antivirus et antispyware	Détecte et supprime de manière proactive un grand nombre de virus, vers, chevaux de Troie et rootkits, tant connus qu'inconnus. La technologie d'heuristique avancée indiquera même les logiciels malveillants encore jamais vus pour ainsi protéger votre ordinateur contre les menaces inconnues et les neutraliser avant même qu'elles ne puissent s'attaquer à votre ordinateur. La protection de l'accès Web et la protection antihameçonnage utilisent la surveillance des communications entre les navigateurs Web et les serveurs distants (y compris SSL). La protection du client de messagerie offre le contrôle de la communication par courriel effectuée par l'entremise des protocoles POP3(S) et IMAP(S).
Mises à jour régulières	Mettre régulièrement à jour le moteur de détection (précédemment appelé « base de données des signatures de virus ») et les modules du programme constitue la meilleure méthode pour obtenir le niveau maximal de sécurité pour votre ordinateur.
ESET LiveGrid® (réputation utilisant le nuage)	Vous pouvez vérifier la réputation de processus en cours d'exécution directement à partir de ESET Internet Security.
Contrôle de périphérique	Analyse automatiquement tous les lecteurs USB, cartes mémoire et CD/DVD. Il bloque l'accès aux supports amovibles selon le type de support, le fabricant, la taille du support et d'autres caractéristiques.
Fonctionnalité HIPS	Vous pouvez personnaliser précisément le comportement du système en précisant notamment des règles pour le registre système, les processus et programmes actifs, ainsi qu'en affiner la sécurité.
Mode jeu	Reporte toutes les fenêtres contextuelles, mises à jour ou autres activités exigeantes en ressources système lors de l'utilisation d'un jeu ou de toute autre activité exigeant le mode plein écran.

Fonctionnalités de ESET Internet Security

Opérations bancaires et navigation sécurisées	L'opérations bancaires et navigation sécurisées vous offre un navigateur sécurisé pour vous assurer que toutes vos transactions en ligne, lorsque vous visitez des sites de comptes bancaires ou de paiements en ligne, sont effectuées dans un environnement fiable et sécurisé.
Prise en charge des signatures de réseau	Les signatures de réseau permettent l'identification rapide et bloquent le trafic malveillant entre les périphériques des utilisateurs comme les bots et les paquets exploit. Cette fonctionnalité peut être considérée comme une amélioration apportée à la protection de réseaux de zombies.
Pare-feu intelligent	Empêche les utilisateurs non autorisés d'accéder à votre ordinateur et d'y découvrir vos données personnelles.
Antipourriel du client de messagerie	Il représente jusqu'à 50 % de toutes les communications par courriel. L'antipourriel du client de messagerie constitue une protection contre ce problème.
Antivol	Antivol étend la sécurité au niveau utilisateur en cas de perte ou de vol d'un ordinateur. Lorsque vous installez ESET Internet Security et Antivol, votre périphérique est répertorié dans l'interface Web. L'interface Web permet de gérer la configuration de Antivol et d'administrer les fonctionnalités de Antivol sur votre périphérique.
Contrôle parental	Protège votre famille contre du contenu Web potentiellement offensant en bloquant diverses catégories de sites Web.

Un abonnement doit être actif pour que les fonctionnalités de ESET Internet Security soient opérationnelles. Nous vous recommandons de renouveler votre abonnement plusieurs semaines avant l'expiration de l'abonnement à ESET Internet Security.

Nouveautés

Quoi de neuf dans ESET Internet Security 17.1

- Petites améliorations sur Inspecteur de réseau
- Petites améliorations sur Opérations bancaires et navigation sécurisées
- Autres corrections et améliorations mineures de bogues

Pour désactiver **les notifications Nouveautés** :
1. Pour désactiver les notifications concernant les nouveautés, accédez à Configuration avancée > **Notifications** > **Notifications de bureau**.
2. Cliquez sur **Modifier** à côté de **notifications de bureau**.
3. Décochez la case **Afficher les notifications Nouveautés**, puis cliquez sur **OK**.
Pour plus d'informations sur les notifications, consultez la section Notifications.

Pour obtenir la liste détaillée des modifications apportées à ESET Internet Security, consultez les journaux des modifications de ESET Internet Security.

Quels sont les produits que je possède ?

ESET offre plusieurs couches de sécurité avec de nouveaux produits qui vont des solutions antivirus rapides et puissantes aux solutions de sécurité tout-en-un avec une empreinte minimale sur le système :

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**
- **ESET Security Ultimate**

Pour déterminer quels produits sont installés sur votre système, ouvrez la fenêtre principale du programme et vous verrez le nom des produits en haut de la fenêtre (voir l'article de la Base de connaissances).

Le tableau ci-dessous donne le détail des fonctionnalités offertes dans chaque produit.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Moteur de détection	✔	✔	✔	✔
Apprentissage automatique avancé	✔	✔	✔	✔
Bloqueur d'exploits	✔	✔	✔	✔
Protection contre les attaques basées sur le script	✔	✔	✔	✔
Anti-hameçonnage	✔	✔	✔	✔
Protection de l'accès Web	✔	✔	✔	✔
HIPS (inclus la Bouclier contre les rançongiciels)	✔	✔	✔	✔
Antipourriel		✔	✔	✔
Pare-feu		✔	✔	✔
Inspecteur de réseau		✔	✔	✔
Protection de la caméra Web		✔	✔	✔
Protection contre les attaques réseau		✔	✔	✔
Protection contre les botnets		✔	✔	✔
Opérations bancaires et navigation sécurisées		✔	✔	✔
Sécurité et confidentialité du navigateur		✔	✔	✔
Contrôle parental		✔	✔	✔
Antivol		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Certains des produits ci-dessus peuvent ne pas être disponibles pour votre langue / région.

Exigences système

Votre système doit répondre aux exigences matérielles et logicielles suivantes pour que ESET Internet Security fonctionne de manière optimale :

Processeurs pris en charge

Processeur Intel ou AMD 32 bits (x86) avec jeu d'instructions SSE2 ou 64 bits (x64), 1 GHz ou plus
processeur basé sur ARM64, 1 GHz ou supérieur

Système d’exploitation pris en charge

Microsoft® Windows® 11

Microsoft® Windows® 10

La prise en charge d’Azure Code Signing doit être effective sur tous les systèmes d’exploitation Windows pour installer ou mettre à niveau les produits ESET sortis après juillet 2023. Plus d'information.

Essayez toujours de garder votre système d'exploitation à jour.

Conditions requises pour les fonctionnalités d’ESET Internet Security

Consultez la exigences du système pour des fonctionnalités spécifiques à ESET Internet Security dans le tableau suivant :

Fonctionnalité	Exigences
Intel® Threat Detection Technology	Consultez la liste des processeurs pris en charge.
Opérations bancaires et navigation sécurisées	Consultez la liste des navigateurs Web pris en charge.
Arrière-plan transparent	Windows 10 version RS4 et les versions ultérieures.
Logiciel de nettoyage spécialisé	Processeur autre que ARM64.
Nettoyage système	Processeur autre que ARM64.
Bloqueur d'exploits	Processeur autre que ARM64.
Inspection approfondie de comportement	Processeur autre que ARM64.

Autre

Une connexion Internet est nécessaire pour que l'activation et les mises à jour de ESET Internet Security fonctionnent correctement.

Deux programmes antivirus fonctionnant simultanément sur un même périphérique provoquent d'inévitables conflits de ressources système, tels que le ralentissement du système pour le rendre inopérant

Version de Microsoft Windows obsolète

Problème

- Vous souhaitez installer la toute dernière version de ESET Internet Security sur un ordinateur sous Windows 7, Windows 8 (8.1) ou Windows Home Server 2011
- ESET Internet Security affiche une erreur **Système d'exploitation obsolète** lors de l'installation

Détails

La dernière version de ESET Internet Security nécessite des systèmes d'exploitation Windows 10 ou Windows 11.

Solution

Les solutions suivantes sont disponibles :

Mise à niveau vers Windows 10 ou Windows 11

Le processus de mise à niveau est relativement simple et, dans de nombreux cas, vous pouvez le faire sans perdre vos fichiers. Avant la mise à niveau vers Windows 10 :

1. Sauvegarde des données importantes.
2. Lisez la FAQ de mise à niveau vers Windows 10 ou FAQ de mise à niveau vers Windows 11 de Microsoft et mettez à jour votre système d'exploitation Windows.

Installer ESET Internet Security version 16.0

Si vous ne pouvez pas mettre à niveau Windows, installez ESET Internet Security version 16.0. Pour plus de détails, consultez l'Aide en ligne de ESET Internet Security version 16.0.

Prévention

Lorsque vous travaillez avec votre ordinateur et particulièrement lorsque vous naviguez sur Internet, gardez toujours à l'esprit qu'aucun antivirus au monde ne peut complètement éliminer le risque d'infiltration et des attaques à distance. Pour assurer une protection et une convivialité maximales, il est essentiel d'utiliser correctement votre solution antivirus et de respecter plusieurs règles utiles :

Effectuer des mises à jour régulières

Selon les statistiques de ESET LiveGrid®, 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 de recherche d'ESET analysent ces menaces chaque jour et conçoivent des mises à jour pour améliorer continuellement le niveau de protection de nos utilisateurs. Pour garantir l'efficacité maximale de ces mises à jour, il est important que celles-ci soient configurées de façon appropriée sur votre système. Pour plus d'information sur la configuration des mises à jour, voir la rubrique Configuration des mises à jour.

Télécharger les correctifs de sécurité

Les auteurs de programmes malveillants exploitent souvent diverses failles du système pour assurer une meilleure propagation du code malveillant. C'est pour cette raison que les sociétés qui commercialisent des logiciels recherchent activement l'apparition de nouvelles failles dans leurs applications pour concevoir les mises à jour de sécurité afin d'éliminer les menaces potentielles sur une base régulière. 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 de sécurité sont régulièrement émises.

Sauvegarde des 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 la perte de données importantes. Il est important de sauvegarder régulièrement vos données importantes et sensibles sur une source externe, telle que DVD ou disque dur externe. Vous pourrez ainsi récupérer vos données beaucoup plus facilement et rapidement en cas de défaillance du système.

Rechercher régulièrement les virus sur votre ordinateur

La détection d'un plus grand nombre de virus, de vers, de chevaux de Troie et de rootkits, tant connus qu'inconnus, est effectuée par le module de protection du système de fichiers en temps réel. Ainsi, chaque fois que vous accédez à un fichier ou ouvrez un fichier, il sera analysé pour y déceler toute activité malveillante. Nous recommandons d'effectuer une analyse complète de l'ordinateur au moins une fois par mois, car les signatures des logiciels malveillants peuvent varier et le moteur de détection se met à jour quotidiennement.

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 considérable à nettoyer les infiltrations. Voici quelques directives 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 ensembles de codec, etc. N'utilisez que des programmes sécurisés et ne consultez que les sites Web sécurisés.
- Soyez prudent lorsque vous ouvrez les pièces jointes aux courriels, en particulier celles provenant de publipostage ou d'expéditeurs inconnus.
- N'utilisez pas de compte Administrateur pour le travail de tous les jours sur votre ordinateur.

Pages d'aide

Bienvenue dans le guide d'utilisateur de ESET Internet Security. Les informations fournies ici vous permettront de vous familiariser avec votre produit et vous aideront à rendre votre ordinateur plus sûr.

Démarrage

Avant d'utiliser ESET Internet Security, vous pouvez vous familiarisiez avec les différents types de détections et d'attaques distantes auxquels vous pourriez faire face lorsque vous utilisez votre ordinateur. Nous avons également compilé la liste des nouvelles fonctionnalités introduites dans ESET Internet Security.

Commencez par l'installation de ESET Internet Security. Si ESET Internet Security est déjà installé, consultez la rubrique Utilisation de ESET Internet Security.

Comment utiliser les pages d'aide de ESET Internet Security

L'aide en ligne est divisée en plusieurs chapitres et sous-chapitres. Appuyez sur **F1** dans ESET Internet Security pour afficher des informations sur la fenêtre actuellement ouverte.

Le programme vous permet de chercher une rubrique d'aide par mot-clé ou de rechercher du contenu en tapant des mots ou des phrases. La différence entre ces deux méthodes est qu'un mot clé peut être associé à des pages d'aide qui ne contiennent pas le mot clé précis dans le texte. La recherche de mots et de phrases fouillera le contenu de toutes les pages et n'affichera que les pages contenant effectivement le mot ou la phrase en question.

Par souci de cohérence et afin d'éviter toute confusion, la terminologie utilisée dans ce guide est basée sur l'interface utilisateur de ESET Internet Security. Nous avons également utilisé un ensemble uniforme de symboles afin de mettre en évidence des sujets ayant une importance ou un intérêt particuliers.

Une remarque est une courte observation. Bien qu'il soit possible de les ignorer, les remarques offrent de précieux renseignements comme des caractéristiques spécifiques ou un lien vers un sujet apparenté.

Ce titre indique des renseignements qui réclament votre attention; il n'est pas recommandé de les ignorer. Habituellement, ce titre indique des renseignements importants, mais non essentiels.

Ce titre indique des renseignements qui exigent une attention et des précautions supplémentaires. Les avertissements sont placés spécialement pour vous dissuader de commettre des erreurs potentiellement dangereuses. Lisez et comprenez le texte, car il fait référence à des paramètres système très sensibles ou à des risques.

Il s'agit d'un cas d'utilisation ou d'un exemple pratique qui vise à vous aider à comprendre comment une certaine fonction ou fonctionnalité peut être utilisée.

Convention	Signification
Texte en gras	Noms d'éléments d'interface comme les boîtes ou les boutons d'options.
Texte en italique	Espaces réservés pour les renseignements que vous fournissez. Par exemple, nom de fichier ou chemin indique que vous devrez saisir les renseignements exacts de chemin ou de nom du fichier.
`Courier New`	Exemples de code ou de commandes.
Lien hypertexte	Fournit un accès rapide et facile aux références croisées ou aux emplacements Web externes. Les hyperliens sont mis en évidence à l'aide de la couleur bleue et peuvent être soulignés.
%ProgramFiles%	Le répertoire système Windows où les programmes installés sur Windows sont stockés.

Aide en ligne est la principale source de contenu d'aide. La version la plus récente de l'Aide en ligne s'affiche automatiquement lorsque vous avez une connexion Internet.

Installation

Il existe différentes méthodes pour installer ESET Internet Security sur votre ordinateur. Les méthodes d'installation peuvent varier en fonction du pays et du mode de distribution :

- Live installer – Téléchargé à partir du site Web d'ESET ou d'un CD/DVD. Le progiciel d'installation est le même pour toutes les langues (choisissez la langue appropriée). Le programme d'installation Live installer est un petit fichier; des fichiers supplémentaires sont nécessaires pour l'installation. ESET Internet Security sont téléchargés automatiquement.

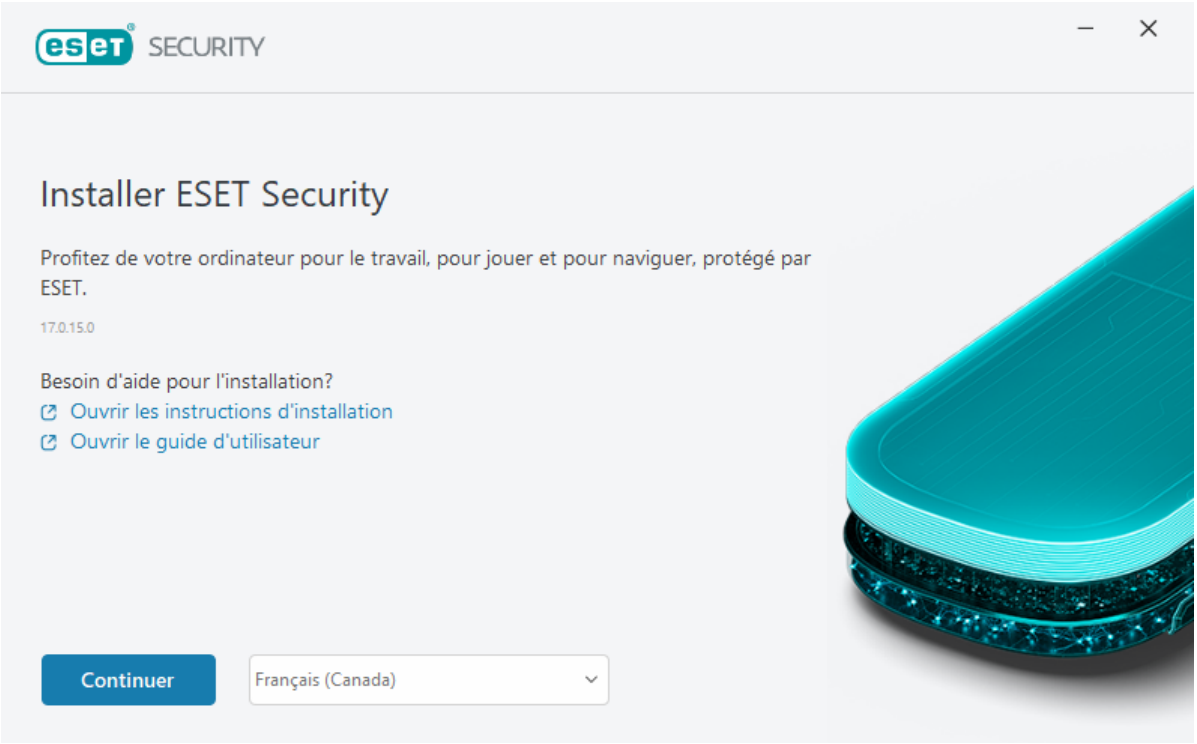
- Installation hors ligne – Utilise un fichier .exe plus volumineux que le fichier d'installation Live installer et qui ne nécessite pas de connexion Internet ni de fichiers supplémentaires pour terminer l'installation.

Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur avant d'installer ESET Internet Security. Si plusieurs solutions antivirus sont installées sur un même ordinateur, elles peuvent entrer en conflit. Nous recommandons de désinstaller tout autre antivirus de votre système. Voir notre article sur la base de connaissances ESET pour une liste des outils de désinstallation pour les logiciels antivirus communs (disponible en anglais et dans plusieurs autres langues).

Live installer

Après avoir téléchargé le progiciel d'installation Live installer, double-cliquez sur le fichier d'installation et suivez les instructions pas-à-pas de l'assistant d'installation.

Pour ce type d'installation, vous devez être connecté à Internet.



1. Sélectionnez la langue appropriée dans le menu déroulant et cliquez sur **Continuer**.

Si vous installez une version plus récente que la version précédente avec des paramètres protégés par mot de passe, tapez votre mot de passe. Vous pouvez configurer le mot de passe des paramètres dans Configuration de l'accès.

2. Sélectionnez votre préférence pour les fonctionnalités suivantes, lisez le contrat de licence de l'utilisateur final et la politique de confidentialité et cliquez sur **Continuer**, ou cliquez sur **Autoriser tout et continuer** pour activer toutes les fonctionnalités suivantes :

- Système de rétroaction ESET LiveGrid®
- Applications potentiellement indésirables
- Programme d\'amélioration de l\'expérience client

En cliquant sur **Continuer** ou **Autoriser tout et continuer**, vous acceptez le contrat de licence de l'utilisateur final et reconnaissez avoir pris connaissance de la politique de confidentialité.

3. Pour activer, gérer et afficher la sécurité du périphérique à l'aide du ESET HOME, connectez votre périphérique au compte ESET HOME. Cliquez sur **Ignorer la connexion** pour continuer sans vous connecter à ESET HOME. Vous pouvez connecter votre périphérique à votre compte ESET HOME ultérieurement.

4. Si vous continuez sans vous connecter à ESET HOME, choisissez une option d'activation. Si vous installez une version plus récente par rapport à la précédente, votre **clé d'activation** sera automatiquement saisie.

5. L'assistant d'installation détermine quel produit ESET est installé en fonction de votre abonnement. La version avec le plus de fonctions de sécurité est toujours présélectionnée. Cliquez sur **Changer de produit** si vous souhaitez installer une autre version du produit ESET. Cliquez sur **Continuer** pour démarrer le processus d'installation. Cela peut prendre un moment.

Si des fichiers ou des dossiers n'ont pas été supprimés lors de la désinstallation des produits ESET, vous serez invité à autoriser leur suppression. Cliquez sur **Installer** pour continuer.

6. Cliquez sur **Terminé** pour quitter l'assistant d'installation.

Utilitaire de résolution des problèmes d'installation.

Une fois le produit installé et activé, le téléchargement des modules commencent. La protection est en cours d'initialisation et certaines fonctionnalités peuvent ne pas être entièrement fonctionnelles tant que le téléchargement n'est pas terminé.

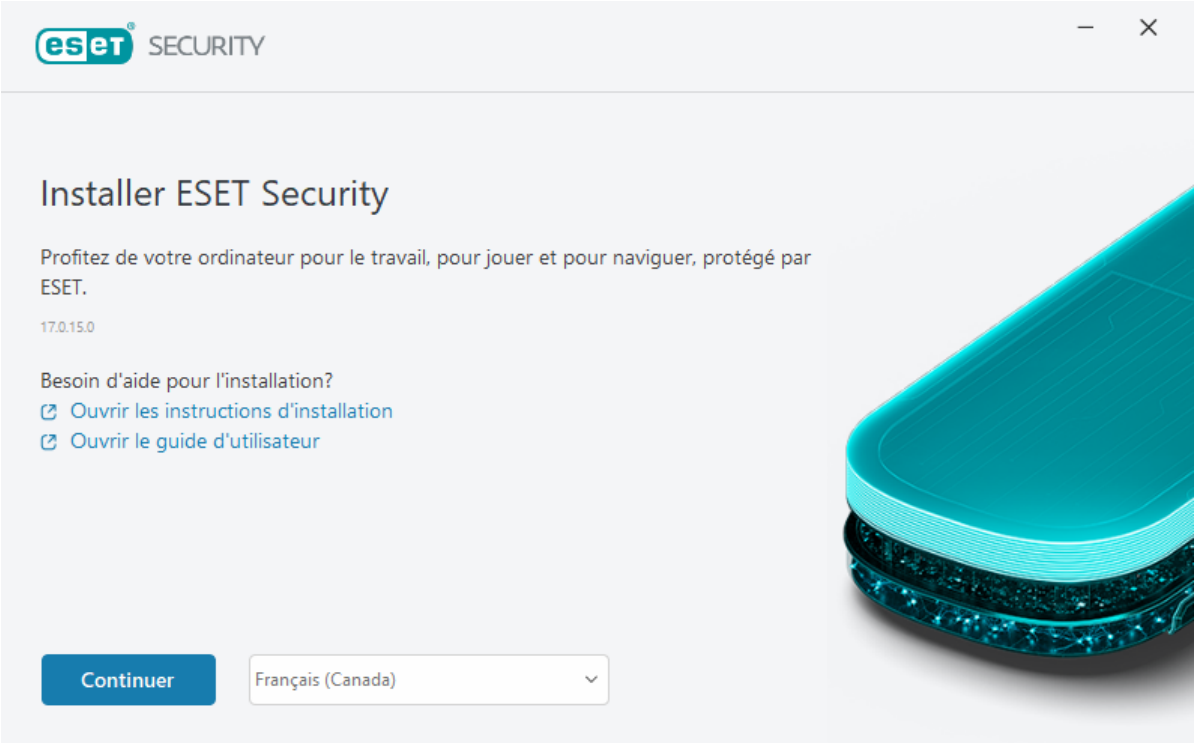
Installation hors connexion

Téléchargez et installez votre produit ESET Windows pour particuliers en utilisant le programme d'installation hors ligne (.exe) ci-dessous. Choisissez la version du produit ESET HOME à télécharger (32 bits, 64 bits ou ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Téléchargement 64 bits Téléchargement 32 bits Téléchargement ARM	Téléchargement 64 bits Téléchargement 32 bits Téléchargement ARM	Téléchargement 64 bits Téléchargement 32 bits Téléchargement ARM	Téléchargement 64 bits Téléchargement 32 bits Téléchargement ARM

Si vous disposez d'une connexion internet active, installez votre produit ESET en utilisant un programme d'installation Live Installer.

Lorsque vous lancez le programme d'installation hors ligne (.exe), l'assistant d'installation vous guide tout au long du processus d'installation.



1. Sélectionnez la langue appropriée dans le menu déroulant et cliquez sur **Continuer**.

Si vous installez une version plus récente que la version précédente avec des paramètres protégés par mot de passe, tapez votre mot de passe. Vous pouvez configurer le mot de passe des paramètres dans Configuration de l'accès.

2. Sélectionnez votre préférence pour les fonctionnalités suivantes, lisez le contrat de licence de l'utilisateur final et la politique de confidentialité et cliquez sur **Continuer**, ou cliquez sur **Autoriser tout et continuer** pour activer toutes les fonctionnalités suivantes :

- Système de rétroaction ESET LiveGrid®
- Applications potentiellement indésirables
- Programme d\'amélioration de l\'expérience client

En cliquant sur **Continuer** ou **Autoriser tout et continuer**, vous acceptez le contrat de licence de l'utilisateur final et reconnaissez avoir pris connaissance de la politique de confidentialité.

3. Cliquez sur **Ignorer la connexion**. Lorsque vous disposez d'une connexion Internet, vous pouvez connecter votre périphérique à votre compte ESET HOME.

4. Cliquez sur **Ignorer l'activation**. ESET Internet Security doit être activé après l'installation pour être pleinement fonctionnel. L'activation du produit nécessite une connexion internet active.

5. L'assistant d'installation montre quel produit ESET sera installé en fonction du programme d'installation

hors ligne téléchargé. Cliquez sur **Continuer** pour démarrer le processus d'installation. Cela peut prendre un moment.

Si des fichiers ou des dossiers n'ont pas été supprimés lors de la désinstallation des produits ESET, vous serez invité à autoriser leur suppression. Cliquez sur **Installer** pour continuer.

6. Cliquez sur **Terminé** pour quitter l'assistant d'installation.

Utilitaire de résolution des problèmes d'installation.

L'abonnement mise à niveau

Cette fenêtre de notification s'affiche lorsque l'abonnement utilisé pour activer votre produit ESET a été modifié. Votre abonnement modifié vous permet d'activer un produit avec plus de fonctionnalités de sécurité. Si aucun changement n'a été effectué, ESET Internet Security affichera une fois une fenêtre d'alerte appelée **Changement vers un produit avec plus de fonctionnalités**.

Oui (recommandé) – le produit avec plus de fonctionnalités de sécurité sera installé automatiquement.

Non, merci – aucune modification ne sera apportée et la notification disparaîtra définitivement.

Pour modifier le produit plus tard, consultez notre article de la base de connaissances ESET. Pour plus d'informations sur l'abonnement à ESET, consultez la FAQ sur l'abonnement.

Le tableau ci-dessous donne le détail des fonctionnalités offertes dans chaque produit.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Moteur de détection	✔	✔	✔	✔
Apprentissage automatique avancé	✔	✔	✔	✔
Bloqueur d'exploits	✔	✔	✔	✔
Protection contre les attaques basées sur le script	✔	✔	✔	✔
Anti-hameçonnage	✔	✔	✔	✔
Protection de l'accès Web	✔	✔	✔	✔
HIPS (inclus la Bouclier contre les rançongiciels)	✔	✔	✔	✔
Antipourriel		✔	✔	✔
Pare-feu		✔	✔	✔
Inspecteur de réseau		✔	✔	✔
Protection de la caméra Web		✔	✔	✔
Protection contre les attaques réseau		✔	✔	✔
Protection contre les botnets		✔	✔	✔
Opérations bancaires et navigation sécurisées		✔	✔	✔
Sécurité et confidentialité du navigateur		✔	✔	✔
Contrôle parental		✔	✔	✔
Antivol		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Mise à niveau du produit

Vous avez téléchargé un programme d'installation par défaut et décidé de changer le produit à activer, ou vous voulez changer votre produit installé pour un produit avec plus de fonctionnalités de sécurité.

Changez de produit pendant l’installation.

Le tableau ci-dessous donne le détail des fonctionnalités offertes dans chaque produit.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Moteur de détection	✔	✔	✔	✔
Apprentissage automatique avancé	✔	✔	✔	✔
Bloqueur d'exploits	✔	✔	✔	✔
Protection contre les attaques basées sur le script	✔	✔	✔	✔
Anti-hameçonnage	✔	✔	✔	✔
Protection de l'accès Web	✔	✔	✔	✔
HIPS (inclus la Bouclier contre les rançongiciels)	✔	✔	✔	✔
Antipourriel		✔	✔	✔
Pare-feu		✔	✔	✔
Inspecteur de réseau		✔	✔	✔
Protection de la caméra Web		✔	✔	✔
Protection contre les attaques réseau		✔	✔	✔
Protection contre les botnets		✔	✔	✔
Opérations bancaires et navigation sécurisées		✔	✔	✔
Sécurité et confidentialité du navigateur		✔	✔	✔
Contrôle parental		✔	✔	✔
Antivol		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Abonnement passer à une version antérieure

La boîte de dialogue s'affiche lorsque l'abonnement utilisé pour activer votre produit ESET a été modifié. Votre abonnement modifié ne peut être utilisé qu'avec un produit ESET différent comportant moins de fonctions de sécurité. Le produit a été modifié automatiquement pour éviter la perte de protection.

Pour plus d'informations sur l'abonnement à ESET, consultez FAQ sur l'abonnement.

Le tableau ci-dessous donne le détail des fonctionnalités offertes dans chaque produit.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Moteur de détection	✔	✔	✔	✔
Apprentissage automatique avancé	✔	✔	✔	✔
Bloqueur d'exploits	✔	✔	✔	✔
Protection contre les attaques basées sur le script	✔	✔	✔	✔
Anti-hameçonnage	✔	✔	✔	✔
Protection de l'accès Web	✔	✔	✔	✔
HIPS (inclus la Bouclier contre les rançongiciels)	✔	✔	✔	✔
Antipourriel		✔	✔	✔
Pare-feu		✔	✔	✔
Inspecteur de réseau		✔	✔	✔
Protection de la caméra Web		✔	✔	✔
Protection contre les attaques réseau		✔	✔	✔
Protection contre les botnets		✔	✔	✔
Opérations bancaires et navigation sécurisées		✔	✔	✔
Sécurité et confidentialité du navigateur		✔	✔	✔
Contrôle parental		✔	✔	✔
Antivol		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Mise à niveau du produit vers une version antérieure

Le produit déjà installé comporte plus de fonctionnalités de sécurité que celui que vous êtes sur le point d'activer.Vous perdrez la protection contre le vol et l'accès aux données qui y sont liées stockées sur ESET HOME.

Le tableau ci-dessous donne le détail des fonctionnalités offertes dans chaque produit.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Moteur de détection	✔	✔	✔	✔
Apprentissage automatique avancé	✔	✔	✔	✔
Bloqueur d'exploits	✔	✔	✔	✔
Protection contre les attaques basées sur le script	✔	✔	✔	✔
Anti-hameçonnage	✔	✔	✔	✔
Protection de l'accès Web	✔	✔	✔	✔
HIPS (inclus la Bouclier contre les rançongiciels)	✔	✔	✔	✔
Antipourriel		✔	✔	✔
Pare-feu		✔	✔	✔
Inspecteur de réseau		✔	✔	✔
Protection de la caméra Web		✔	✔	✔
Protection contre les attaques réseau		✔	✔	✔
Protection contre les botnets		✔	✔	✔
Opérations bancaires et navigation sécurisées		✔	✔	✔
Sécurité et confidentialité du navigateur		✔	✔	✔
Contrôle parental		✔	✔	✔
Antivol		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Utilitaire de résolution des problèmes d’installation

Si des problèmes surviennent pendant l'installation, l'assistant d'installation fournit un outil de dépannage qui propose une solution au problème si cela est possible.

Cliquez sur **Exécuter l’utilitaire de résolution des problèmes** pour démarrer l’utilitaire de résolution des problèmes. Lorsque l'utilitaire termine son diagnostique, suivez la solution recommandée.

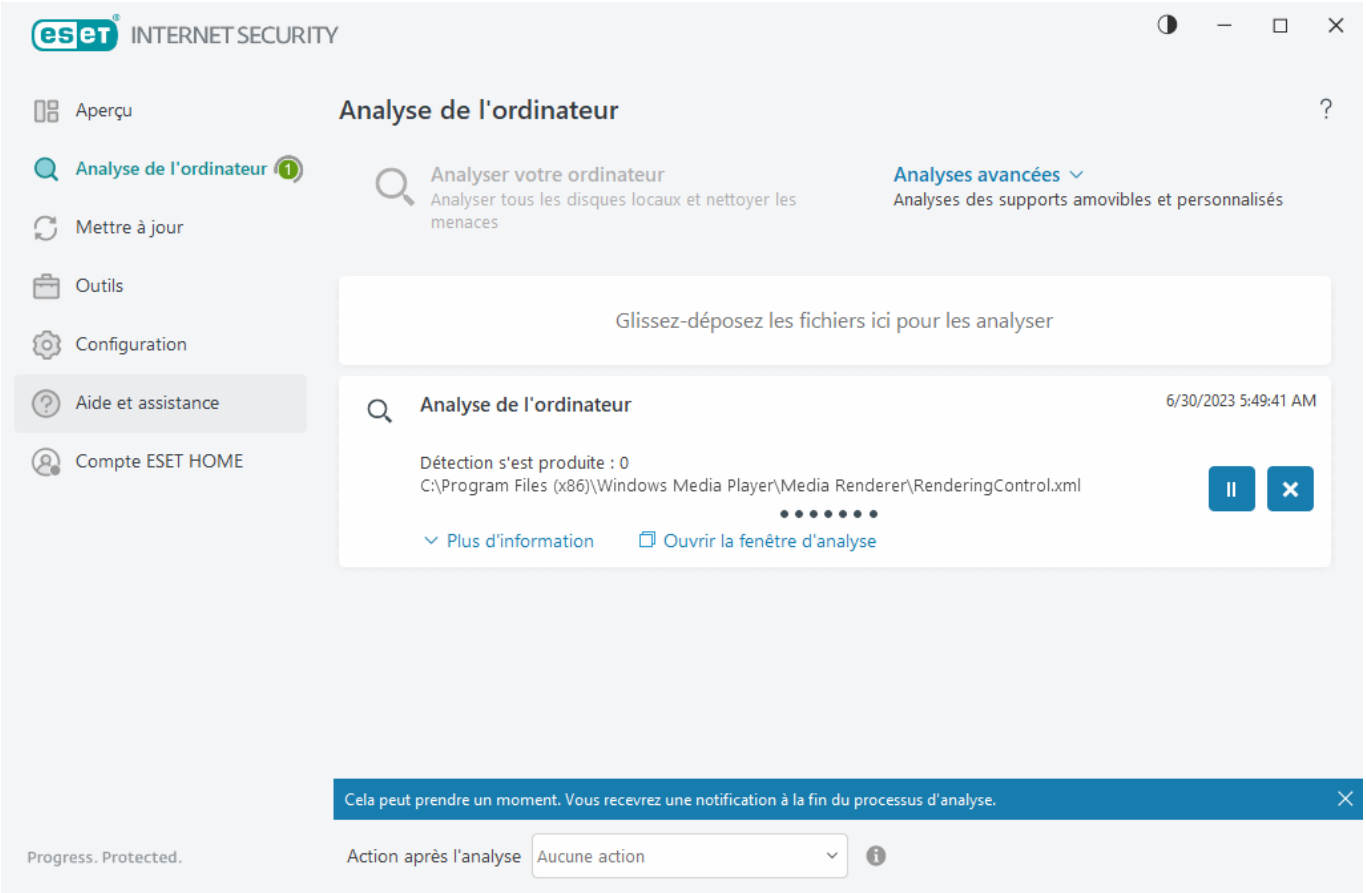
Si le problème persiste, consultez la liste des erreurs d’installation courantes et les solutions recommandées.

Première analyse après l'installation

Après l'installation de ESET Internet Security, une analyse de l'ordinateur débutera automatiquement après la première mise à jour réussie afin de vérifier la présence de code malveillant.

Vous pouvez également lancer manuellement une analyse de l'ordinateur depuis la fenêtre principale du programme > **Analyse de l'ordinateur** > **Analyse intelligente**. Pour plus d'information sur l'analyse de

l'ordinateur, consultez la section Analyse de l'ordinateur.



Mise à niveau à une version plus récente

Les nouvelles versions de ESET Internet Security sont diffusées afin d'apporter des améliorations ou de corriger des problèmes qui ne peuvent être réglés par la mise à jour automatique des modules du programme. La mise à niveau vers une version plus récente peut être effectuée de plusieurs façons :

1. Automatiquement, à l'aide d'une mise à jour du programme.
Puisque la mise à jour du programme est envoyée à tous les utilisateurs et qu'elle peut avoir des répercussions sur les configurations système, elle n'est émise qu'après une longue période de test pour s'assurer qu'elle fonctionne sans heurts avec toutes les configurations système possibles. Si vous devez effectuer la mise à niveau vers une version plus récente, immédiatement après le lancement de cette dernière, utilisez l'une des méthodes indiquées ci-dessous.
Assurez-vous d'avoir activé la **Mises à jour des fonctionnalités de l'application** dans Configuration avancée > **Mise à jour** > **Profils** > **Mises à jour**.

2. Manuellement, dans la fenêtre principale du programme, en cliquant sur **Vérifier les mises à jour** dans la section **Mise à jour**.

3. manuellement, en téléchargeant la mise à niveau et en installant une version plus récente par-dessus l'installation antérieure.

Pour plus d'informations et des instructions illustrées, consultez :

- Mettre à jour les produits ESET – recherher les derniers modules de produit

- Quels sont les différents types de mises à jour et de versions des produits ESET ?

Mise à niveau automatique des anciens produits

La version de votre produit ESET n'est plus prise en charge, et votre produit a été mis à niveau vers la dernière version.

⚠ Problèmes courants d'installation

> ℹ Chaque nouvelle version des produits ESET comporte de nombreuses corrections de bogues et améliorations. Les clients existants possédant un abonnement valide pour un produit ESET peuvent passer gratuitement à la dernière version du même produit.

Suivez ces étapes pour terminer l'installation :

1. Cliquez sur **Accepter et continuer** pour accepter le contrat de licence d'utilisateur final et indiquer avoir pris connaissance de la politique de confidentialité. Si vous n'acceptez pas le contrat de licence d'utilisateur final, cliquez sur **Désinstaller**. Il n'est pas possible de revenir à la version précédente.

2. Cliquez sur **Tout autoriser et continuer** pour autoriser le système de rétroaction ESET LiveGrid® et le programme d'amélioration de l'expérience client ou cliquez sur **Continuer** si vous ne souhaitez pas participer.

3. Après avoir activé le nouveau produit ESET avec votre clé d'activation, la page Vue d'ensemble s'affiche. Si vos informations d'abonnement ne sont pas trouvées, continuez avec un essai gratuit. Si votre abonnement utilisé avec le produit précédent n'est pas valide, activez votre produit ESET.

4. Vous devez redémarrer le périphérique pour terminer l'installation.

ESET Internet Security sera installé

Cette fenêtre de dialogue peut s'afficher :

- Pendant le processus d'installation : cliquez sur **Continuer** pour installer ESET Internet Security.

- Lorsque vous modifiez un abonnement dans ESET Internet Security — Cliquez sur **Activer** pour modifier l'abonnement et activer ESET Internet Security.

L'option **Changer de produit** vous permet de basculer entre différents produits ESET Windows Home en fonction de votre abonnement à ESET. Voir la rubrique Quels sont les produits que je possède ? pour plus de renseignements.

Passer à une autre gamme de produit

En fonction de votre abonnement ESET, vous pouvez basculer entre les différents produits ESET Windows Home. Voir la rubrique Quels sont les produits que je possède ? pour plus de renseignements.

Enregistrement

Veuillez enregistrer votre abonnement en remplissant les champs contenus dans le formulaire d'enregistrement et en cliquant sur **Activer**. Les champs obligatoires doivent absolument être remplis. Cette information ne sera utilisée que pour les questions concernant votre abonnement ESET.

Progression de l'activation

Veuillez allouer quelques secondes pour l'exécution du processus d'activation (le temps requis varie selon la vitesse de votre connexion Internet ou de votre ordinateur).

Activation réussie

Le processus d'activation est terminé. Utilisez l'assistant de post-installation pour terminer la configuration de ESET Internet Security.

Une mise à jour du module commencera dans quelques secondes. Les mises à jour régulières de ESET Internet Security commenceront immédiatement.

Une analyse initiale démarrera automatiquement dans les 20 minutes suivant la mise à jour du module.

> Le processus d'activation peut être interrompu si l'offre n'est pas associée à ESET HOME. Connectez-vous à votre ESET HOME ou créez un compte.

Guide du débutant

Cette rubrique présente un aperçu initial de ESET Internet Security et de ses paramètres de base.

Icône de la barre d'état système

Certaines des options de configuration les plus importantes ainsi que des fonctions sont disponibles en cliquant à l'aide du bouton droit de la souris sur l'icône de la barre d'état système .

Suspendre la protection - Affiche la boîte de dialogue de confirmation qui désactive le Moteur de détection, ce qui protège contre les attaques que pourraient faire des systèmes malveillants en contrôlant la communication par fichiers, au moyen du Web et par courriel. Le menu déroulant **Intervalle** vous permet de spécifier la période pendant laquelle la protection sera désactivée.

Suspendre le coupe-feu (autoriser tout le trafic) - Bascule le coupe-feu à l'état inactif. Voir Réseau pour de plus amples renseignements.

Bloquer le trafic sur tout le réseau - Bloque tout le trafic du réseau. Pour le réactiver, cliquez sur **Arrêter le blocage de tout le trafic du réseau**.

Configuration - Ouvre la configuration avancée de ESET Internet Security. Pour ouvrir la configuration avancée à partir de la fenêtre principale du produit, appuyez sur F5 sur votre clavier ou cliquez sur **Configuration** > **Configuration avancée**.

Fichiers journaux - Les fichiers journaux contiennent les événements importants qui se sont produits et donnent un aperçu des détections.

Ouvrir ESET Internet Security : permet d'ouvrir la fenêtre principale de programme de ESET Internet Security.

Rétablir la disposition de fenêtre - Réinitialise la fenêtre de ESET Internet Security à sa taille et position par défaut, à l'écran.

Mode couleur : permet d'ouvrir les paramètres de l'interface utilisateur où vous pouvez changer la couleur de l'interface utilisateur graphique.

Vérifier les mises à jour : démarre une mise à jour de module ou de produit afin d'assurer votre protection. ESET Internet Security vérifie la mise à jour automatiquement plusieurs fois par jour.

À propos : fournit de l'information sur le système, les détails à propos de la version installée de ESET Internet Security et les modules de programme installés. Vous y trouverez aussi des renseignements sur le système d'exploitation et les ressources du système.

Raccourcis clavier

Pour une navigation plus facile dans ESET Internet Security, vous pouvez utiliser les raccourcis clavier suivants :

Raccourcis clavier	Action
F1	ouvre les pages d'aide
F5	ouvre la configuration avancée
Flèche vers le haut / Flèche vers le bas	navigation dans les éléments du menu déroulant
TAB	passer à l'élément d'interface graphique suivant dans une fenêtre
Shift+TAB	passer à l'élément d'interface graphique précédent dans une fenêtre

Raccourcis clavier	Action
ESC	ferme la boîte de dialogue active
Ctrl+U	affiche des informations sur l'abonnement à ESET et votre ordinateur (Détails pour le service d'assistance technique)
Ctrl+R	rétablit la fenêtre du produit à sa taille et à sa position par défaut à l'écran
ALT + Flèche gauche	Précédent
ALT + Flèche droite	Suivant
ALT+Home	Accueil

Vous pouvez également utiliser les boutons de la souris Précédent ou Suivant pour la navigation.

Profils

Le gestionnaire de profils est utilisé à deux endroits dans ESET Internet Security - dans la section **Analyse à la demande** et dans la section **Mise à jour**.

Analyse de l'ordinateur

Il existe 4 profils d'analyse prédéfinis dans ESET Internet Security :

- **Analyse intelligent** : Il s'agit du profil de numérisation avancée par défaut. Le profil d'analyse intelligente utilise la technologie d'optimisation intelligente, qui exclut les fichiers qui ont été détectés comme étant sains lors d'une analyse précédente et qui n'ont pas été modifiés depuis cette analyse. Cela permet de réduire les temps d'analyse avec un impact minimal sur la sécurité du système.

- **Analyse par menu contextuel :** Vous pouvez démarrer une analyse à la demande de n'importe quel fichier à partir du menu contextuel. Le profil d'analyse du menu contextuel vous permet de définir une configuration d'analyse qui sera utilisée lorsque vous déclencherez l'analyse de cette manière.

- **Analyse détaillée** – Le profil d'analyse approfondie n'utilise pas l'optimisation intelligente par défaut. Par conséquent, aucun fichier n'est exclu de l'analyse lorsque ce profil est utilisé.

- **Analyse de l'ordinateur** : Il s'agit du profil par défaut utilisé dans l'analyse standard de l'ordinateur.

Vos paramètres d'analyse préférés peuvent être enregistrés pour analyse future. Nous vous recommandons de créer un profil différent (avec différentes cibles et méthodes ainsi que d'autres paramètres d'analyse) pour chacune des analyses utilisées régulièrement.

Pour créer un nouveau profil, ouvrez Configuration avancée > **Moteur de détection** > **Analyse des logiciels malveillants** > **Analyse à la demande** > **Liste des profils** > **Modifier**. La fenêtre **Gestionnaire de profils** comprend le menu déroulant **Profil sélectionné** qui affiche les profils d'analyse existants, ainsi que l'option permettant d'en créer un nouveau. Pour vous aider à créer un profil d'analyse répondant à vos besoins, consultez la rubrique ThreatSense pour une description de chacun des paramètres de configuration de l'analyse.

Imaginez que vous vouliez créer votre propre profil d'analyse et que la configuration associée au profil **Analyse de l'ordinateur** vous convienne en partie, mais que vous ne voulez ni analyser les fichiers exécutables compressés par un compresseur d'exécutables ni les applications potentiellement dangereuses et que vous voulez également utiliser un **Toujours corriger la détection**. Entrez le nom de votre nouveau profil dans la fenêtre **Gestionnaire de profil**, puis cliquez sur **Ajouter**. Sélectionnez votre nouveau profil à partir du menu déroulant de **Profil sélectionné**, puis ajustez les paramètres restants pour répondre à vos exigences ; cliquez ensuite sur **OK** pour enregistrer votre nouveau profil.

Mettre 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 opportun de créer et d'utiliser des profils personnalisés (autres que l'option par défaut **Mon profil**) si votre ordinateur utilise plusieurs moyens pour se connecter aux serveurs de mise à jour.

Par exemple, 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) pourrait utiliser deux profils : le premier pour se connecter au serveur local, le second pour se connecter 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 de mise à jour - Le profil de mise à jour actuellement sélectionné. Pour le changer, choisissez un profil dans le menu déroulant.

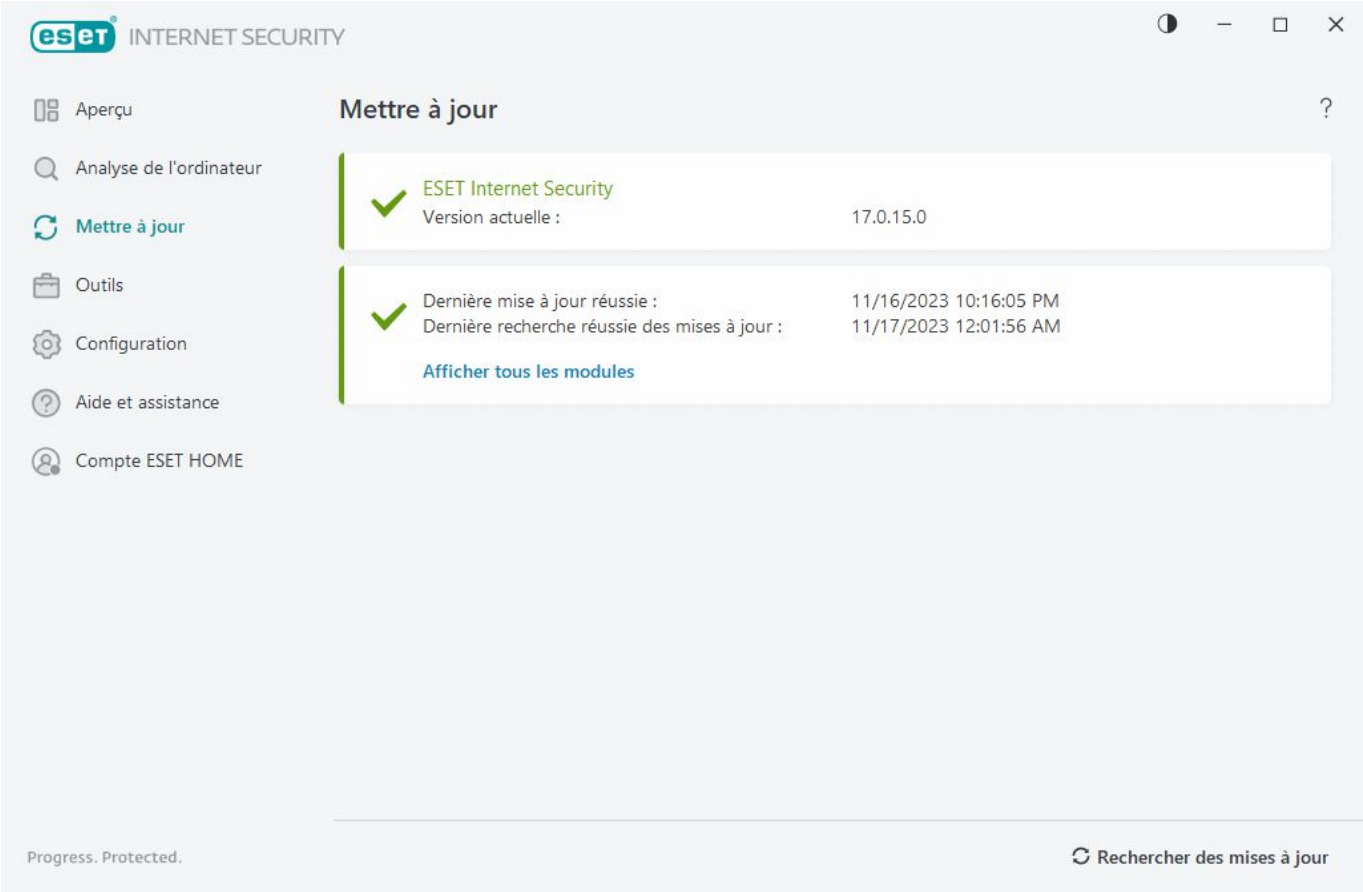
Liste des profils - Créer un nouveau profil ou modifier des profils de mise à jour existants.

Mises à jour

La mise à jour régulière de ESET Internet Security constitue la meilleure méthode pour garantir le niveau maximal de sécurité pour votre ordinateur. Le module Mise à jour garantit que les modules de programme et les composants du système sont toujours à jour.

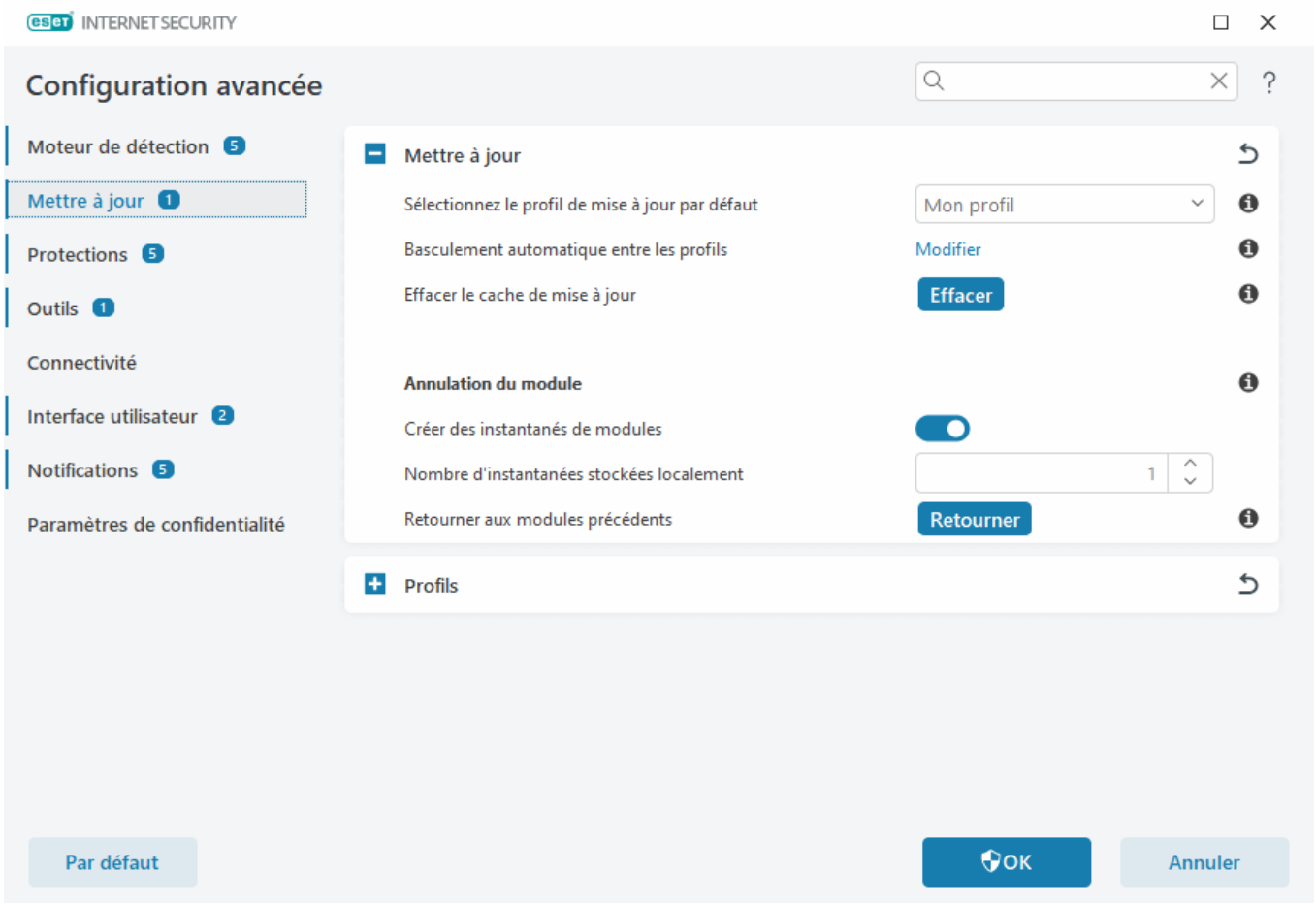
En cliquant sur **Mettre à jour** dans la fenêtre principale du programme, vous pourrez consulter l'état actuel des mises à jour, y compris la date et l'heure de la dernière mise à jour réussie et si une nouvelle mise à jour est requise.

Outre les mises à jour automatiques, vous pouvez cliquer sur **Rechercher les mises à jour** pour déclencher une mise à jour manuelle.



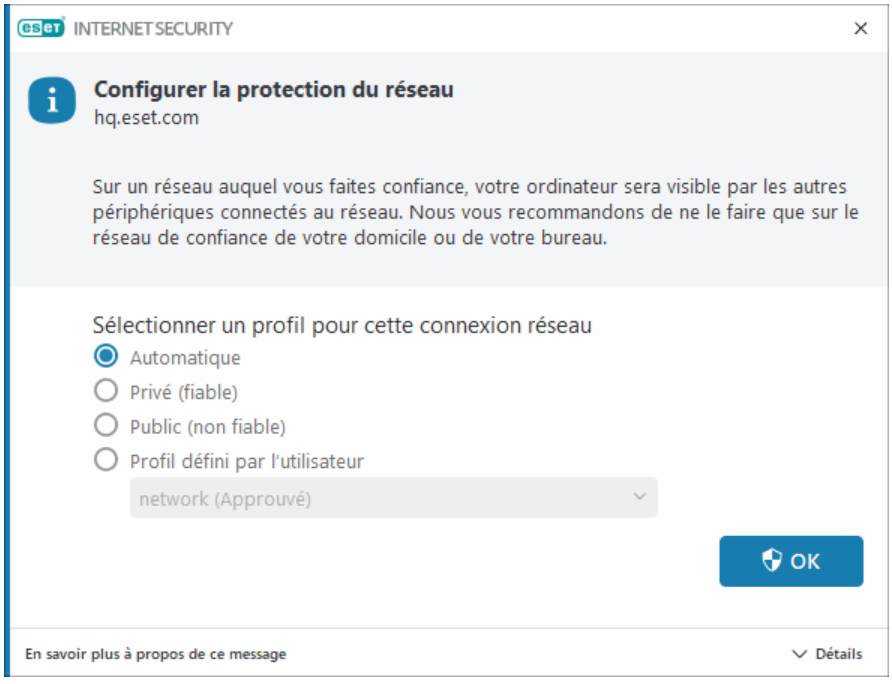
L'option Configuration avancée > **Mises à jour** contient des options de mise à jour supplémentaires telles que le mode de mise à jour, l'accès au serveur mandataire et les connexions LAN.

Si vous rencontrez des problèmes avec une mise à jour, cliquez sur **Effacer** pour effacer le cache de mise à jour. Si vous n'arrivez toujours pas à mettre à jour les modules du programme, reportez-vous à la section Dépannage relatif au message « Échec de la mise à jour des modules ».



Configurer la protection du réseau

Par défaut, ESET Internet Security utilise les paramètres de Windows lorsqu'une nouvelle connexion réseau est détectée. Pour afficher une fenêtre de dialogue lorsqu'un nouveau réseau est détecté, définissez l'affectation du profil de protection du réseau sur **Demander**. La configuration de la protection du réseau s'affichera chaque fois que votre ordinateur se connectera à un nouveau réseau.



Vous pouvez choisir parmi les profils de connexion réseau suivants :

Automatique : ESET Internet Security sélectionnera le profil automatiquement, en fonction des activateurs configurés pour chaque profil.

Privé : pour les réseaux fiables (réseaux domestiques ou professionnels). Votre ordinateur et les fichiers partagés stockés sur votre ordinateur sont visibles par les autres utilisateurs du réseau et les ressources système sont accessibles aux autres utilisateurs du réseau (l'accès aux fichiers et aux imprimantes partagés est activé, la communication RPC entrante est activée et le partage de bureau à distance est disponible). Nous vous recommandons d'utiliser ce paramètre lors de l'accès à un réseau local sécurisé. Ce profil est automatiquement affecté à une connexion réseau si elle est configurée en tant que domaine ou réseau privé dans Windows.

Public : pour les réseaux non fiables (réseaux publics). Les fichiers et les dossiers de votre système ne sont pas partagés ni visibles par d'autres utilisateurs du réseau et le partage des ressources système est désactivé. Nous vous recommandons d'utiliser ce paramètre lors de l'accès aux réseaux sans fil. Ce profil est automatiquement affecté à toute connexion réseau qui n'est pas configurée en tant que domaine ou réseau privé dans Windows.

Profil défini par l'utilisateur : vous pouvez sélectionner un profil que vous avez créé dans le menu déroulant. Cette option n'est disponible que si vous avez créé au moins un profil personnalisé.

⚠ Une configuration incorrecte du réseau peut poser un risque pour la sécurité de votre ordinateur.

Activer Antivol

Les périphériques personnels risquent constamment d'être perdus ou volés lors de nos déplacements quotidiens entre la maison et le travail ou d'autres lieux publics. Antivol est une fonctionnalité qui étend la sécurité au niveau de l'utilisateur lorsque le périphérique est perdu ou volé. Antivol vous permet de surveiller l'utilisation du périphérique et de retrouver votre périphérique disparu grâce à la localisation par adresse IP dans ESET HOME, ce qui vous aide à retrouver votre périphérique et à protéger vos données personnelles.

L'utilisation de technologies modernes telles que la géolocalisation d'adresses IP, la capture d'images de caméra Web, la protection du compte utilisateur et la surveillance de l'appareil dans Antivol peut vous aider ou aider un organisme chargé de l'application de la loi à localiser votre ordinateur ou votre appareil en cas de perte ou de vol. Dans ESET HOME, vous pouvez voir quelle activité a lieu sur votre ordinateur ou votre périphérique.

Pour en savoir plus sur la fonctionnalité Antivol de ESET HOME, consultez l'aide en ligne de ESET HOME.

Antivol peut ne pas fonctionner correctement sur les ordinateurs appartenant à certains domaines en raison de restrictions dans la gestion des comptes d'utilisateurs.

Pour activer Antivol et protéger votre périphérique en cas de perte ou de vol, choisissez l'une des options suivantes :

- Dans la fenêtre principale du programme, accédez à **Vue d'ensemble**, puis cliquez sur **CONFIGURER** en regard de **Antivol**.
- Si le message « Anti-Theft est disponible » s'affiche à l'écran d'**Aperçu** de la fenêtre principale du programme, cliquez sur **Activer Antivol**.
- À partir de la fenêtre principale du programme, cliquez sur **Configuration** > **Outils de sécurité**. Activez le bouton bascule de **Antivol** et suivez les instructions qui s'affichent à l'écran.

Si votre périphérique n'est pas connecté à ESET HOME, vous devez procéder comme indiqué ci-dessous :
1. Connectez-vous à votre compte ESET HOME lors de l'activation de Antivol.
2. Définir un nom pour votre périphérique.

Antivol ne prend pas en charge Microsoft Windows Home Server.

Après avoir activé Antivol, vous pouvez optimiser la sécurité de votre périphérique dans la fenêtre principale du programme > en cliquant sur **Configuration** >**Outils de sécurité** > **Antivol**.

Contrôle parental

Si vous avez déjà activité le contrôle parental dans ESET Internet Security, vous devez également configurer le contrôle parental pour tous les comptes utilisateurs associés.

Lorsque le contrôle parental est actif et que les comptes utilisateur ne sont pas configurés, ESET Internet Security affiche la notification « Le contrôle parental n'est pas configuré » à l'écran **Vue d'ensemble**. Cliquez sur **Configurer les règles** et reportez-vous à la rubrique Contrôle parental pour plus de renseignements.

Activer votre produit

Il existe plusieurs méthodes pour activer votre produit. La disponibilité d'un scénario d'activation particulier dans la fenêtre d'activation peut varier selon le pays, ainsi que selon le moyen de distribution (CD/DVD, page Web d'ESET, etc.).

- Si vous avez acheté une version du produit en boîte au magasin ou si vous avez reçu un courriel avec les détails de l'abonnement, activez votre produit en cliquant sur **Utiliser une clé d'activation achetée**. Pour réussir l'activation, vous devez entrer la clé d'activation telle qu'elle vous a été fournie. La clé d'activation est une chaîne de caractères unique dans le format XXXX-XXXX-XXXX-XXXX-XXXX ou XXXX-XXXXXXXX utilisée pour l'identification du propriétaire de l'abonnement et pour l'activation de ce dernier. La clé d'activation se trouve généralement à l'intérieur ou sur la face arrière de l'emballage du produit.

- Après avoir sélectionné Utiliser le compte ESET HOME, il vous sera demandé de vous connecter à votre compte ESET HOME.

- Si vous souhaitez évaluer ESET Internet Security avant de l'acheter, sélectionnez Licence d'essai gratuite. Inscrivez votre adresse courriel et votre pays pour activer ESET Internet Security pour une durée limitée. Votre essai gratuit vous sera envoyé par courriel. Les essais gratuits ne peuvent être activés qu'une seule fois par client.

- Si vous n'avez pas d'abonnement et souhaitez en acheter un, cliquez sur **Acheter un abonnement**. Vous serez redirigé vers le site Web de votre distributeur ESET local. Les abonnements aux produits ESET Windows pour particuliers ne sont pas gratuits.

Vous pouvez changer votre abonnement de produit à tout moment. Pour ce faire, cliquez sur **Aide et assistance** > **Changer d'abonnement** dans la fenêtre principale du programme. L'identifiant public qui est utilisé pour identifier votre abonnement au sSoutien ESET s'affichera.

Impossible d'activer le produit ?

Saisie de votre clé d’activation pendant l’activation

Les mises à jour automatiques sont importantes pour votre sécurité. ESET Internet Security ne recevra des mises à jour qu'une fois activé.

Lorsque vous entrez votre **clé d’activation**, il est important de l'entrer exactement comme elle est écrite. Votre clé d’activation est une chaîne de caractères unique au format XXXX-XXXX-XXXX-XXXX-XXXX utilisée pour l'identification du propriétaire de l’abonnement et pour l'activation de ce dernier.

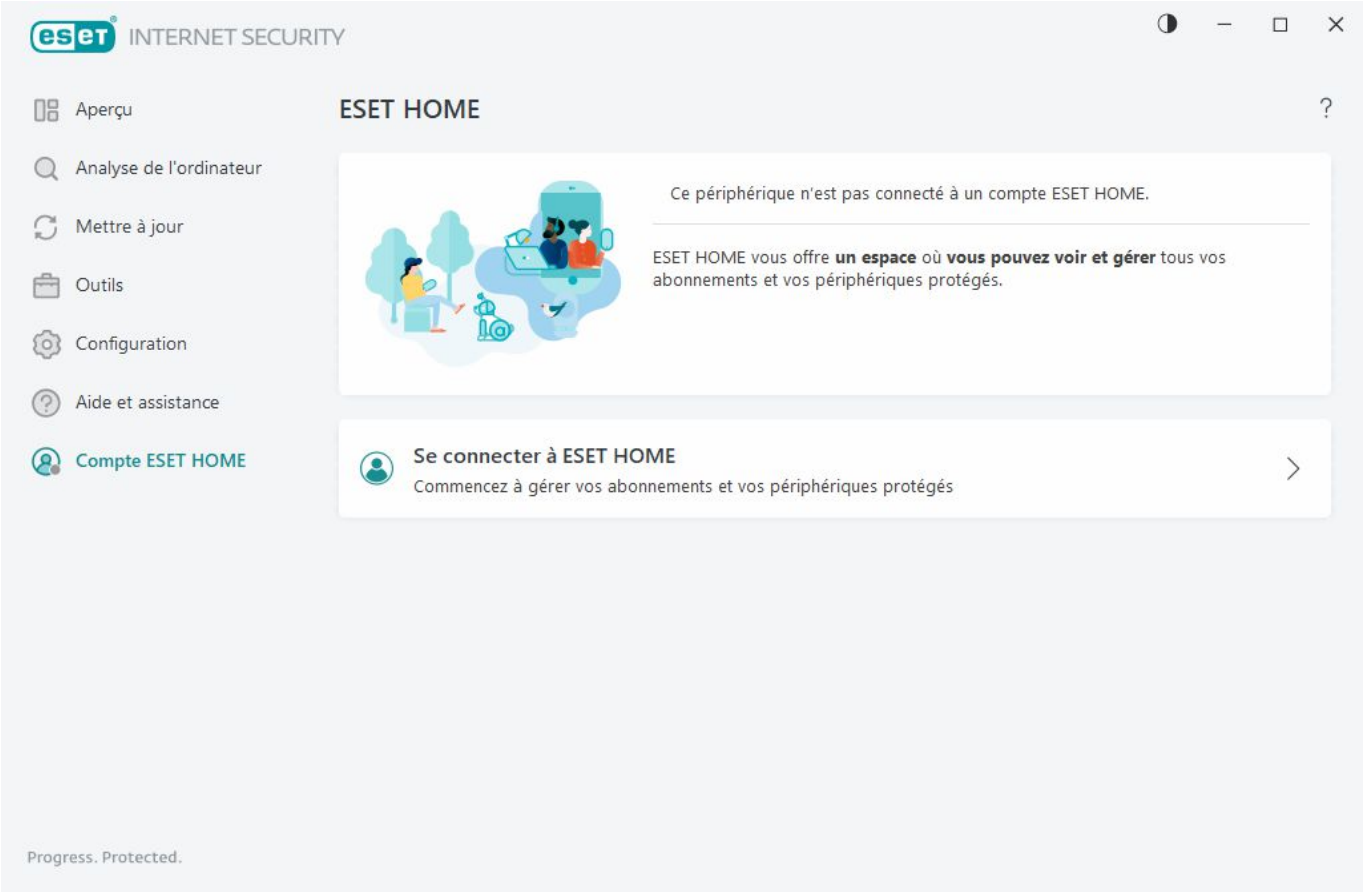
Il est recommandé de copier et de coller votre clé d’activation à partir du courriel d'inscription reçu pour assurer l'exactitude.

Si vous n'avez pas saisi votre clé d’activation après l'installation, votre produit ne sera pas activé. Dans la fenêtre principale du programme, cliquez sur **Aide et assistance** > **Activer l’abonnement** pour activer ESET Internet Security.

Les abonnements aux produits ESET Windows pour particuliers ne sont pas gratuits.

Utiliser le ESET HOME compte

Connectez votre périphérique au ESET HOME pour consulter et gérer tous vos abonnements à ESET activés et vos périphériques. Vous pouvez renouveler, mettre à niveau ou prolonger votre abonnement et afficher les détails importants. Dans le portail de gestion de ESET HOME ou dans l'application mobile, vous pouvez ajouter différents abonnements, télécharger des produits sur vos périphériques, vérifier l'état de sécurité des produits ou partager des abonnements par courriel. Pour plus d'informations, visitez l'aide en ligne de ESET HOME.



Après avoir sélectionné **Utiliser le compte ESET HOME** comme méthode d'activation ou lors de la connexion au compte ESET HOME pendant l'installation :

1. Connectez-vous à votre compte ESET HOME.

> Si vous n'avez pas encore de compte ESET HOME, cliquez sur **Créer un compte** pour vous inscrire ou consultez les instructions dans l'aide en ligne de ESET HOME.
> Si vous avez oublié votre mot de passe, cliquez sur **J'ai oublié mon mot de passe** et suivez les instructions qui s'affichent à l'écran ou consultez les instructions dans l'aide en ligne de ESET HOME.

2. Définissez un **nom pour votre périphérique** qui sera utilisé dans tous les services ESET HOME et cliquez sur **Continuer**.

3. Choisissez un abonnement pour l'activation ou ajoutez un nouvel abonnement. Cliquez sur **Continuer** pour activer ESET Internet Security.

Activer l\'essai gratuit

Pour activer la version d'essai de votre ESET Internet Security, entrez une adresse courriel valide dans le champ **Adresse courriel** et **confirmez l'adresse courriel**. Après l'activation, votre abonnement ESET sera générée et vous sera envoyée par courriel. Cette adresse courriel sera également utilisée pour les notifications d'expiration du produit et pour toute autre communication avec ESET. La version d'essai ne peut être activée qu'une seule fois.

Sélectionnez votre pays dans le menu déroulant **Pays** pour enregistrer ESET Internet Security auprès de votre distributeur local qui vous fournira de l'assistance technique.

Clé d’activation ESET gratuite

L’abonnement à ESET Internet Security n’est pas gratuit.

La clé d’activation ESET consiste en une séquence unique de lettres et de chiffres séparés par des tirets, fournis par ESET afin de permettre l'utilisation légale de ESET Internet Security, conformément au Contrat de licence d'utilisateur final. Chaque utilisateur final est autorisé à utiliser la clé d’activation uniquement dans la mesure où il a le droit d'utiliser ESET Internet Security en fonction du nombre de licences accordées par ESET. La clé d’activation est considérée comme confidentielle et ne peut pas être partagée; toutefois, vous pouvez partager un abonnement à l’aide du fichier ESET HOME.

Vous pouvez vous procurer une clé d’activation ESET « gratuite » sur Internet, mais gardez à l’esprit les éléments suivants :

- Cliquer sur une publicité « Abonnement ESET gratuite » peut endommager votre ordinateur ou votre périphérique et faire en sorte qu'il soit infecté par des logiciels malveillants. Les logiciels malveillants peuvent être cachés dans des contenus non officiels (par exemple des vidéos), des sites Web qui affichent des publicités pour gagner de l'argent en fonction de vos visites, etc. Il s'agit généralement de pièges.

- ESET est en mesure de désactiver les abonnements piratés.

- Utiliser une clé d’activation piratée constitue une violation du Contrat de licence d'utilisateur final que vous devez accepter avant d'installer ESET Internet Security.

- Achetez des abonnements à ESET uniquement par l’intermédiaire de circuits officiels tels que www.eset.com, les distributeurs ou les revendeurs ESET (n'achetez pas d’abonnements sur des sites tiers non officiels tels que eBay ni d’abonnements partagées provenant d’un tiers).

- Télécharger un ESET Internet Security est gratuit, mais l’activation pendant l’installation nécessite une clé d’activation ESET valide (le produit peut être téléchargé et installé, mais doit être activé pour fonctionner).

- Ne partagez pas votre abonnement sur Internet ou sur les réseaux sociaux (il pourrait se propager).

Pour détecter un abonnement pirate à ESET et le signaler, consultez notre article sur la base de connaissances.

Si vous n'êtes pas sûr de vouloir acheter un produit de sécurité ESET, vous pouvez utiliser une version d'essai afin de prendre une décision :

1. Activez ESET Internet Security à l’aide d’un essai gratuit

2. Participez au programme bêta d'ESET

3. Installez ESET Mobile Security si vous utilisez un périphérique mobile Android; il s'agit d'un freemium.

Pour obtenir une réduction ou prolonger votre licence, renouvelez votre licence ESET.

Échec de l'activation – scénarios courants

Si l’activation de ESET Internet Security échoue, les scénarios les plus courants sont les suivants :

- La clé d’activation est déjà utilisée.
- Vous avez entré une clé d\'activation non valide.
- Les informations du formulaire d’activation sont absentes ou non valides.
- Échec de la communication avec le serveur d’activation.
- Aucune connexion ou connexion désactivée aux serveurs d'activation ESET.

Vérifiez que vous avez saisi la clé d’activation appropriée et que votre connexion Internet est active. Réessayez d’activer ESET Internet Security. Si vous utilisez un compte ESET HOME pour l’activation, consultez l’aide en ligne sur l’abonnement et la gestion des abonnements à ESET HOME.

Si vous recevez une erreur spécifique (par exemple, abonnement suspendu ou abonnement surutilisé), suivez les instructions dans l’état de l’abonnement.

Si vous ne reussissez toujours pas à effectuer l'activation ESET Internet Security, l’utilitaire de résolution des problèmes d’activation d'ESET vous guidera à travers les questions courantes, les erreurs et les problèmes liés à l’activation et aux licences (disponibles en anglais et dans plusieurs autres langues).

État d’abonnement

Votre abonnement peut avoir différents états. Vous trouverez l’état de votre abonnement dans la section ESET HOME. Si vous souhaitez ajouter votre abonnement à votre compte ESET HOME, consultez la rubrique Ajouter un abonnement.

Si vous n’avez pas de compte ESET HOME, vous pouvez créer un compte ESET HOME.

Si l’état de l’abonnement est autre qu’**Actif**, vous recevez une erreur pendant l’activation ou une notification dans la fenêtre principale du programme.

Pour désactiver les notifications d’état de l’abonnement, ouvrez Configuration avancée > **Notifications** > **États de l'application**. Cliquez sur **Modifier** à côté du menu **États de l'application**, développez **Licence** et décochez la case à côté de la notification que vous souhaitez désactiver. La désactivation des notifications ne permet pas de résoudre le problème.

Consultez les descriptions et les solutions recommandées pour différents états d’abonnement dans le tableau suivant :

État d'abonnement	Description	Solution
Active	L'abonnement est valide, et il n'y a pas besoin de votre intervention. ESET Internet Security peut être activé, et vous pouvez trouver les détails de l'abonnement dans la fenêtre principale du programme sous **Aide et assistance**.	
Surutilisée	Le nombre de périphériques utilisant cet abonnement est supérieur à celui autorisé. Vous recevrez une erreur d'activation.	Consultez la rubrique Échec de l'activation en raison d'un abonnement surutilisé pour plus d'information.
Suspendue	Votre abonnement a été suspendu en raison de problèmes de paiement. Pour utiliser l'abonnement, assurez-vous que vos informations de paiement dans ESET HOME sont à jour ou contactez votre revendeur d'abonnement. Cette erreur peut se produire lors de l'activation ou dans la fenêtre principale du programme.	Produit installé : si vous possédez un compte ESET HOME, accédez à la notification affichée dans la fenêtre principale du programme, cliquez sur **Gérer votre abonnement dans ESET HOME** et vérifiez les informations relatives à votre paiement. Sinon, contactez votre revendeur d'abonnement. Erreur d'activation : si vous possédez un compte ESET HOME, accédez à la notification d'erreur d'activation, cliquez sur **Ouvrir ESET HOME** et vérifiez les informations relatives à votre paiement. Sinon, contactez votre revendeur d'abonnement.
Expirée	Votre abonnement est arrivé à expiration. Vous ne pouvez donc pas l'utiliser pour activer ESET Internet Security. Cette erreur peut se produire lors de l'activation ou dans la fenêtre principale du programme. Si ESET Internet Security est déjà installé, votre ordinateur n'est pas protégé ou sa protection n'est pas à jour.	Produit installé : à partir de la notification affichée dans la fenêtre principale du programme, cliquez sur **Renouveler l'abonnement** et suivez les instructions de renouvellement de l'abonnement dans Comment renouveler mon abonnement? ou cliquez sur **Activer le produit** et choisissez la méthode d'activation. Erreur d'activation : à partir de la fenêtre d'erreur d'activation, cliquez sur **Renouveler l'abonnement** et suivez les instructions de renouvellement de l'abonnement dans Comment renouveler mon abonnement? Vous pouvez également saisir une nouvelle clé d'activation ou une clé renouvelée, puis cliquer sur **Renouveler l'abonnement**.
Annulée	Votre abonnement a été annulé par ESET ou par votre revendeur d'abonnement.	Si vous recevez l'erreur suivante : Abonnement annulé dans la fenêtre principale du programme ou pendant l'activation et que votre abonnement devrait fonctionner correctement, contactez votre revendeur d'abonnement.

L'activation a échoué en raison d'une surutilisation d’abonnement

Problème

- Votre abonnement peut être surutilisé ou abusé
- L'activation a échoué en raison d'une surutilisation d’abonnement

Solution

Le nombre de périphériques utilisant cet abonnement est supérieur à celui qu’il autorise. Il se peut que vous soyez victime de piratage ou de contrefaçon de logiciels. L’abonnement ne peut pas être utilisé pour activer un autre produit ESET. Vous pouvez résoudre ce problème directement si vous êtes autorisé à gérer l’abonnement dans votre compte ESET HOME ou si vous avez acheté l’abonnement auprès d'une source légitime. Si vous n'avez pas encore de compte, créez-en un.

Si vous êtes propriétaire d’un abonnement et que vous n'avez pas été invité à saisir votre adresse de courriel :

1. Pour gérer votre abonnement à ESET, ouvrez un navigateur Web et naviguez vers le site https://home.eset.com. Accédez à ESET License Manager et supprimez ou désactivez des sièges. Pour plus d'informations, consultez la rubrique Que faire en cas de surutilisation d’un abonnement?.

2. Pour identifier et signaler un abonnement ESET piraté, consultez l'article Reconnaitre et signaler des abonnements piratés à ESET pour obtenir des instructions.

3. En cas de doute, cliquez sur **Retour** et envoyez un courriel au service d'assistance technique d'ESET.

Si vous n’êtes pas le propriétaire d’un abonnement, communiquez avec le propriétaire de cet abonnement en lui indiquant que vous ne pouvez pas activer le produit ESET en raison d'une surutilisation de l’abonnement. Le propriétaire peut résoudre le problème dans le portail ESET HOME.

Si vous êtes invité à confirmer votre adresse de courriel (dans plusieurs casseulement), entrez l'adresse de courriel utilisée à l'origine pour acheter ou activer votre ESET Internet Security.

Utilisation de ESET Internet Security

La fenêtre principale de ESET Internet Security est divisée en deux sections. La fenêtre principale, du côté droit, affiche l'information qui correspond à l'option sélectionnée à partir du menu principal de gauche.

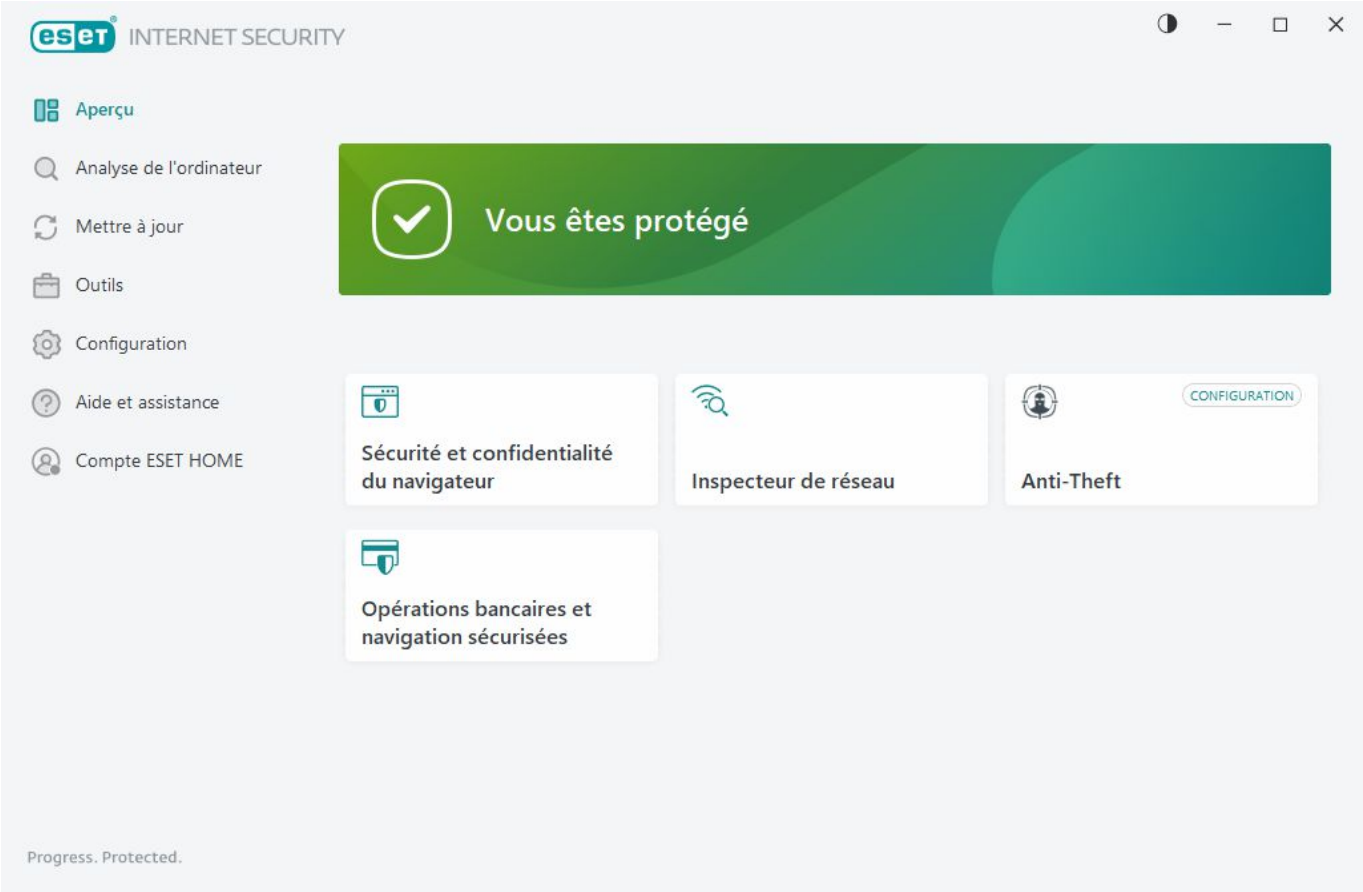
> **Instructions illustrées**
> Reportez-vous à la rubrique Ouvrir la fenêtre principale du programme des produits ESET pour Windows pour obtenir des instructions illustrées disponibles en anglais et dans plusieurs autres langues.

Vous pouvez sélectionner le jeu de couleurs de l’interface graphique de ESET Internet Security dans le coin supérieur droit de la fenêtre principale du programme. Cliquez sur l'icône **Jeu de couleurs** (l'icône change en fonction du jeu de couleurs sélectionné) à côté de l'icône **Minimiser** et sélectionnez le jeu de couleurs dans le menu déroulant :

• L’option **Identique à la couleur du système** définit le jeu de couleurs de ESET Internet Security selon la configuration du système d’exploitation.

• **Sombre** : ESET Internet Security utilisera un jeu de couleurs sombres (mode sombre).

• **Clair** : ESET Internet Security utilisera un jeu de couleur clair standard.



Options du menu principal :

Aperçu - Donne de l'information sur l'état de protection de ESET Internet Security.

Analyse de l'ordinateur - Configurez et lancez une analyse de votre ordinateur ou créez une analyse personnalisée.

Mise à jour : affiche des informations sur les mises à jour du module et du moteur de détection.

Outils : donne accès à Inspecteur de réseau et à d’autres fonctionnalités qui contribuent à simplifier l'administration du programme et offrent des options supplémentaires aux utilisateurs expérimentés.

Configuration : propose des options de configuration pour les fonctionnalités de protection de ESET Internet Security (protection de l'ordinateur, protection de l'Internet, protection du réseau et outils de sécurité) et donne accès à la configuration avancée.

Aide et assistance : affiche des informations sur votre abonnement, le produit ESET installé, ainsi que des liens vers l’aide en ligne, la base de connaissances ESET et l’assistance technique.

Compte ESET HOME : connectez votre périphérique à ESET HOME ou vérifiez l’état de connexion du compte ESET HOME. Utilisez ESET HOME pour consulter et gérer vos paramètres Antivol ainsi que les abonnements et les périphériques ESET activés.

Vue d'ensemble

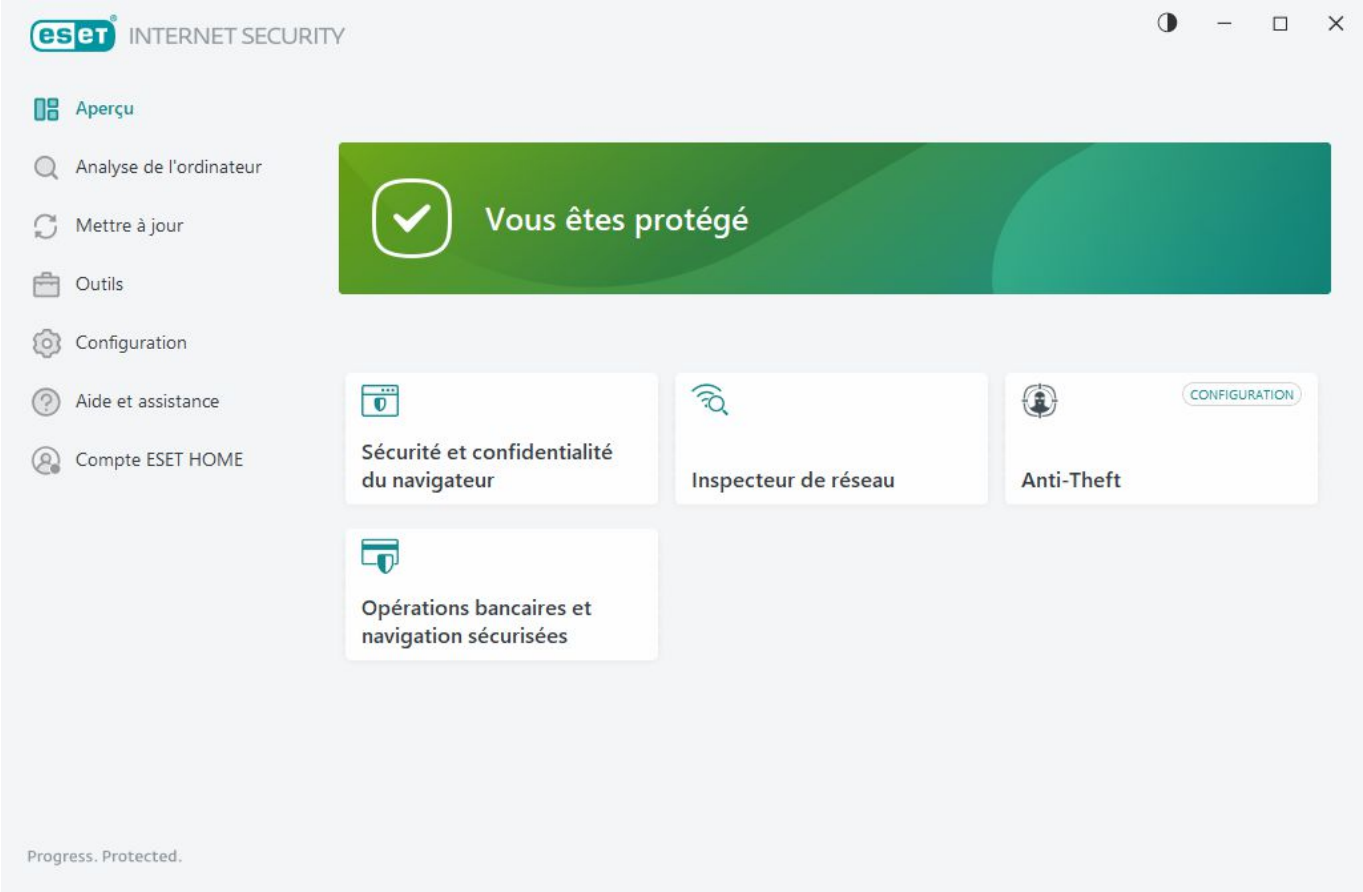
La fenêtre **Vue d'ensemble** affiche des informations sur la protection actuelle de votre ordinateur et offre des liens rapides vers les fonctionnalités de sécurité de ESET Internet Security.

La fenêtre **Vue d'ensemble** affiche des notifications avec des informations détaillées et des solutions recommandées pour améliorer la sécurité de ESET Internet Security, activer d'autres fonctionnalités ou garantir une protection maximale. S'il y a plusieurs notifications, cliquez sur **X plus de notifications** pour tout développer.

Inspecteur de réseau – Vérifiez la sécurité de votre réseau

Opérations bancaires et navigation sécurisées : lance le navigateur, défini par défaut dans Windows, en mode sécurisé.

Antivol : démarre la configuration de Antivol. Si vous avez déjà configuré Antivol, le lien rapide ouvre la page de Antivol.



L'icône verte, tout comme le message d'état **Vous êtes protégé(e)** qui s'affiche en vert, indique que la protection maximale est assurée.

Que faire lorsque le programme ne fonctionne pas correctement?

Si un module de protection actif fonctionne correctement, l'icône de l'état de la protection sera vert. Un point d'exclamation rouge ou une icône de notification orange indique que la protection maximale n'est pas assurée. Des renseignements supplémentaires sur l'état de la protection de chaque module, ainsi que des suggestions de

solution pour restaurer la protection complète, seront alors affichés sous forme de notification dans la fenêtre **Aperçu**. Pour modifier l'état de chacun des modules, cliquez sur **Configuration** et sélectionnez le module voulu.

L'icône rouge et l'état rouge de l'**alerte de sécurité** indiquent des problèmes critiques. Plusieurs motifs peuvent entraîner l'affichage de cet état, notamment :

- **Produit non activé** ou **Abonnement expiré** - Ce problème est signalé par une icône d'état de la protection rouge. Une fois votre abonnement expiré, le programme ne pourra plus effectuer de mise à jour. Suivez les instructions indiquées dans la fenêtre d'alerte pour renouveler votre abonnement.
- **Le moteur de détection n'est plus à jour** - Cette erreur apparaît après plusieurs tentatives infructueuses de mise à jour du moteur de détection. Nous recommandons de vérifier les paramètres de mise à jour. La cause la plus courante de cette erreur est une entrée incorrecte des données d'authentification ou une configuration incorrecte des paramètres de connexion.
- **Protection en temps réel du système de fichiers désactivée** - La protection en temps réel a été désactivée par l'utilisateur. Votre ordinateur n'est pas protégé contre les menaces. Cliquez sur **Activer la protection en temps réel du système de fichiers** pour réactiver cette fonctionnalité.
- **Protection antivirus et anti-logiciel espion désactivée** - Vous pouvez réactiver la protection antivirus et antispyware en cliquant sur **Activer la protection antivirus et anti-logiciel espion**.
- **Pare-feu d'ESET désactivé** - Ce problème est indiqué par une notification de sécurité à côté de l'élément **Réseau** de votre poste de travail. Vous pouvez réactiver la protection réseau en cliquant sur **Activer le pare-feu**.

L'icône orange indique que la protection est limitée. Par exemple, il pourrait y avoir un problème dans la mise à jour du programme ou la date d'expiration de votre abonnement pourrait approcher.

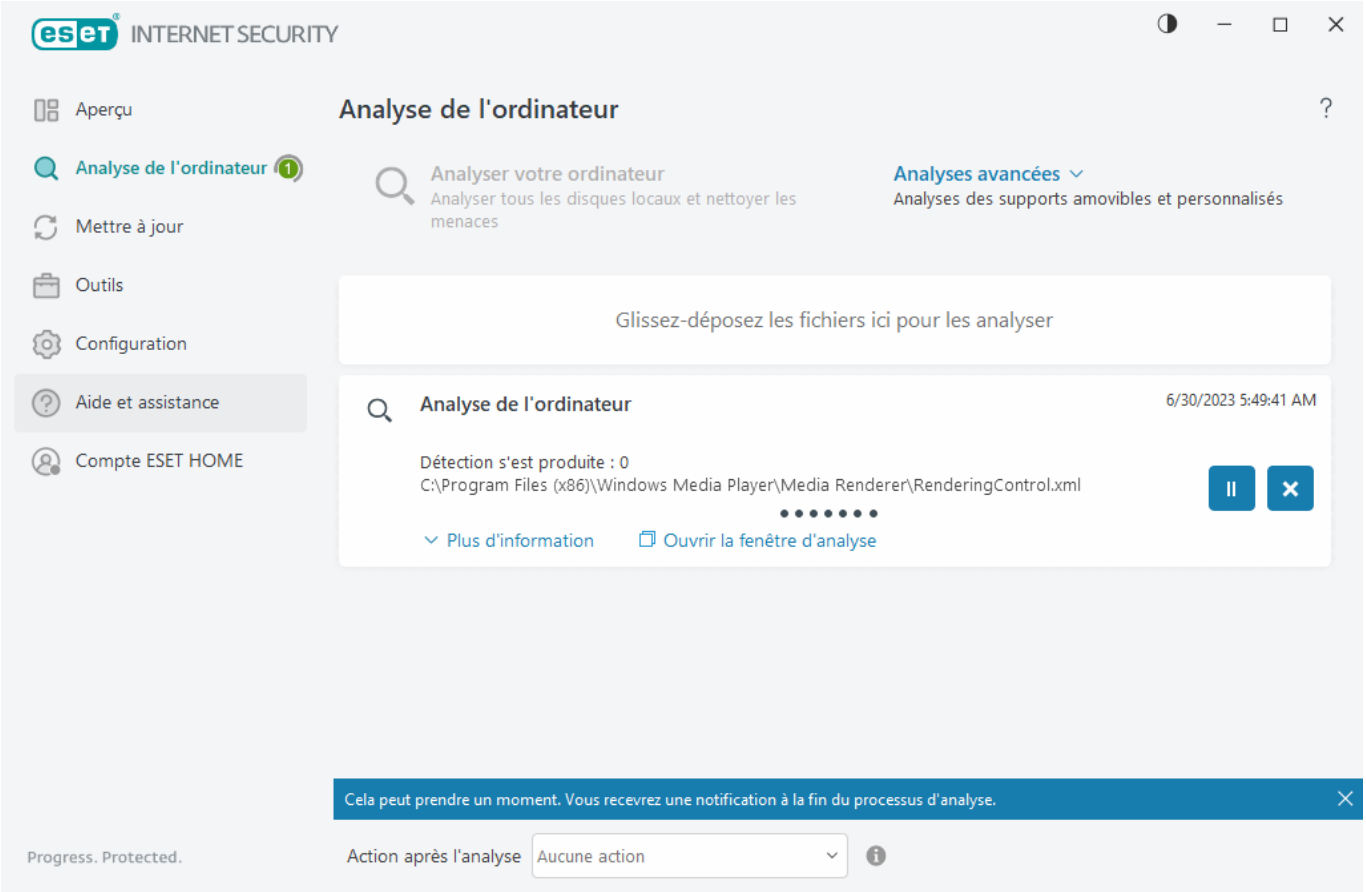
Plusieurs motifs peuvent entraîner l'affichage de cet état, notamment :

- **Avertissement sur l'optimisation d'Antivol** - Cet appareil n'est pas optimisé pour Antivol. Par exemple, un compte fantôme (fonction de sécurité qui se déclenche automatiquement lorsque vous signalez votre appareil comme manquant) pourrait ne pas avoir été créé sur votre ordinateur. Vous pouvez créer un compte fantôme à l'aide de la fonction Optimisation dans l'interface Web d'Antivol.
- **Mode jeu activé** - Activer le mode Jeu entraîne un risque potentiel à la sécurité. En activant cette fonctionnalité, toutes les fenêtres de notification ou d'alerte seront désactivées et les tâches planifiées seront suspendues.
- **Votre abonnement va bientôt expirer/Votre abonnement expire aujourd'hui** : l'icône de l'état de la protection affiche un point d'exclamation à côté de l'horloge du système. Une fois votre abonnement expiré, le programme ne pourra plus se mettre à jour et l'icône de l'état de protection du logiciel deviendra rouge.

S'il vous est impossible de régler un problème à l'aide des solutions suggérées, cliquez sur **Aide et assistance** pour accéder aux fichiers d'aide ou effectuez une recherche dans la base de connaissances d'ESET. Pour obtenir plus d'assistance, vous pouvez envoyer une demande d'assistance. Le service d'assistance technique d'ESET répondra rapidement à vos questions et essaiera de trouver une solution à votre problème.

Analyse de l'ordinateur

L'analyseur à la demande est un élément important de votre solution antivirus. Il permet d'analyser les fichiers et répertoires stockés sur votre ordinateur. Pour votre sécurité, il est essentiel que l'ordinateur soit analysé régulièrement dans le cadre de mesures de sécurité routinières et non seulement en cas de suspicion d'une infection. Nous vous recommandons d'effectuer régulièrement des analyses en profondeur de votre système pour détecter les virus qui ne sont pas capturés par la protection en temps réel du système de fichiers lors de leur écriture sur le disque. Cela peut arriver si la protection en temps réel du système de fichiers est désactivée à un moment, si le moteur de détection est obsolète ou si le fichier n'a pas été détecté comme un virus au moment où il a été enregistré sur le disque.



Deux types d'**analyse de l'ordinateur** sont disponibles. **Analyse de votre ordinateur** analyse rapidement le système, sans avoir à préciser de paramètres d'analyse. L'**analyse personnalisée** (sous Analyse avancée) permet quant à elle de sélectionner parmi des profils d'analyse prédéfinis conçus pour cibler des emplacements spécifiques, et de choisir des cibles d'analyse spécifiques.

Voir la section Progression de l'analyse pour plus de détails sur le processus d'analyse.

> Par défaut, ESET Internet Security tente de nettoyer ou de supprimer automatiquement les détections trouvées lors de l'analyse de l'ordinateur. Dans certains cas, si aucune action ne peut être effectuée, vous recevez une alerte interactive et devez sélectionner une action de nettoyage (par exemple, supprimer ou ignorer). Pour modifier le niveau de nettoyage et obtenir des informations plus détaillées, consultez la rubrique Nettoyage. Pour consulter les analyses précédentes, consultez les fichiers journaux.

Analyse de votre ordinateur

L'analyse de votre ordinateur vous permet de lancer rapidement une analyse de l'ordinateur et de nettoyer les fichiers infectés sans intervention de l'utilisateur. L'avantage de l'**analyse de votre ordinateur** est qu'elle est facile à utiliser et n'exige pas une configuration détaillée de l'analyse. Cette vérification analyse tous les fichiers sur les disques durs locaux et nettoie ou supprime automatiquement les infiltrations détectées. Le niveau de nettoyage est automatiquement réglé à une valeur par défaut. Pour plus de détails sur les types de nettoyage, consultez la rubrique Nettoyage.

Vous pouvez également utiliser la fonction **Glisser-déposer pour analyser** pour analyser un fichier ou un dossier manuellement en cliquant sur le fichier ou le dossier, en déplaçant le pointeur de la souris sur la zone marquée tout en maintenant le bouton de la souris enfoncé, puis en le relâchant. Après cela, l'application est déplacée au premier plan.

Les options d'analyse suivantes sont disponibles sous **Analyses avancées** :

 Analyse personnalisée

L'analyse personnalisée permet de préciser des paramètres d'analyse tels que les cibles et les méthodes. L'avantage de l'**analyse personnalisée** est que vous pouvez configurer les paramètres de façon détaillée. Les configurations peuvent être enregistrées comme des profils d'analyse définis par l'utilisateur, ce qui peut être utile pour effectuer régulièrement une analyse avec les mêmes paramètres.

 Analyse des supports amovibles

Semblable à **Analyse de votre ordinateur** - lance rapidement une analyse des supports amovibles (comme les CD/DVD/USB) actuellement connectés à 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.

Ce type d'analyse peut aussi être lancé en cliquant sur **Analyse personnalisée**, en sélectionnant **Supports amovibles** dans le menu déroulant **Cibles à analyser**, avant de cliquer sur **Analyser**.

 Répéter la dernière analyse utilisée

Vous permet de lancer rapidement la dernière analyse utilisée, avec les même paramètres.

Le menu déroulant**Action après analyse** vous permet de définir une action à effectuer automatiquement une fois l'analyse terminée :

- **Aucune action** - À la fin de l'analyse, aucune action ne sera effectuée.
- **Éteindre** - L'ordinateur s'éteint après l'analyse.
- **Redémarrer si nécessaire :** l'ordinateur redémarre uniquement si cela est nécessaire pour terminer le nettoyage des menaces détectées.
- **Redémarrer** - Ferme tous les programmes et redémarre l'ordinateur après l'analyse.
- **Forcer le redémarrage si nécessaire :** l'ordinateur redémarre uniquement si cela est nécessaire pour terminer le nettoyage des menaces détectées.
- **Forcer le redémarrage** - Force la fermeture de tous les programmes ouverts sans attendre aucune action de l'utilisateur et redémarre l'ordinateur après la fin de l'analyse.
- **Mettre en veille** - Enregistre votre session et met l'ordinateur dans un état de basse consommation afin que vous puissiez reprendre rapidement votre travail.
- **Hiberner** - Met tout ce qui est en cours d'exécution sur la RAM dans un fichier spécial de votre disque dur. Votre ordinateur s'éteint, mais retrouvera son état précédent au prochain démarrage.

Les actions **Mettre en veille** ou **Hiberner** sont disponibles en fonction des paramètres d'alimentation et de veille du système d'exploitation ainsi que des capacités de votre ordinateur. Gardez présent à l'esprit qu'un ordinateur en veille fonctionne toujours. Les fonctions de base s'exécutent toujours et votre ordinateur reste alimenté lorsqu'il fonctionne sur batterie. Pour préserver la batterie, par exemple lorsque vous êtes en dehors de votre bureau, nous vous recommandons d'utiliser l'option Hiberner.

L'action sélectionnée commencera une fois que toutes les analyses en cours sont terminées. Lorsque vous sélectionnez **Arrêter** ou **Redémarrer**, une boîte de dialogue de confirmation affiche un compte à rebours de 30 secondes (cliquez sur **Annuler** pour désactiver l'action demandée).

Il est recommandé d'exécuter une analyse de l'ordinateur au moins une fois par mois. Cette analyse peut être configurée comme tche planifiée dans **Outils** > **Planificateur**. Comment planifier une analyse hebdomadaire d'un ordinateur ?

Analyse personnalisée

Vous pouvez utiliser l'analyse personnalisée pour analyser la mémoire d'exploitation, le réseau ou des parties spécifiques d'un disque plutôt que le disque entier. Pour le faire, cliquez sur **Analyse avancée** > **Analyse personnalisée** ou des cibles particulières dans la structure arborescente des dossiers.

Vous pouvez choisir le profil à utiliser pour analyser des cibles précises dans le menu déroulant **Profil**. Le profil par défaut est celui de l'**analyse intelligente**. Il existe trois autres profils d'analyse prédéfinis appelés **Analyse approfondie** et **Analyse par menu contextuel** et **Analyse de l'ordinateur**. Ces profils d'analyse utilisent différents paramètres ThreatSense. Les options disponibles sont décrites dans Configuration avancée > **Moteur de détection** > **Analyse de logiciels malveillants** > **Analyse de l'ordinateur à la demande** > ThreatSense.

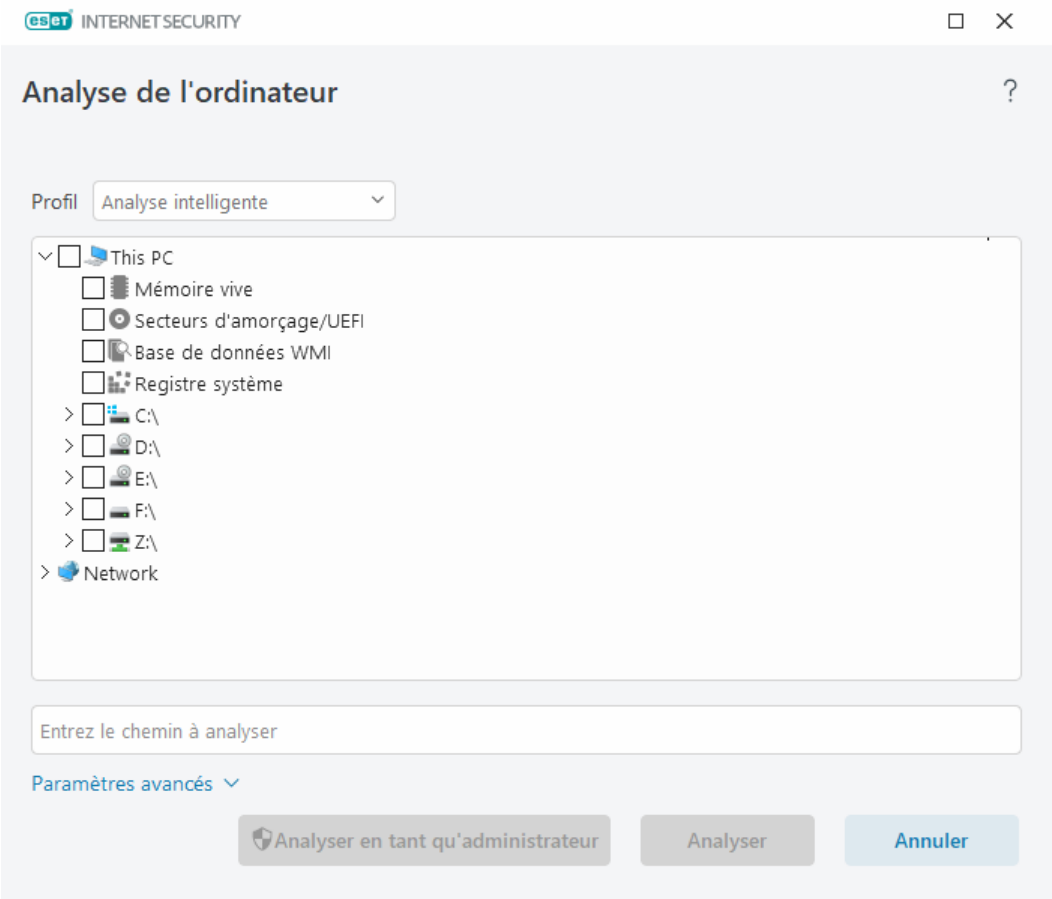
La structure des dossiers (arborescence) contient également des cibles d'analyse spécifiques.

- **Mémoire opérationnelle** : Analyse tous les processus et données actuellement utilisés par la mémoire opérationnelle.
- **Secteurs de démarrage/UEFI** : Analyse les secteurs de démarrage et UEFI à la recherche de logiciels malveillants. Pour en savoir plus sur le scanner UEFI, consultez le glossaire.
- **Base de données WMI** – Analyse la totalité de la base de données Windows Management Instrumentation WMI, tous les espaces de noms, toutes les instances de classe et toutes les propriétés. Recherche les références à des fichiers infectés ou à des logiciels malveillants incorporés sous forme de données.
- **Registre du système** : Analyse l'ensemble du registre du système, toutes les clés et les sous-clés. Recherche les références à des fichiers infectés ou à des logiciels malveillants incorporés sous forme de données. Lors du nettoyage des détections, la référence reste dans le registre pour s'assurer qu'aucune donnée importante ne sera perdue.

Pour accéder rapidement à une cible d'analyse (fichier ou dossier), tapez son chemin d'accès dans le champ de texte sous l'arborescence. Le chemin est sensible à la casse. Pour inclure la cible dans l'analyse, cochez la case correspondante dans l'arborescence.

Comment planifier une analyse hebdomadaire d'un ordinateur

Pour planifier une tâche régulière, consultez le chapitre Comment planifier une analyse hebdomadaire d'un ordinateur.



Vous pouvez configurer les paramètres de nettoyage pour l'analyse sous Configuration avancée > **Moteur de détection** > **Analyse des logiciels malveillants** > **Analyse à la demande** > **ThreatSense** > **Nettoyage**. Pour exécuter une analyse sans action de nettoyage, cliquez sur **Paramètres avancés** et sélectionnez **Analyser sans nettoyage**. L'historique des analyses est enregistré dans le journal des analyses.

Lorsque l'option **Ignorer les exclusions** est sélectionnée, les fichiers avec des extensions qui étaient auparavant exclues de l'analyse sont analysés, sans aucune exception.

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

L'option **Analyser en tant qu'administrateur** permet d'exécuter l'analyse avec le compte d'administrateur. Utilisez cette option si l'utilisateur actuel n'a pas les privilèges requis pour accéder aux fichiers que vous voulez analyser. Ce bouton n'est pas disponible si l'utilisateur actuel ne peut appeler les opérations UAC en tant qu'administrateur.

Vous pouvez afficher le journal d'analyse de l'ordinateur lorsqu'une analyse est terminée en cliquant sur Afficher le journal.

Progression de l'analyse

La fenêtre de progression de l'analyse affiche l'état actuel de l'analyse ainsi que de l'information sur le nombre de fichiers contenant du code malveillant trouvés.

Il est normal que certains fichiers, comme les fichiers protégés par mot de passe ou les fichiers utilisés exclusivement par le système (généralement, les fichiers *pagefile.sys* et certains fichiers journaux), ne puissent pas être analysés. Vous trouverez plus de détails dans cet article de la base de connaissances.

> **Comment planifier une analyse hebdomadaire d'un ordinateur**
> Pour planifier une tâche régulière, consultez le chapitre Comment planifier une analyse hebdomadaire d'un ordinateur.

Progression de l'analyse : la barre de progression affiche l'état de l'analyse en cours d'exécution.

Cible - Le nom de l'objet en cours d'analyse et son emplacement.

Des détections se sont produites - Affiche le nombre total de fichiers analysés, de menaces trouvées et nettoyées pendant une analyse.

Cliquez sur Plus d'informations pour afficher les informations suivantes :

- **Utilisateur :** nom du compte d'utilisateur qui a démarré l'analyse.
- **Objets analysés :** nombre d'objets déjà analysés.
- **Durée :** temps écoulé.

Icône pause : suspend une analyse.

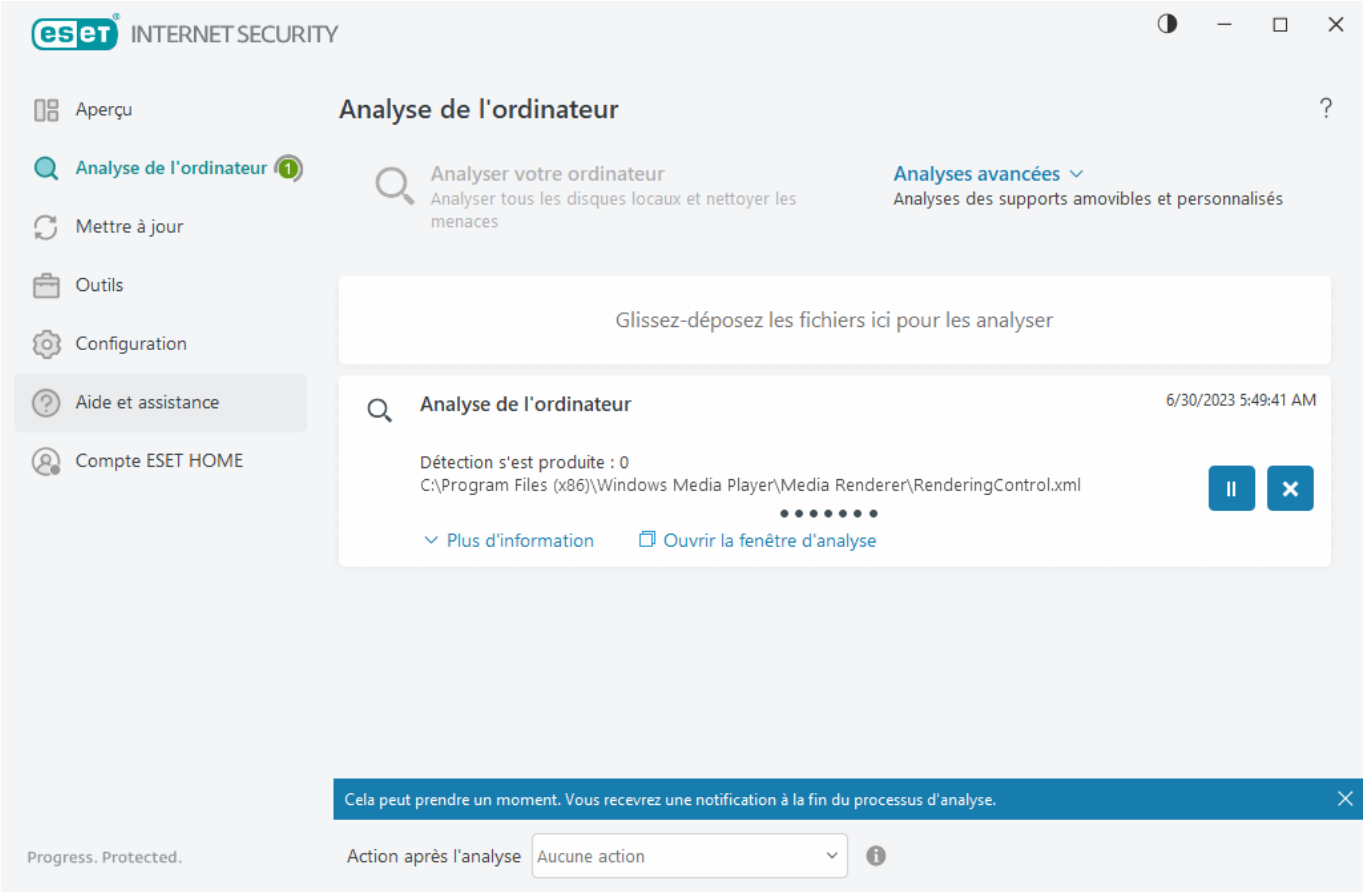
Reprendre : cette option n'est visible que si l'analyse a été suspendue. Cliquez sur l'icône pour continuer l'analyse.

Icône d'arrêt : met fin à l'analyse.

Cliquez sur **Ouvrir la fenêtre Analyse** pour ouvrir le journal d'analyse de l'ordinateur qui contient plus de détails sur l'analyse.

Faire défiler le journal de l'analyse - Si cette option est activée, le journal d'analyse défilera automatiquement lorsque de nouvelles entrées seront ajoutées afin que les entrées les plus récentes soient visibles.

> Cliquez sur la loupe ou la flèche pour afficher les détails de l'analyse en cours. Vous pouvez effectuer une autre analyse en parallèle en cliquant sur **Analyse de l'ordinateur** ou **Analyse avancée** > **Analyse personnalisée**.



Le menu déroulant**Action après analyse** vous permet de définir une action à effectuer automatiquement une fois l’analyse terminée :

- **Aucune action** - À la fin de l'analyse, aucune action ne sera effectuée.
- **Éteindre** - L'ordinateur s'éteint après l'analyse.
- **Redémarrer si nécessaire :** l'ordinateur redémarre uniquement si cela est nécessaire pour terminer le nettoyage des menaces détectées.
- **Redémarrer** - Ferme tous les programmes et redémarre l'ordinateur après l'analyse.
- **Forcer le redémarrage si nécessaire :** l'ordinateur redémarre uniquement si cela est nécessaire pour terminer le nettoyage des menaces détectées.
- **Forcer le redémarrage** - Force la fermeture de tous les programmes ouverts sans attendre aucune action de l’utilisateur et redémarre l’ordinateur après la fin de l’analyse.
- **Mettre en veille** - Enregistre votre session et met l'ordinateur dans un état de basse consommation afin que vous puissiez reprendre rapidement votre travail.
- **Hiberner** - Met tout ce qui est en cours d'exécution sur la RAM dans un fichier spécial de votre disque dur. Votre ordinateur s'éteint, mais retrouvera son état précédent au prochain démarrage.

Les actions **Mettre en veille** ou **Hiberner** sont disponibles en fonction des paramètres d'alimentation et de veille du système d'exploitation ainsi que des capacités de votre ordinateur. Gardez présent à l'esprit qu'un ordinateur en veille fonctionne toujours. Les fonctions de base s'exécutent toujours et votre ordinateur reste alimenté lorsqu'il fonctionne sur batterie. Pour préserver la batterie, par exemple lorsque vous êtes en dehors de votre bureau, nous vous recommandons d'utiliser l'option Hiberner.

L'action sélectionnée commencera une fois que toutes les analyses en cours sont terminées. Lorsque vous sélectionnez **Arrêter** ou **Redémarrer**, une boîte de dialogue de confirmation affiche un compte à rebours de 30 secondes (cliquez sur **Annuler** pour désactiver l'action demandée).

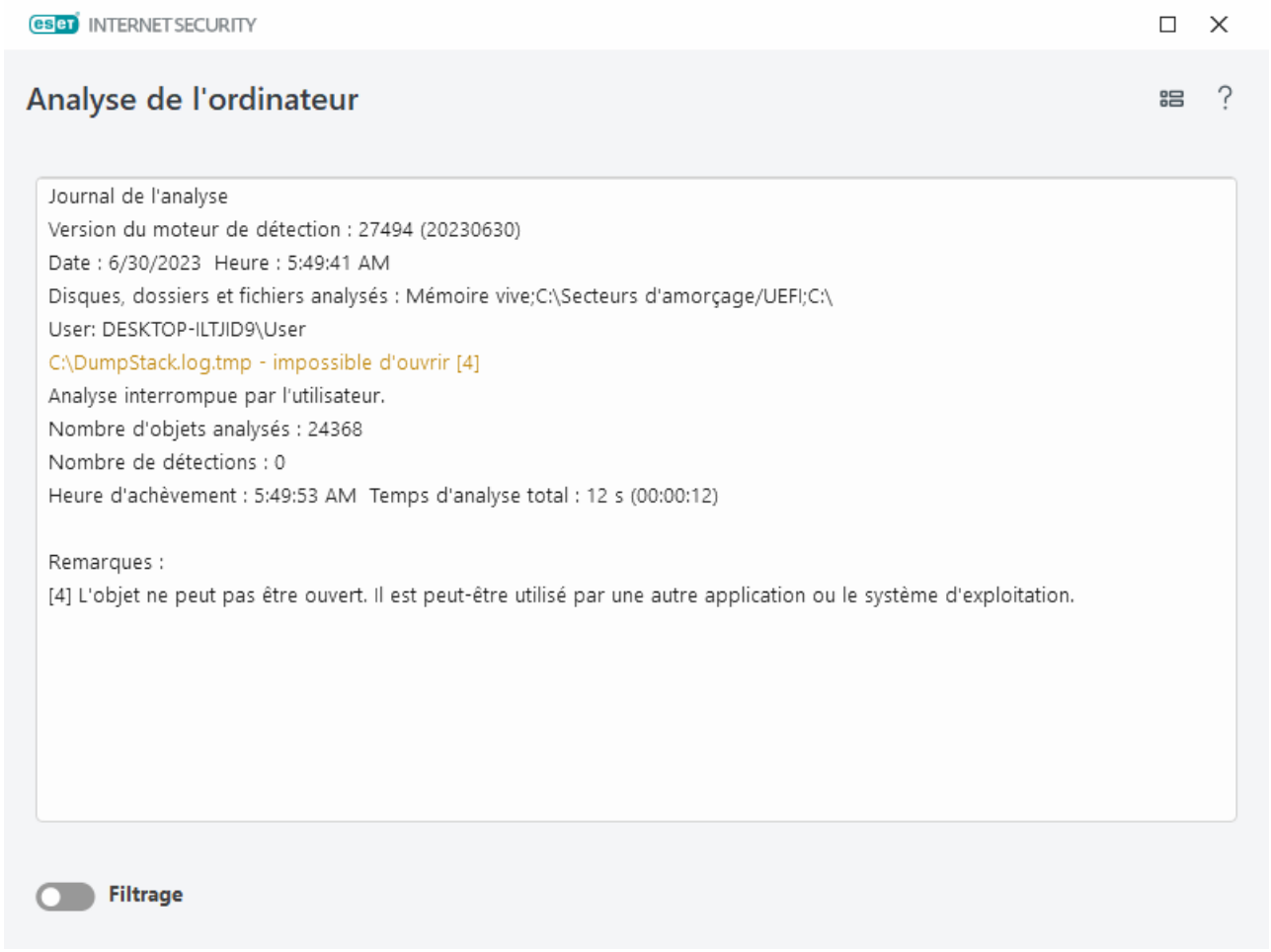
Journal de l'analyse de l'ordinateur

Vous pouvez afficher des informations détaillées relatives à une analyse spécifique dans les fichiers journaux. Le journal d'analyse contient les informations suivantes :

- Version du moteur de détection
- Date et heure de début
- Liste des disques, des dossiers et des fichiers analysés
- Nom de l'analyse planifiée (analyse planifiée uniquement)
- Utilisateur ayant lancé l'analyse.
- État de l'analyse
- Nombre d'objets analysés
- Nombre de détections trouvées
- Heure d'achèvement
- Temps d'analyse total

Si une tâche planifiée d'analyse de l'ordinateur est toujours en cours d'exécution, le redémarrage de cette tâche est ignoré. La tâche d'analyse planifiée ignorée crée un journal d'analyse de l'ordinateur avec 0 objet analysé et l'état suivant : **L'analyse n'a pas démarré, car l'analyse précédente était toujours en cours d'exécution**.

Pour trouver les journaux d'analyse précédents, dans la fenêtre principale du programme, sélectionnez **Outils** > **Fichiers journaux**. Dans le menu déroulant, sélectionnez **Analyse de l'ordinateur** et double-cliquez sur l'enregistrement souhaité.



Pour en savoir plus sur les enregistrements suivants : « Impossibles d'ouvrir », « Erreur lors de l'ouverture » ou « Archives endommagées », consultez cet article de la base de connaissances d'ESET.

Cliquez sur l'icône du bouton bascule **Filtrage** pour ouvrir la fenêtre Filtrage des journaux dans laquelle vous pouvez définir des critères de recherche personnalisés. Pour afficher le menu contextuel, cliquez avec le bouton droit de la souris sur une entrée spécifique du journal :

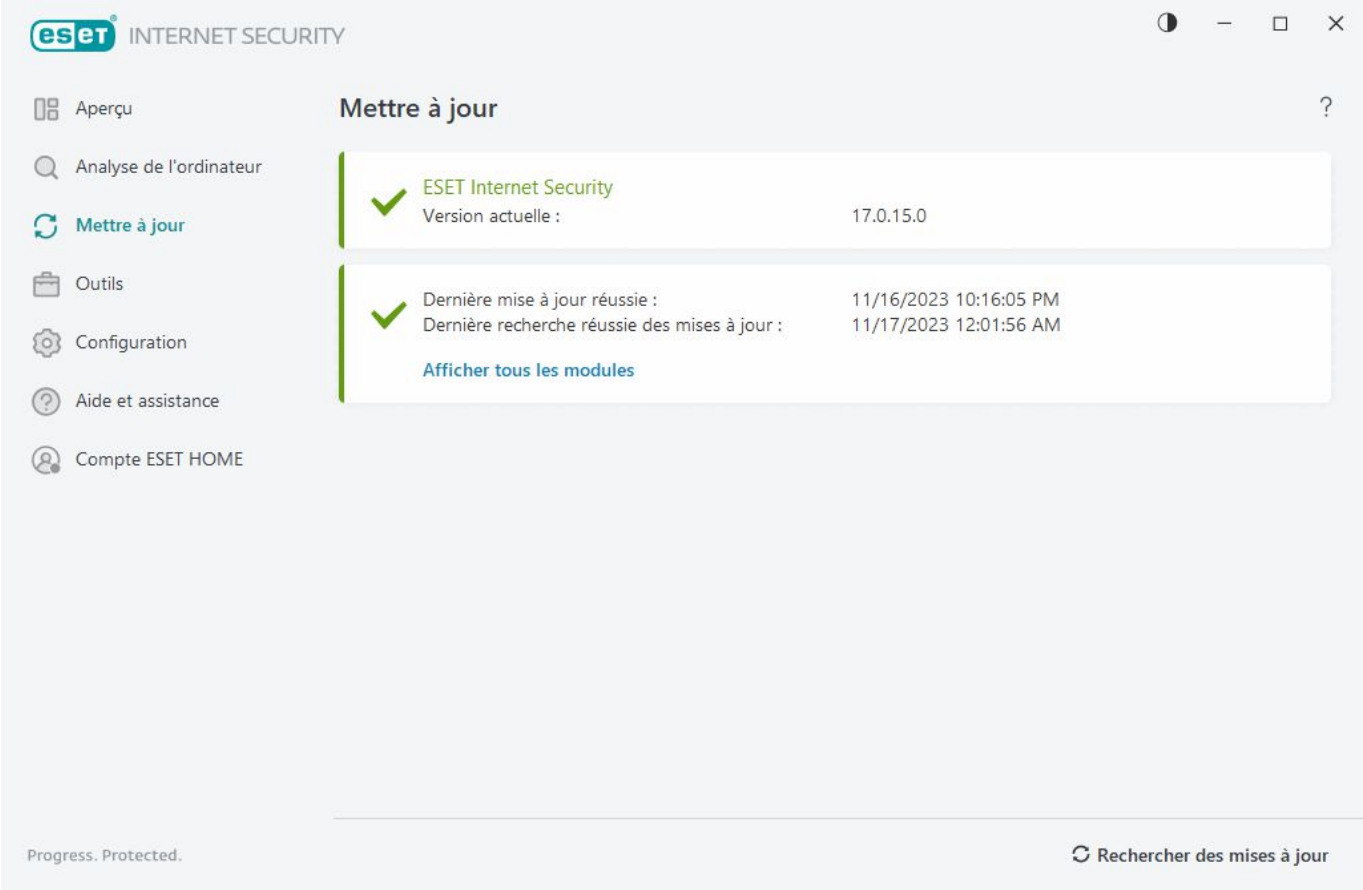
Action	Utilisation
Filtrer les mêmes dossiers	Active le filtrage des journaux. Le journal n'affichera que les enregistrements du même type que celui sélectionné.
Filtrer	Cette option ouvre la fenêtre de filtrage du journal et vous permet de définir des critères pour des entrées de journal spécifiques. Raccourci : `Ctrl+Shift+F`
Désactiver le filtre	Active les paramètres du filtre. Si vous activez le filtre pour la première fois, vous devez définir les paramètres ; la fenêtre de filtrage des journaux s'ouvre alors.
Désactiver le filtre	Désactive le filtre (équivaut à cliquer sur l'interrupteur en bas).
Copier	Copie les enregistrements mis en évidence dans le presse-papiers. Raccourci : `Ctrl+C`
Tout copier	Copie tous les enregistrements dans la fenêtre.
Exporter	Exporte les enregistrements mis en évidence dans le presse-papiers vers un fichier XML.
Tout exporter	Cette option exporte tous les enregistrements de la fenêtre vers un fichier XML.
Description de la détection	Ouvre l'encyclopédie des menaces ESET, qui contient des informations détaillées sur les dangers et les symptômes de l'infiltration en surbrillance.

Mettre à jour

La mise à jour régulière de ESET Internet Security constitue la meilleure méthode pour garantir le niveau maximal de sécurité pour votre ordinateur. Le module Mise à jour garantit que les modules de programme et les composants du système sont toujours à jour.

En cliquant sur **Mettre à jour** dans la fenêtre principale du programme, vous pourrez consulter l'état actuel des mises à jour, y compris la date et l'heure de la dernière mise à jour réussie et si une nouvelle mise à jour est requise.

Outre les mises à jour automatiques, vous pouvez cliquer sur **Rechercher les mises à jour** pour déclencher une mise à jour manuelle. La mise à jour régulière des modules et des composants du programme est un aspect important de la protection complète contre les codes malveillants. Il faut donc accorder une grande attention aux modules du produit et à leur fonctionnement. Vous devez activer votre produit à l'aide de la clé d'activation pour recevoir des mises à jour. Si vous ne l'avez pas déjà fait lors de l'installation, vous devez activer ESET Internet Security pour accéder aux serveurs de mise à jour d'ESET. Votre clé d'activation vous a été envoyée dans un courriel provenant d'ESET, après votre achat de ESET Internet Security.



Version actuelle – Indique le numéro de la version actuelle du produit que vous avez installée.

Dernière mise à jour réussie - Indique la date de la dernière mise à jour réussie. Si vous ne voyez pas une date récente, cela signifie que les modules de vos produits pourrait ne pas être à jour.

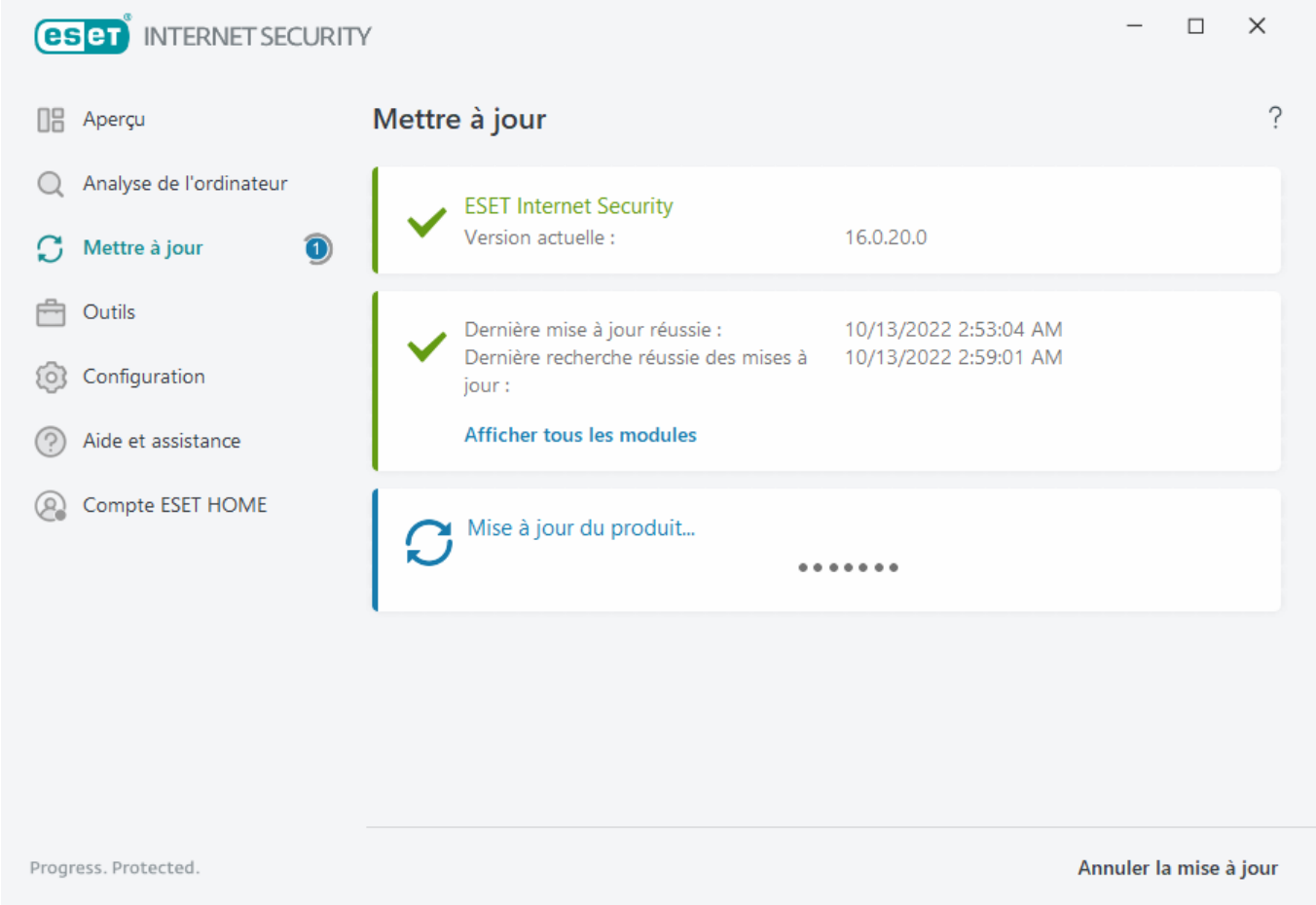
Dernière vérification des mises à jour réussie - Indique la date de la dernière vérification des mises à jour réussie.

Afficher tous les modules – Affiche la liste des modules de programme installés.

Cliquez sur **Vérifier les mises à jour** pour vérifier la dernière version disponible de ESET Internet Security.

Processus de mise à jour

Une fois que vous aurez cliqué sur le bouton **Vérifier les mises à jour**, le processus de téléchargement commencera. Une barre de progression s'affiche indiquant le temps de téléchargement restant. Pour interrompre la mise à jour, cliquez sur **Annuler la mise à jour**.



Dans des circonstances normales, vous verrez la marque de vérification verte dans la fenêtre **Mise à jour** indiquant que ce programme est à jour. Si ce n'est pas le cas, le programme n'est pas à jour et est donc plus vulnérable à une infection. Veuillez mettre à jour les modules du programme le plus tôt possible.

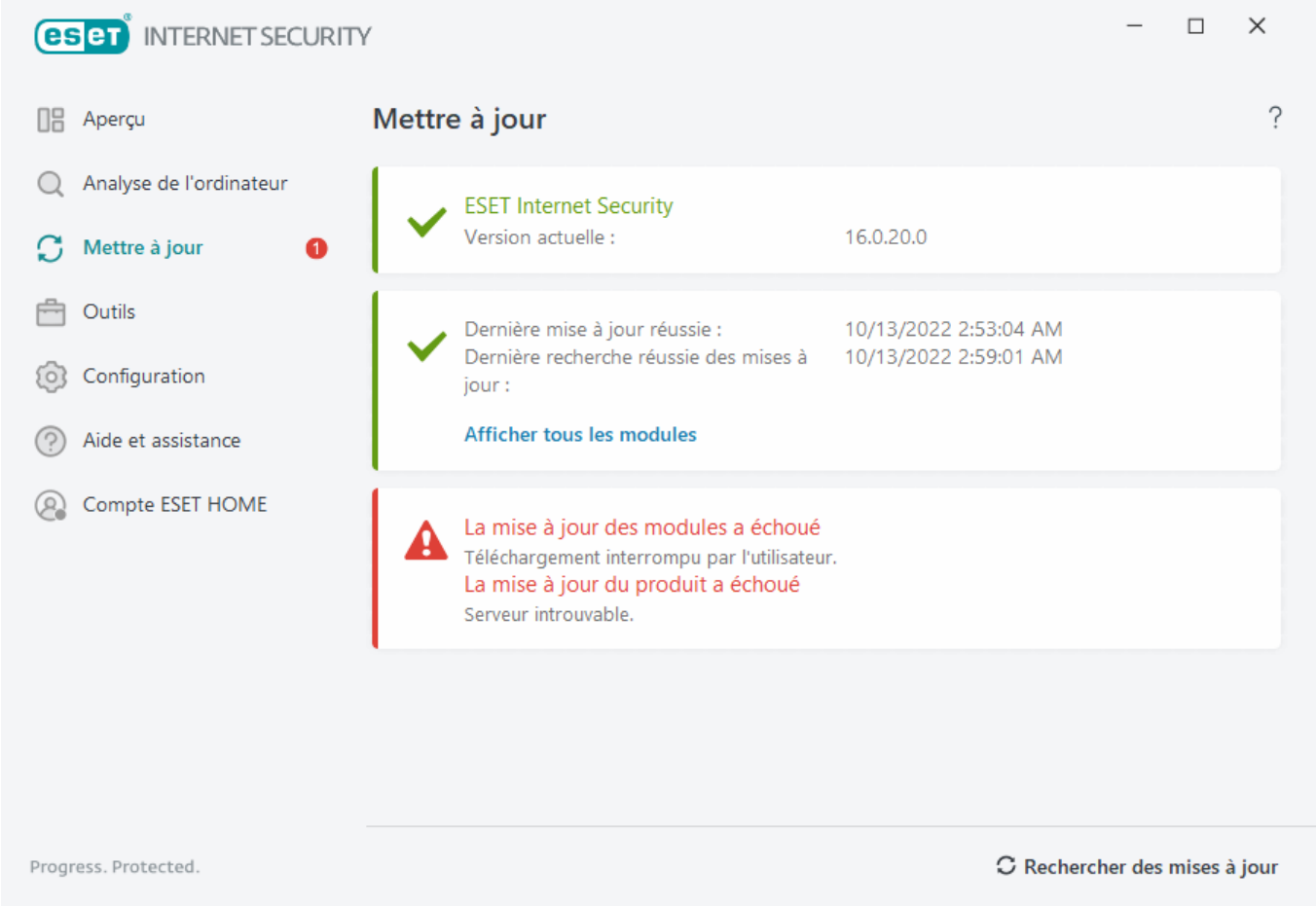
Échec de la mise à jour

Si vous recevez un message d'échec de la mise à jour des modules, cela peut être dû aux problèmes suivants :

1. **Abonnement non valide** – L'abonnement utilisé pour l'activation n'est pas valide ou a expiré. Dans la fenêtre principale du programme, cliquez sur **Aide et assistance** > **Changer d'abonnement** et activez votre produit.

2. **Une erreur est survenue pendant le téléchargement des fichiers de mise à jour** - Des paramètres de connexion Internet incorrects sont une cause possible de cette erreur. 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, il est probable qu'aucune connexion à Internet ne soit établie ou que votre ordinateur ait des problèmes de connectivité. Consultez votre fournisseur de services Internet si vous ne disposez pas d'une connexion Internet active.



Vous devez redémarrer votre ordinateur après une mise à jour réussie de ESET Internet Security pour vous assurer que tous les modules du programme ont été correctement mis à jour. Il n'est pas nécessaire de redémarrer votre ordinateur après les mises à jour régulières des modules.

Pour plus d'informations, veuillez consulter l'article Dépannage lorsque le message « Échec de la mise à jour des modules » s'affiche.

Fenêtre de dialogue - Redémarrage requis

Un redémarrage de l'ordinateur est requis après la mise à jour de ESET Internet Security vers une nouvelle version. De nouvelles versions de ESET Internet Security sont publiées afin de mettre en œuvre des améliorations ou résoudre des problèmes que les mises à jour automatiques des modules de programme n'ont pas réussi à faire.

La nouvelle version de ESET Internet Security peut être installée automatiquement, en fonction de vos paramètres de mise à jour de programme, ou manuellement, en téléchargeant et en installant une version plus récente que la précédente.

Cliquez sur **Redémarrer maintenant** pour redémarrer votre ordinateur. Si vous prévoyez de redémarrer votre ordinateur ultérieurement, cliquez sur **Me le rappeler plus tard**. Le moment venu, vous pouvez redémarrer votre ordinateur manuellement à partir de la section **Aperçu** dans la fenêtre principale du programme.

Comment créer des tâches de mise à jour

Les mises à jour peuvent être déclenchées manuellement en cliquant sur **Vérifier les mises à jour** dans la principale fenêtre d'information qui s'affiche après avoir cliqué sur **Mise à jour** dans le menu principal.

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

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

Chaque tâche de mise à jour peut être modifiée en fonction de vos besoins. Outre les tâches de mise à jour par défaut, vous pouvez en créer des nouvelles avec vos propres paramètres. Pour plus d'information sur la création et la configuration des tâches de mise à jour, se reporter à la section Planificateur.

Outils

Le menu **Outils** comprend des fonctionnalités qui offrent une sécurité supplémentaire et aident à simplifier l'administration ESET Internet Security. Les outils suivants sont disponibles :

 Fichiers journaux

 Processus en cours (si ESET LiveGrid® est activé dans ESET Internet Security)

 Rapport de sécurité

 Connexions réseau (si Pare-feu est activé dans ESET Internet Security)

 ESET SysInspector

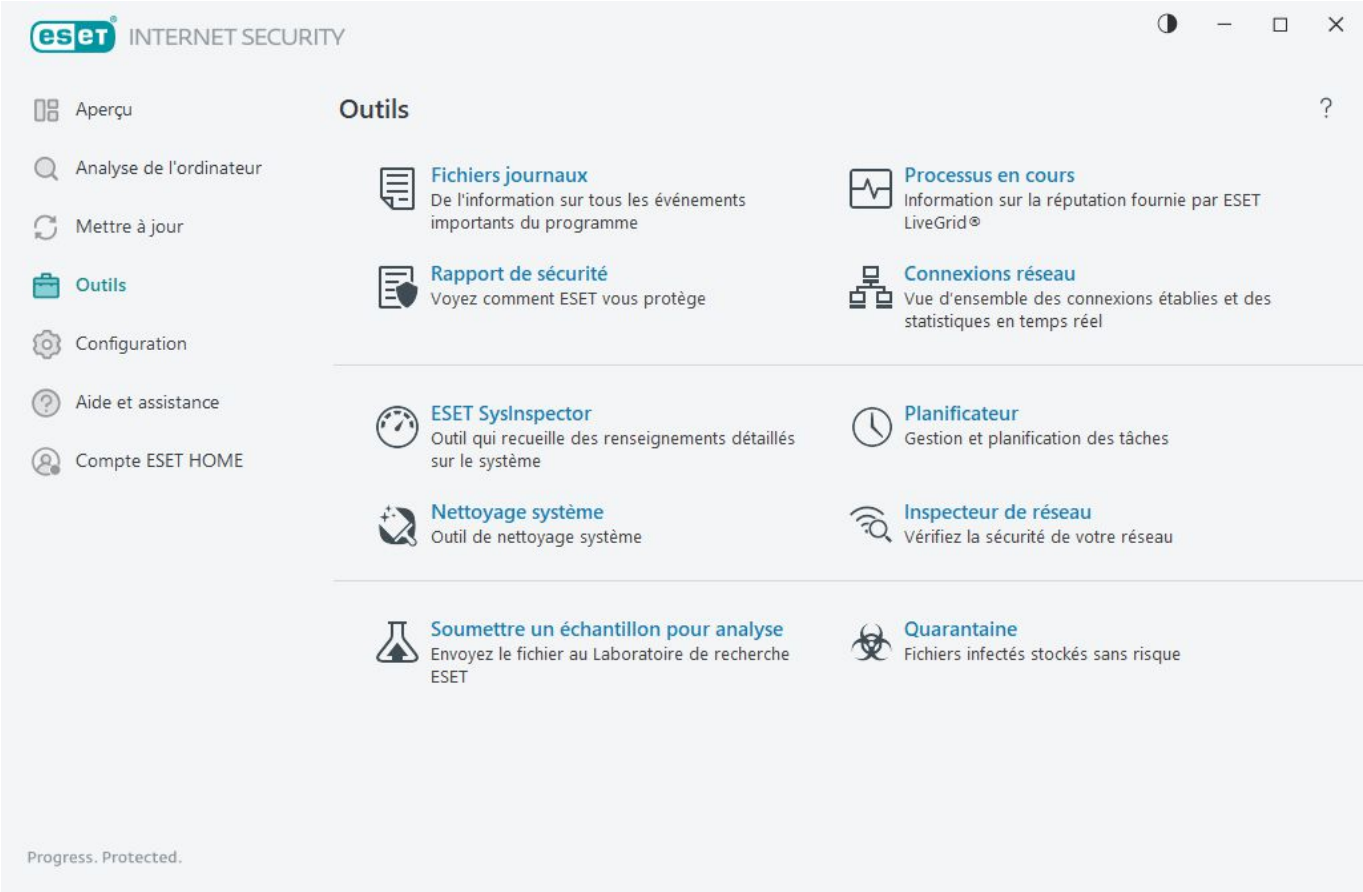
 Planificateur

 Nettoyage système

 Inspecteur de réseau

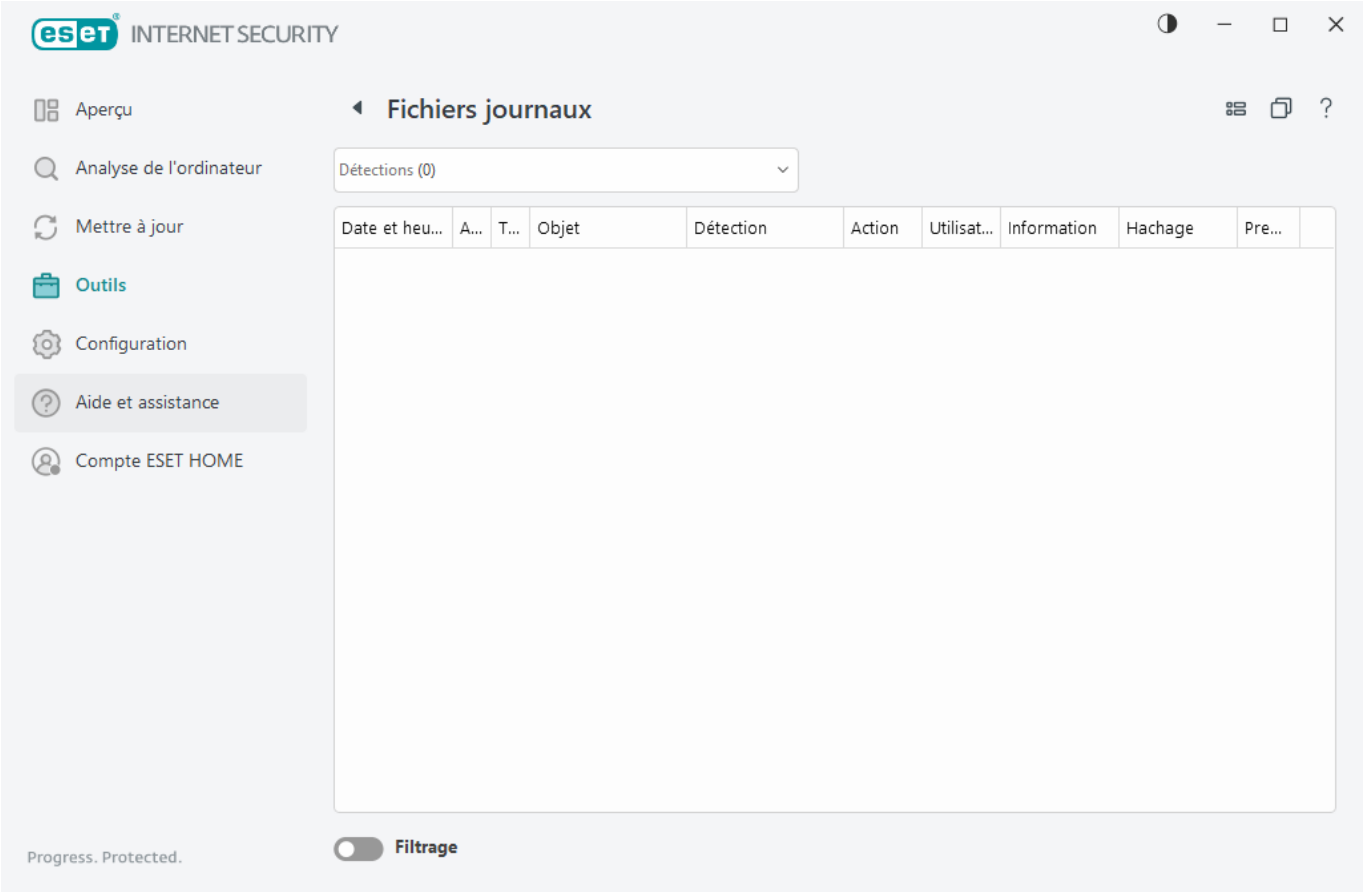
 Soumettre l'échantillon pour analyse (peut ne pas être disponible en fonction de votre configuration ESET LiveGrid®).

 Quarantaine



Fichiers journaux

Les fichiers journaux contiennent de l'information sur les événements importants qui ont eu lieu et donnent un aperçu des menaces détectées. La consignation est un composant essentiel de l'analyse système, de la détection de menaces et du dépannage. Elle est toujours active en arrière-plan, sans interaction de l'utilisateur. Les données sont enregistrées en fonction des paramètres actifs de verbosité. Il est possible de consulter les messages texte et les journaux directement à partir de l'environnement ESET Internet Security, ainsi que d'archiver les journaux.



Les fichiers journaux sont accessibles à partir de la fenêtre principale du programme en cliquant sur **Outils** > **Fichiers journaux**. Sélectionnez le type de journal souhaité dans le menu déroulant Journal.

- **Detections** – Ce journal offre des informations détaillées sur les détections et les infiltrations détectées par ESET Internet Security. Les informations du journal incluent l'heure de détection, le type d'analyseur, le type d'objet, l'emplacement de l'objet, le nom de la détection, l'action entreprise, le nom de l'utilisateur connecté lorsque l'infiltration a été détectée, le hachage et la première occurrence. Les infiltrations non nettoyées sont toujours marquées d'un texte rouge sur fond rouge clair. Les infiltrations nettoyées sont marquées d'un texte jaune sur fond blanc. Les applications potentiellement indésirables non nettoyés ou les applications potentiellement dangereuses sont marquées d'un texte jaune sur fond blanc.

- **Événements** - Toutes les actions importantes exécutées par ESET Internet Security sont enregistrées dans le journal des événements. Le journal des événements contient de l'information sur les événements qui se sont produits dans le programme. Il permet aux administrateurs système et aux utilisateurs de résoudre des problèmes. L'information qu'on y trouve peut souvent permettre de trouver une solution à un problème qui s'est produit dans le programme.

- **Analyse de l'ordinateur** – Les résultats de toutes les analyses effectuées sont affichés dans cette fenêtre. Chaque ligne correspond à un seul analyse de l'ordinateur. Double-cliquez sur n'importe quelle entrée pour afficher les détails de l'analyse correspondante.

- **HIPS** - Contient des enregistrements de règles HIPS particulières ayant été marquées pour enregistrement. Ce protocole affiche l'application ayant déclenché l'opération, le résultat (si la règle a été autorisée ou non) et le nom de la règle.

- **Protection du navigateur** : contient les enregistrements des fichiers non vérifiés/non fiables chargés dans le navigateur.

• **Protection du réseau** – Le journal de protection du réseau affiche toutes les attaques distantes détectées par le pare-feu, la protection contre les attaques de réseau (IDS) et la protection contre les botnets). Il comprend des renseignements sur toutes les attaques lancées contre votre ordinateur. La colonne Événement reprend la liste des attaques détectées. La colonne Source fournit des renseignements sur l'attaquant. La colonne Protocole indique le Protocole de communication utilisé pour l'attaque. L'analyse du journal de protection réseau peut vous permettre de détecter à temps les tentatives d'infiltration du système pour ainsi empêcher l'accès non autorisé à votre système. Pour plus d'information sur les attaques réseau, consultez la section Options IDS et avancées.

• **Sites Web filtrés :** cetteCette liste est utile si vous souhaitez afficher une liste de sites Web qui ont été bloqués par la protection de l'accès Web ou le contrôle parental. Chaque journal permet de voir le moment, l'adresse URL, l'utilisateur et l'application ayant créé une connexion vers un site Web en particulier.

• **Antipourriel du client de messagerie** : contient des enregistrements liés aux courriels marqués comme Pourriel.

• **Contrôle parental** - Affiche les pages Web bloquées ou autorisées par le Contrôle parental. Les colonnes Type de correspondance et Valeurs de correspondance vous indiquent comment les règles de filtrage ont été appliquées.

• **Contrôle de périphérique** – Contient les enregistrements relatifs aux supports amovibles ou périphériques ayant été connectés à l'ordinateur. Seuls les périphériques liés à une règle de contrôle des périphériques particulière seront inscrits dans le fichier journal. Si un périphérique connecté ne satisfait pas les critères de la règle, aucune entrée journal ne sera créée à la connexion de ce périphérique. Vous pouvez aussi y voir différents détails, comme le type de périphérique, le numéro de série, le nom du fournisseur et la taille du support (si elle est disponible).

• **Protection de la caméra Web** - Contient des enregistrements sur les applications bloquées par la protection de la caméra Web.

Sélectionnez le contenu de n'importe quel journal et appuyez sur **CTRL + C** pour le copier dans le presse-papier. Appuyez à la fois sur **CTRL** ou **SHIFT** pour sélectionner plusieurs entrées.

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

Faites un clic droit sur un enregistrement en particulier pour ouvrir le menu contextuel. Les options suivantes sont disponibles dans le menu contextuel :

• **Afficher** - Affiche plus des informations plus détaillées sur le journal sélectionné dans une nouvelle fenêtre.

• **Filtrer les enregistrements du même type** - Après avoir activé ce filtre, vous ne verrez que les entrées de même type (diagnostics, avertissements, etc.).

• **Filtrer** - Après avoir cliqué sur cette option, la fenêtre Filtrage du journal vous permettra de définir les critères de filtrage à utiliser pour des entrées particulières du journal.

• **Activer le filtre** - Active les paramètres du filtre.

• **Désactiver le filtrage** - Efface tous les paramètres du filtre (comme décrit ci-dessus).

• **Copier/Copier tout** – Copie des informations sur les enregistrements sélectionnés.

• **Copier la cellule** : copie le contenu de la cellule à la suite d'un clic du bouton droit.

• **Supprimer/Supprimer tout** – Supprime les enregistrements sélectionnés ou tous les enregistrements affichés. Cette action nécessite des privilèges d'administrateur.

• **Exporter/Exporter tout –** Exporte des informations sur les enregistrements sélectionnés ou tous les enregistrements au format XML.

• **Rechercher/Rechercher suivant/Rechercher précédent** – Après avoir cliqué sur cette option, vous pouvez définir des critères de filtrage pour mettre en surbrillance l'entrée spécifique à l'aide de la fenêtre Filtrage du journal.

• **Description de la détection** – Ouvre l'encyclopédie des menaces ESET, qui contient des informations détaillées sur les dangers et les symptômes de l'infiltration enregistrée.

• **Créer une exclusion** – Permet de créer une exclusion de détection à l'aide d'un assistant (cette option n'est pas disponible pour la détection de logiciels malveillants).

• **Ajouter à la liste autorisée de protection du navigateur** — ouvre la fenêtre de la liste autorisée de protection du navigateur et ajoute l'élément à la liste.

Filtrage des journaux

Cliquez sur **Filtrage** dans **Outils** > **Fichiers journaux** pour définir le critère de filtrage.

La fonctionnalité de filtrage des journaux vous aidera à trouver les informations que vous recherchez, en particulier lorsque les enregistrements sont nombreux. Il vous permet de limiter les enregistrements de journal, par exemple, si vous recherchez un type d'événement, un état ou une période précise. Vous pouvez filtrer les entrées de journal en spécifiant certaines options de recherche. Seules les entrées pertinentes (en fonction de ces options de recherche) sont affichées dans la fenêtre Fichiers journaux.

Tapez le mot-clé que vous recherchez dans le champ **Recherche de texte**. Utilisez le menu déroulant **Rechercher dans les colonnes** pour affiner votre recherche. Choisissez un ou plusieurs enregistrements dans le menu déroulant **Types d'enregistrement de journaux** . Définissez la **période** à partir de laquelle vous souhaitez afficher les résultats. Vous pouvez également utiliser d'autres options de recherche, telles que **Correspondre uniquement aux mots entiers** ou **Sensible à la casse**.

Rechercher texte

Tapez une chaîne (mot ou partie de mot). Seuls les enregistrements contenant cette chaîne seront affichés. Les autres enregistrements seront omis.

Rechercher dans les colonnes

Sélectionnez les colonnes à prendre en compte lors de la recherche. Vous pouvez cocher une ou plusieurs colonnes à utiliser pour la recherche.

Types d'enregistrement

Choisissez un ou plusieurs types d'enregistrement de journaux dans le menu déroulant :

- **Diagnostic** - Consigne l'information requise pour mettre au point le programme et tous les enregistrements préalables.
- **Informative** - Enregistre des messages informatifs, y compris les messages de mise à jour réussie, ainsi que toutes les entrées préalables.
- **Avertissements** - Enregistre les erreurs critiques et les messages d'avertissement.
- **Erreurs** - Des erreurs comme « Erreur de téléchargement de fichier » et les erreurs critiques seront enregistrées.
- **Critique** - Ne consigne que les erreurs critiques (échec de démarrage de la protection antivirus).

Période

Définir la période pendant laquelle vous voulez que les résultats soient affichés:

- **Non spécifié** (valeur par défaut) - Ne recherche pas dans la période, recherche dans tout le journal.
- **Dernier jour**
- **Dernière semaine**
- **Dernier mois**
- **Période** - Vous pouvez spécifier la période exacte (De : et À :) pour ne filtrer que les enregistrements de la période spécifiée.

Mots entiers seulement

Cochez cette case si vous voulez rechercher des mots entiers particuliers pour obtenir des résultats de recherche plus précis.

Sensible à la casse

Activez cette option si vous devez utiliser des majuscules ou des minuscules lors du filtrage. Une fois que vous avez configuré vos options de filtrage/recherche, cliquez sur **OK** pour afficher les enregistrements de journal filtrés ou sur **Rechercher** pour lancer la recherche. La recherche des fichiers journaux s'effectue de haut en bas, à partir de votre position actuelle (l'enregistrement en surbrillance). La recherche s'arrête lorsqu'elle trouve le premier enregistrement correspondant. Appuyez sur **F3** pour rechercher le prochain enregistrement ou faites un clic droit et sélectionnez **Rechercher** pour affiner vos options de recherche.

Processus en cours

Processus en cours affiche les programmes ou processus en cours d'exécution sur votre ordinateur et s'assure que ESET est continuellement avisé des nouvelles infiltrations, et ce, dès qu'elles se produisent. ESET Internet Security

donne de l'information détaillée sur les processus en cours d'exécution pour protéger les utilisateurs grâce à la technologie ESET LiveGrid®.

Réputation - Le plus souvent, ESET Internet Security affecte, grâce à la technologie ESET LiveGrid®, des niveaux de risque aux objets (fichiers, processus, clés de registre, etc.) à l'aide d'une série de règles heuristiques qui examinent les caractéristiques de chaque objet, puis pondèrent son potentiel d'activité nuisible. Sur la base de cette heuristique, un niveau de risque de sera attribué aux objets : 1 - Bon (vert) à 9 - Risqué (rouge).

Processus - Nom de l'image du programme ou du processus actuellement en cours d'exécution sur votre ordinateur. Vous pouvez aussi utiliser le Gestionnaire des tâches de Windows pour afficher tous les processus en cours d'exécution sur votre ordinateur. Pour ouvrir le Gestionnaire des tâches, cliquez à droite dans une zone vide de la barre des tâches, puis sur **Gestionnaire des tâches**, ou appuyez sur les touches **Ctrl**+**Maj**+**Esc** de votre clavier.

Les applications connues marquées Saines (en vert) sont assurément saines (liste blanche) et sont exclues de l'analyse afin d'améliorer les performances.

PID - Le numéro d'identification de processus peut être utilisé en tant que paramètre dans les différents appels de fonctions tels que le réglage de la priorité du processus.

Nombre d'utilisateurs - Le nombre d'utilisateurs qui utilisent une application donnée. Cette information est colligée par la technologie ESET LiveGrid®.

Heure de découverte - Période depuis que l'application a été découverte par la technologie ESET LiveGrid®.

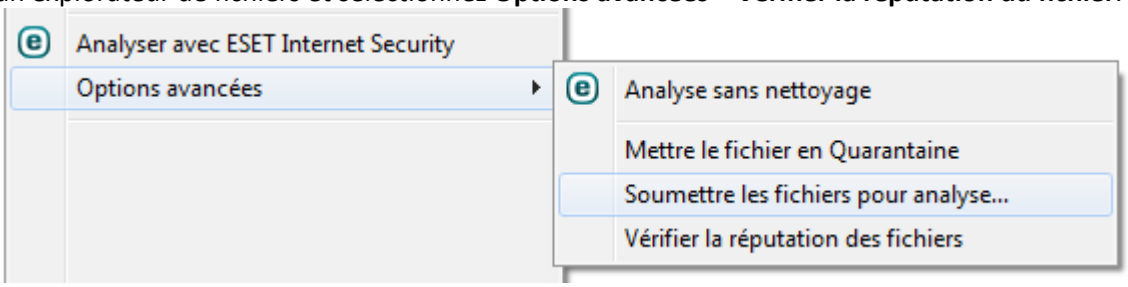
Une application marquée comme Inconnue (orange) n'est pas nécessairement un logiciel malveillant. C'est souvent simplement une nouvelle application. Si vous n'êtes pas certain du fichier, vous pouvez envoyer le fichier pour analyse aux laboratoires de recherche d'ESET. Si le fichier s'avère être une application malveillante, sa détection sera ajoutée à une mise à jour ultérieure.

Nom de l'application - Le nom d'un programme ou d'un processus donné.

Cliquez sur une application pour afficher les détails suivants de cette application :

- **Chemin** - Emplacement d'une application sur votre ordinateur.
- **Taille** - Taille du fichier indiquée en Ko (kilooctets) ou en Mo (mégaoctets).
- **Description** - Caractéristiques du fichier, en fonction de la description provenant du système d'exploitation.
- **Société** - Nom du fournisseur ou du processus d'application.
- **Version** - Information de l'éditeur de l'application.
- **Produit** - Nom de l'application et/ou nom de l'entreprise.
- **Créé le/Modifié le** - Date et heure de la création (modification).

Vous pouvez également vérifier la réputation des fichiers qui ne se comportent pas comme des programmes ou processus en cours d'exécution. Pour ce faire, cliquez dessus à l'aide du bouton droit dans un explorateur de fichiers et sélectionnez **Options avancées** > **Vérifier la réputation du fichier**.



Rapport de sécurité

Cette fonctionnalité donne un aperçu des statistiques pour les catégories suivantes :

- **Pages Web bloquées** - Affiche le nombre de pages Web bloquées (dont l'URL se trouve sur la liste noire pour PUA, hameçonnage, routeur, adresse IP ou certificat piratés).
- **Objets de courriel infectés détectés** - Affiche le nombre d'objets de courriel infectés qui ont été détectés.
- **Pages Web du contrôle parental bloquées** - Affiche le nombre de pages Web bloquées dans Contrôle parental.
- **PUA détecté** – Affiche le nombre d'applications potentiellement indésirables (PUA).
- **Pourriels détectés** – Affiche le nombre de pourriels détectés.

- **Accès à la webcam bloqué** - Affiche le nombre d'accès bloqués à la webcam.
- **Documents analysés** – Affiche le nombre d'objets de document analysés.
- **Applications analysées** – Affiche le nombre d'objets exécutables analysés.
- **Autres objets analysés** – Affiche le nombre d'autres objets analysés.
- **Page Web analysées** – Affiche le nombre d'objets de pages Web analysés.
- **Objets de courriel analysés** – Affiche le nombre d'objets de courriels analysés.

L'ordre de ces catégories est basé sur la valeur numérique du plus élevé au plus bas. Les catégories avec des valeurs nulles ne sont pas affichées. Cliquez sur **Afficher plus** pour développer et afficher les catégories masquées.

La dernière partie du rapport de sécurité vous offre la possibilité d'activer les fonctions suivantes :

- Contrôle parental
- Antivol

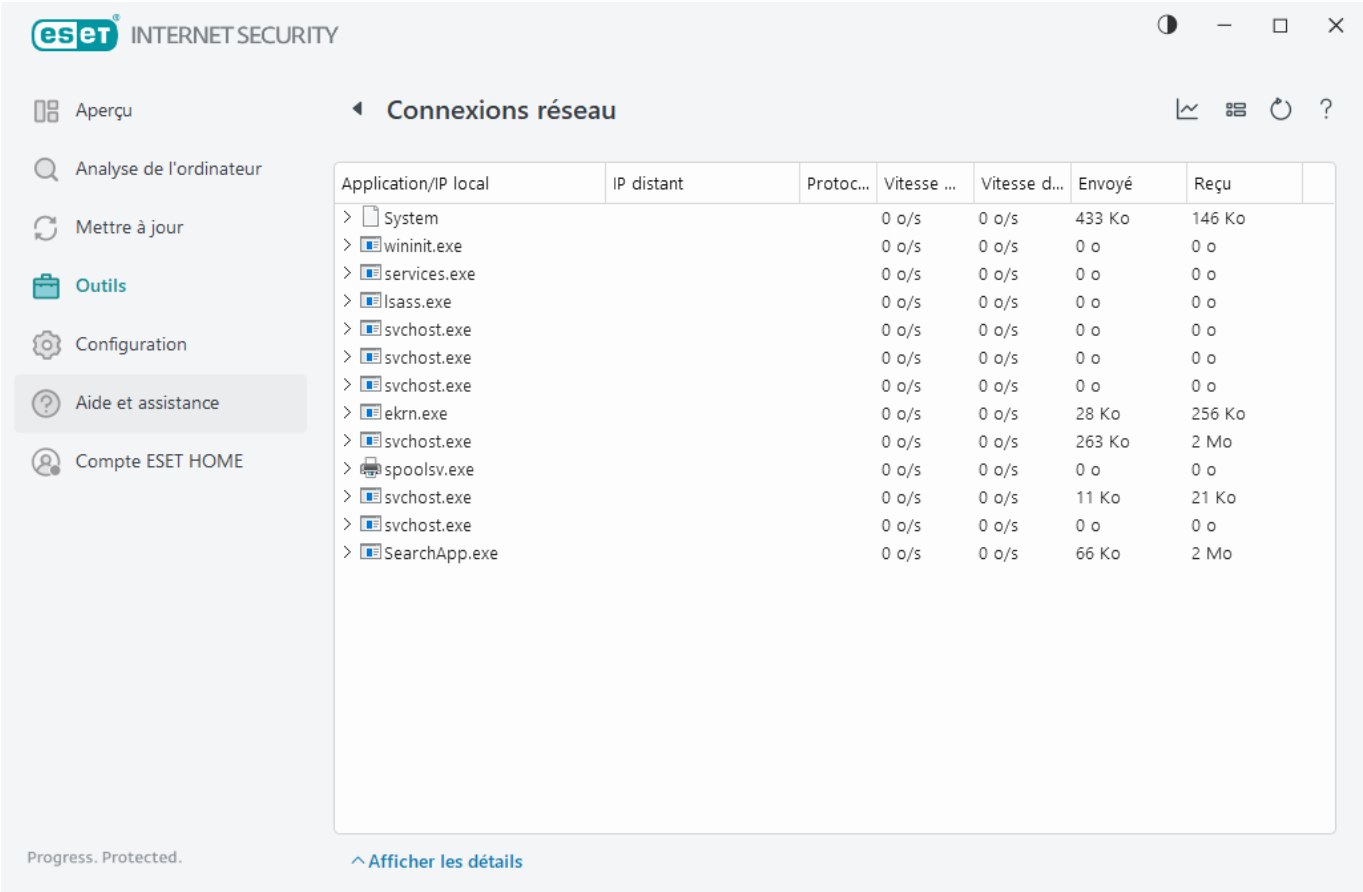
Une fois la fonction activée, elle n'apparait plus comme non fonctionnelle dans le rapport de sécurité.

Cliquez sur l'icône de l'engrenage dans le coin supérieur droit. vous pouvez **Activer ou Désactiver les notifications de rapport de sécurité** ou choisir d'afficher les données des 30 derniers jours ou celles enregistrées depuis l'activation du produit. Si ESET Internet Security est installé depuis moins de 30 jours, seul le nombre de jours à partir de l'installation peut être sélectionné. Le délai de 30 jours est fixé par défaut.

Réinitialiser les données effacera toutes les statistiques et supprimera les données existantes du rapport de sécurité. Cette action doit être confirmée à l'exception des cas où vous désélectionnez l'option **Demander avant de réinitialiser les statistiques** dans Configuration avancée > **Notifications** > **Alertes interactives** > **Messages de confirmation** > **Modifier**.

Connexions réseau

La section Connexions réseau contient la liste des connexions actives et en attente. Elle vous aide à contrôler toutes les applications qui établissent des connexions sortantes.



Cliquez sur l'icône de graphique pour ouvrir Activité réseau.

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.

IP distante - Adresse IP et numéro de port d'un ordinateur distant particulier.

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 détails de la connexion sélectionnée.

Cliquez à droite sur une connexion pour voir des options supplémentaires, y compris :

Résoudre les noms d'hôtes - Si possible, toutes les adresses réseau sont affichées dans le format DNS plutôt que dans le format d'adresse IP numérique.

Afficher uniquement les connexions avec le protocole TCP - Cette liste affiche uniquement les connexions appartenant à la suite de protocoles TCP.

Afficher les connexions à l'écoute - Cette option permet d'afficher seulement les connexions sans communication actuellement établie, mais pour lesquelles le système a ouvert un port et est en attente de connexion.

Afficher les connexions à l'intérieur de l'ordinateur - Cette option permet de n'afficher que les connexions où le côté distant est un système local, aussi appelées connexions localhost.

Vitesse de rafraîchissement - Sélectionner la fréquence de rafraîchissement des connexions actives.

Rafraîchir maintenant - Recharge la fenêtre des **connexions réseau**.

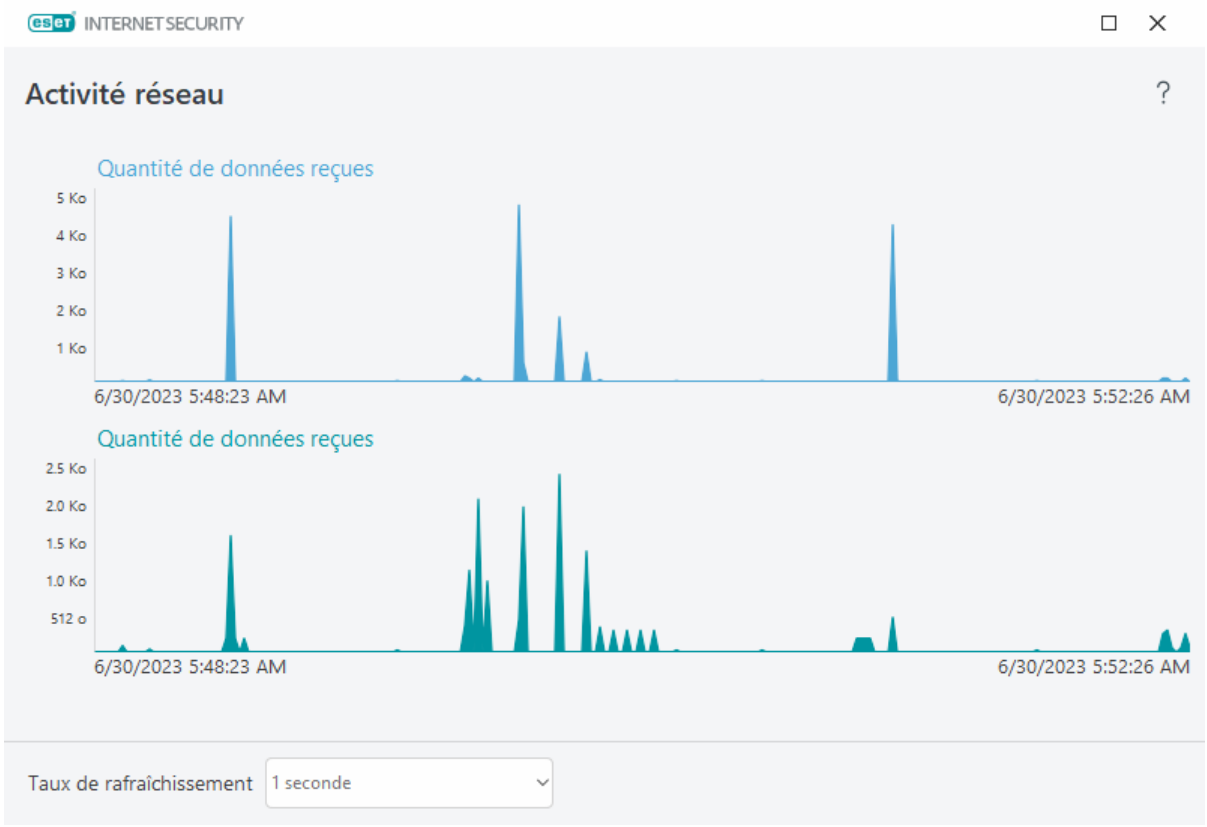
Les options suivantes ne sont disponibles qu'après avoir cliqué sur une application ou un processus, non sur une connexion active :

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 du pare-feu.

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 du pare-feu.

Activité réseau

Pour voir **l'activité réseau** actuelle sous forme de graphique, cliquez sur **Outils** > **Connexions réseau** et cliquez sur l'icône du graphique . Au bas du graphique se trouve une chronologie qui enregistre l'activité du réseau en temps réel en fonction de la période sélectionnée. Pour modifier la plage de temps, sélectionnez la valeur applicable dans le menu déroulant **Taux de rafraîchissement** .



Les options suivantes sont disponibles :

- **1 seconde** - Le graphique est actualisé toutes les secondes et la chronologie couvre les 4 dernières minutes.
- **1 minute (24 dernières heures)** - Le graphique est actualisé toutes les minutes et la chronologie couvre les 24 dernières heures.
- **1 heure (dernier mois)** - Le graphique est actualisé toutes les heures et la chronologie couvre le dernier mois.

L'axe vertical du graphique représente la quantité de données reçues ou envoyées. Passez votre souris sur le graphique pour voir la quantité exacte de données reçues/envoyées à un moment précis.

ESET SysInspector

ESET SysInspector est une application qui inspecte complètement votre ordinateur et collige de l'information détaillée sur les composants système, tels que les pilotes et applications, les connexions réseau ou des entrées de registre importantes, et évalue le niveau de risque de chacun des composants. Ces données 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 logiciel malveillant. Pour savoir comment utiliser ESET SysInspector, reportez-vous à l'aide en ligne de ESET SysInspector.

La fenêtre de ESET SysInspector affiche les informations suivantes sur les journaux :

- **Heure** - L'heure de création du journal.
- **Commentaire** - Un bref commentaire.

- **Utilisateur** - Le nom de l'utilisateur ayant créé le journal.
- **État** - L'état de création du journal.

Les actions suivants sont disponibles :

- **Afficher –** Ouvre le journal sélectionné dans ESET SysInspector. Vous pouvez aussi cliquer à l'aide du bouton droit de la souris sur un fichier journal donné et sélectionner **Afficher** à partir du menu contextuel.
- **Créer** - Crée un journal. Attendez jusqu'à ce que ESET SysInspector soit généré (état **Créé**) avant de tenter d'accéder au journal. Le journal est enregistré dans C:\ProgramData\ESET\ESET Security\SysInspector.
- **Supprimer** - Supprime les journaux sélectionnés de la liste.

Les éléments suivants sont disponibles dans le menu contextuel lorsqu'un ou plusieurs fichiers journaux sont sélectionnés:

- **Afficher** - Ouvre le journal sélectionné dans ESET SysInspector (ou double-cliquez sur un journal pour la même fonction).
- **Créer** - Crée un journal. Attendez jusqu'à ce que ESET SysInspector soit généré (état **Créé**) avant de tenter d'accéder au journal.
- **Supprimer** - Supprime les journaux sélectionnés de la liste.
- **Supprimer tout** - Supprime tous les journaux.
- **Exporter** - Exporte le journal vers un fichier .xml ou un fichier .xml zippé.

Planificateur

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

Vous pouvez accéder au Planificateur à partir de la fenêtre principale de ESET Internet Security, en cliquant sur **Outils** > **Planificateur**. Le **Planificateur** contient une liste de toutes les tâches planifiées avec leurs propriétés de configuration telles que la date prédéfinie, l'heure et le profil d'analyse utilisé.

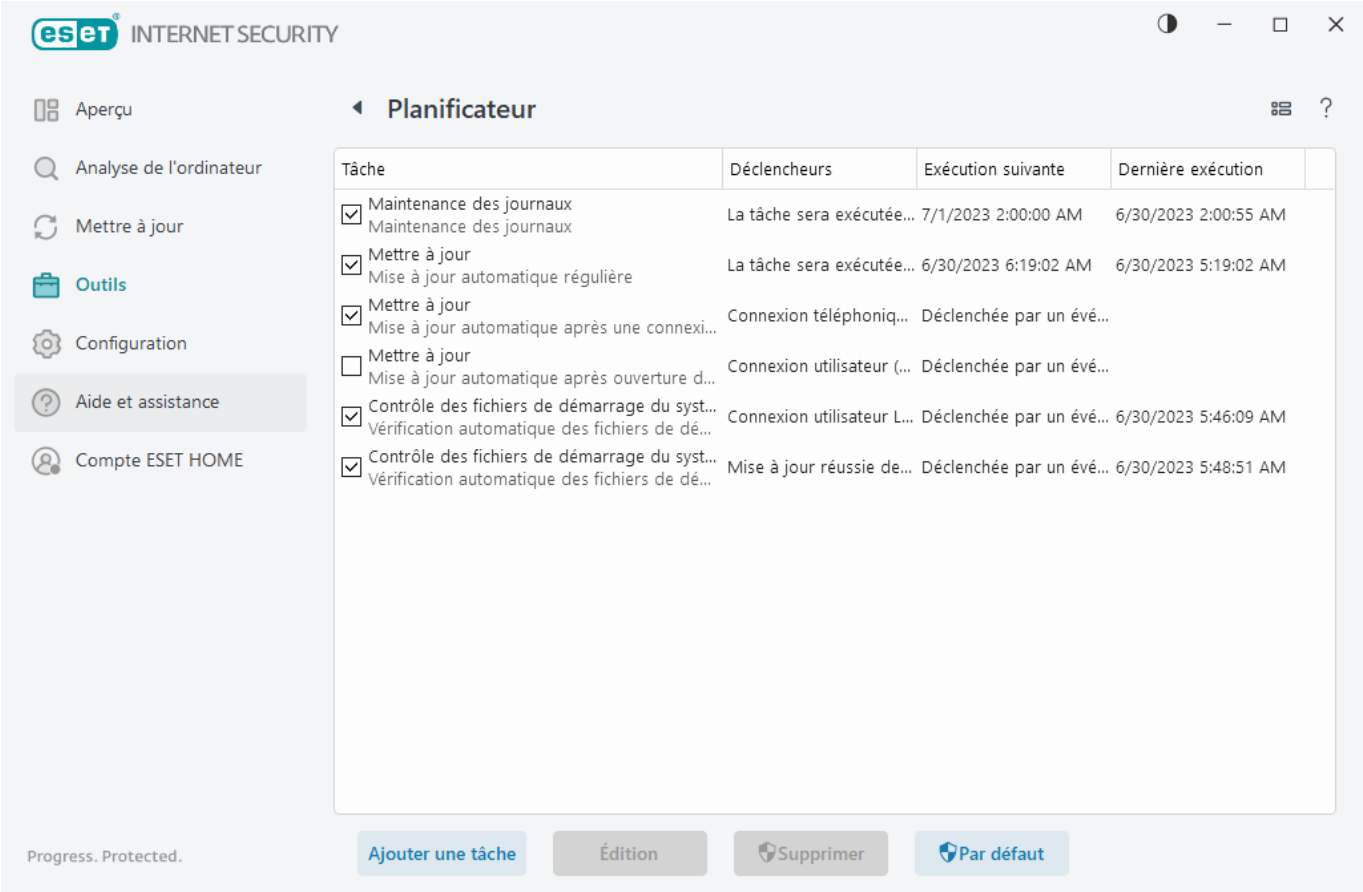
Le Planificateur permet de planifier les tâches suivantes : la mise à jour des modules, les tâches d'analyse, le contrôle des fichiers de démarrage du système et la maintenance des journaux. Vous pouvez ajouter ou supprimer des tâches directement à partir de la fenêtre principale du Planificateur (cliquez sur **Ajouter une tâche** ou **Supprimer**, dans le bas). Vous pouvez rétablir la liste des tâches planifiées par défaut et supprimer toutes les modifications en cliquant sur **Défaut**. Cliquez avec le bouton droit en un point quelconque de la fenêtre du planificateur pour effectuer les actions suivantes : afficher de l'information détaillée, 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 ou désactiver les tâches.

Par défaut, les tâches planifiées suivantes s'affichent dans le **Planificateur** :

- **Maintenance des journaux**
- **Mise à jour automatique régulière**

- **Mise à jour automatique après ouverture de session utilisateur**
- **Vérification automatique des fichiers de démarrage** (après ouverture de session utilisateur)
- **Vérification automatique des fichiers au démarrage** (après la mise à jour réussie du moteur de détection)

Pour modifier la configuration d'une tâche planifiée existante (tant par défaut que définie par l'utilisateur), cliquez avec le bouton droit sur la tâche, puis sur **Modifier** ou sélectionnez la tâche que vous voulez modifier, puis cliquez sur le bouton **Modifier**



Ajouter une nouvelle tâche

1. Cliquez sur **Ajouter une tâche** au bas de la fenêtre.
2. Entrez un nom pour la tâche.
3. Sélectionnez la tâche souhaitée dans le menu déroulant :
   - **Exécuter une application externe** - Planifie l'exécution d'une application externe.
   - **Maintenance des journaux** - Les fichiers journaux contiennent les restes des enregistrements supprimés. Cette tâche optimise les enregistrements dans les fichiers journaux de façon régulière, afin qu'ils puissent fonctionner de façon efficace.
   - **Contrôle des fichiers de démarrage du système** - Vérifier les fichiers qui peuvent être exécutés au démarrage du système ou lors de l'ouverture de session.
   - **Créer un instantané de l'état de l'ordinateur** - Crée un instantané de l'ordinateur ESET SysInspector -

recueille de l'information détaillée sur les composants système (pilotes, applications, par ex.) et évalue le niveau de risque de chacun des composants.

- **Analyse de l'ordinateur à la demande** - Effectue l'analyse des fichiers et dossiers de votre ordinateur.
- **Mise à jour –** Planifie une tâche de mise à jour en mettant à jour les modules.

4. Activez le bouton bascule en regard de l'option **Activé** pour activer la tâche (vous pouvez le faire ultérieurement en cochant ou en décochant la case située dans la liste des tâches planifiées); cliquez sur **Suivant** et sélectionnez l'une des options de périodicité :

- **Une fois** - La tâche sera exécutée à la date et l'heure prédéfinies.
- **Plusieurs fois** - La tâche sera exécutée à chaque intervalle précisé.
- **Quotidiennement** - La tâche sera exécutée plusieurs fois, chaque jour, à l'heure indiquée.
- **Chaque semaine** - La tâche sera exécutée une ou plusieurs fois par semaine, à l'heure et au jour prédéfinis.
- **Déclenchée par un événement** - La tâche sera exécutée lorsque l'événement précisé se produira.

5. Sélectionnez **Ignorer la tâche lors du fonctionnement sur batterie** afin de minimiser les ressources systèmes lorsqu'un portable est alimenté par batterie. La tâche sera exécutée à la date et à l'heure indiquées dans les champs **Exécution de la tâche**. Si une tâche n'a pas pu être exécutée à l'heure définie, il est possible de préciser le moment où elle sera exécutée de nouveau :

- **À la prochaine heure planifiée**
- **Dès que possible**
- **Immédiatement, si le temps écoulé depuis la dernière exécution dépasse (heures)** – Représente le temps écoulé depuis la première exécution ignorée de la tâche. Si ce temps est dépassé, la tâche s’exécutera immédiatement. Réglez l’heure à l’aide de la roulette ci-dessous.

Pour examiner une tâche planifiée, cliquez avec le bouton droit de la souris sur la tâche et cliquez sur **Afficher les détails de la tâche**.

Options d’analyse planifiées

Dans cette fenêtre, vous pouvez spécifier des options avancées pour une tâche d’analyse d’ordinateur planifiée.

Pour exécuter une analyse sans action de nettoyage, cliquez sur **Paramètres avancés** et sélectionnez **Analyser sans nettoyage**. L’historique des analyses est enregistré dans le journal d’analyse.

Lorsque l'option **Ignorer les exclusions** est sélectionnée, les fichiers avec des extensions qui étaient auparavant exclues de l'analyse sont analysés, sans aucune exception.

Le menu déroulant**Action après analyse** vous permet de définir une action à effectuer automatiquement une fois l’analyse terminée :

- **Aucune action** - À la fin de l'analyse, aucune action ne sera effectuée.

- **Éteindre** - L'ordinateur s'éteint après l'analyse.

- **Redémarrer si nécessaire :** l'ordinateur redémarre uniquement si cela est nécessaire pour terminer le nettoyage des menaces détectées.

- **Redémarrer** - Ferme tous les programmes et redémarre l'ordinateur après l'analyse.

- **Forcer le redémarrage si nécessaire :** l'ordinateur redémarre uniquement si cela est nécessaire pour terminer le nettoyage des menaces détectées.

- **Forcer le redémarrage** - Force la fermeture de tous les programmes ouverts sans attendre aucune action de l'utilisateur et redémarre l'ordinateur après la fin de l'analyse.

- **Mettre en veille** - Enregistre votre session et met l'ordinateur dans un état de basse consommation afin que vous puissiez reprendre rapidement votre travail.

- **Hiberner** - Met tout ce qui est en cours d'exécution sur la RAM dans un fichier spécial de votre disque dur. Votre ordinateur s'éteint, mais retrouvera son état précédent au prochain démarrage.

> Les actions **Mettre en veille** ou **Hiberner** sont disponibles en fonction des paramètres d'alimentation et de veille du système d'exploitation ainsi que des capacités de votre ordinateur. Gardez présent à l'esprit qu'un ordinateur en veille fonctionne toujours. Les fonctions de base s'exécutent toujours et votre ordinateur reste alimenté lorsqu'il fonctionne sur batterie. Pour préserver la batterie, par exemple lorsque vous êtes en dehors de votre bureau, nous vous recommandons d'utiliser l'option Hiberner.

L'action sélectionnée commencera une fois que toutes les analyses en cours sont terminées. Lorsque vous sélectionnez **Arrêter** ou **Redémarrer**, une boîte de dialogue de confirmation affiche un compte à rebours de 30 secondes (cliquez sur **Annuler** pour désactiver l'action demandée).

Sélectionnez **L'analyse ne peut être annulée** pour empêcher les utilisateurs non autorisés d'annuler des actions d'après l'analyse.

Sélectionnez **L'analyse pourra être suspendue par l'utilisateur pendant (min)** pour permettre aux utilisateurs non autorisés de suspendre l'analyse de l'ordinateur pendant une période précise.

Voir aussi Progression de l'analyse.

Aperçu des tâches planifiées

Cette boîte de dialogue affiche des informations détaillées sur la tâche planifiée sélectionnée lorsque vous double-cliquez sur une tâche personnalisée ou lorsque vous faites un clic droit sur une tâche du planificateur personnalisé et cliquez sur **Afficher les détails de la tâche**.

Détails de la tâche

Tapez le **nom de la tâche**, sélectionnez l'une des options de **type de tâche**, puis cliquez sur **Suivant** :

- **Exécuter une application externe** - Planifie l'exécution d'une application externe.

- **Maintenance des journaux** - Les fichiers journaux contiennent les restes des enregistrements supprimés.

Cette tâche optimise les enregistrements dans les fichiers journaux de façon régulière, afin qu'ils puissent fonctionner de façon efficace.

• **Contrôle des fichiers de démarrage du système** - Vérifier les fichiers qui peuvent être exécutés au démarrage du système ou lors de l'ouverture de session.

• **Créer un instantané de l'état de l'ordinateur** - Crée un instantané de l'ordinateur ESET SysInspector - recueille de l'information détaillée sur les composants système (pilotes, applications, par ex.) et évalue le niveau de risque de chacun des composants.

• **Analyse de l'ordinateur à la demande** - Effectue l'analyse des fichiers et dossiers de votre ordinateur.

• **Mise à jour** – Planifie une tâche de mise à jour en mettant à jour les modules.

Calendrier de la tâche

La tâche sera exécutée de façon répétée à l'intervalle de temps spécifié. Sélectionnez l'une des options de périodicité :

• **Une fois** - La tâche ne sera exécutée qu'une fois, à la date et à l'heure définies.

• **Plusieurs fois** - La tâche sera exécutée à chaque intervalle de temps (en heures) précisé.

• **Quotidiennement** - La tâche sera exécutée chaque jour à l'heure indiquée.

• **Chaque semaine** - La tâche sera exécutée une ou plusieurs fois par semaine, à l'heure et au(x) jour(s) définis.

• **Déclenchée par un événement** - La tâche sera exécutée lorsque l'événement précisé se produira.

Ignorer la tâche lors du fonctionnement sur batterie - Aucune tâche ne sera exécutée si l'ordinateur est alimenté par batterie au moment ou elle doit démarrer. Cela s'applique également aux ordinateurs alimentés par un onduleur.

Calendrier de la tâche - Une fois

Exécution de tâche- La tâche en question ne sera exécutée qu'une seule fois à la date et à l'heure indiquées.

Calendrier de la tâche - Tous les jours

La tâche sera exécutée chaque jour à l'heure indiquée.

Calendrier de la tâche - Hebdomadaire

La tâche s’exécutera à plusieurs reprises chaque semaine aux jours et heures sélectionnés.

Calendrier de la tâche - Déclenché par un événement

La tâche sera déclenchée par l'un des événements suivants :

- **Chaque fois que l'ordinateur démarre**
- **Chaque jour au premier démarrage de l'ordinateur**
- **Connexion commutée à Internet/VPN**
- **Mise à jour réussie de module**
- **Mise à jour réussie de produit**
- **Ouverture de session utilisateur**
- **Détection de menace**

Vous pouvez préciser l'intervalle de temps minimum entre deux exécutions de la tâche déclenchée par événement. Par exemple, si vous ouvrez plusieurs sessions pendant une journée, il est préférable de choisir 24 heures afin de n'exécuter la tâche qu'à la première connexion de la journée et puis le jour suivant.

Tâche ignorée

Une tâche peut être ignorée si l'ordinateur est éteint ou est alimenté par batterie. Sélectionner le moment d'exécution de la tâche parmi les options suivantes, puis cliquez sur **Suivant** :

- **À l'heure planifiée suivante** – la tâche s'exécutera si l'ordinateur est allumé à l'heure planifiée suivante.
- **Dès que possible** – la tâche s'exécutera lorsque l'ordinateur est allumé.
- **Immédiatement, si le temps écoulé depuis la dernière exécution planifiée dépasse (heures)** – cette valeur représente le temps écoulé depuis la première exécution ignorée de la tâche. Si ce temps est dépassé, la tâche s'exécutera immédiatement.

Immédiatement, si le temps écoulé depuis la dernière exécution planifiée dépasse (heures) : exemples

Par exemple, une tâche est configurée pour s'exécuter toutes les heures. L'option **Immédiatement, si le temps depuis la dernière exécution planifiée dépasse (heures)** est sélectionné et la limite de temps est de deux heures. La tâche s'exécute à 13 h 00 et, une fois terminée, l'ordinateur se met en veille :

- L'ordinateur se réveille à 15 h 30. La première exécution ignorée de la tâche était à 14 h 00. Seulement 1,5 heure se sont écoulées depuis 14 h 00. Par conséquent, la tâche s'exécutera à 16 h 00.
- L'ordinateur se réveille à 16 h 30. La première exécution ignorée de la tâche était à 14 h 00. Deux heures et demie se sont écoulées depuis 14 h 00, donc la tâche s'exécutera immédiatement.

Détails de la tâche - Mise à jour

Pour mettre à jour le programme à partir de deux serveurs de mise à jour, vous devez créer deux profils de mise à jour distincts. Si le premier ne permet pas de télécharger les fichiers de mise à jour, le programme bascule

automatiquement vers le second. Cela convient, par exemple, pour les portables dont la mise à jour s'effectue normalement à partir d'un serveur de mise à jour sur le réseau local, mais dont les propriétaires se connectent souvent à Internet à partir d'autres réseaux. Ainsi, en cas d'échec du premier profil, le second télécharge automatiquement les fichiers de mise à jour à partir des serveurs de mise à jour d'ESET.

Détails de la tâche - Exécuter l'application

Cette tâche permet de programmer l'exécution d'une application externe.

Fichier exécutable - Choisissez un fichier exécutable dans l'arborescence de répertoire, cliquez sur l'option **...** ou entrez manuellement le chemin d'accès.

Dossier de travail - Définit le dossier de travail de l'application externe. Tous les fichiers temporaires du **fichier exécutable** sélectionné seront créés dans ce dossier.

Paramètres - Paramètres de ligne de commande à utiliser pour l'application (facultatif).

Cliquez sur **Terminer** pour appliquer la tâche.

Nettoyage système

Nettoyage système est un outil qui vous aide à restaurer l'ordinateur dans un état utilisable après avoir nettoyé la menace. Un logiciel malveillant peut désactiver les utilitaires système tels que l'Éditeur du registre, le Gestionnaire de tâches ou les Mises à jour Windows. Le nettoyeur de système restaure les valeurs par défaut et les paramètres d'un système donné en un seul clic.

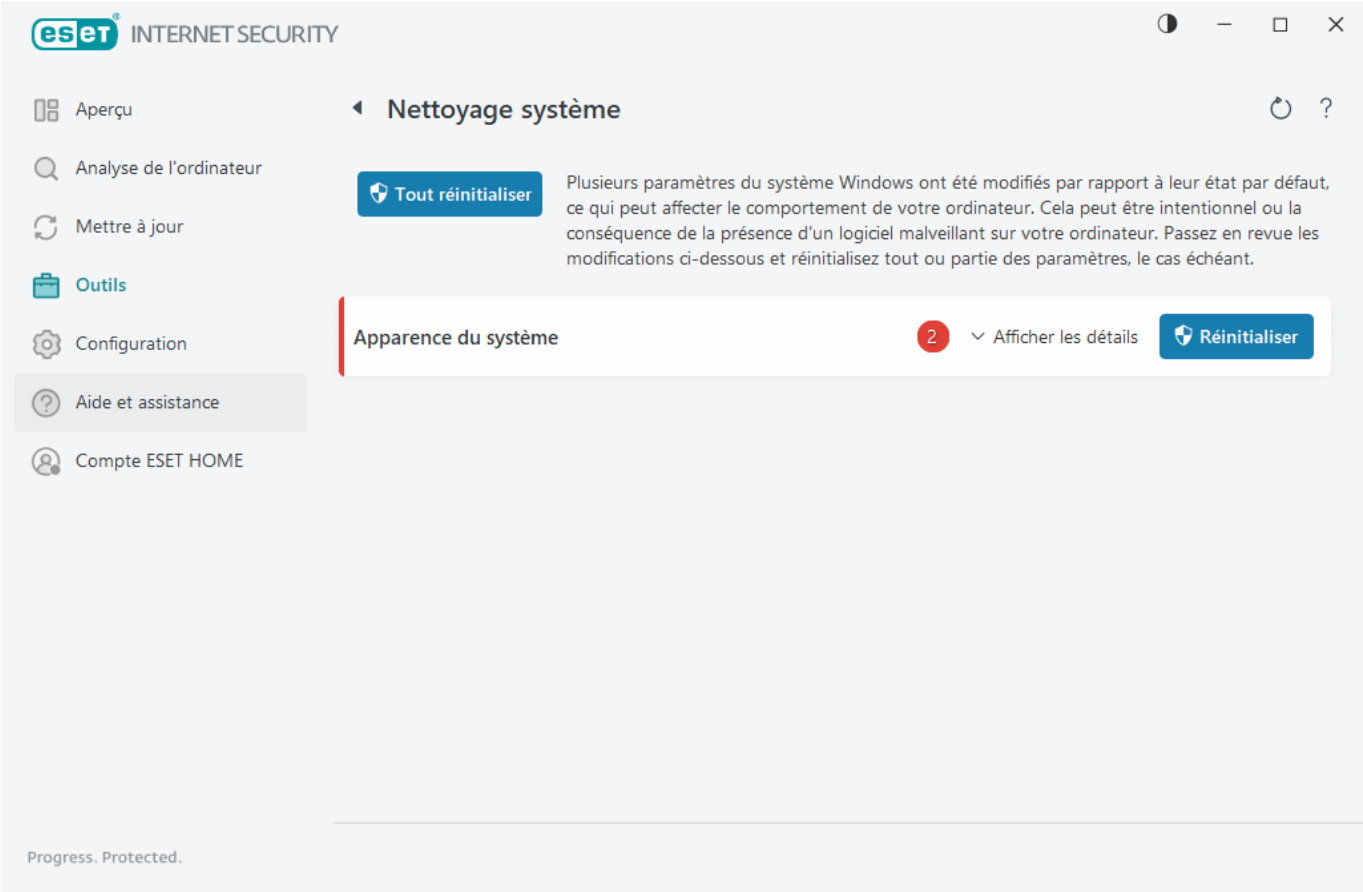
Le nettoyeur de système signale les problèmes de cinq catégories de paramètres :

- **Paramètres de sécurité** : les changements dans les paramètres qui peuvent causer une vulnérabilité accrue de votre ordinateur, tels que les mises à jour de Windows
- **Paramètres du système** : les changements dans les paramètres du système, qui peuvent modifier le comportement de votre ordinateur, tels que les associations de fichiers.
- **Apparence du système** : Paramètres qui affectent l'apparence de votre système, par exemple, le papier peint de votre bureau.
- **Fonctionnalités désactivées** : Certaines fonctionnalités et applications importantes qui peuvent être désactivées
- **Restauration du système Windows** : Paramètres de la fonction Restauration du système Windows, qui vous permet de revenir à un état antérieur

Le nettoyage du système peut être effectué :

- En cas de menace
- Lorsque l'utilisateur clique sur **Réinitialiser**

Vous pouvez examiner les modifications et réinitialiser les paramètres si nécessaire.



Seul un utilisateur possédant des droits d'administrateur peut effectuer des actions dans l'outil Nettoyage système.

Inspecteur de réseau

Inspecteur de réseau peut aider à identifier les vulnérabilités de votre réseau de confiance (domestique ou professionnel), par exemple, des ports ouverts ou un mot de passe de routeur faible. Il fournit également une liste de périphériques connectés, classés par type de périphériques (par exemple, imprimante, routeur, périphérique mobile, etc.) pour vous montrer ce qui est connecté à votre réseau (par exemple, console de jeu, IdO ou autres périphériques domestiques intelligents).

Inspecteur de réseau vous permet de reconnaitre les vulnérabilités d'un routeur et augmente le niveau de protection en cas de connexion à un réseau.

Inspecteur de réseau ne reconfigure pas votre routeur pour vous. Vous effectuerez les modifications vous-même en utilisant l'interface spécialisée de votre routeur. Les routeurs domestiques peuvent être très vulnérables aux logiciels malveillants utilisés pour lancer des attaques par déni de service (DDoS). Si le mot de passe par défaut du routeur n'a pas été modifié par l'utilisateur, il est facile pour les pirates de le deviner, puis de se connecter à votre routeur et de le reconfigurer ou de compromettre votre réseau.

Nous vous recommandons vivement de créer un mot de passe fort qui est assez long et comprend des chiffres, des symboles ou des majuscules. Pour rendre le mot de passe plus difficile à craquer, utilisez un mélange de différents types de caractères.

Si le réseau auquel vous êtes connecté est configuré comme fiable, vous pouvez marquer le réseau comme « Mon réseau ». Cliquez sur **Marquer comme « Mon réseau »** pour ajouter une étiquette Mon réseau au réseau. Cette

étiquette sera affichée à côté du réseau partout dans ESET Internet Security afin de permettre une meilleure identification des réseaux et une vue d'ensemble de la sécurité. Cliquez sur **Supprimer le marquage « Mon réseau »** pour supprimer l'étiquette.

Chaque périphérique connecté à votre réseau est affiché avec des informations de base dans une vue de liste. Cliquez sur un périphérique spécifique pour le modifier ou afficher des informations détaillées sur celui-ci.

Dans la vue de liste, le menu déroulant **Réseaux** vous permet de filtrer les périphériques en fonction des critères suivants :

- Périphériques connectés à un réseau spécifique
- Périphériques connectés à **tous les réseaux**
- périphériques sans catégorie

Cliquez sur l'icône d'un périphérique pour le modifier ou pour afficher des renseignements détaillés sur celui-ci. Les périphériques récemment connectés sont plus proches d'un routeur, ce qui vous permet de les repérer facilement.

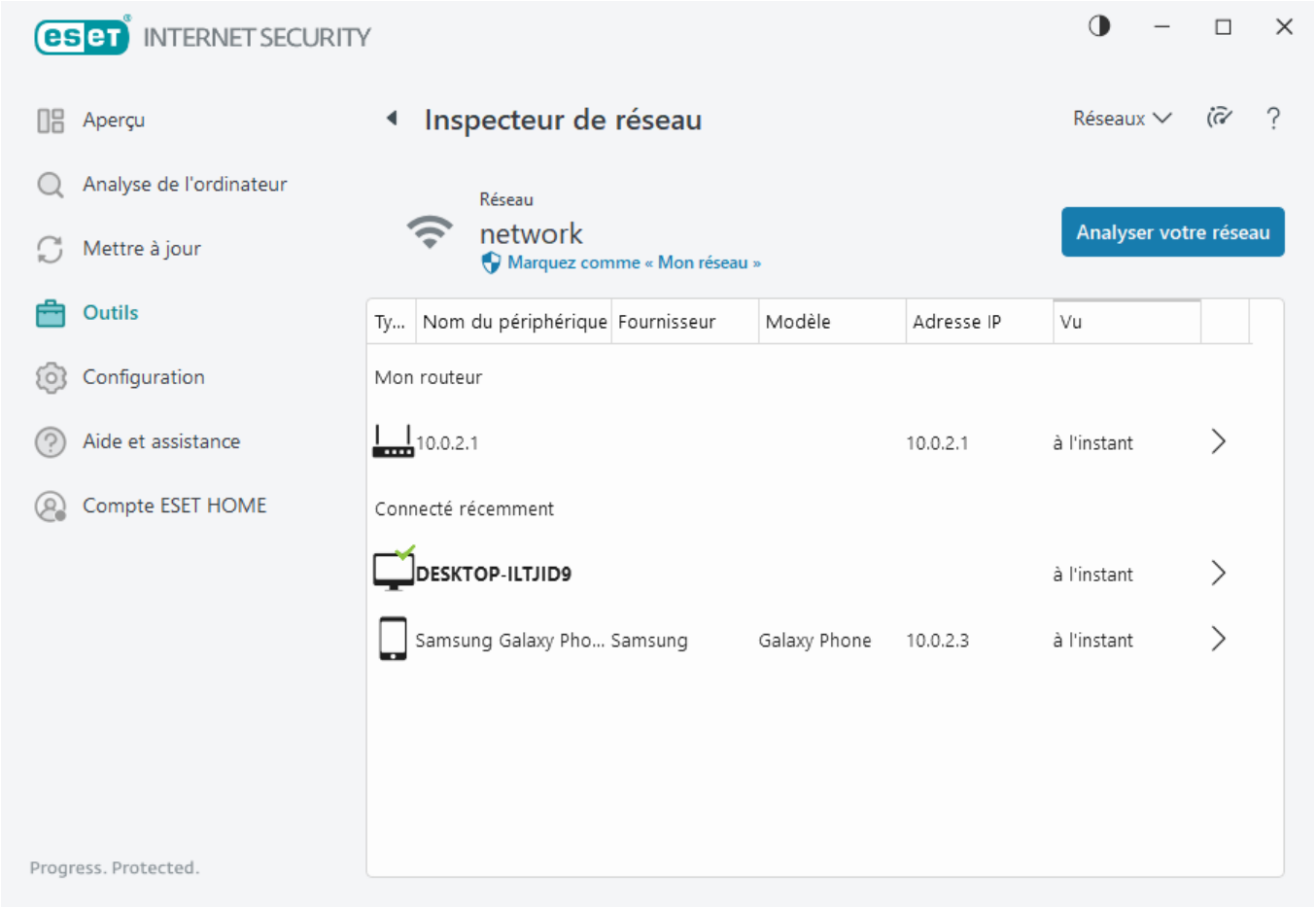
Cliquez sur la roue denté ⚙ dans le coin supérieur droit pour sélectionner s'il faut envoyer une notification lorsqu'un nouveau périphérique est découvert dans le réseau.

Cliquez sur **Analyser votre réseau** pour effectuer manuellement une analyse du réseau auquel vous êtes actuellement connecté. L'option **Analyser votre réseau** n'est disponible que pour un réseau fiable. Consultez la rubrique Profils de connexion réseau pour examiner ou modifier vos paramètres réseau.

Vous pouvez choisir parmi les options d'analyse suivantes :

- Tout analyser
- Analyser uniquement le routeur
- Analyser uniquement les appareils

⚠ Effectuez des analyses de réseau uniquement sur un réseau fiable! Sachez que cela comporte des risques si vous le faites sur des réseaux non fiables.



Lorsque l'analyse est terminée, une notification avec un lien vers les renseignements de base sur le périphérique s'affiche. Vous pouvez également double-cliquer sur le périphérique suspect en mode liste ou sonar. Cliquez sur **Dépannage** pour afficher les communications récemment bloquées. Plus d'informations sur le dépannage du pare-feu.

Il existe deux types de notifications affichées par le module Inspecteur de réseau :

- **Nouveau périphérique connecté au réseau** - Si un périphérique qui n'a jamais été vu se connecte au réseau pendant que l'utilisateur est connecté, cette notification s'affiche.

- **Nouveaux périphérique réseau trouvés** - Si vous vous reconnectez à votre réseau fiable et qu'un périphérique qui n'a jamais été vu est présent, cette notification générique s'affiche.

Dans les deux cas, la notification vous informe qu'un périphérique non autorisé tente de se connecter à votre réseau. Cliquez sur **Afficher les détails du périphérique** pour afficher les détails sur les périphériques.

Que signifient les icônes sur les périphériques dans Inspecteur de réseau ?

	L'icône en étoile jaune indique les périphériques qui sont nouveaux sur le réseau ou qui ont été détectés par ESET pour la première fois.
	L'icône d'avertissement jaune indique la présence probable de vulnérabilités sur votre routeur. Cliquez sur l'icône de votre produit pour obtenir des informations plus détaillées sur le problème.
	L'icône d'avertissement rouge indique la présence de vulnérabilités sur votre routeur et que ce dernier est peut être infecté. Cliquez sur l'icône de votre produit pour obtenir des informations plus détaillées sur le problème.

L'icône bleue peut apparaître lorsque votre produit ESET contient des informations supplémentaires pour votre routeur mais ne nécessite pas une attention immédiate car il n'y a pas de risque de sécurité. Cliquez sur l'icône de votre produit pour obtenir des informations plus détaillées.

Périphérique réseau dans Inspecteur de réseau

Des informations détaillées sur le périphérique peuvent être trouvées ici, y compris les informations suivantes :

- Nom de l'appareil
- Type de périphérique
- Dernière apparition
- Nom du réseau
- Adresse IP
- Adresse MAC
- Système d'exploitation

L'icône du crayon indique que vous pouvez modifier le nom ou le type de périphérique.

Supprimer de l'historique - supprimez le périphérique de la liste des périphériques. Cette option est disponible uniquement pour les périphériques qui ne sont pas connectés à votre réseau en ce moment.

Pour chaque type de périphérique, les actions suivantes sont disponibles :

Routeur

Paramètres du routeur - Accédez aux paramètres du routeur depuis l'interface Web, une application mobile ou cliquez sur **Ouvrir l'interface du routeur**. Si votre fournisseur de services Internet fournit un routeur, il peut être nécessaire d'obtenir l'aide de ce fournisseur ou le fabricant du routeur pour résoudre les problèmes de sécurité détectés. Suivez toujours les précautions de sécurité appropriées indiquées dans le guide de l'utilisateur de votre routeur.
Protection – Pour protéger votre routeur et votre réseau contre les attaques cybernétiques, suivez ces recommandations de base.

Périphérique réseau

Identification du périphérique – Si vous n'êtes pas sûr du périphérique connecté à votre réseau, vérifiez le nom du fournisseur ou du fabricant sous le nom du périphérique. Vous pourrez ainsi savoir de quel type de périphérique il s'agit. Vous pouvez changer le nom du périphérique pour pouvoir vous retrouver la prochaine fois.
Déconnexion du périphérique – Si vous n'êtes pas sûr qu'un périphérique connecté est sans danger pour votre réseau ou pour vos périphériques, gérez l'accès au réseau de ce périphérique dans les paramètres de votre routeur ou modifiez le mot de passe de votre réseau.
Protection – Pour protéger votre périphérique contre les attaques et les logiciels malveillants, installez une protection pour la cybersécurité sur votre périphérique et assurez-vous que votre système d'exploitation et les logiciels installés sont toujours à jour. Pour rester protégé, ne vous connectez pas à des réseaux Wi-Fi non sécurisés.

Ce périphérique

Cet périphérique représente votre ordinateur sur le réseau.
Cartes réseau – Affiche les informations sur vos cartes réseau.

Notifications | Inspecteur de réseau

Voici plusieurs notifications qui peuvent être affichées lorsque ESET Internet Security détecte un problème de vulnérabilité sur votre routeur. Chaque notification contient une brève description et fournit des solutions ou des étapes qui devraient être effectuées afin de minimiser les risques de vulnérabilité de votre routeur. Si vous n'êtes pas familiarisé avec les modifications apportées aux routeurs, nous vous recommandons de contacter le fabricant de votre routeur ou votre fournisseur d'accès Internet.

Vulnérabilité potentielle trouvée
Votre routeur peut contenir des vulnérabilités connues qui pourraient en faire une cible facile d'attaque et d'exploitation. Mettre à jour le micrologiciel du routeur.

Vulnérabilité trouvée
Votre routeur contient des vulnérabilités connues qui en font une cible facile d'attaque et d'exploitation. Mettre à jour le micrologiciel du routeur.

Menace détectée
Votre routeur est infecté par des logiciels malveillants. Redémarrez votre routeur et effectuez à nouveau l'analyse.

Mot de passe du routeur faible
Le mot de passe de votre routeur est faible et peut être facilement deviné par quelqu'un d'autre. Modifiez le mot de passe de votre routeur.

Redirection réseau malveillante
Votre trafic sur Internet semble être redirigé vers des sites Web malveillants. Cela peut signifier que votre routeur est compromis. Modifiez les paramètres du serveur DNS de votre routeur.

Services de réseau ouverts
Votre routeur exécute des services réseau qui peuvent être exploités par d'autres. Cela peut être dû à une mauvaise configuration ou à un routeur compromis. Vérifier la configuration du routeur.

Services réseau sensibles ouverts
Votre routeur exécute des services réseau sensibles qui peuvent être exploités par d'autres. Cela peut être dû à une mauvaise configuration ou à un routeur compromis. Vérifier la configuration du routeur.

Micrologiciel obsolète
Le micrologiciel de votre routeur est obsolète et peut contenir des vulnérabilités. Mettre à jour le micrologiciel du routeur.

Paramètre malveillant de routeur
Ce serveur DNS que vous utilisez est malveillant et peut vous envoyer vers des sites Web dangereux. Cela peut signifier que votre routeur est compromis. Modifiez les paramètres du serveur DNS de votre routeur.

Services réseau
Votre routeur exécute des services réseau communs. Ils sont nécessaire pour le réseau et sont probablement sécurisés. Vérifier la configuration du routeur.

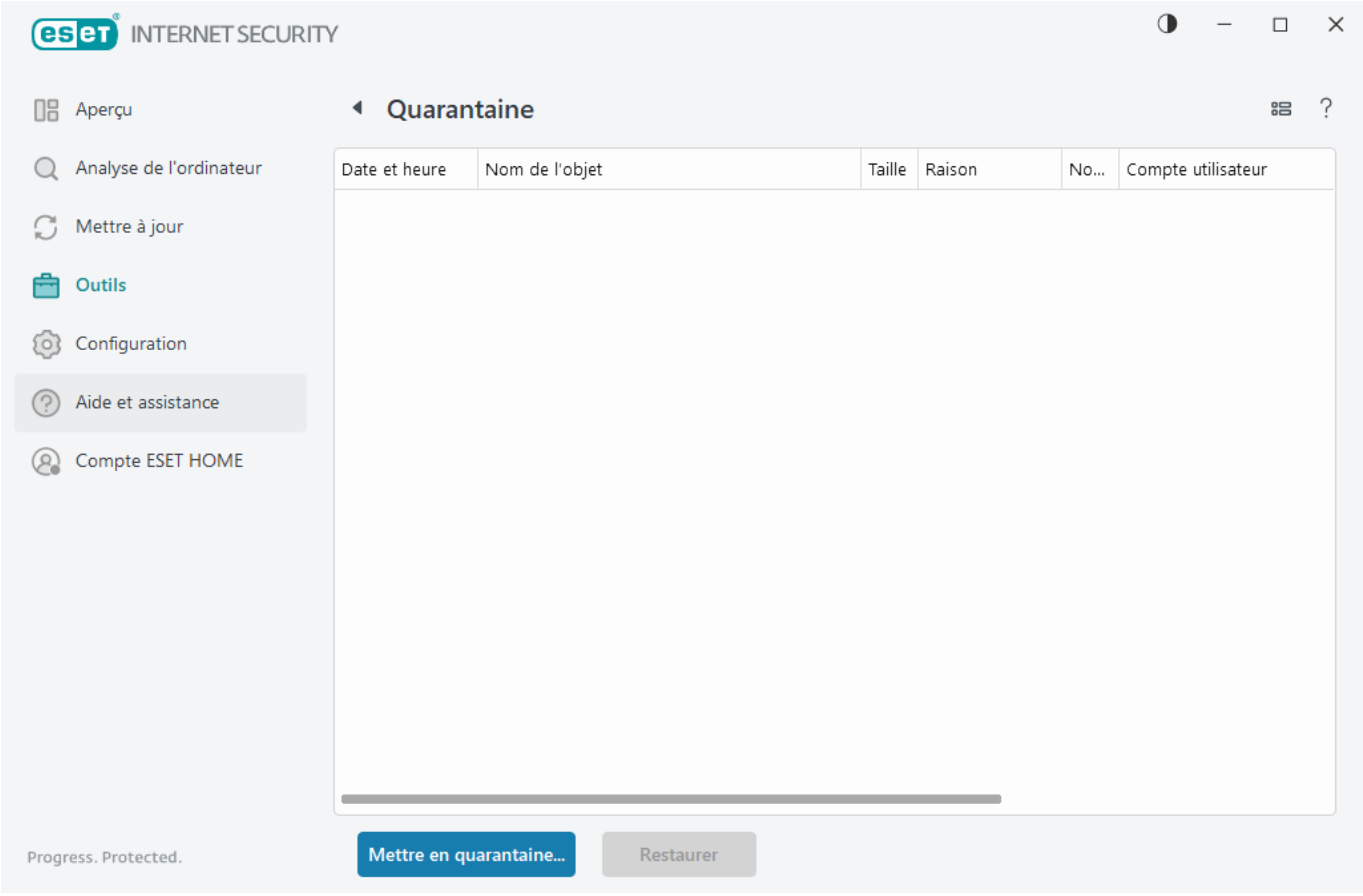
Quarantaine

La fonction principale de la quarantaine est de stocker en toute sécurité les objets signalés (tels que les logiciels malveillants, les fichiers infectés ou les applications potentiellement indésirables).

Vous pouvez accéder à la quarantaine à partir de la fenêtre principale de ESET Internet Security, en cliquant sur **Outils** > **Quarantaine**.

Les fichiers stockés dans le dossier de quarantaine peuvent être visualisés dans un tableau indiquant :

- la date et l'heure de mise en quarantaine,
- le chemin de l'emplacement d'origine du fichier infecté,
- sa taille en octets,
- la raison (par exemple, un objet ajouté par l'utilisateur),
- et le nombre de détections (par exemple, les détections dupliquées d'un même fichier ou s'il s'agit d'une archive contenant de multiples infiltrations).



Mise de fichiers en quarantaine

ESET Internet Security met automatiquement en quarantaine les fichiers supprimés (si vous n'avez pas annulé cette option dans la fenêtre d'alerte).

Les fichiers supplémentaires doivent être mis en quarantaine s'ils ont l'une des caractéristiques suivantes :

a.il est impossible de les supprimer,

b.il est dangereux de déconseillé de les supprimer,

c.ils sont faussement détectés par ESET Internet Security,

d.ils se comportent de façon suspecte, mais n'ont pas été détectés par les modules de protection.

Pour mettre un fichier en quarantaine, vous disposez de plusieurs options :

a.Utilisez la fonction Glisser-déposer pour mettre un fichier en quarantaine manuellement : cliquez sur le fichier; en maintenant le bouton de la souris enfoncé, déplacez le pointeur de la souris sur la zone marquée puis relâchez-le. Après cela, l'application est déplacée au premier plan.

b.Cliquez à l'aide du bouton droit sur le fichier > Cliquez sur **Options avancées** > **Fichier en quarantaine**.

c.Cliquez sur **Déplacer dans la quarantaine** à partir de la fenêtre **Quarantaine**.

d.Il est également possible d'utiliser le menu contextuel à cette fin. Il suffit de cliquer avec le bouton droit dans la fenêtre **Quarantaine** et de sélectionner **Quarantaine**.

Restaurer depuis la quarantaine

Les fichiers mis en quarantaine peuvent également être restaurés à leur emplacement d'origine :

- Utilisez à cet effet la fonction **Restaurer**, disponible dans le menu contextuel en cliquant avec le bouton droit de la souris sur un fichier donné en quarantaine.

- Si un fichier est marqué comme Application potentiellement indésirable, l'option **Restaurer et exclure de l'analyse** est activée. Voir aussi Exclusions.

- Le menu contextuel offre également l'option **Restaurer vers** qui permet de restaurer des fichiers vers un emplacement autre que celui d'où ils ont été supprimés.

- La fonctionnalité de restauration n'est pas disponible dans certains cas, par exemple, pour les fichiers situés sur un partage réseau en lecture seule.

Suppression de la quarantaine

Cliquez à droite sur un élément donné et sélectionnez **Supprimer du dossier de quarantaine**, ou sélectionnez l'élément que vous voulez supprimer et cliquez sur la touche **Supprimer** de votre clavier. Si vous souhaitez sélectionner et supprimer tous les éléments en quarantaine, vous pouvez appuyer sur **Ctrl + A**, puis sur **Delete** sur votre clavier. Les éléments supprimés seront définitivement supprimés de votre périphérique et mis en quarantaine.

Soumission d'un fichier de quarantaine

Si vous avez placé en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été jugé infecté par erreur (par exemple, par l'analyse heuristique du code) et mis en quarantaine, envoyez l'échantillon pour analyse à ESET Research Lab. Pour envoyer un fichier, cliquez sur ce dernier avec le bouton droit de la souris, puis, dans le menu contextuel, sélectionnez **Envoyer pour analyse**.

Description de la détection

Cliquez avec le bouton droit sur un élément et cliquez sur **Description de détection** pour ouvrir l'encyclopédie des menaces ESET, qui contient des informations détaillées sur les dangers et les symptômes de l'infiltration enregistrée.

> **Instructions illustrées**
> Les articles suivants de la base de connaissances ESET peuvent n'être disponibles qu'en anglais :
> - Restaurer un fichier en quarantaine dans ESET Internet Security
> - Supprimer un fichier de la quarantaine dans ESET Internet Security
> - Mon produit ESET m'a informé d'une détection : que dois-je faire ?

Échec de la mise en quarantaine

Les raisons pour lesquelles des fichiers spécifiques ne peuvent pas être déplacés vers la quarantaine sont les suivantes :

- **Vous ne disposez pas d'autorisations de lecture** – indique que vous ne pouvez pas visualiser le contenu d'un fichier.
- **Vous ne disposez pas d'autorisations d'écriture** – indique que vous ne pouvez pas modifier le contenu du fichier, c'est-à-dire ajouter un nouveau contenu ou supprimer le contenu existant.
- **Le fichier que vous essayez de mettre en quarantaine est trop volumineux.** – vous devez réduire la taille du fichier.

Lorsque vous recevez le message d'erreur « Échec de la mise en quarantaine », cliquez sur **Plus d'informations**. La fenêtre de la liste des erreurs de quarantaine apparaît et vous verrez le nom du fichier et la raison pour laquelle le fichier ne peut pas être mis en quarantaine.

Sélectionner l'échantillon pour analyse

Si vous trouvez un fichier suspect sur votre ordinateur ou un site suspect sur Internet, vous pouvez l'envoyer à ESET Research Lab pour analyse (cette option peut ne pas être disponible en fonction de votre configuration de ESET LiveGrid®).

> **Avant d'envoyer des échantillons à ESET**
> N'envoyez des échantillons que s'ils répondent au moins à l'un des critères suivants :
> - L'échantillon n'est pas du tout détecté par votre produit ESET.
> - L'échantillon est identifié à tort comme une menace
> - Nous n'acceptons pas vos fichiers personnels (que vous souhaitez analyser à la recherche de logiciels malveillants par ESET) comme échantillons (ESET Research Lab n'effectue pas d'analyses à la demande pour les utilisateurs).
> - Pensez à utiliser un objet clair et compréhensible et fournissez le plus de détails possible sur le fichier (par ex., une capture d'écran ou le site Web à partir duquel vous l'avez téléchargé)

Vous pouvez envoyer un échantillon (un fichier ou un site Web) à ESET pour analyse en utilisant l'une des méthodes suivantes :

1. Utilisez le formulaire d'envoi d'échantillon dans votre produit. Il se trouve à l'emplacement suivant : **Outils** >

Envoyer un échantillon pour analyse. La taille maximale d'un échantillon soumis est de 256 Mo.

2. Vous pouvez également envoyer le fichier par courriel. Si vous préférez cette option, compressez le ou les fichiers avec WinRAR/WinZIP, protégez l'archive avec le mot de passe « infected », puis envoyez-la à samples@eset.com.

3. Pour signaler un pourriel, un faux positif ou des sites Web mal classés par le module de contrôle parental, veuillez consulter cet article de la base de connaissances d'ESET.

Dans le formulaire**Sélectionner l'échantillon pour analyse**, sélectionnez dans le menu déroulant **Raison de la soumission de l'échantillon** la description qui correspond le mieux à votre message :

- Fichier suspect
- Site suspect (un site Web infecté par quelque logiciel malveillant que ce soit)
- Site faux positif
- Fichier faux positif (fichier jugé infecté, mais qui ne l'est pas),
- Autre

Fichier/site - Le chemin d'accès vers le fichier ou le site Web que vous voulez soumettre.

Adresse courriel du contact : L'adresse courriel du contact est envoyée avec les fichiers suspects à ESET et peut être utilisée pour communiquer avec vous si des informations complémentaires sont nécessaires pour l'analyse. L'entrée de l'adresse courriel est facultative. Sélectionnez **Envoyer anonymement** pour laisser ce champ vide.

> **Vous ne recevrez peut-être pas de réponse d'ESET**
> Vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires sont nécessaires. Il en est ainsi parce que nos serveurs reçoivent, chaque jour, des dizaines de milliers de fichiers; nous ne pouvons donc pas répondre à tous ces envois.
> Si le fichier se révèle être une application ou un site Web malveillant, il sera ajoutée à l'une des mises à jour suivantes.

Sélectionner un échantillon pour analyse - fichier suspect

Signes et symptômes d'une infection par un logiciel malveillant - Entrez une description du comportement du fichier suspect observé sur votre ordinateur.

Origine du fichier (URL ou fournisseur) - Veuillez entrer l'origine du fichier (source) et indiquer comment vous avez obtenu ce fichier.

Remarques et renseignements supplémentaires - Ici, vous pouvez ajouter des renseignements ou des descriptions supplémentaires qui faciliteront le traitement du fichier suspect.

> Le premier paramètre - **Signes et symptômes d'une infection observés** - Est requis, mais le fait de fournir de l'information supplémentaire aidera grandement nos laboratoires lors du processus d'identification et du traitement des échantillons.

Sélectionner un échantillon pour analyse - site suspect

Veuillez sélectionner l'une des options suivantes du menu déroulant **Qu'est-ce qui ne va pas avec ce site** :

- **Infecté** - Un site Web qui contient des virus ou d'autres logiciels malveillants diffusés par différentes méthodes.
- **Hameçonnage** : Le hameçonnage est souvent utilisé pour accéder à des données sensibles, telles que numéros de comptes bancaires, NIP, etc. Pour en savoir plus sur ce type d'attaque, consultez le glossaire.
- **Fraude** - Un site de canular ou un site frauduleux spécialement conçu pour réaliser des profits rapides.
- Sélectionnez **Autre** si les options susmentionnées ne décrivent pas le site que vous allez soumettre.

Remarques et renseignements supplémentaires : Ici, vous pouvez ajouter des renseignements ou des descriptions supplémentaires qui faciliteront l'analyse du site Web suspect.

Sélectionner un échantillon pour analyse - fichier faux positif

Nous vous demandons de soumettre les fichiers qui sont détectés comme étant infectés, alors qu'ils ne le sont pas, et ce, afin de nous aider à améliorer notre moteur antivirus et anti-logiciel espion et augmenter la protection des autres. Les faux positifs peuvent se produire lorsque le modèle d'un fichier correspond au modèle contenu dans un moteur de détection.

Nom et version de l'application - Titre et version du programme (numéro, alias ou nom de code, par ex.).

Origine du fichier (URL ou fournisseur) - Veuillez entrer l'origine du fichier (source) et indiquer comment vous avez obtenu ce fichier.

Objectifs de l'application - La description générale de l'application, le type d'application (navigateur, lecteur média, par ex.) et sa fonctionnalité.

Remarques et renseignements supplémentaires - Ici, vous pouvez ajouter des renseignements ou des descriptions supplémentaires qui faciliteront le traitement du fichier suspect.

> Les trois premiers paramètres sont requis pour identifier les applications légitimes et les distinguer du code malveillant. Le fait de fournir de l'information supplémentaire aidera grandement nos laboratoires lors du processus d'identification et du traitement des échantillons.

Sélectionner un échantillon pour analyse - site faux positif

Nous vous demandons de nous soumettre des sites qui sont détectés comme étant infectés, des sites de fraude ou de hameçonnage, et qui ne le sont pas. Les faux positifs peuvent se produire lorsque le modèle d'un fichier correspond au modèle contenu dans un moteur de détection. Veuillez nous soumettre ce site Web afin de nous aider à améliorer notre moteur antivirus et antispyware et augmenter la protection des autres.

Remarques et renseignements supplémentaires : Ici, vous pouvez ajouter des renseignements ou des descriptions supplémentaires qui faciliteront le traitement du site Web suspect.

Sélectionner un échantillon pour analyse - autre

Utilisez ce formulaire si le fichier ne peut être catégorisé comme un **Fichier suspect** ou comme un **Faux positif**.

Raison de l'envoi du fichier - Veuillez entrer une description détaillée ainsi que la raison de l'envoi du fichier.

Configuration

Vous pouvez trouver des groupes de fonctionnalités de protection disponibles dans la fenêtre principale du programme, sous **Configuration**.

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

Protection de l'ordinateur

Protection internet

Protection du réseau

Outils de sécurité

D'autres options sont également disponibles au bas de la fenêtre de configuration. Utilisez le lien Configuration avancée pour configurer d'autres paramètres détaillés pour chacun des modules. L'option Importer et exporter les paramètres permet de charger des paramètres de configuration à l'aide d'un fichier de configuration .xml ou d'enregistrer les paramètres de configuration actuels dans un fichier de configuration.

Protection de l'ordinateur

Cliquez sur **Protection de l'ordinateur** dans la fenêtre principale du programme, puis sur **Configuration** pour avoir une vue d'ensemble de tous les modules de protection :

- Protection en temps réel du système de fichiers - Elle analyse tous les fichiers à la recherche de code malveillant au moment de l'ouverture, de la création ou de l'exécution de ces fichiers.
- Contrôle de périphérique - Ce module permet d'analyser, de bloquer ou de régler les filtres ou permissions étendus et de sélectionner la façon dont l'utilisateur peut accéder à un périphérique donné (CD/DVD/USB, etc.) et travailler avec celui-ci.
- HIPS - Le système HIPS surveille les événements qui se produisent dans le système d'exploitation et réagit à ces derniers, en fonction d'un ensemble personnalisé de règles.
- Mode Jeu - Active ou désactive le mode Jeu. Un message d'avertissement s'affichera (risque potentiel à la sécurité) et la fenêtre principale s'affichera en orange après l'activation du mode jeu.
- Protection de la webcam : contrôle les processus et les applications qui accèdent à la webcam connectée.

Pour suspendre ou désactiver des modules de protection individuels, cliquez sur le bouton bascule .

⚠ La désactivation des modules de protection peut diminuer le niveau de protection de votre ordinateur.

Cliquez sur l'icône de l'engrenage à côte d'un module de protection pour accéder aux paramètres avancés de ce module.

Pour la **protection en temps réel du système de fichiers**, cliquez sur l'icône et choisissez l'une des options suivantes :

- **Configurer** - Ouvre lenêtre de configuration avancée de la protection en temps réel du système de fichiers.
- **Modifier les exclusions** – Ouvre la fenêtre de configuration des exclusions afin que vous puissiez exclure les fichiers et les dossiers de l'analyse.

Pour la **protection de la webcam**, cliquez sur l'icône de l'engrenage et choisissez l'une des options suivantes :

- **Configurer** - Ouvre la fenêtre de configuration avancée de la protection de la webcam.
- **Bloquer tout accès jusqu'au redémarrage** - Bloque tout accès à la webcam jusqu'à ce que l'ordinateur redémarre.
- **Bloquer tout accès de façon permanente** – Bloque tout accès à la webcam jusqu'à ce que ce paramètre soit désactivé.
- **Arrêter de bloquer tout accès** – Désactive la possibilité de bloquer l'accès à la webcam. Cette option n'est

disponible que si l’accès à la webcam est bloqué.

Interrompre la protection contre les virus et les logiciels espions - Désactive tous les modules de protection antivirus et antispyware. Lorsque vous désactivez la protection, une fenêtre s’ouvre pour vous permettre de choisir la durée pendant laquelle la protection sera désactivée à l’aide du menu déroulant **Intervalle de temps.** À utiliser uniquement si vous êtes un utilisateur expérimenté ou si vous avez reçu des instructions du service d'assistance technique d’ESET.

Une infiltration est détectée

Des infiltrations peuvent utiliser différents points d'entrée pour attaquer votre système, comme les pages Web, dossiers partagés, courriel ou périphériques amovibles (USB, disques externes, CD, DVD, etc.).

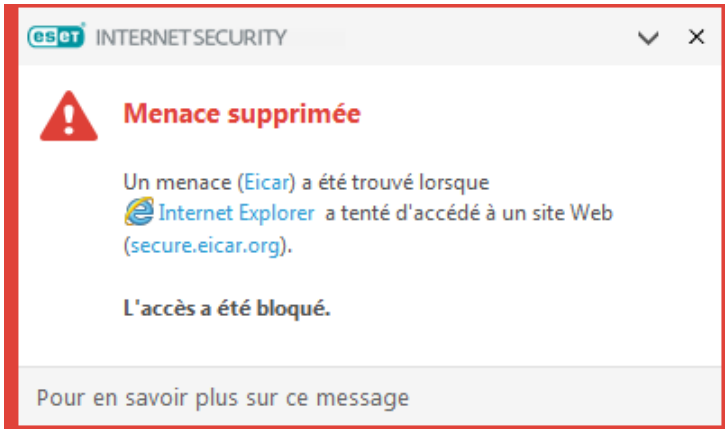
Comportement normal

À titre d'exemple général de la façon dont les infiltrations sont traitées par ESET Internet Security, elles peuvent notamment être détectées en utilisant :

- 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

Chacun de ces modules utilise le niveau de nettoyage standard et tentera de nettoyer le fichier et de le mettre en

quarantaine ou de mettre fin à la connexion. Une fenêtre de notification s'affiche dans la zone de notification, dans le coin inférieur droit de l'écran. Pour obtenir des informations détaillées sur les objets détectés/nettoyés, consultez les fichiers journaux. Pour plus d'informations sur les niveaux de nettoyage et le comportement, consultez la rubrique Niveau de nettoyage.



Analyse de l'ordinateur à la recherche de fichiers infectés

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

1.Ouvrir ESET Internet Security et cliquer sur **Analyse de l'ordinateur**.

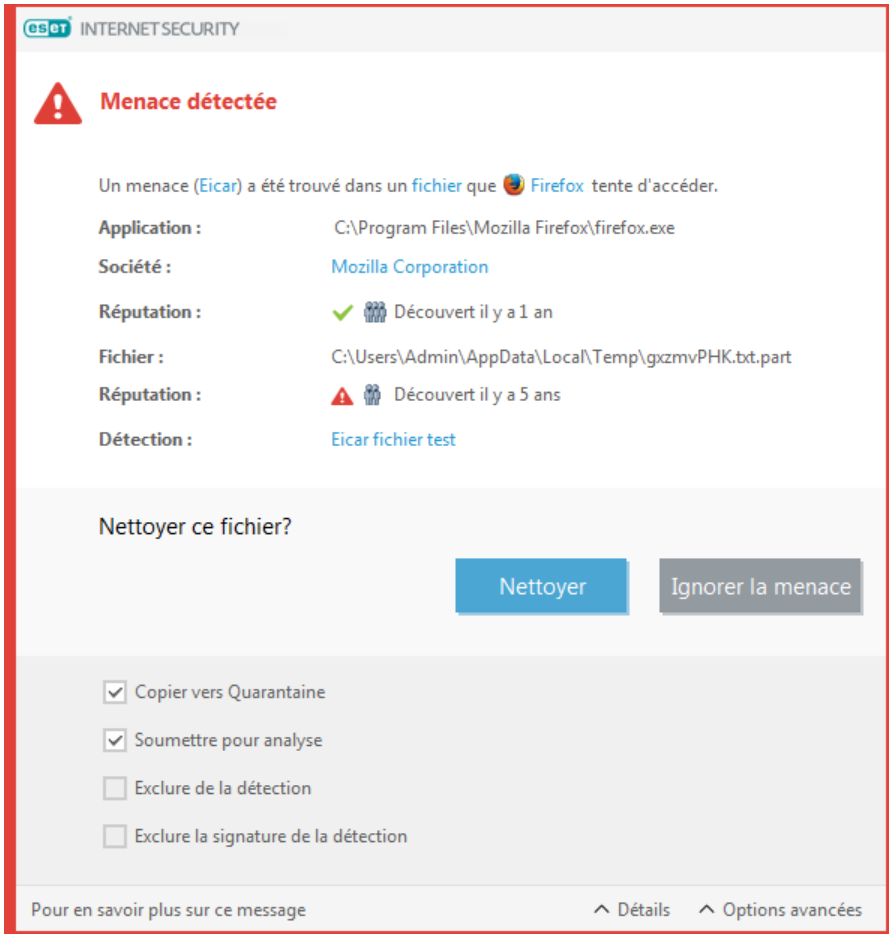
2.Cliquer sur **Analyse de l'ordinateur** (pour plus d'information, se reporter à la rubrique Analyse de l'ordinateur).

3.Lorsque l'analyse est terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés.

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

Nettoyage et suppression

Si aucune action n'est prédéfinie pour la protection en temps réel, vous serez invité à sélectionner une option dans une fenêtre d'avertissement. Les options **Nettoyer**, **Supprimer** et **Aucune action** sont généralement disponibles. Sélectionner **Aucune action** n'est pas recommandé puisque cela ne nettoiera pas les fichiers infectés. La seule exception concerne les situations où vous êtes sûr que le fichier est inoffensif et a été détecté par erreur.



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

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

Restaurer depuis la quarantaine

Vous pouvez accéder à la quarantaine à partir de la fenêtre principale de ESET Internet Security, en cliquant sur **Outils** > **Quarantaine**.

Les fichiers mis en quarantaine peuvent également être restaurés à leur emplacement d'origine :

- Utilisez à cet effet la fonction **Restaurer**, disponible dans le menu contextuel en cliquant avec le bouton droit de la souris sur un fichier donné en quarantaine.
- Si un fichier est marqué comme Application potentiellement indésirable, l'option **Restaurer et exclure de l'analyse** est activée. Voir aussi Exclusions.
- Le menu contextuel offre également l'option **Restaurer vers** qui permet de restaurer des fichiers vers un emplacement autre que celui d'où ils ont été supprimés.
- La fonctionnalité de restauration n'est pas disponible dans certains cas, par exemple, pour les fichiers situés sur un partage réseau en lecture seule.

Menaces multiples

Si aucun des fichiers infectés n'a été nettoyé pendant l'analyse de l'ordinateur (ou le niveau de nettoyage a été défini à **Aucun nettoyage**), une fenêtre d'alerte vous invitant à choisir des actions pour ces fichiers s'affichera. Sélectionnez des actions pour les fichiers (les actions sont définies individuellement pour chaque fichier de la liste), puis cliquez sur **Terminer**.

Suppression de fichiers dans des archives

En mode de nettoyage par défaut, l'archive entière 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 aussi des fichiers sains. Soyez cependant prudent si vous choisissez un nettoyage strict : dans ce mode, l'archive sera supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

Protection sur Internet

La connectivité Internet est un élément standard des ordinateurs personnels. Malheureusement, c'est aussi devenu le principal moyen de transférer et disséminer du code malveillant. Dans la fenêtre principale du programme, cliquez sur **Configurer** > **Protection Internet** pour configurer les fonctionnalités de ESET Internet Security qui augmentent votre protection Internet.

Pour suspendre ou désactiver des modules de protection individuels, cliquez sur le bouton bascule .

⚠ La désactivation des modules de protection peut diminuer le niveau de protection de votre ordinateur.

Cliquez sur l'icône de l'engrenage à côte d'un module de protection pour accéder aux paramètres avancés de ce module.

Le module de contrôle parental protège vos enfants en bloquant les contenus inappropriés ou nuisibles sur Internet.

La protection de l'accès Web analyse les communications HTTP/HTTPS à la recherche de logiciels malveillants et des tentatives d'hameçonnage. La protection de l'accès Web ne doit être désactivée que pour le dépannage.

La protection anti-hameçonnage permet de bloquer les pages Web connues pour diffuser du contenu lié au hameçonnage. Il est fortement recommandé de laisser la protection antihameçonnage activée.

Signaler un site d'hameçonnage : signalez un site Web d'hameçonnage ou malveillant à ESET pour analyse.

> Avant de soumettre un site Web à ESET, assurez-vous qu'il répond à un ou à plusieurs des critères suivants :
> • Le site Web n'est pas du tout détecté.
> • Le site Web est erronément détecté comme une menace. Dans ce cas, vous pouvez Signaler une page bloquée par erreur.

La protection du client de messagerie offre le contrôle des communications par courriel effectuées par l'entremise des protocoles POP3(S) et IMAP(S). À l'aide du plugiciel pour votre client de messagerie, ESET Internet Security assure le contrôle de toutes les communications utilisant le client de messagerie.

L'antipourriel du client de messagerie filtre les messages électroniques non sollicités.

Pour accéder à **l'antipourriel du client de messagerie**, cliquez sur l'icône de l'engrenage et choisissez l'une des options suivantes :

- **Configurer** : cette option ouvre les paramètres avancés de l'antipourriel du client de messagerie.
- **Liste d'adresses de l'utilisateur** (si elle est activée) : Ouvre une fenêtre de dialogue où vous pouvez ajouter, modifier ou supprimer des adresses pour définir les règles antipourriels. Les règles de cette liste seront appliquées à l'utilisateur actuel.
- **Liste d'adresses globale** (si elle est activée) : Ouvre une fenêtre de dialogue où vous pouvez ajouter, modifier ou supprimer des adresses pour définir les règles antipourriels. Les règles de cette liste seront appliquées à tous les utilisateurs.

Anti-Phishing protection

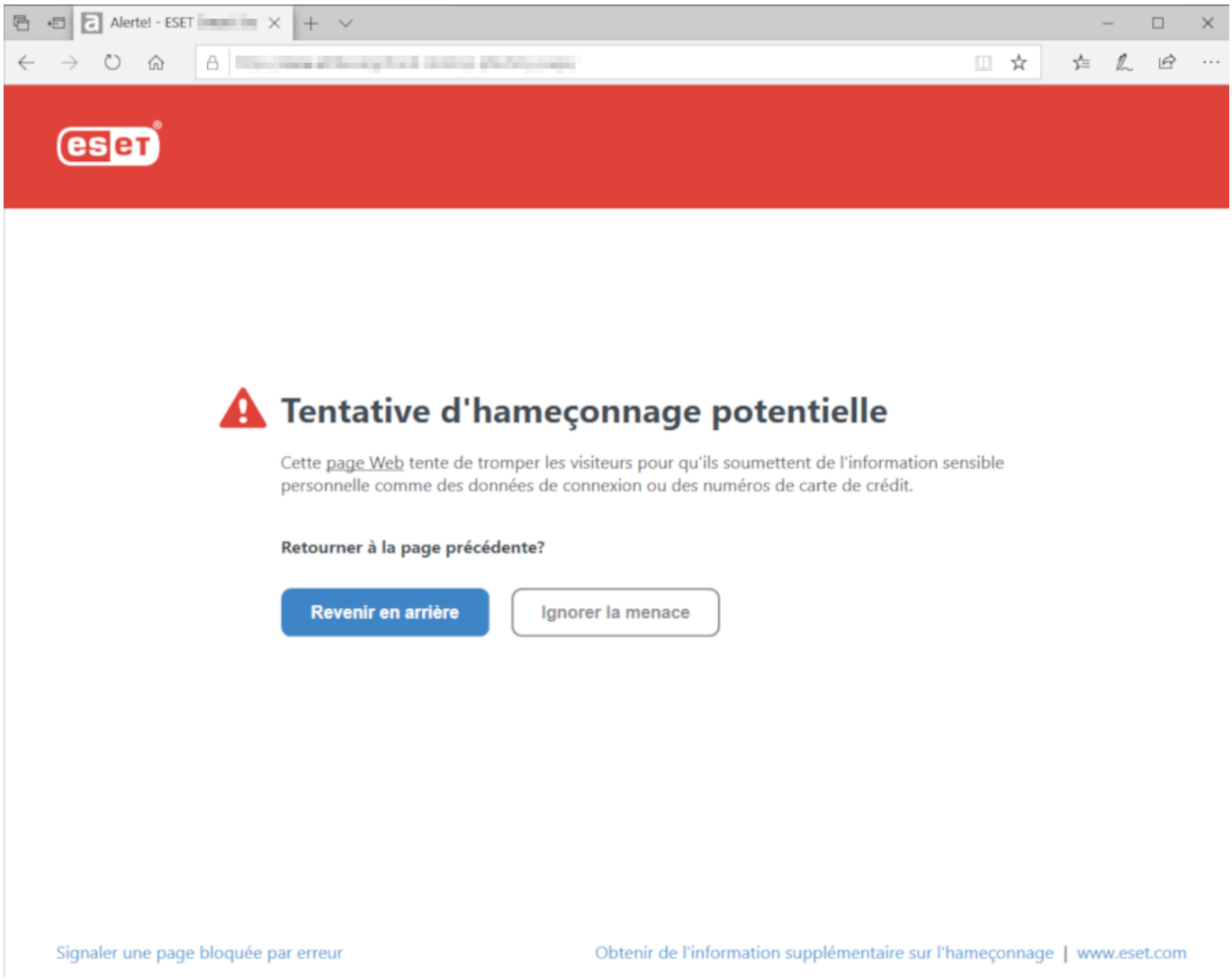
L'hameçonnage (phishing) est une activité criminelle utilisant une ingénierie sociale qui consiste à manipuler les utilisateurs pour obtenir des informations confidentielles. Le hameçonnage permet d'accéder à des données sensibles, telles que numéros de comptes bancaires, des NIP, etc. Pour obtenir de plus amples renseignements, consultez le glossaire. ESET Internet Security contient une protection anti-hameçonnage qui bloque les pages Web connues pour distribuer ce type de contenu.

La protection anti-hameçonnage est activée par défaut. Ce paramètre peut être configuré dans Configuration avancée > **Protections** > **Protection de l'accès Web**.

Consultez l'article de notre base de connaissances à ce sujet pour plus de renseignements sur la protection anti-hameçonnage de ESET Internet Security.

Accéder à un site Web de hameçonnage

Lorsque vous accédez à un site Web connu pour distriburer du contenu d'hameçonnage, votre navigateur Web affiche la boîte de dialogue suivante. Si vous voulez quand même accéder au site Web, cliquez sur **Ignorer la menace** (non recommandé).



Les sites Web présentant des possibilités de hameçonnage qui ont été ajoutés à la liste blanche expireront par défaut plusieurs heures après l'ajout. Pour autoriser un site de façon permanente, utilisez l'outil Gestion d'adresse URL. À partir de Configuration avancée > **Protections** > **Protection de l'accès Web** > **Gestion d'adresses URL**> **Liste d'adresse** > **Modifier**, puis ajoutez le site Web que vous voulez modifier à la liste.

Signaler un site d'hameçonnage

Le lien **Signaler une page bloquée par erreur** vous permet de signaler un site Web qui est détecté par erreur comme une menace.

Vous pouvez également soumettre le site Web par courriel. Envoyez votre message à samples@eset.com. N'oubliez pas d'utiliser un objet clair et compréhensible et fournissez le plus de détails possible sur le site Web

(par ex., le site Web d'où vous y avez accédé, comment vous en avez entendu parler, etc.).

Contrôle parental

Le module Contrôle parental vous permet de configurer les paramètres du contrôle parental qui offre aux parents des outils automatisés pour les aider à protéger leurs enfants en définissant des restrictions quant à l'utilisation des périphériques et des services. L'objectif est d'empêcher les enfants et les jeunes adultes d'accéder à des pages contenant du contenu inapproprié ou malveillant.

Le contrôle parental vous permet de bloquer des pages Web dont le contenu est potentiellement offensant. En outre, les parents peuvent interdire l'accès à plus de 40 catégories de sites Web prédéfinies et à plus de 140 sous-catégories.

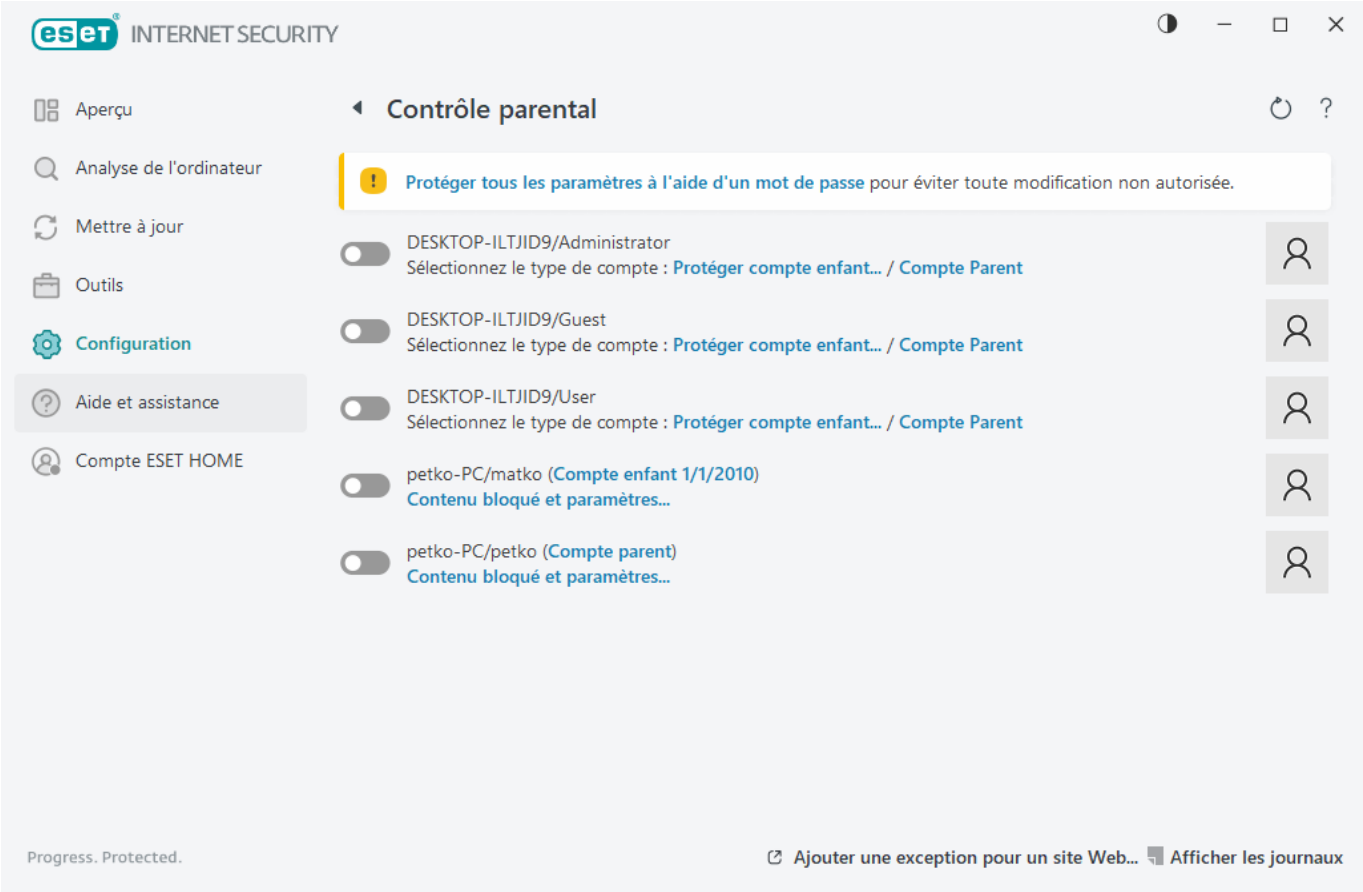
Pour activer le contrôle parental pour un compte utilisateur particulier, effectuez les étapes ci-dessous :

1. Par défaut, le contrôle parental est désactivé dans ESET Internet Security. Deux méthodes permettent d'activer le contrôle parental :

   • Cliquez sur l'icone du bouton bascule  dans **Configuration** > **Protection Internet** > **Contrôle parental** à partir de la fenêtre principale du programme et faites passer l'état du contrôle parental à activé.

   • Ouvrez Configuration avancée > **Protections** > **Protection de l'accès Web Contrôle parental**, puis activez le bouton bascule en regard de **Activer le contrôle parental**.

2. Cliquez sur **Configuration** > **Protection internet** > **Contrôle parental** à partir de la fenêtre principale du programme. Même si **Activé** s'affiche à côté de **Contrôle parental**, vous devez configurer le contrôle parental pour le compte souhaité. Pour cela, cliquez sur le symbole de la flèche, puis dans la fenêtre suivante, sélectionnez **Protéger ce compte enfant** ou ce **Compte parent**. Dans la fenêtre suivante, sélectionnez la date de naissance afin de déterminer le niveau d'accès et les pages Web adaptées à l'âge qui sont recommandées. Le contrôle parental est désormais activé pour le compte spécifié. Cliquez sur **Contenu bloqué et paramètres** sous un nom de compte pour personnaliser les catégories que vous souhaitez autoriser ou bloquer dans l'onglet Catégories. Pour autoriser ou bloquer des pages Web personnalisées ne correspondant à aucune catégorie, cliquez sur l'onglet Exceptions.



Si vous cliquez sur **Configuration** > **Protection internet** > **Contrôle parental** à partir de la fenêtre principale de ESET Internet Security, vous verrez la fenêtre principale qui contient les éléments suivants :

Comptes utilisateur Windows

Si vous avez créé un rôle pour un compte existant, il sera affiché ici. Cliquez sur le bouton bascule pour que s'affiche une coche verte à côté de l'option Contrôle parental du compte. Sous le compte actif, cliquez sur Contenu bloqué et paramètres pour voir une liste des catégories de pages Web autorisées pour ce compte, ainsi que des pages Web bloquées et autorisées.

La section inférieure d'une fenêtre contient les éléments suivants

Ajouter une exception pour un site Web - Un site Web en particulier peut être autorisé ou bloqué en fonction de votre préférences pour chacun des comptes parentaux.

Afficher journaux - Cela affiche un journal détaillé de l'activité du contrôle parental (pages bloquées, compte pour lequel la page Web a été bloquée, catégorie, etc.). Vous pouvez également filtrer ce journal en fonction des critères de votre choix en cliquant sur **Filtrage**.

Contrôle parental

Après avoir désactivé un contrôle parental, une fenêtre **Désactiver le contrôle parental** sera affichée. Vous pouvez y régler l'intervalle pendant lequel la protection est désactivée. Cette option est alors remplacée par **Suspendu** ou **Désactivé en permanence**.

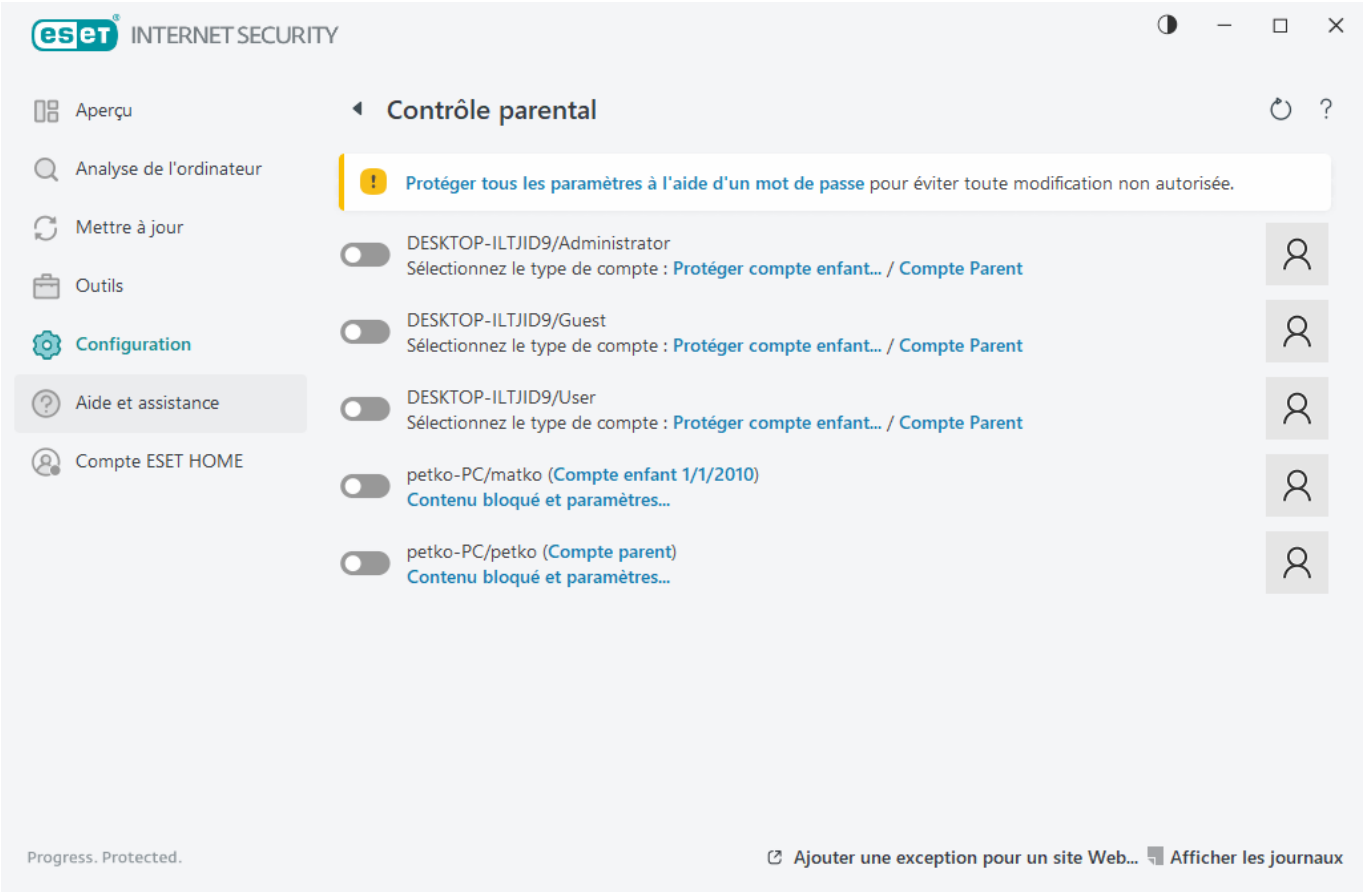
Il est important d'utiliser un mot de passe pour protéger les paramètres de ESET Internet Security. Ce mot de

passe peut être défini dans la section Configuration de l'accès. Si aucun mot de passe n'est défini, l'avertissement suivant apparaît - **Protéger tous les paramètres avec un mot de passe** afin d'éviter les modifications non autorisées. Les restrictions définies dans le contrôle parental n'affectent que les comptes d'utilisateur standards. Puisqu'un administrateur peut contourner toutes les restrictions, elles n'auront aucun effet sur ce type de compte.

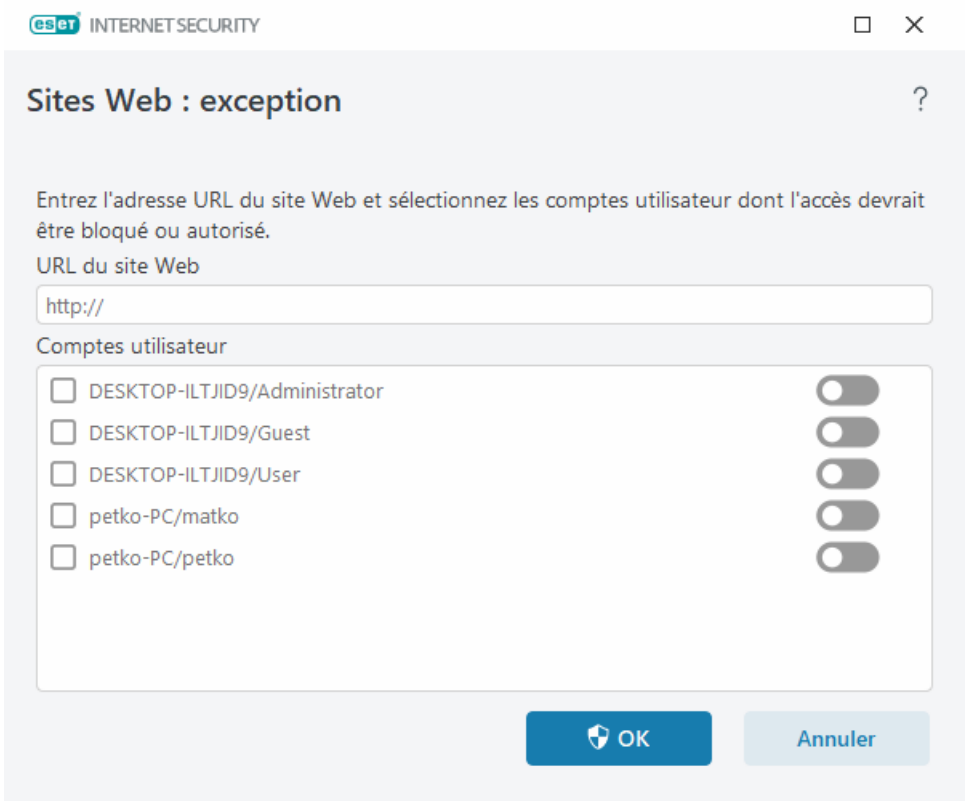
Le contrôle parental nécessite l'activation de l'analyseur de trafic réseau, de l'analyseur du trafic HTTP(S) et du pare-feu pour fonctionner correctement. Toutes ces fonctionnalités sont activées par défaut.

Exceptions pour site Web

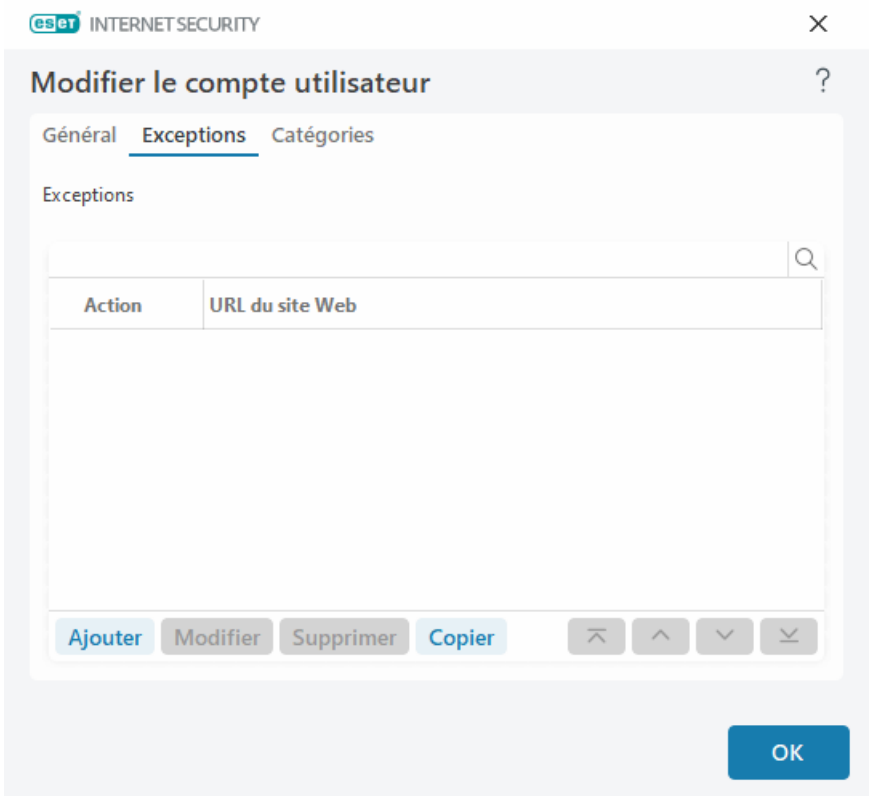
Pour ajouter une exception pour un site Web, cliquez sur **Configuration** > **Protection internet** > **Contrôle parental**, puis cliquez sur **Ajouter une exception pour un site Web**.



Entrez une URL dans le champ **URL du site Web**, puis sélectionnez (autorisée) ou (bloquée) pour chaque compte utilisateur, puis cliquez sur **OK** pour l'ajouter à la liste.



Pour supprimer une adresse URL de la liste, cliquez sur **Configuration** > **Protection internet** > **Contrôle parental**, cliquez sur **Contenu bloqué et paramètres** sous le compte utilisateur désiré, cliquez sur l'onglet **Exceptions**, sélectionnez l'exception et cliquez sur **Supprimer**.



Dans la liste des adresses URL, vous pouvez utiliser les symboles spéciaux * (astérisque) et ? (point d'interrogation) peuvent être utilisés. Par exemple, les adresses des pages Web avec plusieurs TLD doivent être saisies manuellement (*examplepage.com*, *examplepage.sk*, etc.). Lorsque vous ajoutez un domaine à la liste, tout le contenu situé dans ce domaine, et dans tous ses sous-domaines (par exemple, *sub.examplepage.com*) sera

bloqué ou autorisé, en fonction de votre choix quant aux actions selon l'adresse URL.

Bloquer ou autoriser une page Web particulière peut se révéler plus précis que de bloquer ou d'autoriser une catégorie complète de pages Web. Soyez prudent lorsque vous changez ces paramètres et ajoutez une catégorie ou page Web à la liste.

Copier une exception à partir de l'utilisateur

Sélectionnez un utilisateur dans le menu déroulant à partir duquel vous voulez copier l'exception créée.

Copier les catégories du compte

Vous permet de copier une liste des catégories bloquées ou autorisées à partir d'un compte existant modifié.

Protection du réseau

Dans la fenêtre principale du programme, cliquez sur **Configuration** > **Protection du réseau** pour configurer les paramètres de base de la protection du réseau ou dépanner la communication réseau.

Pour suspendre ou désactiver des modules de protection individuels, cliquez sur le bouton bascule .

La désactivation des modules de protection peut diminuer le niveau de protection de votre ordinateur.

Cliquez sur l'icône de l'engrenage à côte d'un module de protection pour accéder aux paramètres avancés de

ce module.

Pare-feu : filtre toutes les communications réseau en fonction de la configuration de ESET Internet Security.

Configurer : permet d'ouvrir la configuration avancée du pare-feu, où vous pouvez définir la façon dont le pare-feu gèrera les communications du réseau.

Mettre le pare-feu en pause (autoriser tout le trafic) : si cette option est activée, toutes les options de filtrage du pare-feu sont désactivées et toutes les connexions entrantes et sortantes sont autorisées. Cliquez sur **Activer le pare-feu** pour réactiver le pare-feu pendant que le filtrage du trafic réseau se trouve dans ce mode.

Bloquer tout le trafic - Toutes les connexions entrantes et sortantes seront bloquées par le pare-feu. N'utilisez cette option que lorsque vous soupçonnez des risques critiques au niveau de la sécurité exigeant que le système soit déconnecté du réseau. Lorsque le filtrage du trafic réseau est en mode **Bloquer tout le trafic**, cliquez sur **Arrêter de bloquer tout le trafic** pour rétablir le fonctionnement normal du pare-feu.

Mode automatique - (lorsqu'un autre mode de filtrage est activé) - Cliquez sur cette option pour mettre le filtrage en mode automatique (règles définies par l'utilisateur).

Mode interactif - (lorsqu'un autre mode de filtrage est activé) - Cliquez sur cette option pour mettre le filtrage en mode interactif.

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. ESET Internet Security vous informera lorsque vous connectez à un réseau sans fil non protégé ou à un réseau dont la protection est faible.

Protection contre un réseau d'ordinateurs zombies - Détecte rapidement et avec précision les logiciels malveillants sur le système.

Connexions aux réseau : affiche les réseaux auxquels les cartes réseau sont connectées avec des informations détaillées.

Résoudre la communication bloquée - Permet de résoudre les problèmes de connectivité causées par le pare-feu d'ESET. Pour de plus amples renseignements, voir Assistant de dépannage.

Résoudre les adresses IP temporairement bloquées – Voir une liste des adresses IP ayant été détectées comme des sources d'attaque et ajoutées à la liste noire pour éviter toute connexion pendant un certain temps.

Afficher les journaux : ouvre le fichier journal de la protection du réseau.

Connexions réseau

Affiche les réseaux auxquels les cartes réseaux sont connectés. Pour afficher les connexions réseau, procédez comme suit : dans la fenêtre principale du programme cliquez sur **Configuration** > **Protection du réseau** > **Connexions aux réseaux**.

Double-cliquez sur une connexion dans la liste pour afficher ses détails et les détails de la carte réseau.

Passez la souris sur une connexion réseau spécifique et cliquez sur l'icône de menu ⋮ dans la colonne **Approuvé** pour choisir l'une des options suivantes :

- **Modifier** : ouvre la fenêtre Configurer la protection du réseau dans laquelle vous pouvez attribuer un

profil de protection du réseau à un réseau spécifique

- **Oublier** : réinitialise la configuration par défaut de la connexion réseau

- **Analyser le réseau avec Inspecteur de réseau** – Cette option permet d'ouvrir Inspecteur de réseau afin d'exécuter une analyse de réseau

- **Marquer comme « Mon réseau »** : ajoute l'étiquette « Mon réseau » au réseau auquel vous êtes connecté. Cette étiquette sera affichée à côté du réseau partout dans ESET Internet Security afin de permettre une meilleure identification des réseaux et une vue d'ensemble de la sécurité

- **Annuler le marquage en tant que « Mon réseau » :** supprime l'étiquette « Mon réseau »; uniquement disponible si le réseau est déjà étiqueté

Détails de la connexion réseau

Double-cliquez sur une connexion dans la liste des connexions réseau pour afficher ses détails ainsi que les détails de la carte réseau. Les détails de la connexion réseau et de la carte réseau peuvent vous aider à identifier le réseau que vous essayez de configurer dans Protection de l'accès au réseau.

Détails de la connexion réseau:

- État de la connexion au réseau
- Date et heure de la première détection du réseau
- Dernière fois que le réseau a été actif
- Durée totale de connexion à ce réseau
- Profil de connexion réseau
- Profil de connexion réseau défini dans Windows
- Configuration de la protection du réseau (si le réseau de confiance)

Détails de la carte réseau :

- Type de connexion (câblée, virtuelle, etc.)
- Nom de la carte réseau
- Description de l'adaptateur
- Adresse IP avec adresse MAC
- L'adresse IPv4 et IPv6 du réseau avec le sous-réseau
- Suffixe DNS
- IP du serveur DNS
- IP du serveur DHCP

- Adresse IP et MAC de passerelle par défaut
- Adresse MAC de la carte

Dépannage de l’accès au réseau

L'assistant de dépannage vous aide à résoudre les problèmes de connectivité causés par le pare-feu. Pour accéder à l’option **Dépannage de l'accès au réseau**, ouvrez la fenêtre principale du programme, puis cliquez sur **Configuration** > **Protection du réseau** > **Résoudre les problèmes de communication**.

Sélectionnez cette option si vous souhaitez afficher les communications bloquées pour les **applications locales** ou les communications bloquées pour les **périphériques distants**.

À partir du menu déroulant, sélectionnez une période pendant laquelle la communication a été bloquée. Une liste des communications récemment bloquées vous donne un aperçu au sujet du type d'application ou de périphérique, de la réputation et du nombre total d'application et de périphériques bloqués pendant cette période. Pour en savoir plus sur les communications bloquées, cliquez sur **Détails**. La prochaine étape consiste à débloquer l'application ou le périphérique avec lequel vous éprouvez des problèmes de connectivité.

Lorsque vous cliquez sur **Débloquer**, la communication qui a été bloquée précédemment sera maintenant autorisée. Si vous continuez à rencontrer des problèmes avec une application, ou si votre périphérique ne fonctionne pas comme prévu, cliquez sur **Créer une autre règle** et toutes les communications qui ont été bloquées précédemment pour ce périphérique seront désormais autorisées. Si le problème persiste, redémarrez l'ordinateur.

Cliquez sur **Ouvrir les règles de pare-feu** pour afficher les règles créées par l’assistant. De plus, vous pouvez afficher les règles créées par l'assistant dans Configuration avancée > **Protections** > **Protection de l'accès au réseau** > **Pare-feu** > **Règles** > **Modifier**.

Si la règle ne peut pas être créée, vous recevrez un message d’erreur. Cliquez sur **Réessayer** et répétez le processus pour débloquer la communication ou créer une autre règle dans la liste des communications bloquées.

Adresse IP ajoutées temporairement à la liste noire

Pour afficher les adresses IP ayant été détectées comme des sources d'attaque et ajoutées à la liste noire pour éviter toute connexion pendant un certain temps, procédez comme suit : dans la fenêtre principale du programme, cliquez sur **Configuration** > **Protection du réseau** > **Résoudre les adresses IP temporairement bloquées**. Les adresses IP bloquées temporairement sont bloquées pendant 1 heure.

Colonnes

Adresse IP - une adresse IP ayant été bloquée.

Raison du blocage - montre le type d'attaque bloquée à partir de l'adresse (par exemple, une attaque de balayage des ports TCP).

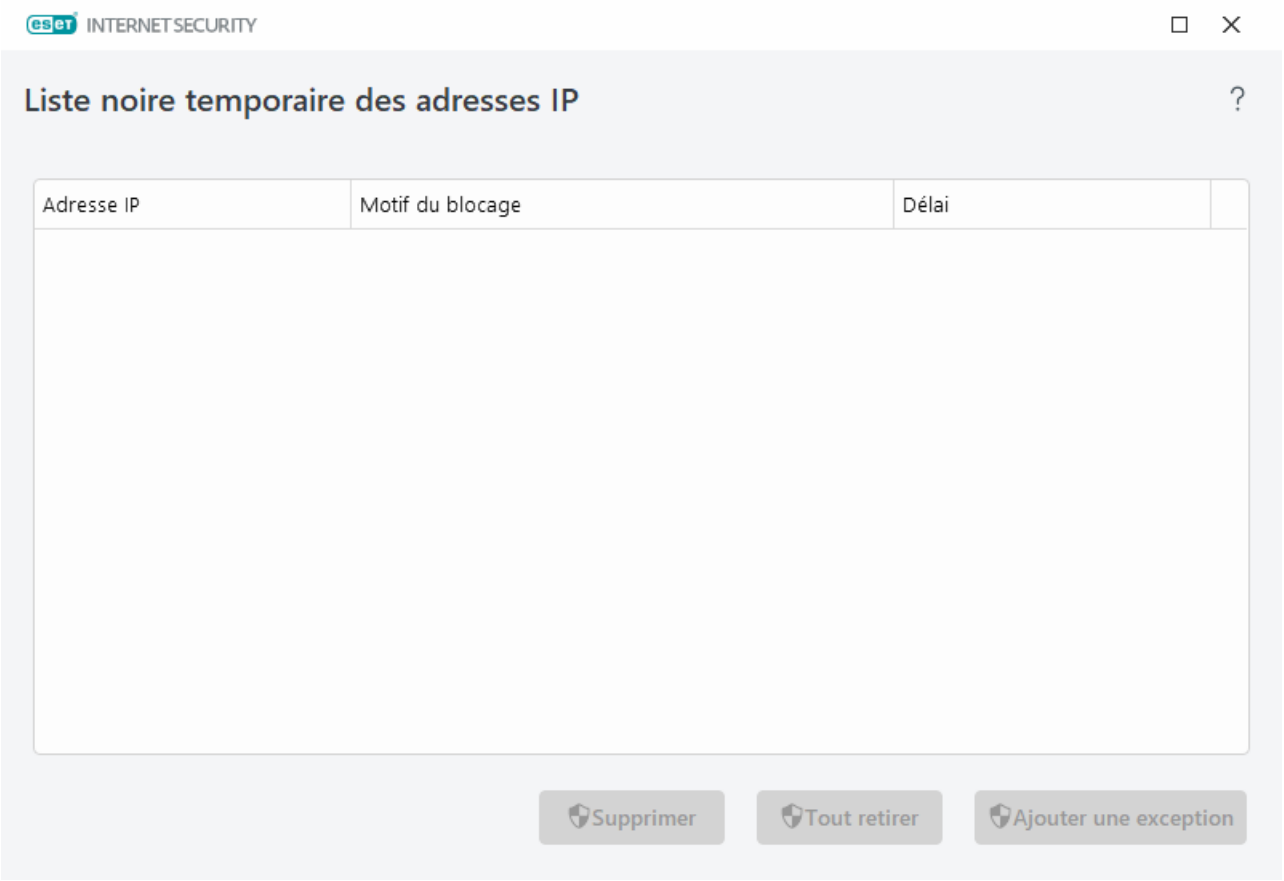
Délai - indique l'heure et la date où l'adresse expirera de la liste noire.

Éléments de contrôle

Supprimer - cliquez pour supprimer une adresse de la liste noire avant qu'elle n'expire.

Supprimer tout - cliquez pour retirer immédiatement toutes les adresses de la liste noire.

Ajouter une exception - cliquez pour ajouter une exception au pare-feu dans le filtrage IDS.



Journaux de protection du réseau

La protection du réseau de ESET Internet Security enregistre tous les événements importants dans un fichier journal. Pour afficher le fichier journal, ouvrez la fenêtre principale du programme > **Configuration** > **Protection du réseau** > **Afficher les journaux**.

Les fichiers journaux peuvent être utilisés pour détecter des erreurs et révéler les intrusions dans le système. Le journal de protection du réseau contient les données suivantes :

- Date et heure de l'événement
- le nom de l'événement
- Source
- l'adresse réseau cible
- le protocole de communication réseau

- La règle appliquée ou le nom du ver, s'il est identifié
- Chemin d’accès et nom de l’application
- Hachage
- Utilisateur
- Signataire de l’application (éditeur)
- Nom du progiciel
- Nom du service

Une analyse approfondie de ces données peut permettre de détecter les tentatives qui risquent de compromettre la sécurité du système. Beaucoup d'autres facteurs peuvent vous informer des risques potentiels de sécurité et vous aider à minimiser leur effet : trop de connexions en provenance de sites inconnus, plusieurs tentatives d'établissement de connexions, des communications issues d'applications inconnues ou l'utilisation de numéros de ports inhabituels.

> **Exploitation d’une vulnérabilité de sécurité**
> Le message de la vulnérabilité de sécurité est consigné même si la vulnérabilité en question est déjà corrigée, car la tentative d'intrusion est détectée et bloquée au niveau du réseau avant que l'intrusion en elle même ne puisse avoir lieu.

Résolution de problèmes de pare-feu

Si vous rencontrez des problèmes de connectivité alors que ESET Internet Security est installé, il y a plusieurs façons de déterminer si le pare-feu est l'origine du problème. En outre, le pare-feu peut vous aider à créer de nouvelles règles ou exceptions pour résoudre les problèmes de connectivité.

Consultez les rubriques suivantes pour de l'aide sur la résolution des problèmes avec le pare-feu :

- Dépannage de l’accès au réseau
- Journalisation et création de règles ou d'exceptions à partir du journal
- Création d'exceptions à partir des notifications du pare-feu
- Journalisation avancée de la protection du réseau
- Résolution des problèmes avec l’analyseur de trafic réseau

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

Par défaut, le pare-feu d'ESET ne consigne pas au journal toutes les connexions bloquées. Si vous voulez voir ce qui a été bloqué par la protection du réseau, ouvrez Configuration avancée > **Outils** > **Diagnostics** > **Journalisation avancée** et activez l’option **Activer la journalisation avancée de la protection du réseau**. Si vous voyez quelque

chose dans le journal que vous ne voulez pas que le pare-feu bloque, vous pouvez créer une règle ou une règle IDS en faisant un clic droit sur cet élément et en sélectionnant **Ne pas bloquer des événements semblables à l'avenir**. Veuillez noter que le journal de toutes les connexions bloquées peut contenir des milliers d'éléments et qu'il peut être difficile de trouver une connexion en particulier dans ce journal. Vous pouvez désactiver la journalisation une fois le problème résolu.

Pour de plus amples renseignements sur le journal, voir Fichiers journaux.

> Utilisez la journalisation pour voir l'ordre dans lequel le Protection du réseau bloque des connexions spécifiques. En outre, la création de règles à partir du journal vous permet de créer des règles qui font exactement ce que vous voulez.

Créer une règle à partir du journal

La nouvelle version de ESET Internet Security permet de créer des règles à partir du journal. À partir du menu principal, cliquez sur **Outils** > **Fichiers journaux**. Choisissez **Protection du réseau** dans le menu déroulant, cliquez du droit sur l'entrée de journal désirée et sélectionnez **Ne pas bloquer les événements semblables à l'avenir** dans le menu contextuel. Une fenêtre de notification affiche votre nouvelle règle.

Pour permettre la création de nouvelles règles à partir du journal, ESET Internet Security doit être configuré avec les paramètres suivants :

1. Mettez la verbosité minimale à **Diagnostic** dans Configuration avancée > **Outils** > **Fichiers journaux**.

2. Activer **Avertir en cas de détection d'une attaque sur des failles de sécurité** dans Configuration avancée > **Protections** > **Protection de l'accès au réseau** > **Protection contre les attaques réseau** > **Options avancées** > **Détection des intrusions**.

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

Lorsque le pare-feu d'ESET détecte une activité malveillante sur le réseau, une fenêtre de notification décrivant l'événement s'affiche. Cette notification contient un lien qui vous permettra d'en apprendre plus sur l'événement et de créer une règle pour cet événement si vous le voulez.

> Si une application ou un périphérique réseau n'applique pas correctement les normes du réseau, cela peut déclencher des notifications IDS de pare-feu répétitives. Vous pouvez créer une exception directement à partir de la notification afin d'empêcher le pare-feu d'ESET de détecter cette application ou ce périphérique.

Journalisation avancée de la protection du réseau

Cette fonctionnalité est destinée à fournir des fichiers journaux plus complexes pour le soutien technique d'ESET. Utilisez cette fonctionnalité uniquement si le soutien technique d'ESET vous le demande, car il peut générer un fichier journal volumineux et ralentir votre ordinateur.

1. Ouvrez Configuration avancée > **Outils** > **Diagnostics** > **Journalisation avancée** et activez l'option **Activer la**

journalisation avancée de la protection du réseau.

2. Essayez de reproduire le problème que vous rencontrez.

3. Désactivez la journalisation avancée de la protection du réseau.

4. Le fichier journal du PCAP créé par la journalisation avancée de la protection du réseau se trouve dans le même répertoire où sont générées les vidages de mémoire de diagnostic : *C:\ProgramData\ESET\ESET Security\Diagnostics*

Résolution des problèmes avec l'analyseur de trafic réseau

Si vous rencontrez des problèmes avec votre navigateur ou votre client de courriel, commencez par déterminer si l'analyseur de trafic réseau en est responsable. Pour ce faire, essayez de désactiver temporairement le filtrage des protocoles d'application dans Configuration avancée > **Moteur de détection** > **Analyseur du trafic réseau** (n'oubliez pas de le réactiver une fois que vous aurez terminé, sinon votre navigateur et votre client de messagerie ne seront pas non protégés). Si votre problème disparaît après cette désactivation, voici une liste des problèmes communs et un moyen de les résoudre :

Problèmes de mise à jour ou de communications sécurisées

Si votre application signale qu'elle ne peut pas effectuer de mise à jour ou qu'un canal de communication n'est pas sécurisé :

- Si SSL/TLS est activé, essayez de le désactiver temporairement. Si cette action règle le problème, vous pouvez continuer à utiliser SSL et effectuer la mise à jour en excluant la communication problématique : Désactiver SSL/TLS. Exécutez à nouveau la mise à jour. Une boîte de dialogue devrait vous informer sur le trafic réseau chiffré. Assurez-vous que l'application correspond à celle que vous êtes en train de dépanner et que le certificat semble provenir du serveur à partir duquel la mise à jour est effectuée. Ensuite, choisissez de mémoriser l'action de ce certificat et cliquez sur ignorer. Si aucune autre boîte de dialogue pertinente ne s'affiche, vous pouvez changer le mode de filtrage et revenir à automatique et le problème devrait être résolu.

- Si l'application en question n'est pas un navigateur ni un client de messagerie, vous pouvez complètement l'exclure de la protection de l'accès Web (le faire pour un navigateur ou un client de messagerie vous exposerait). Toute application dont les communications étaient déjà filtrées devrait être dans la liste qui vous est fournie lors de l'ajout de l'exception ; un ajout manuel ne devrait donc pas être nécessaire.

Problème d'accès à un périphérique sur votre réseau

Si vous ne parvenez pas à utiliser une fonctionnalité d'un périphérique sur votre réseau (il peut s'agir de l'ouverture d'une page Web de votre webcam ou de la lecture vidéo sur un lecteur multimédia de maison), essayez d'ajouter ses adresses IPv4 et IPv6 à la liste des adresses exclues.

Problèmes avec un site Web en particulier

Vous pouvez exclure des sites Web précis de la protection de l'accès Web en utilisant la gestion d'adresse URL. Par exemple, si vous ne parvenez pas à accéder à la page https://www.gmail.com/intl/en/mail/help/about.html, essayez d'ajouter *gmail.com* à la liste des adresses exclues.

Erreur « Certaines des applications capables d'importer le certificat racine s'exécutent encore »

Lorsque vous activez SSL/TLS, ESET Internet Security veille à ce que les applications installées fassent confiance à sa façon de filtrer le protocole SSL en important un certificat dans leurs magasins de certificats. Pour importer un certificat, certaines applications doivent être redémarrées. Ces applications incluent Firefox et Opera. Assurez-vous qu'aucune d'entre elles n'est en cours d'exécution (la meilleure façon de le faire est d'ouvrir le Gestionnaire des tâches et de s'assurer qu'il n'y a pas de firefox.exe ou d'opera.exe sous l'onglet Processus), puis essayez de nouveau.

Erreur sur un émetteur non fiable ou une signature non valide

Cela signifie probablement que l'importation décrite ci-dessus a échoué. D'abord, assurez-vous qu'aucune des applications mentionnées n'est en cours d'exécution. Ensuite, désactivez SSL/TLS et réactivez-le. L'importation s'exécute alors de nouveau.

> Consultez l'article de la base de connaissances pour savoir Comment gérer l’analyseur du trafic réseau dans le produit ESET Windows pour les particuliers.

Menace réseau bloquée

Cette situation peut se produire lorsqu'une application sur votre ordinateur tente de transmettre un trafic malveillant à un autre périphérique sur le réseau, d'exploiter une faille de sécurité, ou même si une tentative d'analyse des ports est détectée sur votre système.

Vous pouvez trouver le type de menace et l’adresse IP du périphérique associée dans la notification. Cliquez sur **Modifier la gestion de cette menace** pour afficher les options suivantes :

Continuer de bloquer - Bloque la menace détectée. Si vous souhaitez ne plus recevoir de notifications concernant ce type de menace provenant de l'adresse distante en question, sélectionnez le bouton radio situé à côté de **Ne pas notifier** avant de cliquer sur **Continuer le blocage**. Cela créera une règle de service de détection d’intrusion (IDS) avec la configuration suivante : **Bloquer** - par défaut, **Notifier** - non, **Journal** - non.

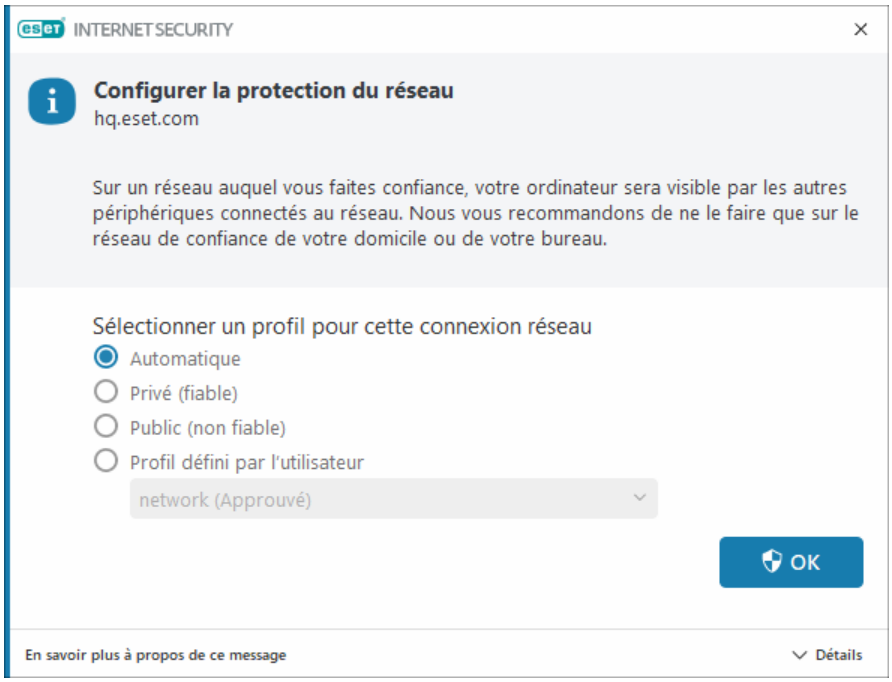
Autoriser : crée une règle de service de détection d’intrusion (IDS) pour autoriser la menace détectée. Sélectionnez-en une parmi les options suivantes avant de cliquer sur **Autoriser** pour spécifier les paramètres de règle :

- **Notifier seulement lorsque cette menace est bloquée :** configuration de la règle : **Bloquer** - non, **Notifier** - non, **Enregistrer** - non.
- **Notifier dès que cette menace survient :** configuration de la règle : **Bloquer** - non, **Notifier** - par défaut, **Journal** - par défaut.
- **Ne pas notifier :** configuration de règle : **Bloquer** - non, **Notifier** - non, **Enregistrer** - non.

Les informations affichées dans la fenêtre de notification peuvent varier selon le type de menace détectée. Pour plus de renseignements au sujet des menaces et d'autres termes associés, consultez les rubriques Types d'attaques à distance ou Types de détection.
Pour résoudre l'événement **Adresses IP en double sur le réseau** , consultez notre article de la base de connaissances d'ESET.

Nouveau réseau détecté

Par défaut, ESET Internet Security utilise les paramètres de Windows lorsqu'une nouvelle connexion réseau est détectée. Pour afficher une fenêtre de dialogue lorsqu'un nouveau réseau est détecté, définissez l'affectation du profil de protection du réseau sur **Demander**. La configuration de la protection du réseau s'affichera chaque fois que votre ordinateur se connectera à un nouveau réseau.



Vous pouvez choisir parmi les profils de connexion réseau suivants :

Automatique : ESET Internet Security sélectionnera le profil automatiquement, en fonction des activateurs configurés pour chaque profil.

Privé : pour les réseaux fiables (réseaux domestiques ou professionnels). Votre ordinateur et les fichiers partagés stockés sur votre ordinateur sont visibles par les autres utilisateurs du réseau et les ressources système sont accessibles aux autres utilisateurs du réseau (l'accès aux fichiers et aux imprimantes partagés est activé, la communication RPC entrante est activée et le partage de bureau à distance est disponible). Nous vous recommandons d'utiliser ce paramètre lors de l'accès à un réseau local sécurisé. Ce profil est automatiquement affecté à une connexion réseau si elle est configurée en tant que domaine ou réseau privé dans Windows.

Public : pour les réseaux non fiables (réseaux publics). Les fichiers et les dossiers de votre système ne sont pas partagés ni visibles par d'autres utilisateurs du réseau et le partage des ressources système est désactivé. Nous vous recommandons d'utiliser ce paramètre lors de l'accès aux réseaux sans fil. Ce profil est automatiquement affecté à toute connexion réseau qui n'est pas configurée en tant que domaine ou réseau privé dans Windows.

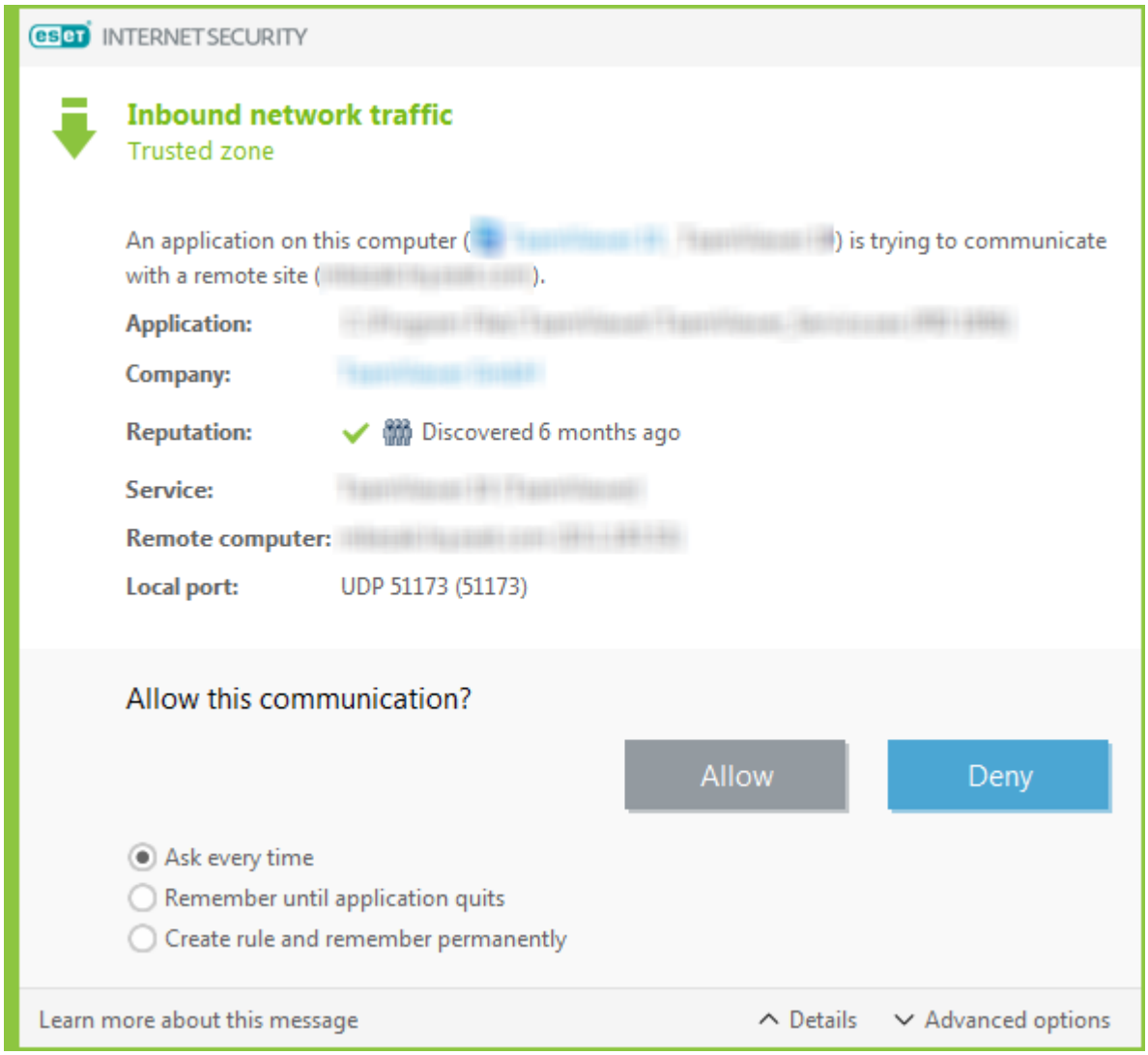
Profil défini par l'utilisateur : vous pouvez sélectionner l'un des profils que vous avez créés dans le menu déroulant. Cette option n'est disponible que si vous avez créé au moins un profil personnalisé.

⚠ Une configuration incorrecte du réseau peut poser un risque pour la sécurité de votre ordinateur.

Établissement d'une connexion - détection

Le pare-feu détecte toute nouvelle connexion au réseau. Le mode Pare-feu actif détermine les actions à exécuter pour la nouvelle règle. Si le **Mode automatique** ou le **Mode basé sur des règles personnalisées** est activé, le pare-feu 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, ainsi que des détails sur la connexion. Vous pouvez choisir d'**autoriser** ou de **refuser** (bloquer) la connexion. 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 **Créer la règle et mémoriser de manière permanente** et sauvegardez l'action comme une nouvelle règle pour le pare-feu. Si le pare-feu personnel reconnaît la même connexion plus tard, il appliquera la règle existante, sans interaction de l'utilisateur.



Lors de la création de nouvelles règles veillez à n'autoriser que les connexions que vous savez sécurisées. Si toutes les connexions sont autorisées, le pare-feu n'a pas atteint son objectif. Voici les paramètres importants pour les connexions :

Application – Emplacement du fichier exécutable et ID de processus. N'autorisez pas les connexions pour des applications et des processus inconnus.

Signataire : nom de l’éditeur de l’application. Cliquez sur le texte pour afficher un certificat de sécurité pour l’entreprise.

Réputation – Niveau de risque de la connexion. Un niveau de risque est attribué aux connexions : Fin (vert), Inconnu (orange) ou Risqué (rouge), à l’aide d’une série de règles heuristiques qui examinent les caractéristiques de chaque connexion, le nombre d’utilisateurs et le temps de découverte. Cette information est colligée par la technologie ESET LiveGrid®.

Service – Nom du service, si l’application est un service Windows.

Ordinateur distant – Adresse du périphérique distant. N'autorisez que les connexions aux adresses fiables et connues.

Port distant – Port de communication. Les communications utilisant les ports communs (par ex. le port Web numéro 80.443) peuvent être autorisées dans les circonstances normales.

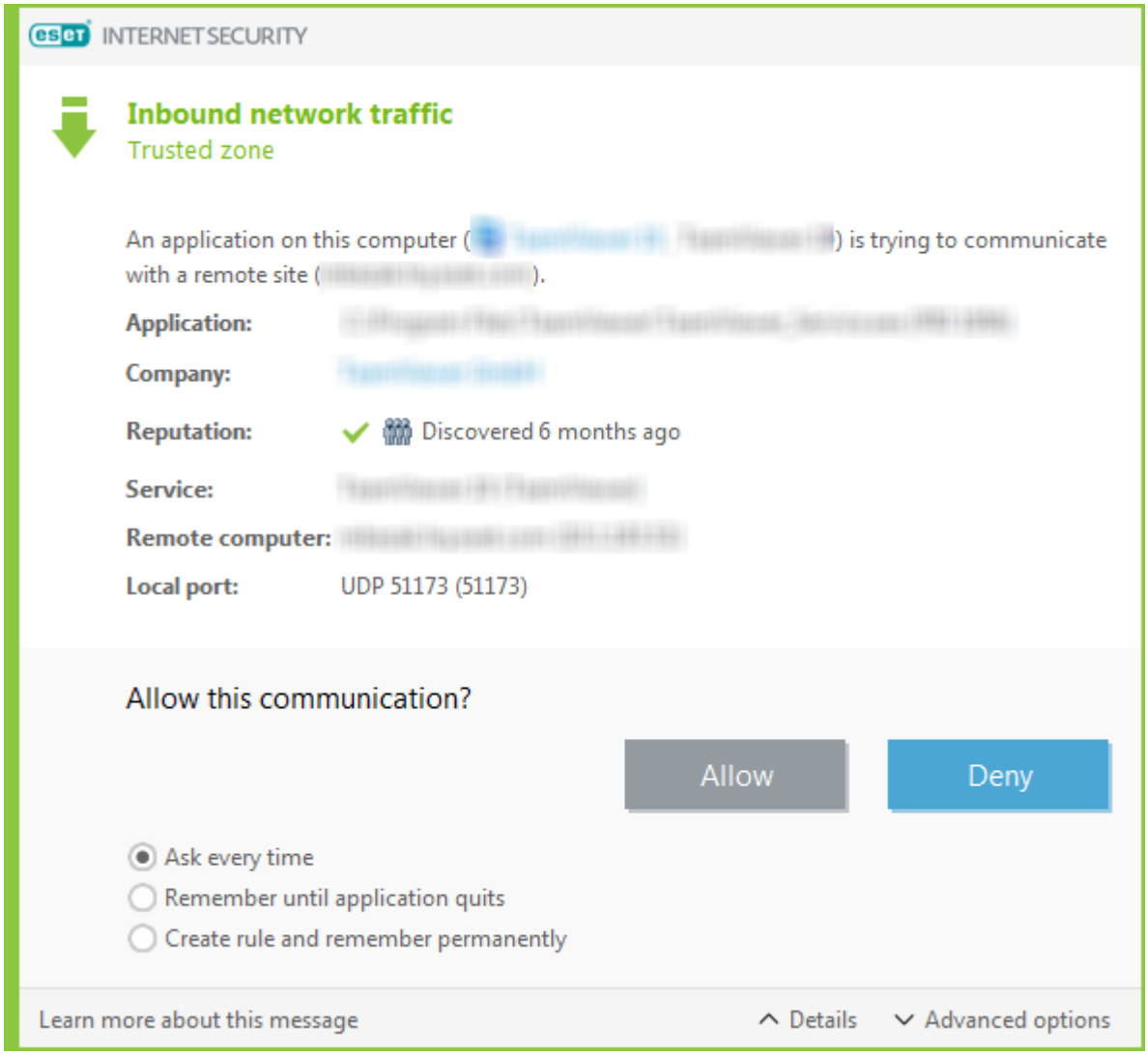
Les infiltrations aux ordinateurs utilisent souvent des connexions masquées et Internet pour infecter les systèmes distants. Si les règles sont correctement configurées, le pare-feu devient un important outil de protection contre les attaques répétées de divers codes malveillants.

Changement d'application

Le pare-feu a détecté une modification dans une application utilisée pour établir des connexions sortantes depuis votre ordinateur. Il se peut que l'application ait simplement été mise à jour. Mais une modification peut aussi être due à une application malveillante. Si vous n'êtes pas au courant qu'une modification légitime ait pu avoir lieu, nous recommandons de refuser la connexion et d'analyser votre ordinateur avec la base des signatures de virus la plus récente.

Communication fiable entrante

Exemple de connexion entrante dans la zone fiable :
Un ordinateur distant dans la zone fiable tente d'établir une communication avec une application locale fonctionnant sur votre ordinateur.



Application - Application contactée par un périphérique distant.

Chemin d'accès à l'application : emplacement de l'application.

Application du Microsoft Store : nom de l'application dans Microsoft Store.

Signataire : nom de l'éditeur de l'application. Cliquez sur le texte pour afficher un certificat de sécurité pour l'entreprise.

Réputation - Réputation de l'application obtenue par la technologie ESET LiveGrid®.

Service - Nom du service en cours d'exécution sur votre ordinateur.

Ordinateur distant - Ordinateur distant qui tente d'établir une communication avec l'application sur votre ordinateur.

Port distant - Port utilisé pour la communication.

Demander à chaque fois - Si l'action par défaut pour une règle est mise à **Demander**, une boîte de dialogue s'affichera chaque fois que la règle est déclenchée.

Mémoriser jusqu'à la fermeture de l'application - ESET Internet Security se souviendra de l'action choisie jusqu'au prochain redémarrage.

Créer la règle et mémoriser de manière permanente - Si vous sélectionnez cette option avant d'autoriser ou de refuser une communication, ESET Internet Security se souviendra de l'action et l'utilisera si l'application est contactée à nouveau par l'ordinateur distant.

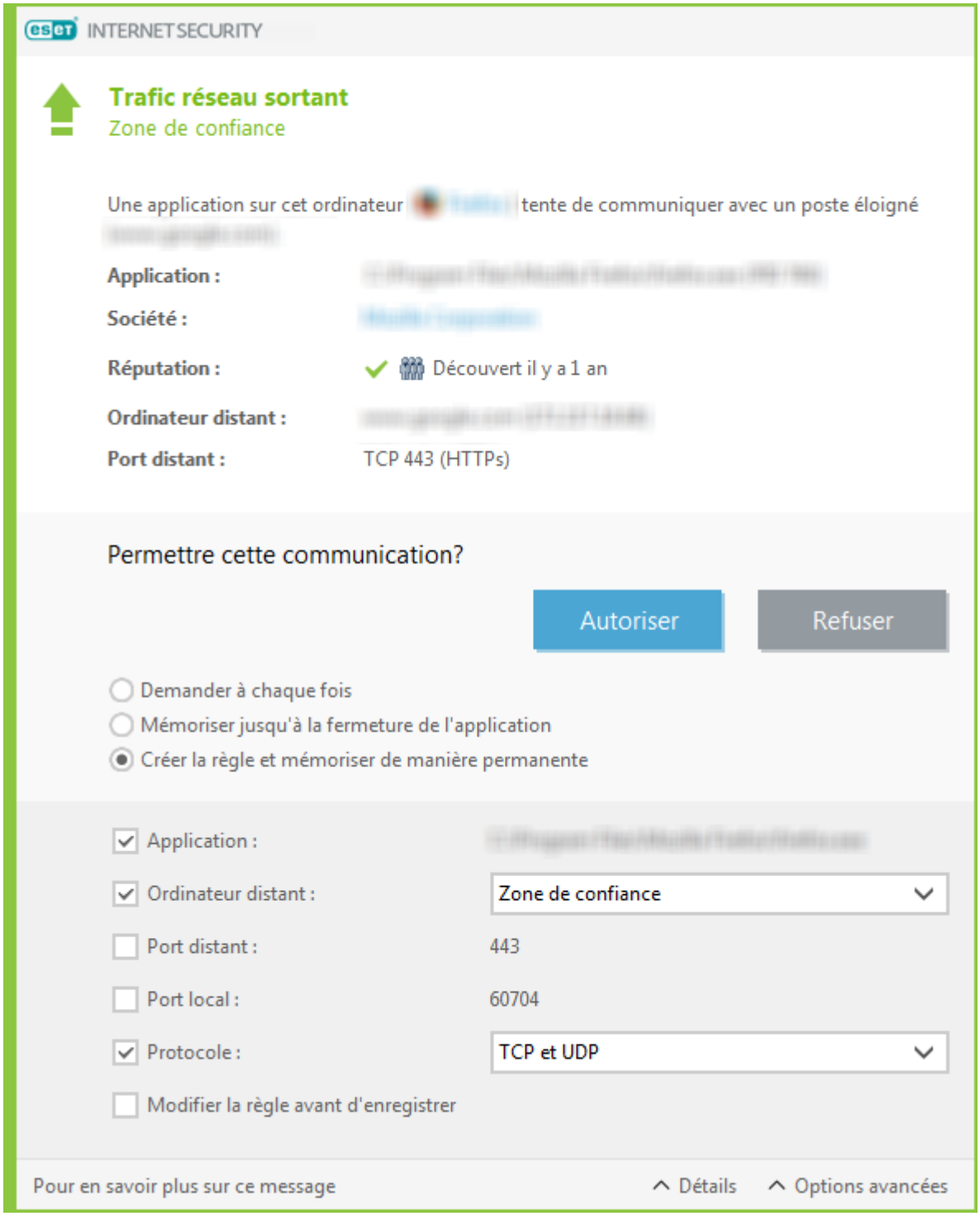
Autoriser - Autorise la communication entrante.

Refuser - Refuse la communication entrante.

Modifier la règle : vous permet de personnaliser les propriétés de règle à l'aide de l'Éditeur des règles de pare-feu.

Communication sortante fiable

Exemple de connexion sortante dans 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.



Application - Application contactée par un périphérique distant.

Chemin d'accès à l'application : emplacement de l'application.

Application du Microsoft Store : nom de l'application dans Microsoft Store.

Signataire : nom de l'éditeur de l'application. Cliquez sur le texte pour afficher un certificat de sécurité pour l'entreprise.

Réputation - Réputation de l'application obtenue par la technologie ESET LiveGrid®.

Service - Nom du service en cours d'exécution sur votre ordinateur.

Ordinateur distant - Ordinateur distant qui tente d'établir une communication avec l'application sur votre ordinateur.

Port distant - Port utilisé pour la communication.

Demander à chaque fois - Si l'action par défaut pour une règle est mise à **Demander**, une boîte de dialogue s'affichera chaque fois que la règle est déclenchée.

Mémoriser jusqu'à la fermeture de l'application - ESET Internet Security se souviendra de l'action choisie jusqu'au prochain redémarrage.

Créer la règle et mémoriser de manière permanente - Si vous sélectionnez cette option avant d'autoriser ou de refuser une communication, ESET Internet Security se souviendra de l'action et l'utilisera si l'application est contactée à nouveau par l'ordinateur distant.

Autoriser - Autorise la communication entrante.

Refuser - Refuse la communication entrante.

Modifier la règle : vous permet de personnaliser les propriétés de règle à l'aide de l'Éditeur des règles de pare-feu.

Communication entrante

Exemple de connexion Internet entrante :
Un ordinateur distant tente de communiquer avec une application fonctionnant sur cet ordinateur.

Application - Application contactée par un périphérique distant.

Chemin d'accès à l'application : emplacement de l'application.

Application du Microsoft Store : nom de l'application dans Microsoft Store.

Signataire : nom de l'éditeur de l'application. Cliquez sur le texte pour afficher un certificat de sécurité pour l'entreprise.

Réputation - Réputation de l'application obtenue par la technologie ESET LiveGrid®.

Service - Nom du service en cours d'exécution sur votre ordinateur.

Ordinateur distant - Ordinateur distant qui tente d'établir une communication avec l'application sur votre ordinateur.

Port distant - Port utilisé pour la communication.

Demander à chaque fois - Si l'action par défaut pour une règle est mise à **Demander**, une boîte de dialogue s'affichera chaque fois que la règle est déclenchée.

Mémoriser jusqu'à la fermeture de l'application - ESET Internet Security se souviendra de l'action choisie jusqu'au prochain redémarrage.

Créer la règle et mémoriser de manière permanente - Si vous sélectionnez cette option avant d'autoriser ou de

refuser une communication, ESET Internet Security se souviendra de l'action et l'utilisera si l'application est contactée à nouveau par l'ordinateur distant.

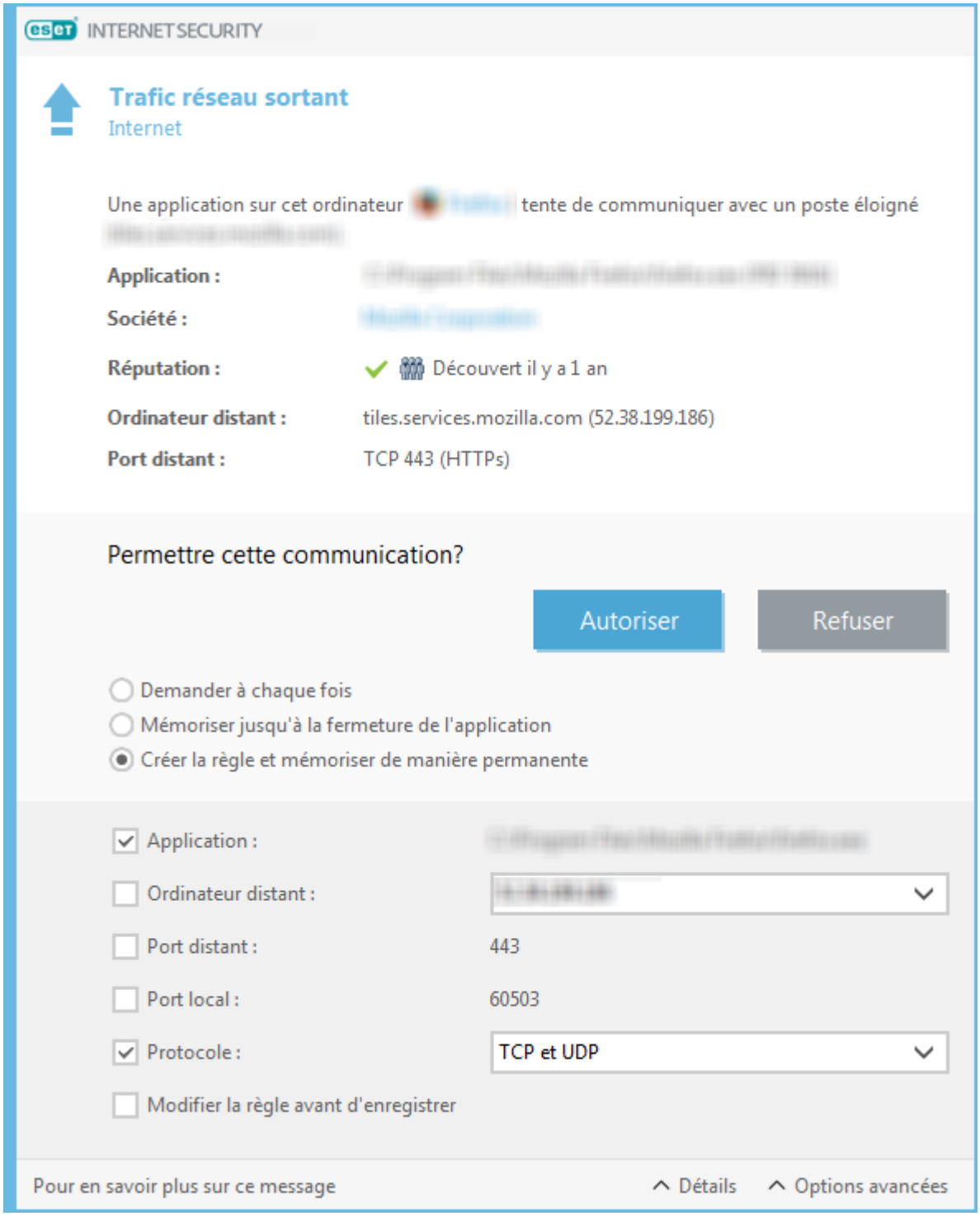
Autoriser - Autorise la communication entrante.

Refuser - Refuse la communication entrante.

Modifier la règle : vous permet de personnaliser les propriétés de règle à l'aide de l'Éditeur des règles de pare-feu.

Communication sortante

Exemple de connexion Internet sortante :
Une application locale tente d'établir une connexion Internet.



Application - Application contactée par un périphérique distant.

Chemin d'accès à l'application : emplacement de l'application.

Application du Microsoft Store : nom de l'application dans Microsoft Store.

Signataire : nom de l'éditeur de l'application. Cliquez sur le texte pour afficher un certificat de sécurité pour l'entreprise.

Réputation - Réputation de l'application obtenue par la technologie ESET LiveGrid®.

Service - Nom du service en cours d'exécution sur votre ordinateur.

Ordinateur distant - Ordinateur distant qui tente d'établir une communication avec l'application sur votre ordinateur.

Port distant - Port utilisé pour la communication.

Demander à chaque fois - Si l'action par défaut pour une règle est mise à **Demander**, une boîte de dialogue s'affichera chaque fois que la règle est déclenchée.

Mémoriser jusqu'à la fermeture de l'application - ESET Internet Security se souviendra de l'action choisie jusqu'au prochain redémarrage.

Créer la règle et mémoriser de manière permanente - Si vous sélectionnez cette option avant d'autoriser ou de refuser une communication, ESET Internet Security se souviendra de l'action et l'utilisera si l'application est contactée à nouveau par l'ordinateur distant.

Autoriser - Autorise la communication entrante.

Refuser - Refuse la communication entrante.

Modifier la règle : vous permet de personnaliser les propriétés de règle à l'aide de l'Éditeur des règles de pare-feu.

Configuration de l'affichage des connexions

Cliquez à droite sur une connexion pour voir des options supplémentaires, y compris :

Résoudre les noms d'hôtes - Si possible, toutes les adresses réseau sont affichées dans le format DNS plutôt que dans le format d'adresse IP numérique.

Afficher uniquement les connexions avec le protocole TCP - Cette liste affiche uniquement les connexions appartenant à la suite de protocoles TCP.

Afficher les connexions à l'écoute - Cette option permet d'afficher seulement les connexions sans communication actuellement établie, mais pour lesquelles le système a ouvert un port et est en attente de connexion.

Afficher les connexions à l'intérieur de l'ordinateur - Cette option permet de n'afficher que les connexions où le côté distant est un système local, aussi appelées connexions localhost.

Vitesse de rafraîchissement - Sélectionner la fréquence de rafraîchissement des connexions actives.

Rafraîchir maintenant - Recharge la fenêtre des **connexions réseau**.

Outils de sécurité

Ouvrez la fenêtre principale du programme, puis cliquez sur **Configuration** > **Outils de sécurité** pour régler les modules suivants :

Opérations bancaires et navigation sécurisées – Ajoute une couche supplémentaire de protection du navigateur conçue pour protéger vos données financières lors des transactions en ligne. Activez **Sécuriser tous les navigateurs** dans configuration avancée Opérations bancaires et navigation sécurisées pour lancer tous les

navigateurs pris en charge en mode sécurisé.

Sécurité et confidentialité du navigateur – Préserve la confidatialité et la sécurité de vos activités en ligne sans laisser d'empreinte numérique.

Anti-Theft – Activez Antivol pour protéger votre ordinateur en cas de perte ou de vol.

Opérations bancaires et navigation sécurisées

L'Opérations bancaires et navigation sécurisées représente un niveau de protection supplémentaire conçue pour la protection de vos données financières lors des transactions effectuées en ligne.

Par défaut, tous les navigateurs Web pris en charge démarrent en mode sécurisé. Cela vous permet de naviguer sur l'internet, d'accéder aux services bancaires en ligne et d'effectuer des achats et des transactions en ligne automatiquement dans une fenêtre de navigateur sécurisée.

Le système de réputation de ESET LiveGrid® doit être activé (activé par défaut) pour garantir le bon fonctionnement de Opérations bancaires et navigation sécurisées.

Pour configurer le comportement du navigateur sécurisé, voir configuration avancée Opérations bancaires et navigation sécurisées. Si vous désactivez **Sécuriser tous les navigateurs**, vous pouvez accéder au navigateur sécurisé dans la fenêtre principale du programme > **Vue d'ensemble** > **Opérations bancaires et navigation sécurisées** ou en cliquant sur l'icône de bureau **Opérations bancaires et navigation sécurisées**. Le navigateur, défini par défaut dans Windows, se lance en mode sécurisé.

L'utilisation de la communication chiffrée HTTPS est nécessaire pour effectuer une navigation protégée. Les navigateurs suivants prennent en charge Opérations bancaires et navigation sécurisées :

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

Seuls Firefox et Microsoft Edge sont pris en charge sur les périphériques équipés de processeurs ARM.

Pour plus d'informations sur les fonctionnalités de Opérations bancaires et navigation sécurisées, lisez les articles suivants de la base de connaissances ESET disponibles en anglais et dans plusieurs autres langues :

- Comment puis-je utiliser Opérations bancaires et navigation sécurisées ESET?
- Suspendre ou désactiver Opérations bancaires et navigation sécurisées dans les produits ESET Windows pour particuliers
- Opérations bancaires et navigation sécurisées ESET – erreurs courantes
- Glossaire ESET | Opérations bancaires et navigation sécurisées

Notification dans le navigateur

Le navigateur sécurisé vous informe de son état actuel par le biais de notifications dans le navigateur et de la couleur du cadre du navigateur.

Les notifications dans le navigateur sont affichées dans l'onglet de droite.

Pour développer une notification dans le navigateur, cliquez sur l'icône d'ESET. Pour réduire la notification, cliquez sur le texte de la notification. Pour ignorer la notification et le cadre vert du navigateur, cliquez sur l'icône de fermeture.

Seules les notifications informatives et le cadre de navigateur vert peuvent être ignorés.

Notifications dans le navigateur

Type de la notification	État
Notification informative et cadre vert du navigateur	Une protection maximale est assurée et la notification dans le navigateur est réduite par défaut. Développez la notification dans le navigateur et cliquez sur **Paramètres** pour ouvrir la configuration des outils de sécurité.
Avertissement et cadre orange du navigateur	Le navigateur sécurisé nécessite votre attention pour un problème non critique. Pour plus d'informations sur le problème ou une solution, suivez les instructions de la notification dans le navigateur.
Alerte de sécurité et cadre rouge du navigateur	Le navigateur n'est pas protégé par Opérations bancaires et navigation sécurisées d'ESET. Redémarrez le navigateur pour vous assurer que la protection est active. Pour résoudre un conflit avec les fichiers chargés dans le navigateur, ouvrez les fichiers journaux puis **Opérations bancaires et navigation sécurisées** et assurez-vous que les fichiers marqués dans les journaux ne sont pas chargés la prochaine fois que vous démarrez le navigateur. Si le problème persiste, contactez l'assistance technique d'ESET en suivant les instructions de cet article de la base de connaissances.

Sécurité et confidentialité du navigateur

Vous pouvez activer la fonctionnalité Sécurité et confidentialité du navigateur au moyen d'une extension personnalisée disponible sur les navigateurs pris en charge (Google Chrome, Mozilla Firefox et Microsoft Edge).

Pour installer et activer l'extension :

1. Assurez-vous d'utiliser la dernière version de ESET Internet Security et de redémarrer votre ordinateur après la mise à jour.
2. Ouvrez votre navigateur.
3. L'extension est installée sur votre navigateur.
4. Activez l'extension et la page de détails du navigateur avec l'extension s'affiche.

Le menu principal de l’extension de navigateur Sécurité et confidentialité du navigateur est divisé dans les sections suivantes :

Vue d'ensemble

Recherche sécurisée

Cliquez sur l’icône de bascule  à côté de **Analyser les résultats de la recherche** pour activer la fonctionnalité et voir les résultats sur lesquels vous pouvez cliquer en toute sécurité. La recherche sécurisée évalue les adresses des liens répertoriés. Cette évaluation ne permet pas nécessairement de conclure que le site Web ne contient pas de logiciels malveillants. Notre moteur de détection détecte ensuite tout logiciel malveillant sur le site Web.

Nettoyage du navigateur

Supprimez vos données de navigation ou configurez des nettoyages réguliers. Vous pouvez ajouter les sites Web pour lesquels vous souhaitez accepter les témoins et rester connecté même après avoir nettoyé le navigateur en les **ajoutant à une liste**.

- **Nettoyage unique :** sélectionnez la plage de temps dans le menu déroulant et le type de données que vous souhaitez supprimer. Vous pouvez choisir parmi les options suivantes : toutes les données, données confidentielles et données personnalisées.

- **Nettoyage régulier :** cliquez sur l’icône de bascule  à côté de **Nettoyage régulier** pour activer la fonctionnalité. Sélectionnez la plage de temps dans le menu déroulant et le type de données que vous souhaitez supprimer régulièrement. Vous pouvez choisir parmi les options suivantes : toutes les données, données confidentielles et données personnalisées.

L’option **Données personnalisées** contient les catégories suivantes :

- Historique de navigation
- Historique des téléchargements
- Témoins et données du site Web
- Images et fichiers mis en cache
- Mots de passe et données de connexion
- Données de remplissage automatique de formulaire

Examen des paramètres du site Web

Accédez aux autorisations des sites Web et gérez-les afin de contrôler les renseignements que les sites Web peuvent utiliser.

- **Notifications :** passez en revue les sites Web pour lesquels vous souhaitez **Autoriser/Bloquer** les notifications ou si vous souhaitez que l’extension du navigateur vous le **Demande à chaque fois**.

Configuration avancée

Nettoyage du navigateur

Paramètres avancés de témoin

Ajoutez à une liste les sites Web pour lesquels vous souhaitez accepter les témoins et rester connecté même après avoir nettoyé le navigateur. Entrez l'adresse URL dans le champ de texte, et cliquez sur **Ajouter**. Vous pouvez la retirer à tout moment de la liste en cliquant sur l'icône moins  à côté du site Web spécifique.

Au bas de la page se trouve la liste des domaines suggérés actuellement ouverts dans le navigateur. Si vous ne pouvez pas voir le site Web spécifique, cliquez sur **l'actualisation de la liste** et ajoutez-la à la liste des témoins acceptés en cliquant sur l'icône plus  .

Examen des paramètres du site Web

Accédez aux autorisations des sites Web et gérez-les afin de contrôler les renseignements que les sites Web peuvent utiliser.

- **Notifications :** passez en revue les sites Web pour lesquels vous souhaitez **Autoriser/Bloquer** les notifications ou si vous souhaitez que l'extension du navigateur vous le **Demande à chaque fois**.

Apparence

Personnalisez la palette de couleurs de l'interface en fonction de vos préférences. Vous pouvez choisir votre thème de couleurs préféré en cliquant sur la case à cocher **Clair** ou **Sombre**.

Antivol

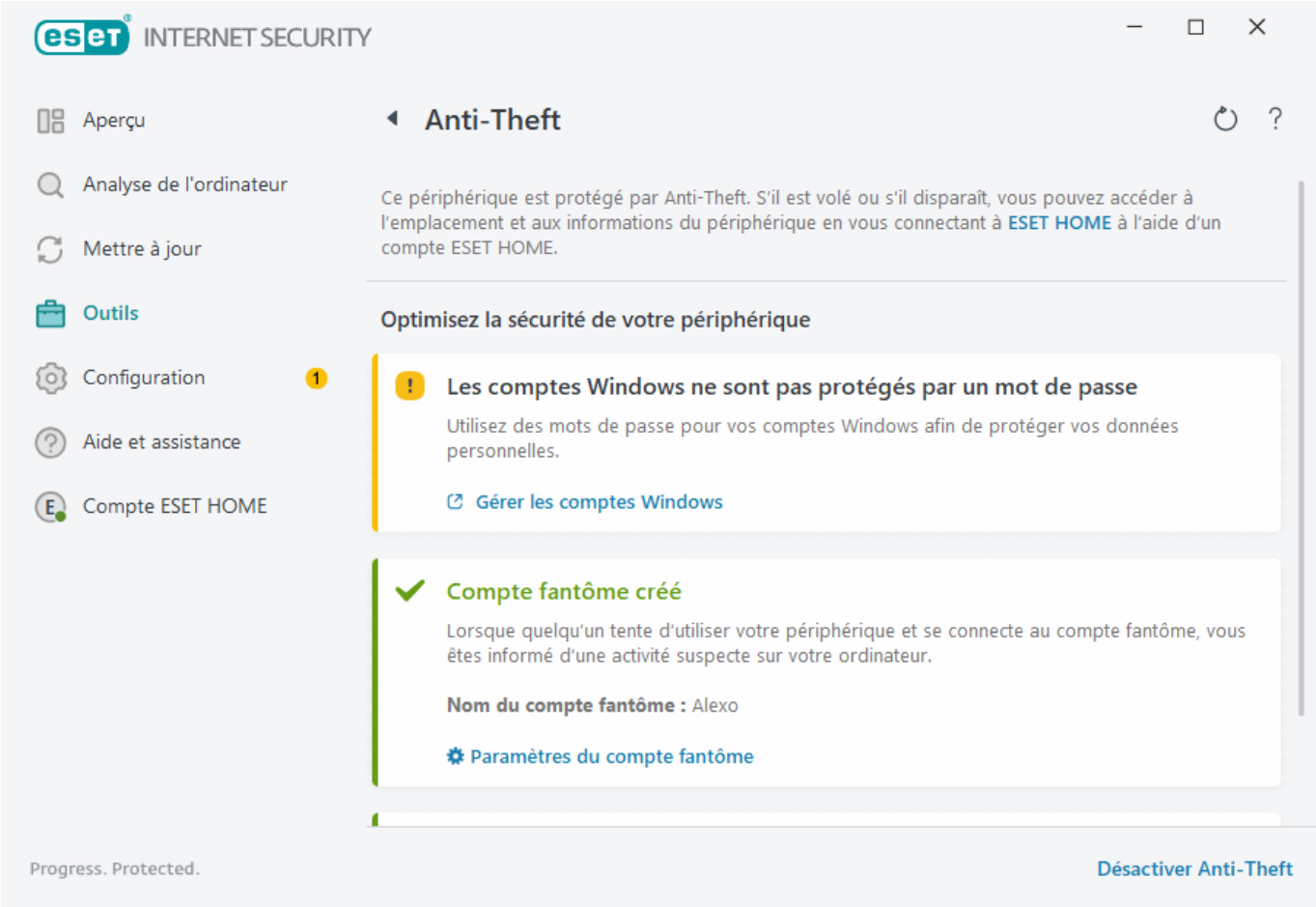
Les périphériques personnels risquent constamment d'être perdus ou volés lors de nos déplacements quotidiens entre la maison et le travail ou d'autres lieux publics. Antivol est une fonctionnalité qui étend la sécurité au niveau de l'utilisateur lorsque le périphérique est perdu ou volé. Antivol vous permet de surveiller l'utilisation du périphérique et de retrouver votre périphérique disparu grâce à la localisation par adresse IP dans ESET HOME, ce qui vous aide à retrouver votre périphérique et à protéger vos données personnelles.

L'utilisation de technologies modernes telles que la géolocalisation d'adresses IP, la capture d'images de caméra Web, la protection du compte utilisateur et la surveillance de l'appareil dans Antivol peut vous aider ou aider un organisme chargé de l'application de la loi à localiser votre ordinateur ou votre appareil en cas de perte ou de vol. Dans ESET HOME, vous pouvez voir quelle activité a lieu sur votre ordinateur ou votre périphérique.

Pour en savoir plus sur la fonctionnalité Antivol de ESET HOME, consultez l'aide en ligne de ESET HOME.

Antivol peut ne pas fonctionner correctement sur les ordinateurs appartenant à certains domaines en raison de restrictions dans la gestion des comptes d'utilisateurs.

Après avoir activé Antivol, vous pouvez optimiser la sécurité de votre périphérique dans la fenêtre principale du programme > en cliquant sur **Configuration** >**Outils de sécurité** > **Antivol**.



Options d’optimisation

Aucun compte fantôme créé

La création d’un compte fantôme augmente les chances de localiser un périphérique perdu ou volé. Si vous marquez votre périphérique comme introuvable, Antivol bloquera l'accès à vos comptes utilisateurs actifs pour protéger vos données sensibles. Toute personne qui tente d'utiliser le périphérique ne sera autorisée à utiliser que le compte fantôme. Le compte fantôme est un type de compte invité avec des autorisations limitées. Dans cette situation, il servira de compte système par défaut jusqu'à ce que votre périphérique soit marqué comme étant retrouvé, ce qui empêchera toute personne de se connecter à d'autres comptes d'utilisateur ou d'accéder aux données de l'utilisateur.

Chaque fois qu'une personne se connecte au compte fantôme alors que votre ordinateur est dans un état normal, vous recevrez par courriel une notification contenant des informations sur l'activité suspecte sur votre ordinateur. Après avoir reçu la notification par courriel, vous pouvez décider si vous souhaitez marquer l’ordinateur comme introuvable.

Pour créer un compte fantôme, cliquez sur **Créer un compte fantôme**, tapez le **nom du compte fantôme** dans le champ de texte et cliquez sur **Créer**.

Lorsque vous avez créé un compte fantôme, cliquez sur **Paramètres du compte fantôme** pour renommer ou supprimer le compte.

Protection par mot de passe des comptes Windows

Votre compte d’utilisateur n’est pas protégé par un mot de passe. Vous recevrez cet avertissement d’optimisation

si au moins un compte d’utilisateur n’est pas protégé par un mot de passe. Pour résoudre ce problème, veuillez créer un mot de passe pour tous les utilisateurs (à l’exception du **compte fantôme**) sur l’ordinateur.

Pour créer un mot de passe pour un compte d’utilisateur, cliquez sur **Gérer les comptes Windows** et modifiez le mot de passe ou suivez les instructions ci-dessous :

1. Appuyez sur CTRL+Alt+Delete sur votre clavier.

2. Cliquez sur **Modifier un mot de passe**.

3. Laissez le champ **Ancien mot de passe** vide.

4. Tapez le mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**, puis appuyez sur **Entrée**.

Connexion automatique pour les comptes Windows

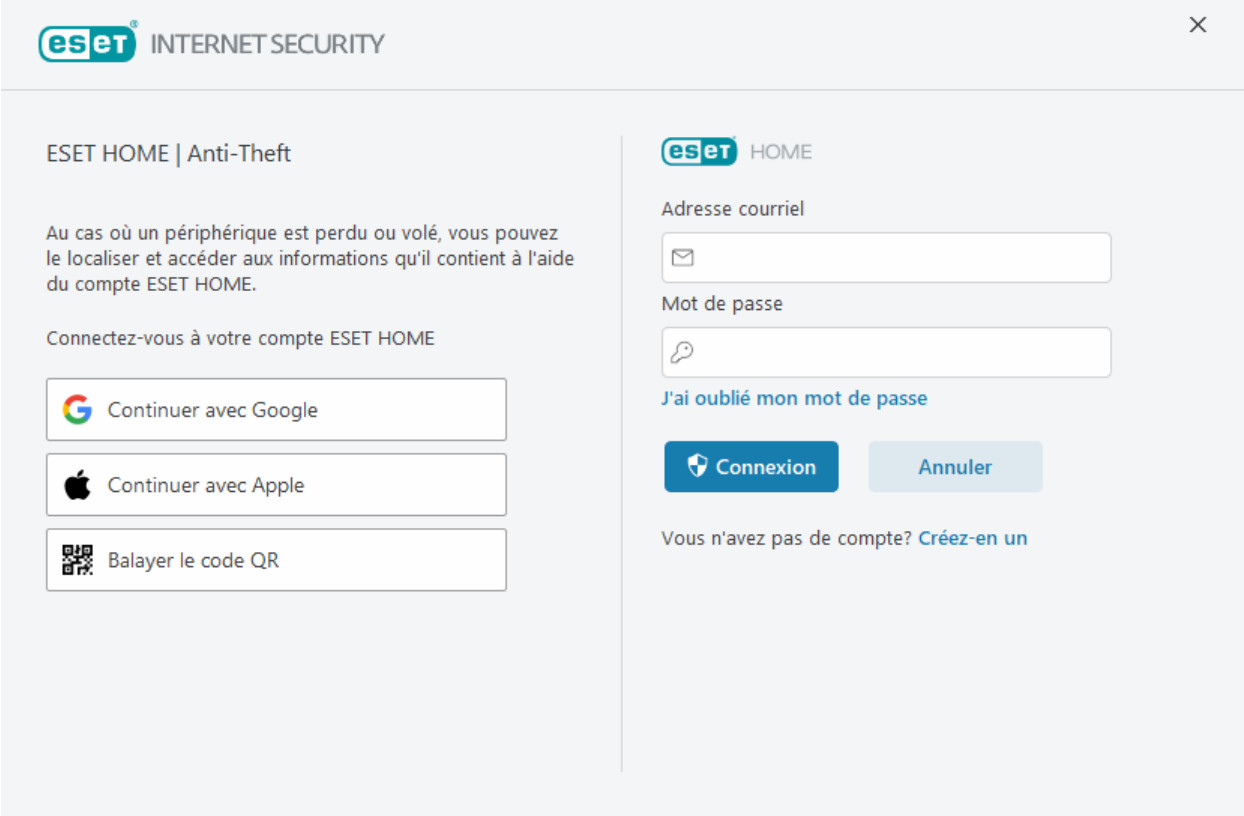
La connexion automatique à votre compte d'utilisateur est activée; par conséquent, votre compte n'est pas protégé contre les accès non autorisés. Vous recevrez cet avertissement d'optimisation si la connexion automatique est activée pour au moins un compte utilisateur. Pour résoudre ce problème d’optimisation, cliquez sur **Désactiver la connexion automatique**.

La connexion automatique pour le compte fantôme

La connexion automatique au **compte fantôme** est activée sur votre périphérique. Lorsque le périphérique est à l'état normal, nous vous déconseillons d'utiliser la connexion automatique, car elle peut entraîner des problèmes d'accès à votre compte utilisateur réel ou envoyer de fausses alertes sur la disparition de votre ordinateur. Pour résoudre ce problème d’optimisation, cliquez sur **Désactiver la connexion automatique**.

Connectez-vous à votre compte ESET HOME.

Pour activer/désactiver Antivol et accéder à l’emplacement du périphérique et aux informations dans ESET HOME, connectez-vous à votre compte ESET HOME.



Il existe plusieurs méthodes pour vous connecter à votre compte ESET HOME :

- **Utilisez votre adresse courriel ESET HOME et votre mot de passe** : saisissez **l'adresse courriel** et le **mot de passe** que vous avez utilisés pour créer votre compte ESET HOME et cliquez sur **Se connecter**.

- **Utilisez votre compte Google/AppleID** : cliquez sur **Continuer avec Google** ou **Continuer avec Apple** et connectez-vous au compte approprié. Après une connexion réussie, vous serez redirigé vers la page Web de confirmation de ESET HOME. Pour continuer, revenez à la fenêtre de votre produit ESET. Pour plus d'informations sur la connexion à l'aide du compte Google/AppleID, consultez les instructions dans l'aide en ligne de ESET HOME.

- **Balayez le code QR** : cliquez sur **Balayer le code QR** pour afficher le code QR. Ouvrez votre application mobile ESET HOME et balayez le code QR ou pointez l'appareil photo de votre périphérique vers le code QR. Pour plus d'informations, reportez-vous aux instructions dans l'aide en ligne de ESET HOME.

⚠ Échec de la connexion : erreurs courantes.

Si vous n'avez pas encore de compte ESET HOME, cliquez sur **Créer un compte** pour vous inscrire ou consultez les instructions dans l'aide en ligne de ESET HOME.
Si vous avez oublié votre mot de passe, cliquez sur **J'ai oublié mon mot de passe** et suivez les instructions qui s'affichent à l'écran ou consultez les instructions dans l'aide en ligne de ESET HOME.

Antivol ne prend pas en charge Microsoft Windows Home Server.

Définir un nom pour votre périphérique

Le champ **Nom du périphérique** représente le nom de votre ordinateur (périphérique) qui sera affiché comme identificateur dans tous les services de ESET HOME. Le nom de votre ordinateur est utilisé par défaut. Tapez le

nom du périphérique ou utilisez celui par défaut et cliquez sur **Continuer**.

Antivol activé/désactivé

Cette fenêtre affiche un message de confirmation lorsque vous activez/désactivez Antivol :

- Activé : votre périphérique est désormais protégé par Antivol, et vous pouvez gérer sa sécurité à distance sur le portail ESET HOME à l'aide de votre compte.
- Désactivé : Antivol est désactivé sur ce périphérique et toutes les données liées à <%ESET_ANTTHEFT%> pour ce périphérique sont supprimées du portail ESET HOME.

Échec de l'ajout d'un nouveau périphérique

Vous avez reçu une erreur pendant l'activation de Antivol.

Les scénarios les plus courants sont les suivants :

- Erreur de connexion à ESET HOME
- Pas de connectivité Internet (ou Internet ne fonctionne pas pour le moment)

Si vous ne parvenez pas à résoudre le problème, contactez le service d'assistance technique d'ESET.

Importer et exporter les paramètres

Vous pouvez importer ou exporter votre fichier de configuration ESET Internet Security.xml personnalisé à partir du menu **Configuration**.

> **Instructions illustrées**
> Reportez-vous à la rubrique Importer ou exporter les paramètres de configuration ESET à l'aide d'un fichier .xml pour obtenir des instructions illustrées disponibles en anglais et dans plusieurs autres langues.

L'importation et l'exportation de fichiers de configuration sont utiles si vous devez faire une copie de sauvegarde de la configuration actuelle de ESET Internet Security pour pouvoir l'utiliser par la suite. L'option d'exportation des paramètres est aussi pratique pour les utilisateurs qui veulent utiliser leur configuration préférée sur plusieurs systèmes. Ils peuvent alors importer facilement un fichier .xml pour transférer ces paramètres.

Pour importer une configuration, accédez à la fenêtre principale du programme, cliquez sur **Configuration** > **Importer et exporter les paramètres**, puis sélectionnez **Importer les paramètres**. Entrez ensuite le nom du fichier de configuration ou cliquez sur le bouton **...** pour parcourir et trouver le fichier de configuration que vous voulez importer.

Pour exporter une configuration, accédez à la fenêtre principale du programme, cliquez sur **Configurer** > **Importer/exporter les paramètres**. Sélectionnez **Exporter les paramètres** et tapez le chemin d'accès complet au fichier, y compris son nom. Cliquez sur **...** pour accéder à un emplacement sur votre ordinateur afin d'enregistrer le fichier de configuration.

Une erreur peur se produire lors de l'exportation de paramètres si vous n'avez pas assez de droits pour écrirer le fichier exporté dans le répertoire spécifié.

Aide et assistance

Cliquez sur **Aide et assistance** dans la fenêtre principale du programme pour afficher les informations de soutien et les outils de dépannage qui vous aident à résoudre les problèmes que vous pouvez rencontrer.

Abonnement

- Dépannage des abonnements – Cliquez sur ce lien pour trouver des solutions aux problèmes d'activation ou de changement d'abonnement.
- Changer d'abonnement - Cliquez sur cette option pour lancer la fenêtre d'activation et activer votre produit. Si votre périphérique est connecté à ESET HOME, choisissez un abonnement à partir de votre compte ESET HOME ou ajoutez-en un autre.

Produit installé

- Nouveautés : Cliquez ici pour ouvrir la fenêtre d'information sur les nouvelles fonctionnalités et les améliorations.
- À propos d'ESET Internet Security - Affiche des informations sur votre copie d'ESET Internet Security.
- Dépannage de produit : cliquez sur ce lien pour trouver des solutions aux problèmes les plus fréquemment rencontrés.
- **Changer de produit** – Cliquez ici pour voir si vous pouvez remplacer ESET Internet Security par une autre gamme de produit avec l'abonnement actuel.

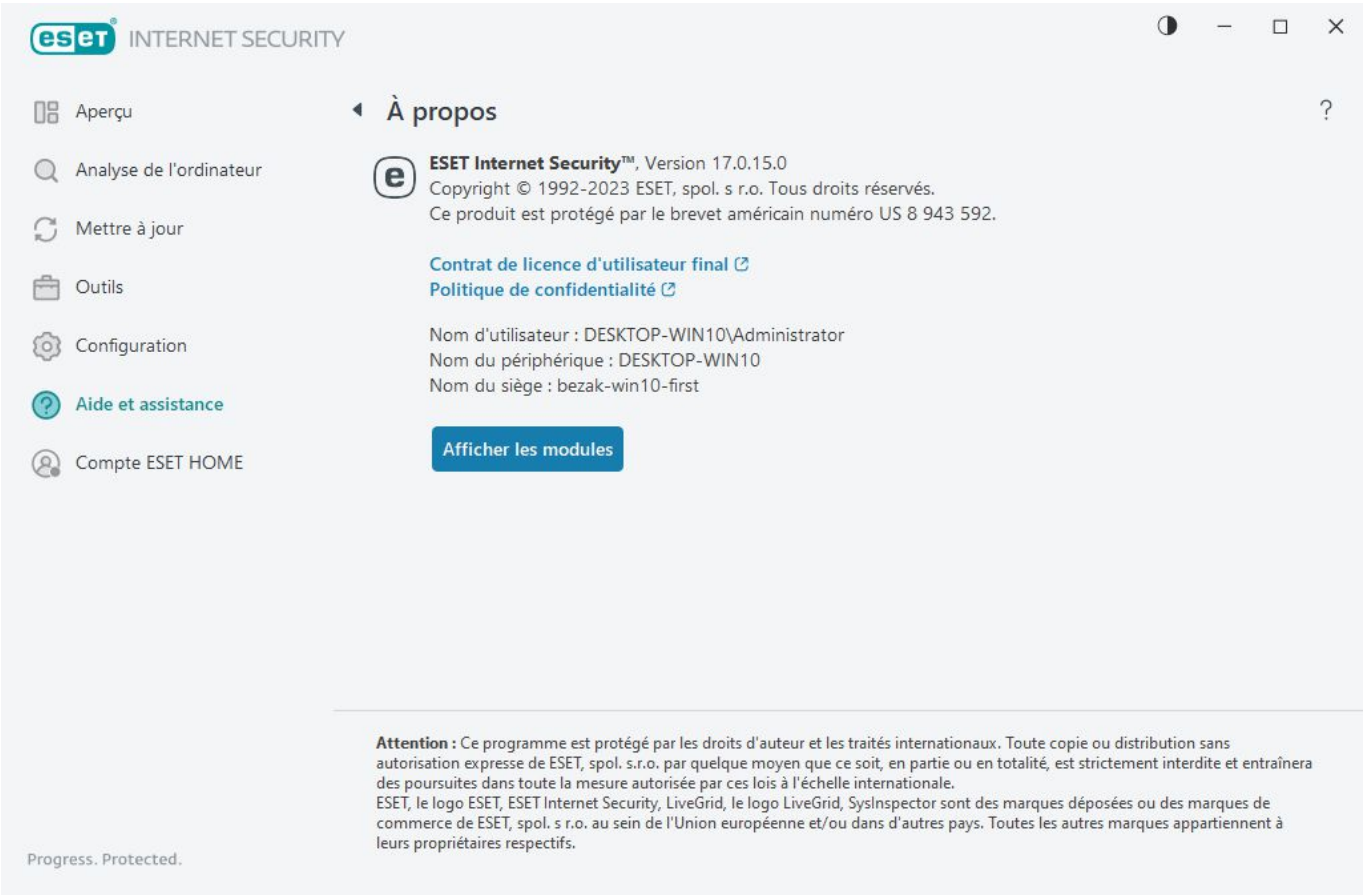
Page d'aide - Cliquez sur ce lien pour lancer les pages d'aide de ESET Internet Security.

Assistance technique

Base de connaissances - La Base de connaissances ESET contient des réponses aux questions les plus fréquentes, ainsi que les solutions recommandées pour résoudre divers problèmes. Des mises à jour régulières effectuées par les conseillers techniques d'ESET font de la base de connaissances l'outil le plus puissant pour résoudre différents problèmes.

À propos de ESET Internet Security

Cette fenêtre fournit des détails sur la version de ESET Internet Security installée sur votre ordinateur.



Cliquez sur **Afficher les modules** pour afficher des informations sur la liste des modules de programme chargés.

- Vous pouvez copier l'information à propos des modules dans le bloc-notes en cliquant sur **Copier**. Cela peut être utile lors du dépannage ou lors de la prise de contact avec le service d'assistance.

- Cliquez sur **Moteur de détection** dans la fenêtre Modules pour ouvrir le radar à virus d'ESET, qui contient des informations sur chaque version du moteur de détection d'ESET.

Nouvelles ESET

Dans cette fenêtre, ESET Internet Security vous informe régulièrement au sujet des nouvelles concernant ESET.

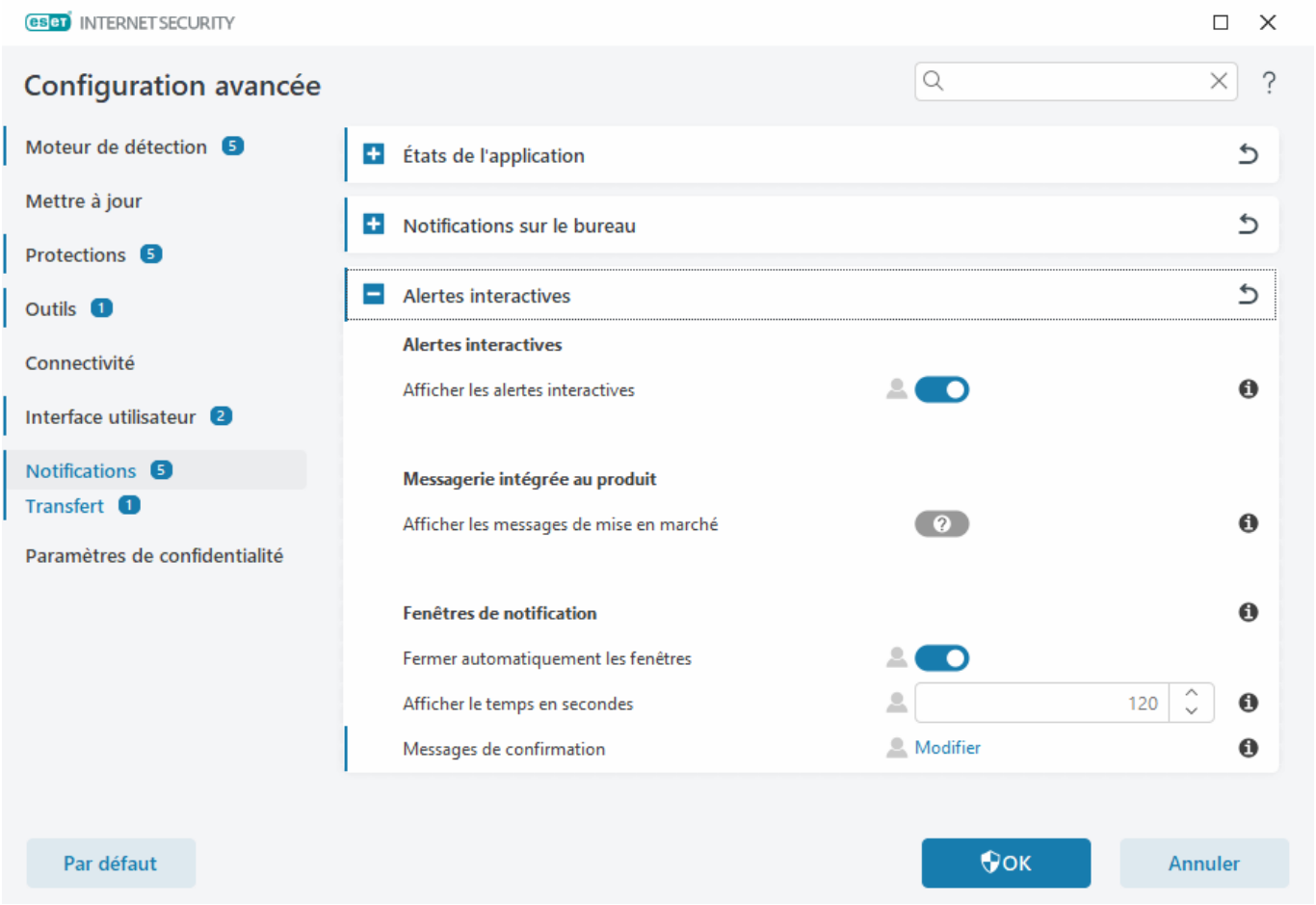
La messagerie intégrée a été conçue afin d'informer les utilisateurs des nouvelles et des autres communications ESET. L'envoi de messages marketing requiert le consentement d'un utilisateur. Par conséquent, les messages marketing ne sont pas envoyés à un utilisateur par défaut (affichés sous la forme d'un point d'interrogation). En activant cette option, vous acceptez de recevoir des messages marketing d'ESET. Si vous ne souhaitez pas **recevoir de message marketing d'ESET**, désactivez cette option.

Pour activer ou désactiver la réception de messages marketing dans la fenêtre de notification, suivez les instructions ci-dessous.

1. Ouvre la configuration avancée.

2. Cliquez sur **Notifications** > **Notifications interactives**.

3. Modifier l'option **Afficher des messages de marketing**.



Soumettre les données de configuration du système

Afin d'offrir l'assistance la plus rapide et la plus précise possible, ESET a besoin des renseignements sur la configuration de ESET Internet Security sur la configuration du système et sur les processus en cours d'exécution (fichier journal ESET SysInspector) ainsi que sur les données du registre. ESET utilisera ces données uniquement pour fournir une assistance technique au client.

Après avoir envoyé le formulaire Web, vos données de configuration du système sont envoyées à ESET. Sélectionnez **Toujours soumettre ces informations** si vous voulez mémoriser cette action pour ce processus. Pour envoyer le formulaire Web sans envoyer de données, cliquez sur **Ne pas envoyer de données** et continuez.

Vous pouvez configurer l'envoi des données de configuration du système dans Configuration avancée > **Outils** > **Diagnostics** > Assistance technique.

> Si vous avez décidé d'envoyer des données de configuration du système, il est nécessaire de remplir et d'envoyer le formulaire Web. Sinon, votre billet ne sera pas créé et vos données de configuration système seront perdues. Si les données de configuration du système ne peuvent pas être envoyées, remplissez le formulaire Web et attendez les instructions du service d'assistance technique.

Assistance technique

Dans la fenêtre principale du programme, cliquez sur **Aide et assistance** > **Assistance technique**.

Communiquez avec le service d'assistance technique

Demander de l'aide – Si vous ne trouvez pas de réponse à votre problème, vous pouvez utiliser ce formulaire situé sur le site Web d'ESET pour contacter rapidement le service d'assistance technique d'ESET. Selon vos paramètres, la fenêtre Envoyer les données de configuration de mon système s'affiche avant de remplir le formulaire Web.

Obtenir de l'information pour de l'assistance technique

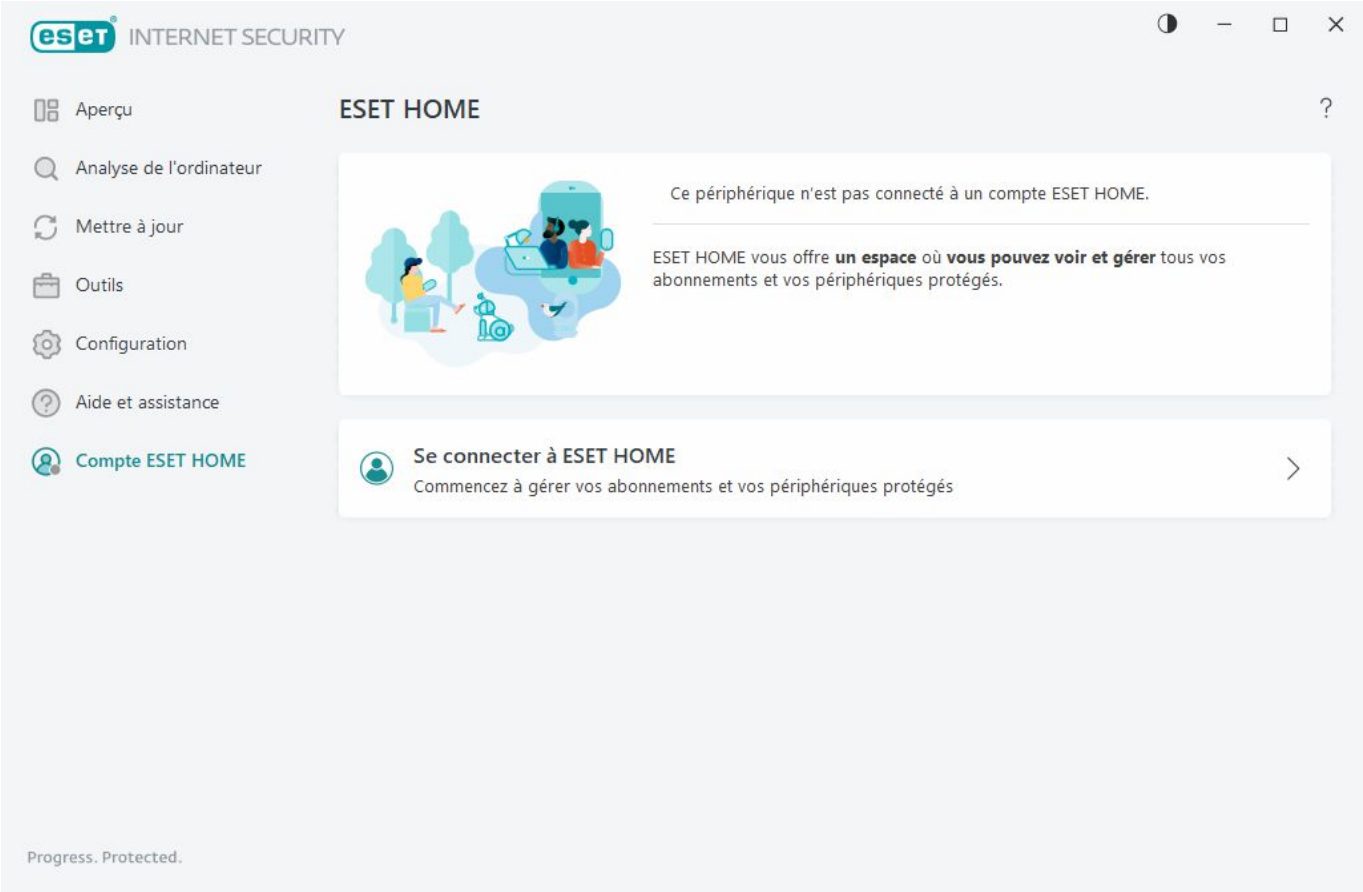
Détails pour le service d'assistance technique – Lorsque vous y êtes invité, vous pouvez copier et envoyer des renseignements au service d'assistance technique d'ESET (tels que les détails de l'abonnement, le nom du produit, la version du produit, le système d'exploitation et les informations sur l'ordinateur).

ESET Log Collector - Établit la liaison avec la base de connaissances d'ESET, où vous pouvez télécharger ESET Log Collector, une application permettant de rassembler automatiquement les informations et les journaux d'un ordinateur afin de résoudre les problèmes plus rapidement. Pour en savoir plus, consultez le guide de l'utilisateur en ligne d'ESET Log Collector.

Activez la journalisation avancée pour créer des journaux avancés pour toutes les fonctionnalités disponibles afin d'aider les développeurs à diagnostiquer et à résoudre les problèmes. La verbosité minimale de journalisation est définie dans **Diagnostic**. La journalisation avancée sera automatiquement désactivée après deux heures, sauf si vous l'arrêtez plus tôt en cliquant sur **Arrêter la journalisation avancée**. Lorsque tous les journaux sont créés, la fenêtre de notification s'affiche pour fournir un accès direct au dossier Diagnostic avec les journaux créés.

Compte ESET HOME

Pour consulter l'état de la connexion du compte ESET HOME, accédez à la fenêtre principale du programme et cliquez sur **Compte ESET HOME**.



Ce périphérique n’est pas connecté à un compte ESET HOME

Cliquez sur Se connecter à ESET HOME pour connecter votre périphérique à ESET HOME et gérer les abonnements et les périphériques protégés. Vous pouvez renouveler, mettre à niveau ou prolonger votre abonnement et afficher les détails importants. Dans le portail de gestion de ESET HOME ou dans l'application mobile, vous pouvez ajouter différents abonnements, télécharger des produits sur vos périphériques, vérifier l'état de sécurité des produits ou partager des abonnements par courriel. Pour plus d'informations, visitez l'aide en ligne de ESET HOME.

Ce périphérique est connecté à un compte ESET HOME

Vous pouvez gérer la sécurité de votre périphérique à distance à l’aide du portail ESET HOME ou de l’application mobile. Cliquez sur **App Store** ou sur **Google Play** pour afficher un code QR que vous pouvez balayer avec votre téléphone mobile pour télécharger l’application mobile ESET HOME sur App Store ou Google Play.

Compte ESET HOME : le nom de votre compte ESET HOME.

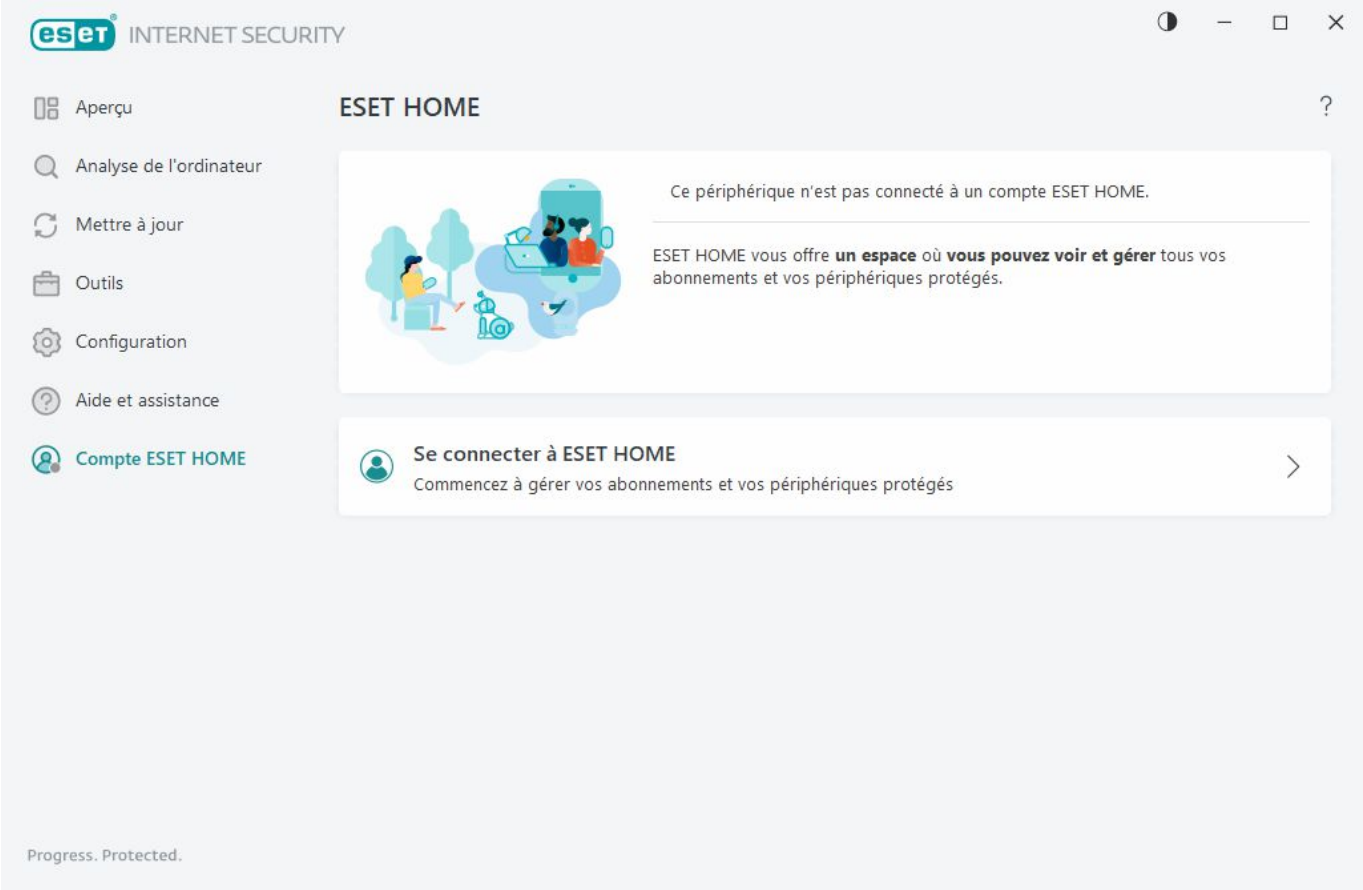
Nom du périphérique : le nom de ce périphérique affiché dans le compte ESET HOME.

Ouvrir ESET HOME : ouvre le portail de gestion ESET HOME.

Pour déconnecter votre périphérique de votre compte ESET HOME, cliquez sur **Se déconnecter de ESET HOME** > **Déconnexion**. L’abonnement utilisé pour l’activation restera actif et votre périphérique sera protégé.

Se connecter à ESET HOME

Connectez votre périphérique au ESET HOME pour consulter et gérer tous vos abonnements à ESET activés et vos périphériques. Vous pouvez renouveler, mettre à niveau ou prolonger votre abonnement et afficher les détails importants. Dans le portail de gestion de ESET HOME ou dans l'application mobile, vous pouvez ajouter différents abonnements, télécharger des produits sur vos périphériques, vérifier l'état de sécurité des produits ou partager des abonnements par courriel. Pour plus d'informations, visitez l'aide en ligne de ESET HOME.



Connectez votre périphérique à ESET HOME:

Si vous vous connectez à ESET HOME pendant l'installation ou lorsque vous sélectionnez **Utiliser le compte ESET HOME** comme méthode d'activation, suivez les instructions de la rubrique Utiliser le compte ESET HOME.

Si vous avez déjà installé ESET Internet Security et l'avez activé à l'aide d'un abonnement ajouté à votre compte ESET HOME, vous pouvez connecter votre périphérique à ESET HOME au moyen du portail ESET HOME. Suivez les instructions du Guide d'assistance en ligne de ESET HOME et autorisez la connexion dans ESET Internet Security.

1. Dans la fenêtre principale du programme, cliquez sur le **compte ESET HOME**, puis **connectez-vous à ESET HOME** ou cliquez sur **Se connecter à ESET HOME** dans la notification **Connectez ce périphérique à un compte ESET HOME**.

2. Connectez-vous à votre compte ESET HOME.

Si vous n'avez pas encore de compte ESET HOME, cliquez sur **Créer un compte** pour vous inscrire ou consultez les instructions dans l'aide en ligne de ESET HOME.
Si vous avez oublié votre mot de passe, cliquez sur **J'ai oublié mon mot de passe** et suivez les instructions qui s'affichent à l'écran ou consultez les instructions dans l'aide en ligne de ESET HOME.

3. Définir un **nom pour votre périphérique** et cliquez sur **Continuer**.

4. CUne fois que la connexion a réussi, une fenêtre de détails s'affiche. Cliquez sur **Terminé**.

Se connecter à ESET HOME

Il existe plusieurs méthodes pour vous connecter à votre compte ESET HOME :

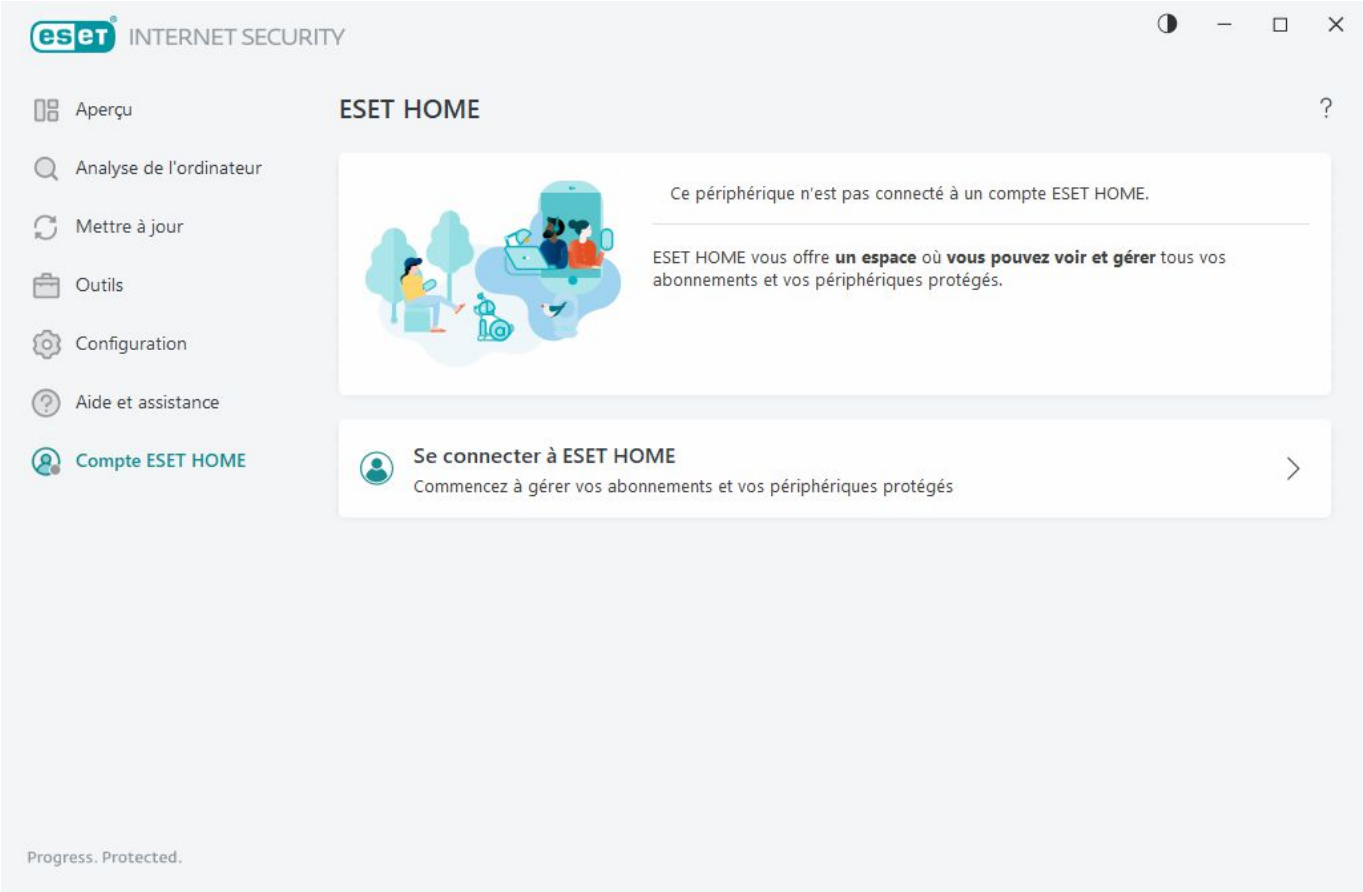
- **Utilisez votre adresse courriel ESET HOME et votre mot de passe** : saisissez **l'adresse courriel** et le **mot de passe** que vous avez utilisés pour créer votre compte ESET HOME et cliquez sur **Se connecter**.

- **Utilisez votre compte Google/AppleID** : cliquez sur **Continuer avec Google** ou **Continuer avec Apple** et connectez-vous au compte approprié. Après une connexion réussie, vous serez redirigé vers la page Web de confirmation de ESET HOME. Pour continuer, revenez à la fenêtre de votre produit ESET. Pour plus d'informations sur la connexion à l'aide du compte Google/AppleID, consultez les instructions dans l'aide en ligne de ESET HOME.

- **Balayez le code QR** : cliquez sur **Balayer le code QR** pour afficher le code QR. Ouvrez votre application mobile ESET HOME et balayez le code QR ou pointez l'appareil photo de votre périphérique vers le code QR. Pour plus d'informations, reportez-vous aux instructions dans l'aide en ligne de ESET HOME.

Si vous n'avez pas encore de compte ESET HOME, cliquez sur **Créer un compte** pour vous inscrire ou consultez les instructions dans l'aide en ligne de ESET HOME.
Si vous avez oublié votre mot de passe, cliquez sur **J'ai oublié mon mot de passe** et suivez les instructions qui s'affichent à l'écran ou consultez les instructions dans l'aide en ligne de ESET HOME.

Échec de la connexion : erreurs courantes.



Échec de la connexion – erreurs courantes

Nous n’avons pas pu trouver de compte qui corresponde à l’adresse de courriel saisie

L’adresse courriel que vous avez entré ne correspond à aucun compte ESET HOME. Cliquez sur **Retour** et tapez l’adresse courriel et le mot de passe corrects.

Pour vous connecter, vous devez créer un compte ESET HOME. Si vous n’avez pas de compte ESET HOME, cliquez sur **Précédent**, puis sur **Créer un compte** ou consultez les instructions de la rubrique Créer un compte ESET HOME.

Le nom d'utilisateur et le mot de passe ne concordent pas

Le mot de passe entré ne correspond pas à l’adresse courriel saisie. Cliquez sur **Retour**, saisissez le mot de passe correct et vérifiez que l'adresse courriel saisie est correcte. Si vous ne parvenez toujours pas à vous connecter, cliquez sur **Précédent** > **J’ai oublié mon mot de passe** pour réinitialiser votre mot de passe et suivez les instructions qui s'affichent à l’écran ou consultez la rubrique J’ai oublié mon mot de passe pour ESET HOME.

L’option de connexion sélectionnée ne correspond pas à votre compte

Votre compte est lié à votre compte de médias sociaux. Pour vous connecter à ESET HOME, cliquez sur **Continuer avec Google** ou **Continuer avec Apple** pour vous connecter au compte approprié. Après une connexion réussie, vous serez redirigé vers la page Web de confirmation de ESET HOME. Vous pouvez déconnecter votre compte de

médias sociaux de votre compte ESET HOME sur le portail ESET HOME.

Mot de passe incorrect

Cette erreur peut se produire si votre ESET Internet Security est déjà connecté à ESET HOME et que vous effectuez des modifications qui vous obligent à vous connecter (par exemple, la désactivation d'Anti-Theft) et que le mot de passe que vous avez entré ne correspond pas à celui de votre compte. Cliquez sur **Retour** et tapez le mot de passe approprié. Si vous ne parvenez toujours pas à vous connecter, cliquez sur **Précédent** > **J'ai oublié mon mot de passe** pour réinitialiser votre mot de passe et suivez les instructions qui s'affichent à l'écran ou consultez la rubrique J'ai oublié mon mot de passe pour ESET HOME.

Ajouter un périphérique dans ESET HOME

Si vous avez déjà installé ESET Internet Security et l'avez activé à l'aide d'un abonnement ajouté à votre compte ESET HOME, vous pouvez connecter votre périphérique à ESET HOME au moyen du portail ESET HOME.

1. Envoyez une demande de connexion à votre périphérique.

2. ESET Internet Security affiche **Connecter ce périphérique à une fenêtre de dialogue de compte ESET HOME** avec un nom de compte ESET HOME. Cliquez sur **Autoriser** pour connecter le périphérique au compte ESET HOME mentionné.

> S'il n'y a pas d'interaction, la demande de connexion sera automatiquement annulée après environ 30 minutes.

Configuration avancée

La configuration avancée vous permet de configurer des paramètres détaillés de ESET Internet Security afin de répondre à vos besoins.

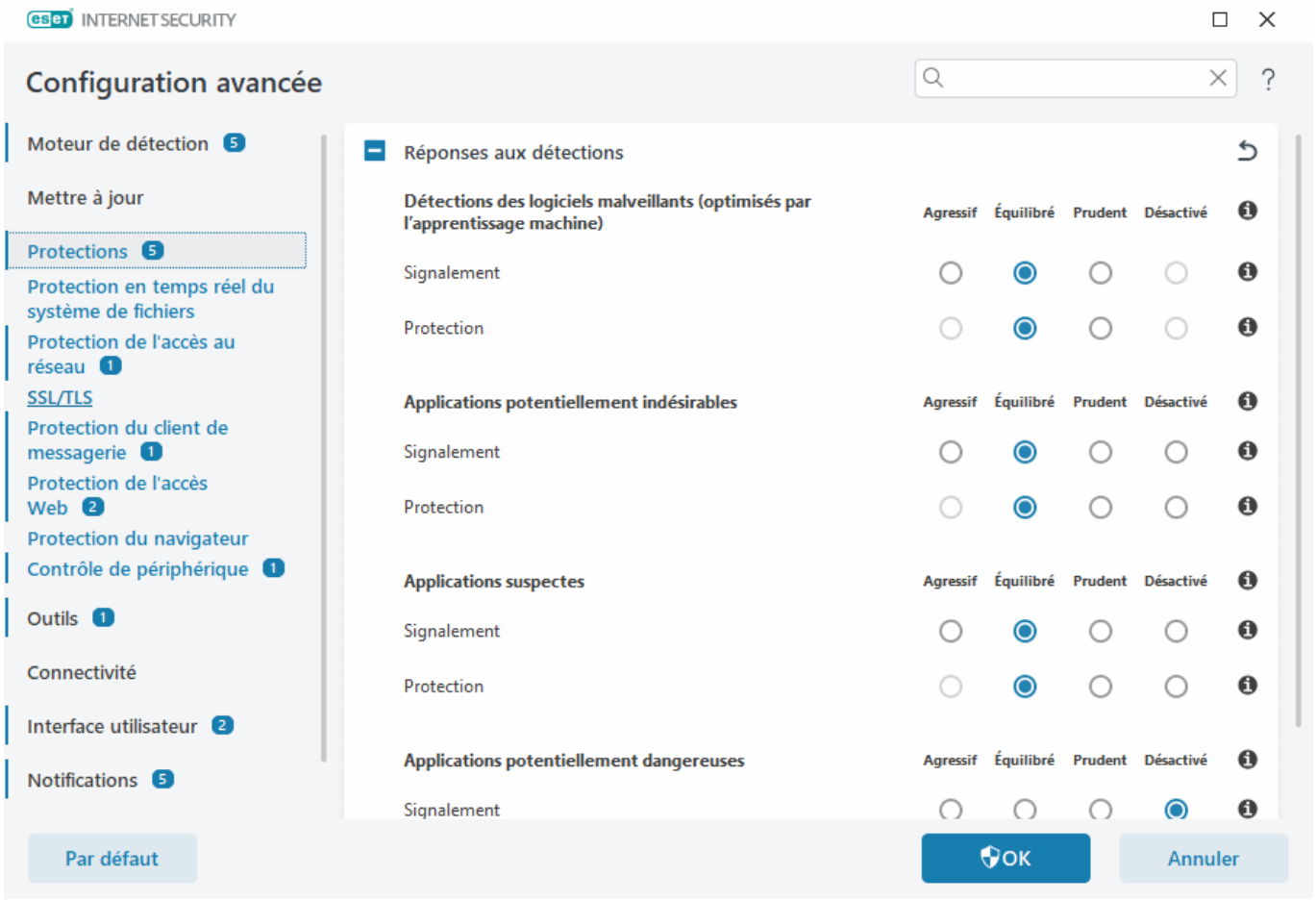
Pour ouvrir Configuration avancée, ouvrez la fenêtre principale du programme et appuyez sur la touche **F5** de votre clavier ou cliquez sur **Configuration** > **Configuration avancée**.

> En fonction de votre Accès à la configuration, vous pouvez être invité à taper un mot de passe pour ouvrir Configuration avancée.

Dans la configuration avancée, vous pouvez configurer les paramètres suivants :

- Moteur de détection
- Mettre à jour
- Protections
- Outils
- Connectivité
- Interface utilisateur

- Notifications
- Paramètres de confidentialité



Moteur de détection

Configuration avancée > **Moteur de détection** vous permet de configurer les options suivantes :

- Exclusions
- Options avancées
- Analyseur du trafic réseau

Exclusions

Les **exclusions** permettent d'exclure des objets de l'analyse du moteur de détection. Pour que la détection des menaces s'applique à tous les objets, il est recommandé de ne créer des exclusions que lorsque cela est 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, le logiciel de sauvegarde).

Les exclusions de performance excluent les fichiers et les dossiers de l'analyse. Les exclusions de performance permettent d'exclure l'analyse au niveau du fichier des applications de jeu ou celles qui provoquent un comportement anormal du système ou demandent des performances accrues.

Les exclusions de détection vous permettent d'exclure des objets du détection à l'aide du nom de détection, du chemin ou de son hachage. Les exclusions de détection n'excluent pas les fichiers et les dossiers de l'analyse comme le font les exclusions de performance. Les exclusions de détection n'excluent les objets que lorsqu'ils sont détectés par le moteur de détection et qu'une règle appropriée figure dans la liste d'exclusion.

Ne pas confondre avec d'autres types d'exclusions :

- Exclusions de processus : Toutes les opérations sur les fichiers attribuées à des processus d'application exclus sont exclues de l'analyse (cela peut être nécessaire pour améliorer la vitesse de sauvegarde et la disponibilité du service),
- Extensions de fichiers exclus,
- Exclusions HIPS,
- Filtre d'exclusion pour la protection basée sur le nuage.

Exclusions de performance

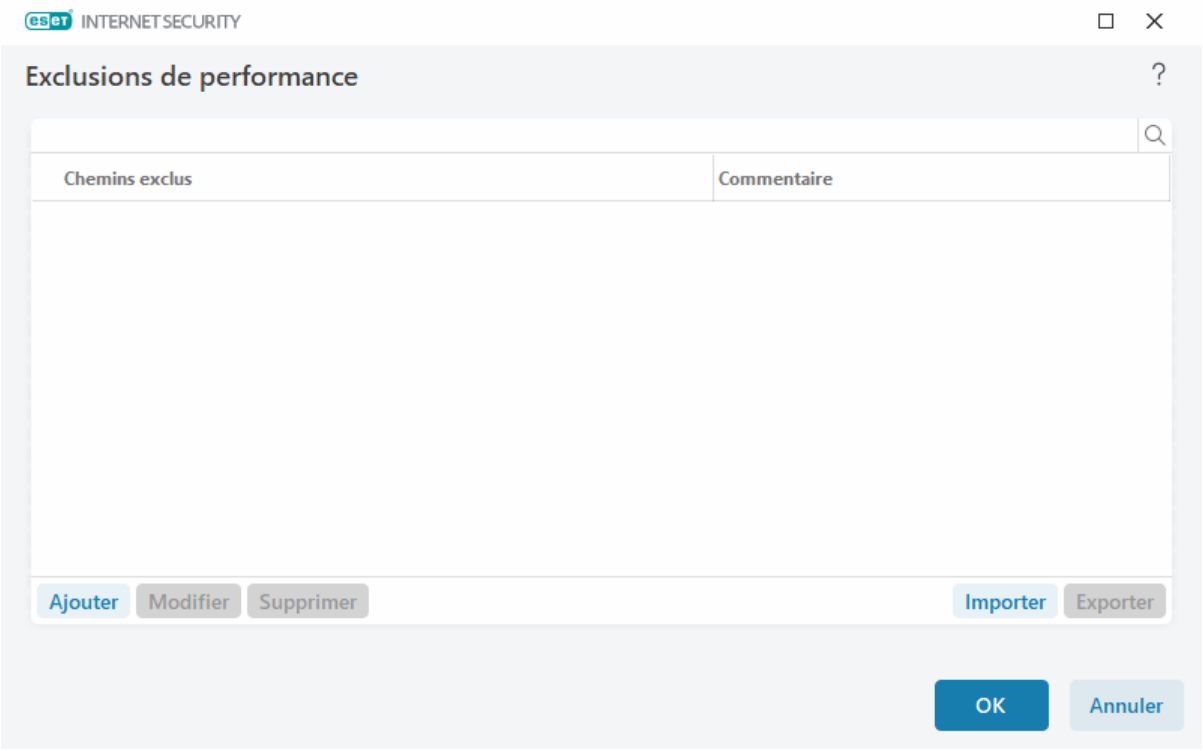
Les exclusions de performance vous permettent d'exclure les fichiers et les dossiers de l'analyse.

Pour que la détection des menaces s'appliquent bien à tous les objets, il est recommandé de ne créer des exclusions de performances 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.

Vous pouvez ajouter des fichiers et des dossiers à exclure de l'analyse dans la liste des exclusions grâce à Configurations avancées > **Moteur de détection** > **Exclusion** > **Exclusions de performance** > **Modifier**.

> Vous ne devez pas les confondre avec les exclusions de détection, les extensions de fichiers exclues, les exclusions HIPS ou les exclusions de processus.

Pour exclure un objet (chemin: fichier ou dossier) de l'analyse, cliquez sur **Ajouter** et entrez le chemin d'accès applicable ou sélectionnez-le dans l'arborescence.



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

Éléments de contrôle

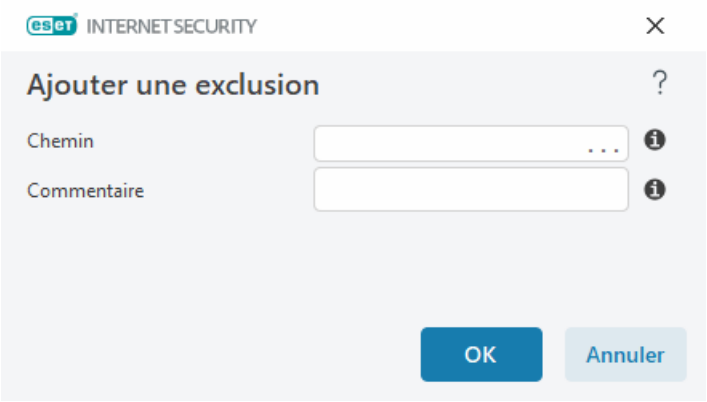
- **Ajouter** - Exclut des objets de la détection.
- **Modifier** - Permet de modifier les entrées sélectionnées.
- **Supprimer** - Supprime les entrées sélectionnées (utilisez CTRL + clic pour sélectionner plusieurs entrées).

Ajouter ou modifier des exclusions de performance

Cette fenêtre de dialogue exclut un chemin précis (fichier ou répertoire) pour cet ordinateur.

Choisissez le chemin ou saisissez-le manuellement

Pour choisir un chemin approprié, cliquez sur **...** dans le champs **Chemin d'accès**.
Consultez les exemples de formats d'exclusion ci-dessous au cas où vous effectuez une saisie manuelle.



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

Format d'exclusion

- Si vous souhaitez exclure tous les fichiers et les sous-dossiers d'un dossier, tapez le chemin d'accès de ce dossier et utilisez le masque *.
- 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 (p. ex « D »), utilisez le format suivant :
D????.exe (les points d'interrogation remplacent les caractères manquants/inconnus)

Exemples :

- *C:\Tools** – Le chemin d'accès doit se terminer par la barre oblique inverse (\) et l'astérisque (*) pour indiquer qu'il s'agit d'un dossier et que tout le contenu du dossier (fichiers et sous-dossiers) sera exclu.
- *C:\Tools*.** – Même comportement que *C:\Tools**
- *C:\Tools* – le dossier *Tools* ne sera pas exclu. Du point de vue de l'analyseur, *Tools* peut aussi être un nom de fichier.
- *C:\Tools*.dat* exclura les fichiers .dat du dossier *Tools*.
- *C:\Tools\sg.dat* exclura ce fichier particulier situé à l'emplacement indiqué par le chemin d'accès.

Variables système dans les exclusions

Vous pouvez utiliser des variables système telles que %PROGRAMFILES% pour définir des exclusions d'analyse.

- Pour exclure le dossier Program Files à l'aide de cette variable système, utilisez le chemin *%PROGRAMFILES%** (n'oubliez pas d'ajouter une barre oblique inverse et un astérisque à la fin du chemin) lors de l'ajout aux exclusions
- Pour exclure tous les fichiers et les dossiers d'un sous-dossier *%PROGRAMFILES%*, utilisez le chemin *%PROGRAMFILES%\Excluded_Directory**

Développez la liste des variables système prises en charge

Les variables suivantes peuvent être utilisées dans le format d'exclusion de chemin :

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

Les variables système spécifiques à l'utilisateur (telles que *%TEMP%* ou *%USERPROFILE%*) ou les variables d'environnement (telles que *%PATH%*) ne sont pas prises en charge.

Les caractères génériques au milieu d'un chemin ne sont pas pris en charge

L'utilisation de caractères génériques au milieu d'un chemin d'accès (par exemple, *C:\Tools*\Data\file.dat*) peut fonctionner, mais n'est pas officiellement prise en charge pour les exclusions de performances.
Il n'y a aucune restriction à l'utilisation de caractères génériques au milieu d'un chemin lorsque vous utilisez l'exclusions de détection.

Ordre des exclusions

- Il n'y a pas d'options pour ajuster le niveau de priorité des exclusions à l'aide des boutons haut/bas (comme c'est le cas pour les règles de pare-feu où les règles sont exécutées de haut en bas).
- Lorsque la première règle applicable est satisfaite par l'analyseur, la deuxième règle applicable est ignorée.
- Moins il y a de règles, meilleures sont les performances de l'analyse.
- Évitez de créer des règles concurrentes.

Format d'exclusion de chemin

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

Format d'exclusion

- Si vous souhaitez exclure tous les fichiers et les sous-dossiers d'un dossier, tapez le chemin d'accès de ce dossier et utilisez le masque ***.
- 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 (p. ex « D »), utilisez le format suivant :
D????.exe (les points d'interrogation remplacent les caractères manquants/inconnus)

Exemples :

- *C:\Tools** – Le chemin d'accès doit se terminer par la barre oblique inverse (\) et l'astérisque (*) pour indiquer qu'il s'agit d'un dossier et que tout le contenu du dossier (fichiers et sous-dossiers) sera exclu.
- *C:\Tools*.** – Même comportement que *C:\Tools**
- *C:\Tools* – le dossier *Tools* ne sera pas exclu. Du point de vue de l'analyseur, *Tools* peut aussi être un nom de fichier.
- *C:\Tools*.dat* exclura les fichiers .dat du dossier *Tools*.
- *C:\Tools\sg.dat* exclura ce fichier particulier situé à l'emplacement indiqué par le chemin d'accès.

Variables système dans les exclusions

Vous pouvez utiliser des variables système telles que %PROGRAMFILES% pour définir des exclusions d'analyse.

- Pour exclure le dossier Program Files à l'aide de cette variable système, utilisez le chemin *%PROGRAMFILES%** (n'oubliez pas d'ajouter une barre oblique inverse et un astérisque à la fin du chemin) lors de l'ajout aux exclusions
- Pour exclure tous les fichiers et les dossiers d'un sous-dossier *%PROGRAMFILES%*, utilisez le chemin *%PROGRAMFILES%\Excluded_Directory**

Développez la liste des variables système prises en charge

Les variables suivantes peuvent être utilisées dans le format d'exclusion de chemin :

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

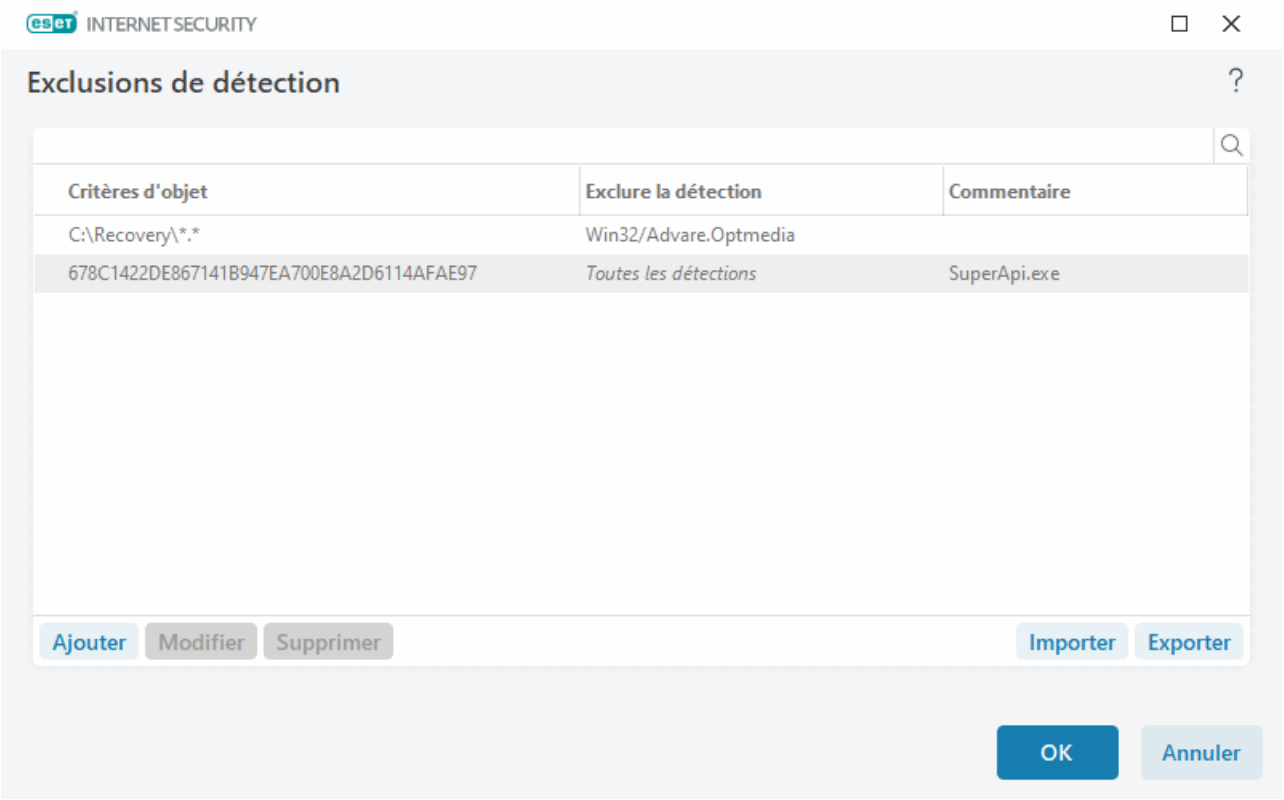
Les variables système spécifiques à l'utilisateur (telles que *%TEMP%* ou *%USERPROFILE%*) ou les variables d'environnement (telles que *%PATH%*) ne sont pas prises en charge.

Exclusions de détection

Les exclusions de détection vous permettent d'exclure des objets du détection en filtrant le nom de détection, le chemin de l'objet ou son hachage.

Comment fonctionnent les exclusions de détection

Les exclusions de détection n'excluent pas les fichiers et les dossiers de l'analyse comme le font les exclusions de performance. Les exclusions de détection n'excluent les objets que lorsqu'ils sont détectés par le moteur de détection et qu'une règle appropriée figure dans la liste d'exclusion.
Par exemple (voir la première ligne de l'image ci-dessous), lorsqu'un objet est détecté comme Win32/Adware.Optmedia et que le fichier détecté est *C:\Recovery\file.exe*. Sur la deuxième ligne, chaque fichier qui possède le hachage SHA-1 approprié sera toujours exclu peu importe le nom de la détection.



Pour s'assurer que toutes les menaces sont détectées, nous recommandons de ne créer des exclusions de détection que lorsque cela est absolument nécessaire.

Pour ajouter des fichiers et des dossiers à la liste des exclusions, accédez à Configurations avancées > **Moteur de détection** > **Exclusions** > **Exclusions de détection** > **Modifier**.

Vous ne devez pas les confondre avec les exclusions de performance, les extensions de fichiers exclues, les exclusions HIPS ou les exclusions de processus.

Pour exclure un objet (par son nom de détection ou son hachage) du moteur de détection, cliquez sur **Ajouter**.

Pour les applications potentiellement indésirables et les applications potentiellement dangereuses, l'exclusion par nom de détection peut également être créée :

- Dans la fenêtre d'alerte signalant la détection (cliquez sur **Afficher les options avancées**, puis sélectionnez **Exclure de la détection**).

• À partir du menu contextuel des fichiers journaux en utilisant Assistant de création d'exclusion de détection.

• En cliquant sur **Outils** > **Quarantaine**, puis en cliquant à droite sur le fichier placé en quarantaine et en sélectionnant **Restaurer et exclure de l'analyse** dans le menu contextuel.

Critères d'objet des exclusions de détection

• **Chemin d'accès :** Permet de limiter une exclusion de détection pour un chemin spécifié (ou tout autre).

• **Nom de la détection** - Si le nom d'une détection est indiqué à côté d'un fichier exclu, cela signifie que le fichier est seulement exclu pour cette détection sans faire l'objet d'une exclusion complète. Si ce fichier devient ensuite infecté par d'autres logiciels malveillants, ceux-ci seront détectés.

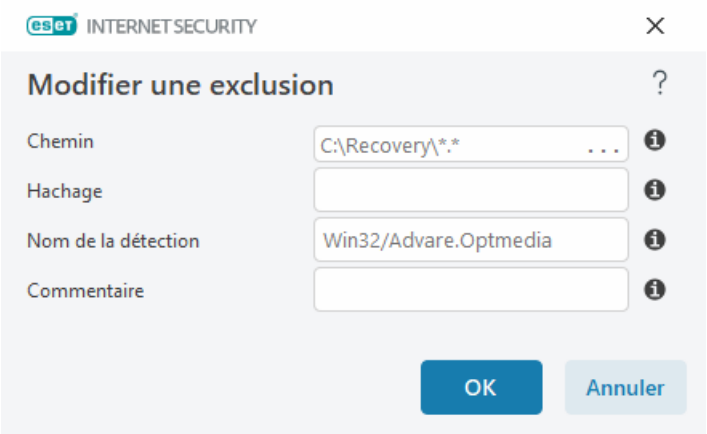
• **Hachage** – Exclut un fichier basé sur le hachage spécifié SHA-1, indépendamment du type de fichier, de l'emplacement, du nom ou de son extension.

Ajouter ou modifier une exclusion de détection

Exclure la détection

Un nom de détection ESET valide doit être fournis. Pour un nom de détection valide, consultez les fichiers journaux, puis sélectionnez **Détections** dans le menu déroulant Fichiers journaux. Cela est utile lorsqu'un faux échantillon positif est détecté dans ESET Internet Security. Les exclusions pour les infiltrations réelles sont très dangereuses; envisagez d'exclure uniquement les fichiers ou les répertoires concernés en cliquant sur **...** dans le champ **Chemin d'accès** ou uniquement pendant une période de temps limitée. Les exclusions s'appliquent également aux applications potentiellement indésirables, aux applications potentiellement dangereuses et aux applications suspectes.

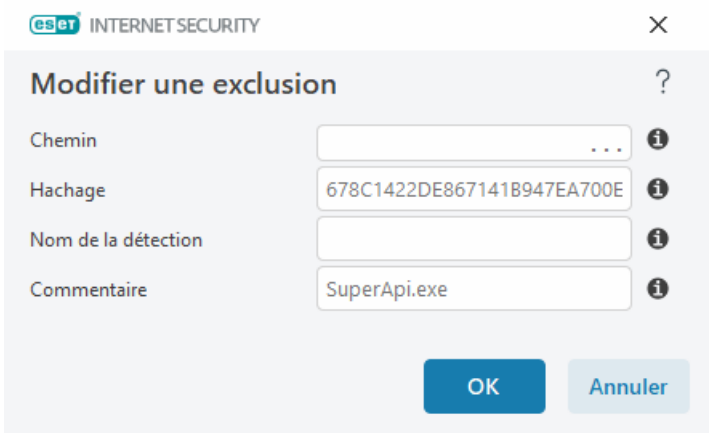
Voir aussi Format de chemin d'exclusion.



Voir l'exemple d'exclusion de détection ci-dessous.

Exclure le hachage

Exclut un fichier basé sur le hachage spécifié SHA-1, indépendamment du type de fichier, de l'emplacement, du nom ou de son extension.



Exclusions par nom de détection

Pour exclure une détection précise en utilisant son nom, entrez un nom de détection valide : Win32/Adware.Optmedia

Vous pouvez également utiliser le format suivant lorsque vous excluez une détection de la fenêtre d'alerte de ESET Internet Security :

@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt

@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan

@NAME=Win32/Bagle.D@TYPE=worm

Éléments de contrôle

- **Ajouter** - Exclut des objets de la détection.
- **Modifier** - Permet de modifier les entrées sélectionnées.
- **Supprimer** - Supprime les entrées sélectionnées (utilisez CTRL + clic pour sélectionner plusieurs entrées).

Assistant de création d'exclusion de détection

Une exclusion de détection peut également être créée à partir du menu contextuel Fichiers journaux (non disponible pour la détection de logiciels malveillants) :

1. Dans la fenêtre principale du programme, cliquez sur **Outils** > **Fichiers journaux**.
2. Cliquez avec le bouton droit de la souris sur une détection dans le **journal des détections**.
3. Cliquez sur **Créer une exclusion**.

Pour exclure une ou plusieurs détections basées sur les **critères d'exclusion**, cliquez sur **Modifier le critère** :

- **Fichiers exacts :** Exclure chaque fichier selon son hachage SHA-1.
- **Détection :** Permet d'exclure chaque fichier selon son nom de détection.
- **Chemin + Détection :** Exclure chaque fichier selon son nom de détection et son chemin, y compris le nom du fichier (par exemple, *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

L'option recommandée est présélectionnée en fonction du type de détection.

Vous pouvez éventuellement ajouter un **Commentaire** avant de cliquer sur **Créer une exclusion**.

Options avancées du moteur de détection

Activer l'analyse avancée à l'aide d'AMSI qui est l'outil de protection contre les programmes malveillants de Microsoft et qui permet l'analyse des scripts PowerShell, des scripts exécutés par Windows Script Host et des données analysées à l'aide de la trousse SDK AMSI.

Analyseur du trafic réseau

L'analyseur du trafic réseau offre une protection contre les logiciels malveillants pour les protocoles d'application, qui intègre plusieurs techniques avancées d'analyse des logiciels malveillants. L'analyseur du trafic réseau analyse automatiquement les protocoles HTTP(S), POP3(S) et IMAP(S), quel que soit le navigateur Internet ou le client de messagerie. Vous pouvez activer/désactiver l'analyseur de trafic réseau dans Configuration avancée > **Moteur de détection** > **Analyseur du trafic réseau**.

Activer l'analyseur du trafic réseau : si vous désactivez cette option, les protocoles HTTP(S), POP3(S) et IMAP(S) ne seront pas analysés. Notez que les fonctionnalités suivantes de ESET Internet Security nécessitent l'activation de l'analyseur du trafic réseau :

- Protection de l'accès Web
- Contrôle parental
- Sécurité et confidentialité du navigateur
- Opérations bancaires et navigation sécurisées
- SSL/TLS
- Protection anti-hameçonnage
- Protection du client de messagerie

Protection basée sur le nuage

ESET LiveGrid® (fondé sur le système avancé d'avertissement anticipé ESET ThreatSense.Net) utilise les données soumises par les utilisateurs ESET de partout dans le monde avant de les envoyer au laboratoire de recherche d'ESET. En fournissant des métadonnées et des échantillons suspects provenant de partout, ESET LiveGrid® nous permet de réagir immédiatement aux besoins de nos clients et de préserver la réactivité d'ESET aux menaces les plus récentes.

Les options suivantes sont disponibles :

Activer le système de réputation d'ESET LiveGrid®

Le système de réputation ESET LiveGrid® fournit une liste blanche et une liste noire basées sur le nuage.

Vérifiez la réputation des processus en cours d'exécution et des fichiers directement à partir de l'interface du

programme ou du menu contextuel grâce à des informations supplémentaires disponibles à partir de ESET LiveGrid®.

Activer le système de rétroaction d'ESET LiveGrid®

En plus du système de réputation de ESET LiveGrid®, le système de rétroaction de ESET LiveGrid® collectera des informations sur votre ordinateur liées aux menaces nouvellement détectées. Ces renseignements peuvent comprendre :

- Échantillon ou copie du fichier dans lequel la menace apparaissait
- Chemin d'accès au fichier
- Nom de fichier
- Date et heure
- Processus par lequel la menace est apparue sur votre ordinateur
- Informations sur le système d'exploitation de votre ordinateur

Par défaut, ESET Internet Security est configuré pour envoyer les fichiers suspects pour une analyse détaillée au laboratoire de virus d'ESET. Les fichiers portant certaines extensions comme *.doc* ou *.xls* sont toujours exclus. Vous pouvez ajouter d'autres extensions à la liste d'exclusion, dont vous ou votre organisation souhaitez éviter l'envoi.

Pour en savoir plus sur l'envoi des données pertinentes, consultez la page Politique de confidentialité.

Vous pouvez choisir de ne pas activer ESET LiveGrid®

Vous ne perdrez aucune fonctionnalité dans le logiciel, mais dans certains cas, ESET Internet Security peut répondre plus rapidement aux nouvelles menaces lorsque ESET LiveGrid® est activé. Si vous l'avez déjà utilisé ESET LiveGrid® et que vous l'avez désactivé, il se peut toujours que des paquets de données soient envoyés. Même après la désactivation, ces paquets seront envoyés à ESET. Lorsque toutes les informations actuelles sont envoyées, aucun autre paquet n'est créé.

Pour en savoir plus sur ESET LiveGrid®, consultez le Glossaire.
Consultez nos instructions illustrées disponibles en anglais et dans plusieurs autres langues pour activer ou désactiver ESET LiveGrid® dans ESET Internet Security.

Configuration de la protection basée sur le nuage dans la configuration avancée

Pour accéder aux paramètres de ESET LiveGrid®, ouvrez Configuration avancée > **Moteur de détection** > **Protection basée sur le nuage**.

- **Activer le système de réputation d'ESET LiveGrid® (recommandé)** - Le système de réputation d'ESET LiveGrid® améliore l'efficacité des solutions de protection contre les logiciels malveillants d'ESET en comparant les fichiers analysés à une base de données d'éléments d'une liste blanche et d'une liste noire

dans le nuage.

• **Activer le système de rétroaction d'ESET LiveGrid®** - Envoie les données de soumission pertinentes (décrites dans la section **Soumission d'échantillons ci-dessous**) ainsi que les rapports d'incident et les statistiques au laboratoire de recherche ESET pour une analyse plus approfondie.

• **Envoyer les rapports de plantage et les données de diagnostic** – Permet envoyer des données de diagnostic associées d'ESET LiveGrid® telles que les rapports de plantage et les vidages de mémoire des modules. Nous recommandons de laisser cette option activée pour aider l'ESET à diagnostiquer les problèmes, à améliorer les produits et à assurer une meilleure protection de l'utilisateur final.

• **Envoyer des données statistiques anonymes** - Autoriser ESET à collecter des renseignements sur les menaces nouvellement détectées comme le nom de la menace, la date et l'heure de la détection, la méthode et les métadonnées associées à la détection, ainsi que la version du produit et sa configuration dont les renseignements sur votre système.

• **Adresse de courriel du contact (facultatif)** - Votre adresse de courriel peut également être incluse avec tout fichier suspect et pourra être utilisée pour communiquer avec vous si nous avons besoin de plus d'information pour l'analyse. Veuillez noter que vous ne recevrez pas de réponse d'ESET sauf si d'autres renseignements sont requis.

Envoi d'échantillons

Envoi manuel d'échantillons – Active l'option permettant l'envoi manuel d'échantillons à ESET à partir du menu contextuel, Quarantaine ou Outils.

Envoi automatique des échantillons détectés

Sélectionnez le type d'échantillons qui sera envoyé à ESET pour être analysé afin d'améliorer les détections futures (la taille maximale par défaut de l'échantillon est de 64 Mo). Les options suivantes sont disponibles :

• **Tous les échantillons détectés** – Tous les objets détecté par le moteur de détection. (y compris les applications potentiellement indésirables lorsque cette option est activée dans les paramètres de l'analyseur).

• **Tous les échantillons sauf les documents** – Tous les objets détectés à l'exception des **documents.** (voir ci-dessous).

• **Ne pas envoyer** – Les objets détectés ne seront pas envoyés à ESET.

Envoi automatique des échantillons suspects

Ces échantillons seront également envoyés à ESET au cas où le moteur de détection ne les a pas détectés. Par exemple, les échantillons qui ont failli ne pas être détectés, ou que l'un des modules de protection de ESET Internet Security considère comme suspects ou qui a un comportement obscur (la taille maximale par défaut des échantillons est de 64 Mo).

• **Exécutables** – Comprend des fichiers exécutables tels que .exe, .dll, .sys.

• **Archives** : Inclut des fichiers de type archive tels que .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.

• **Scripts** : Inclut des fichiers de type script tels que .bat, .cmd, .hta, .js, .vbs, .ps1.

• **Autre** : Inclut les types de fichiers .jar, .reg, .msi, .sfw, .lnk.

• **Pourriels éventuels** - Cette option permet d'envoyer des parties d'un éventuel pourriel ou des éventuels pourriels en entier avec une pièce jointe à ESET pour une analyse plus approfondie. L'activation de cette option améliore la détection des pourriels par tous les autres utilisateurs dans le monde et vous permet d'avoir une meilleure protection contre les pourriels à l'avenir.

• **Documents** – Inclut les documents Microsoft Office ou PDF avec ou sans contenu actif.

Développer pour afficher la liste de tous les types de fichiers de document inclus

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Exclusions

Le filtre d'exclusion permet d'exclure certains fichiers/dossiers de l'envoi (par exemple, il peut être utile d'exclure les fichiers contenant des informations confidentielles comme des documents ou des classeurs). Les fichiers de cette liste ne seront jamais envoyés aux laboratoires d'ESET pour analyse, même s'ils contiennent du code suspect. Les types de fichiers les plus courants sont exclus par défaut (.doc, etc.). Vous pouvez ajouter des fichiers à cette liste, au besoin.

Pour exclure les fichiers téléchargés à partir `download.domain.com`, cliquez sur Configuration avancée >**Moteur de détection** > **Protection basée sur le nuage** > **Envoi d'échantillons**; cliquez alors sur **Modifier** en regard de **Exclusions**. Et ajoutez l'exclusion `.download.domain.com`.

Taille maximale des échantillons (Mo) : définit la taille maximale des échantillons envoyés automatiquement (1 à 64 Mo).

Filtre d'exclusion pour la protection basée sur le nuage

Le filtre d'exclusion permet d'exclure certains fichiers ou dossiers de la soumission d'échantillons. Les fichiers de cette liste ne seront jamais envoyés aux laboratoires d'ESET pour analyse, même s'ils contiennent du code suspect. Les types de fichiers courants (par exemple, .doc, etc.) sont exclus par défaut.

Cette fonctionnalité permet d'exclure des fichiers qui peuvent comporter des données confidentielles, tels que des documents ou des feuilles de calcul.

Pour exclure les fichiers téléchargés à partir download.domain.com, cliquez sur Configuration avancée > **Moteur de détection** > **Protection basée sur le nuage** > **Envoi d'échantillons** > **Exclusions** et ajoutez l'exclusion *download.domain.com*.

Analyses de logiciels malveillants

La section **Analyses de logiciels malveillants** est accessible à partir Configuration avancée > **Moteur de détection** > **Analyses de logiciels malveillants** et vous permet de configurer les paramètres d'analyse pour les profils d'analyse.

Analyse à la demande

Profil sélectionné – Un ensemble précis de paramètres utilisés par l'analyseur à la demande. Pour en créer un nouveau, cliquez sur **Modifier** situé à côté de la **liste des profils**. Pour plus de détails, consultez la section Profils d'analyse.

Après avoir sélectionné le profil d'analyse, vous pouvez configurer les options suivantes :

Cibles à analyser : si vous souhaitez analyser une cible en particulier ou un groupe de cibles, cliquez sur **Modifier** à côté de **Cibles à analyser** et choisissez une option dans le menu déroulant ou choisissez des cibles spécifiques dans la structure des dossiers (arborescence). Pour plus de détails, consultez la section Cibles à analyser.

Protection à la demande et par apprentissage automatique : vous pouvez configurer les niveaux de protection et la création des rapports pour chaque profil d'analyse. Par défaut, les profils d'analyse utilisent la même configuration que celle définie dans la protection en temps réel du système de fichiers. Désactivez le bouton bascule en regard de **Utiliser les paramètres de protection en temps réel** pour configurer les niveaux de protection et la création de rapports personnalisés. Reportez-vous à la section Protections pour obtenir une explication détaillée sur les rapports et les niveaux de protection.

ThreatSense : options de configuration avancées, telles que les extensions de fichier que vous souhaitez contrôler et les méthodes de détection utilisées. Reportez-vous à ThreatSense pour plus d'informations.

Profils d'analyse

Il existe 4 profils d'analyse prédéfinis dans ESET Internet Security :

- **Analyse intelligent** : Il s'agit du profil de numérisation avancée par défaut. Le profil d'analyse intelligente utilise la technologie d'optimisation intelligente, qui exclut les fichiers qui ont été détectés comme étant sains lors d'une analyse précédente et qui n'ont pas été modifiés depuis cette analyse. Cela permet de réduire les temps d'analyse avec un impact minimal sur la sécurité du système.

- **Analyse par menu contextuel :** Vous pouvez démarrer une analyse à la demande de n'importe quel fichier à partir du menu contextuel. Le profil d'analyse du menu contextuel vous permet de définir une configuration d'analyse qui sera utilisée lorsque vous déclencherez l'analyse de cette manière.

- **Analyse détaillée** – Le profil d'analyse approfondie n'utilise pas l'optimisation intelligente par défaut. Par conséquent, aucun fichier n'est exclu de l'analyse lorsque ce profil est utilisé.

- **Analyse de l'ordinateur** : Il s'agit du profil par défaut utilisé dans l'analyse standard de l'ordinateur.

Vos paramètres d'analyse préférés peuvent être enregistrés pour analyse future. Nous vous recommandons de créer un profil différent (avec différentes cibles et méthodes ainsi que d'autres paramètres d'analyse) pour chacune des analyses utilisées régulièrement.

Pour créer un nouveau profil, ouvrez Configuration avancée > **Moteur de détection** > **Analyse des logiciels malveillants** > **Analyse à la demande** > **Liste des profils** > **Modifier**. La fenêtre **Gestionnaire de profils** comprend le menu déroulant **Profil sélectionné** qui affiche les profils d'analyse existants, ainsi que l'option permettant d'en créer un nouveau. Pour vous aider à créer un profil d'analyse répondant à vos besoins, consultez la rubrique ThreatSense pour une description de chacun des paramètres de configuration de l'analyse.

Imaginez que vous vouliez créer votre propre profil d'analyse et que la configuration associée au profil **Analyse de l'ordinateur** vous convienne en partie, mais que vous ne voulez ni analyser les fichiers exécutables compressés par un compresseur d'exécutables ni les applications potentiellement dangereuses et que vous voulez également utiliser un **Toujours corriger la détection**. Entrez le nom de votre nouveau profil dans la fenêtre **Gestionnaire de profil**, puis cliquez sur **Ajouter**. Sélectionnez votre nouveau profil à partir du menu déroulant de **Profil sélectionné**, puis ajustez les paramètres restants pour répondre à vos exigences ; cliquez ensuite sur **OK** pour enregistrer votre nouveau profil.

Cibles à analyser

Le menu déroulant **Cibles à analyser** permet de sélectionner des cibles à analyser prédéfinies.

- **Par paramètres de profil** - Sélectionne les cibles spécifiés par le profil d'analyse sélectionné.
- **Supports amovibles** - Sélectionne les disquettes, les périphériques de stockage USB, les CD/DVD.
- **Disques locaux** - Sélectionne tous les disques durs du système.
- **Lecteurs réseau** - Sélectionne tous les disques réseau mappés.
- **Sélection personnalisée** : Annule toutes les sélections précédentes.

La structure des dossiers (arborescence) contient également des cibles d'analyse spécifiques.

- **Mémoire opérationnelle** : Analyse tous les processus et données actuellement utilisés par la mémoire opérationnelle.
- **Secteurs de démarrage/UEFI** : Analyse les secteurs de démarrage et UEFI à la recherche de logiciels malveillants. Pour en savoir plus sur le scanner UEFI, consultez le glossaire.
- **Base de données WMI** : Analyse l'ensemble de la base de données Windows Management Instrumentation (WMI), tous les espaces de noms, toutes les instances de classe et toutes les propriétés. Recherche les références à des fichiers infectés ou à des logiciels malveillants incorporés sous forme de données.
- **Registre du système** : Analyse l'ensemble du registre du système, toutes les clés et les sous-clés. Recherche les références à des fichiers infectés ou à des logiciels malveillants incorporés sous forme de données. Lors du nettoyage des détections, la référence reste dans le registre pour s'assurer qu'aucune donnée importante ne sera perdue.

Pour accéder rapidement à une cible d'analyse (fichier ou dossier), tapez son chemin d'accès dans le champ de texte sous l'arborescence. Le chemin est sensible à la casse. Pour inclure la cible dans l'analyse, cochez la case correspondante dans l'arborescence.

Analyse à l'état de repos

Vous pouvez activer l'analyseur à l'état inactif dans Configuration avancée > **Moteur de détection** > **Analyses de logiciels malveillants** > **Analyse à l'état inactif**.

Analyse à l'état de repos

Activez le bouton bascule à côté de **Activer l'analyse au repos** pour activer cette fonctionnalité. Lorsque l'ordinateur est inactif, une analyse silencieuse de l'ordinateur est effectuée sur tous les disques locaux.

Par défaut, l'analyseur au repos ne sera pas exécuté lorsque l'ordinateur (portable) est alimenté par batterie. Vous pouvez écraser ce paramètre en activant le bouton bascule à côté de l'option **Exécuter même si l'ordinateur est alimenté par batterie** dans Configuration avancée.

Activez le bouton bascule en regard de **Activer la journalisation** dans la Configuration avancée pour enregistrer le résultat de l'analyse de l'ordinateur dans la section Fichiers journaux (dans la fenêtre principale du programme, cliquez sur **Outils** > **Fichiers journaux**, puis sélectionnez **Analyse de l'ordinateur** dans le menu déroulant **Journal**).

Détection de l'état inactif

Consulter la rubrique Déclencheurs de détection de l'état inactif pour une liste complète des conditions requises pour que soit déclenché l'analyseur en état actif.

ThreatSense : options de configuration avancées, telles que les extensions de fichier que vous souhaitez contrôler et les méthodes de détection utilisées. Voir ThreatSense pour plus d'informations.

Détection de l'état inactif

Vous pouvez configurer les paramètres de détection de l'état inactif dans Configuration avancée > **Moteur de détection** > **Analyses de logiciels malveillants** > **Analyse à l'état inactif** > **Détection de l'état inactif**. Ces paramètres définissent un déclencheur pour l'analyse en état inactif :

- **Écran ou écran de veille désactivé**
- **Verrouillage de l'ordinateur**
- **Fermeture de session de l'utilisateur**

Utilisez le bouton bascule pour chaque état respectif afin d'activer ou de désactiver les différents déclencheurs de détection de l'état d'inactivité.

Analyse au démarrage

La vérification automatique des fichiers de démarrage sera effectuée par défaut au démarrage du système et pendant la mise à jour du moteur de détection. Cette analyse dépend de la configuration et des tâches du Planificateur.

Les options pour l'analyse au démarrage font partie d'une tâche du planificateur axée sur le **contrôle des fichiers de démarrage du système**. Pour modifier ses paramètres, accédez à **Outils** > **Planificateur**, cliquez sur **Vérification automatique des fichiers au démarrage**, puis sur **Modifier**. Une fenêtre Vérification automatique des fichiers de démarrage s'affichera ensuite. Pour des instructions détaillées sur la création et la gestion des tâches dans le Planificateur, consultez la section Création de nouvelles tâches.

ThreatSense : options de configuration avancées, telles que les extensions de fichier que vous souhaitez contrôler

et les méthodes de détection utilisées. Voir ThreatSense pour plus d'informations.

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 **Cibles à analyser** indique la profondeur de l'analyse pour les fichiers exécutés au démarrage du système selon un algorithme sophistiqué. Les fichiers sont classés en ordre décroissant, selon les critères suivants :

- **Tous les fichiers enregistrés** (le plus grand nombre de fichiers analysés)
- **Fichiers rarement utilisés**
- **Fichiers couramment utilisés**
- **Fichiers fréquemment utilisés**
- **Seulement les fichiers les plus fréquemment utilisés** (le plus petit nombre de fichiers analysés)

Deux groupes spécifiques sont aussi inclus :

- **Fichiers exécutés avant la connexion de l'utilisateur** - Contient les fichiers enregistrés dans des emplacements qui permettent d'y accéder sans que l'utilisateur n'ait ouvert de session (comprend presque tous les emplacements de démarrage comme les services, les objets application d'assistance du navigateur, la notification winlogon, les entrées dans le planificateur de Windows, les dll connus, etc.).
- **Fichiers exécutés après la connexion de l'utilisateur** - Contient les fichiers enregistrés dans des emplacements qui permettent d'y accéder seulement que lorsque l'utilisateur a ouvert une session. Comprend généralement les fichiers enregistrés dans le dossier *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Les listes de fichiers à analyser sont corrigées pour chaque groupe ci-dessus. Si vous choisissez une profondeur d'analyse inférieure pour les fichiers exécutés au démarrage du système, les fichiers non analysés le seront à leur ouverture ou exécution.

Priorité de l'analyse - Le niveau de priorité à utiliser pour déterminer à quel moment débutera l'analyse :

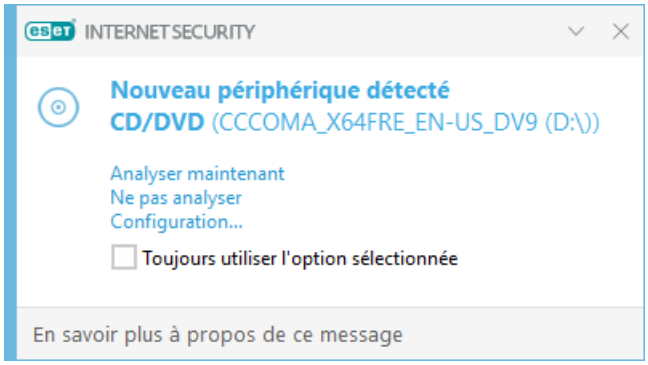
- **Quand inactif** - La tâche ne sera exécutée que lorsque le système sera inactif,
- **Minimale** - Lorsque la charge système est la plus faible possible.
- **Faible** - Lorsque la charge système est faible.
- **Normal** - Pour une charge système moyenne.

Supports amovibles

ESET Internet Security effectue une analyse automatique des supports amovibles (CD/DVD/USB/...) lorsqu'ils sont insérés dans un ordinateur. Cela peut être utile si l'administrateur de l'ordinateur veut empêcher les utilisateurs

d'utiliser des supports amovibles comportant un contenu non sollicité.

Lorsqu'un support amovible est inséré, et que l'option **Afficher les options d'analyse** est activée dans Configuration avancée > **Moteur de détection** > **Analyse des logiciels malveillants** > **Supports amovibles**, la boîte de dialogue suivante s'affiche :



Options pour cette boîte de dialogue :

- **Analyser maintenant** - Déclenche l'analyse du support amovible.
- **Ne pas analyser** – Les supports amovibles ne seront pas analysés.
- **Configuration** - Ouvre la configuration avancée.
- **Toujours utiliser l'option sélectionnée** - Lorsque cette case est cochée, la même action sera effectuée la prochaine fois qu'un support amovible sera inséré.

De plus, ESET Internet Security comprend également la fonctionnalité de contrôle du périphérique qui offre la possibilité de définir des règles pour l'utilisation des périphériques externes sur un ordinateur particulier. Vous trouverez plus de détails sur le contrôle de périphérique dans la section Contrôle de périphérique.

Pour accéder aux paramètres d'analyse des supports amovibles, ouvrez Configuration avancée > **Moteur de détection** > **Recherche de logiciels malveillants** > **Supports amovibles**.

Action à effectuer après l'insertion d'un support amovible - Sélectionnez l'action par défaut qui sera effectuée lorsqu'un support amovible est inséré dans l'ordinateur (CD/DVD/USB). Choisissez l'action souhaitée lorsqu'un support amovible est inséré dans un ordinateur :

- **Ne pas analyser** - Aucune action ne sera effectuée et la fenêtre **Nouveau périphérique détecté** ne s'ouvrira pas.
- **Analyse automatique du périphérique** - Une analyse informatique du support amovible inséré sera effectuée.
- **Afficher les options d'analyse** - Ouvre la section de configuration du **supports amovibles**.

Protection des documents

La fonctionnalité de protection des documents analyse les documents Microsoft Office avant leur ouverture, comme les fichiers téléchargés automatiquement par Internet Explorer, tels que les éléments Microsoft ActiveX. La protection des documents offre une couche de protection, en plus de la protection en temps réel du système de fichiers et peut être désactivée afin d'améliorer la performance de systèmes qui ne gèrent pas un volume élevé de documents Microsoft Office.

Pour activer la protection des documents, ouvrez la fenêtre Configuration avancées > **Moteur de détection** > **Analyse de logiciels malveillants** > **Protection des documents** et cliquez sur le bouton bascule en regard de **Activer la protection des documents**.

ThreatSense : options de configuration avancées, telles que les extensions de fichier que vous souhaitez contrôler et les méthodes de détection utilisées. Voir ThreatSense pour plus d'informations.

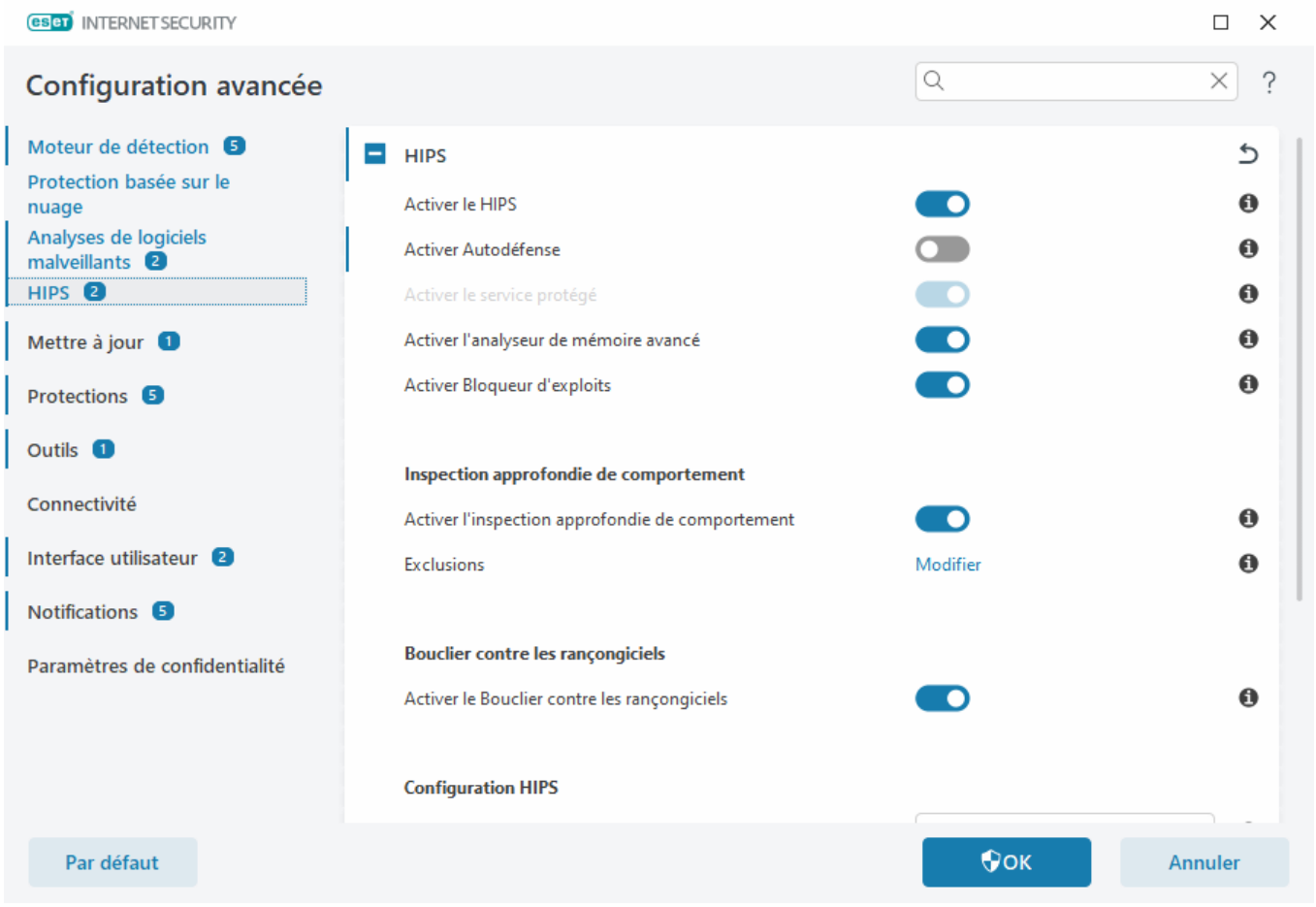
Cette fonctionnalité est activée par des applications utilisant Microsoft Antivirus API (par ex., Microsoft Office 2000 et les versions ultérieures ou Microsoft Internet Explorer 5.0 et les versions ultérieures).

HIPS – Host Intrusion Prevention System

Seul un utilisateur d'expérience devrait apporter des modifications aux paramètres de HIPS. Une mauvaise configuration des paramètres HIPS peut rendre le système instable.

Le **Système de prévention des intrusions sur l'ordinateur hôte** (HIPS) protège votre système des logiciels malveillants ou de toute activité indésirable qui tentent de de nuire à votre ordinateur. Il utilise, pour ce faire, une analyse comportementale évoluée combinée aux fonctionnalités de détection de filtrage du réseau utilisées dans la surveillance des processus en cours, fichiers et 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.

Vous pouvez configurer les paramètres HIPS dans Configuration avancée > **Moteur de détection** > **HIPS** > **Host Intrusion Prevention System (Système de prévention des intrusions dans l'hôte)**. L'état du HIPS (activé/désactivé) s'affiche dans la fenêtre principale du programme ESET Internet Security > **Configuration** > **Protection de l'ordinateur**.



HIPS

Activer HIPS – HIPS est activé par défaut dans ESET Internet Security. La désactivation de HIPS désactivera le reste des fonctionnalités HIPS telles que le Bloqueur d'exploit.

Activer Autodéfense – ESET Internet Security comporte une technologie d'**autodéfense** intégrée faisant partie de HIPS qui empêche les logiciels malveillants de corrompre ou de désactiver votre protection antivirus et anti-logiciel espion. L'autodéfense protège le système crucial et les processus d'ESET, les clés de registre et les fichiers contre les falsifications.

Activer le service protégé - Active la protection du Service ESET (ekrn.exe). Lorsqu'il est activé, le service est démarré en tant que processus Windows protégé pour défendre les attaques de logiciels malveillants.

Activer l'analyseur avancé de la mémoire - fonctionne avec le Bloqueur d'exploit pour renforcer la protection contre les logiciels malveillants qui ont été conçus pour contourner la détection par les protection anti-logiciels malveillants en utilisant l'obscurcissement ou le chiffrement. L'analyseur avancé de la mémoire est activé par défaut. Pour en savoir plus sur ce type de protection, consultez le glossaire.

Activer le Bloqueur d'exploit - cette fonction est conçue pour protéger les types d'applications souvent exploités, comme les navigateurs, les lecteurs les PDF, les clients de messagerie et les composants MS Office. Le bloqueur d'exploit est activé par défaut. Pour en savoir plus sur ce type de protection, consultez le glossaire.

Inspection approfondie de comportement

Activer l'inspection approfondie de comportement - Il s'agit d'une autre couche de protection qui fait partie de la fonctionnalité HIPS. Cette extension de HIPS analyse le comportement de tous les programmes en cours

d'exécution sur l'ordinateur et vous avertit si le comportement du processus est malveillant.

Les exclusions HIPS de l'inspection approfondie de comportement vous permettent d'exclure des processus de l'analyse. Pour s'assurer que tous les processus sont analysés à la recherche de menaces possibles, nous recommandons de ne créer des exclusions que lorsque cela est absolument nécessaire.

Bouclier anti-rançongiciel

Activer le Bouclier anti-rançongiciels - il s'agit d'une autre couche de protection qui fait partie de la fonctionnalité HIPS. Le système de réputation ESET LiveGrid® doit être activé pour que le bouclier anti-rançongiciels fonctionne. Pour en savoir plus sur ce type de protection, consultez le lien suivant.

Activer Intel® Threat Detection Technology : elle permet de détecter les attaques de rançongiciels en utilisant la télémétrie unique des processeurs Intel pour augmenter l'efficacité de la détection, réduire les alertes de faux positifs et étendre la visibilité afin de détecter les techniques d'évasion avancées. Consultez la liste des processeurs pris en charge.

Configuration HIPS

Le **filtrage** peut être effectué selon l'un des modes suivants :

Mode de filtrage	Description
Mode automatique	Les opérations sont activées, à l'exception de celles bloquées par des règles prédéfinies qui protègent votre système.
Mode intelligent	L'utilisateur ne sera informé que des événements vraiment suspects.
Mode interactif	L'utilisateur sera invité à confirmer les opérations.
Mode basé sur des règles personnalisées	Boque toutes les opérations qui ne sont pas définies par une règle précise qui les autorise.
Mode d'apprentissage	Les opérations sont activées et une règle est créée, après chaque opération. Les règles créées dans ce mode peuvent être affichées dans l'Éditeur des **Règles HIPS**, mais leur priorité sera inférieure aux règles créées manuellement ou en mode automatique. Lorsque vous sélectionnez le **mode d'apprentissage** dans le menu déroulant **Mode de filtrage** HIPS, le paramètre **Mode d'apprentissage se termine le** devient disponible. Sélectionnez la plage de temps pendant laquelle vous souhaitez que le mode d'apprentissage soit activé; la durée maximale est de 14 jours. Une fois que la durée indiquée sera écoulée, vous serez invité à modifier les règles créées par HIPS alors qu'il était en mode d'apprentissage. Vous pouvez également choisir un mode de filtrage différent, ou reporter la décision et continuer à utiliser le mode d'apprentissage.

Mode défini après l'expiration du mode d'apprentissage - Sélectionnez le mode de filtrage qui sera utilisé après l'expiration du mode d'apprentissage. Après expiration, l'option **Demander à l'utilisateur** nécessite des privilèges administratifs pour effectuer une modification du mode de filtrage HIPS.

Le système HIPS surveille les événements qui se produisent dans le système d'exploitation et réagit à ces derniers en fonction des règles semblables à celles utilisées par le pare-feu. Cliquez sur **Modifier** à côté de **Règles** pour ouvrir l'éditeur des **règles HIPS**. Dans la fenêtre des règles HIPS, vous pouvez sélectionner, ajouter, modifier ou supprimer des règles. Plus de détails sur la création de règles et les opérations HIPS sont disponibles dans Modifier une règle HIPS.

Exclusions HIPS

Les exclusions vous permettent d'exclure des processus de l'inspection comportementale approfondie HIPS (HIPS Deep Behavioral Inspection).

Pour modifier les exclusions HIPS, ouvrez Configuration avancée > **Moteur de détection** > **HIPS** > **Host Intrusion Prevention System (Système de prévention des intrusions dans l'hôte)** > **Exclusions** > **Modifier**.

> Vous ne devez pas les confondre avec les extensions de fichiers exclues, les exclusions de détection, les exclusions de performance ou les exclusions de processus.

Pour exclure un objet, cliquez sur **Ajouter** et entrez le chemin d'accès à un objet ou sélectionnez-le dans l'arborescence. Vous pouvez également modifier ou supprimer les entrées sélectionnées.

Configuration avancée de HIPS

Les options suivantes sont utiles pour déboguer et analyser le comportement d'une application :

Le chargement des pilotes est toujours autorisé - Le chargement des pilotes sélectionnés est toujours autorisé, indépendamment du mode de filtrage défini, à l'exception des cas où un pilote est explicitement bloqué par une règle de l'utilisateur.

Enregistrez toutes les opérations bloquées - Toutes les opérations bloquées seront écrites dans le journal HIPS. Utilisez cette fonctionnalité uniquement lors du dépannage ou à la demande du service d'assistance technique d'ESET, car elle peut générer un énorme fichier journal et ralentir votre ordinateur.

Aviser lorsqu'un changement est effectué dans les applications de démarrage - Affiche une notification sur le bureau chaque fois qu'une application est ajoutée au démarrage du système ou supprimée lors de celui-ci.

Le chargement des pilotes est toujours autorisé

Les pilotes affichés dans cette liste pourront toujours être chargés indépendamment du mode de filtrage HIPS, à moins qu'ils soient explicitement bloqués par une règle de l'utilisateur.

Ajouter - Permet d'ajouter un nouveau pilote.

Modifier - Permet de modifier le pilote sélectionné.

Retirer - Permet de supprimer des pilotes de la liste.

Réinitialiser - Permet de recharger un ensemble de pilotes système.

> Cliquez sur **Réinitialiser** si vous ne voulez pas que les pilotes que vous avez ajoutés manuellement soient inclus. Cela peut être utile si vous avez ajouté plusieurs pilotes et ne pouvez pas les supprimer de la liste manuellement.

> Après l'installation, la liste des pilotes est vide. ESET Internet Security remplit automatiquement la liste au fil du temps.

Fenêtre interactive HIPS

La fenêtre de notification HIPS vous permet de créer une règle basée sur les nouvelles actions détectées par HIPS, puis de définir les conditions dans lesquelles autoriser ou refuser cette action.

Les règles créées à partir de la fenêtre de notification sont jugées équivalentes aux règles créées manuellement. Une règle créée à partir d'une fenêtre de notification peut être moins précise que la règle qui a déclenché la fenêtre de dialogue. Cela signifie qu'après la création d'une règle dans la boîte de dialogue, la même opération peut déclencher la même fenêtre. Pour plus d'informations, consultez Priorité pour les règles HIPS.

Si l'action par défaut pour une règle est mise à **Demander chaque fois**, une boîte de dialogue s'affichera chaque fois que la règle est déclenchée. Vous pouvez choisir de **Refuser** ou d'**Autoriser** l'opération. Si aucune action n'est sélectionnée dans le temps imparti, une nouvelle action sera sélectionnée, en fonction des règles.

Mémoriser jusqu'à la fermeture de l'application provoque le recours à une action (**Autoriser/Refuser**) qui devra être utilisée 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.

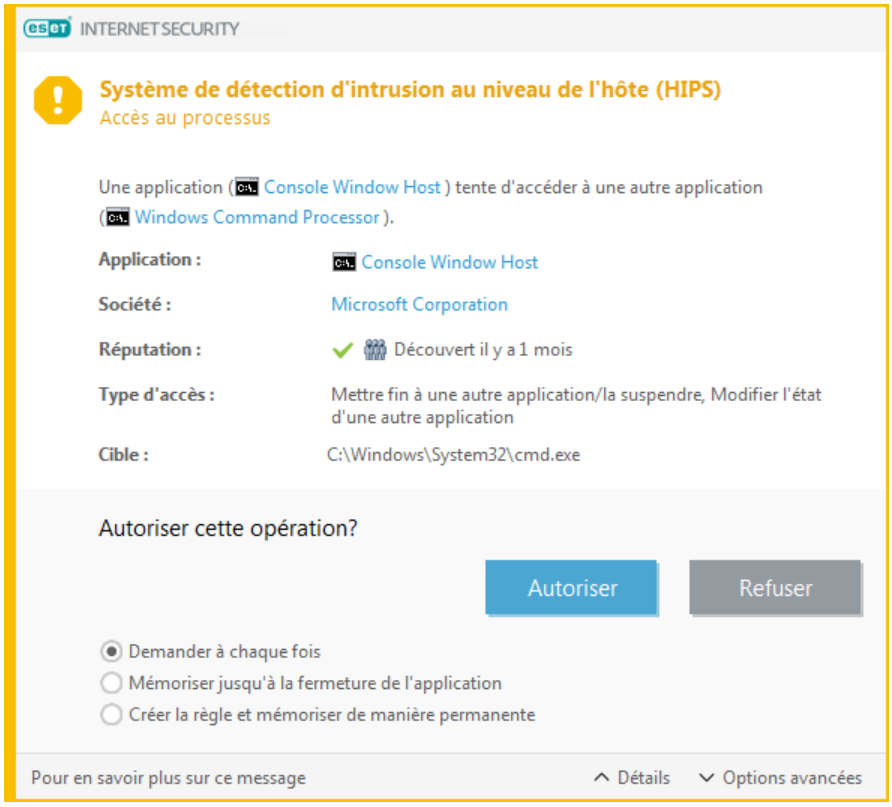
L'option **Créer une règle et se souvenir de manière permanente** créera une nouvelle règle HIPS qui pourra être modifiée ultérieurement dans la section Gestion des règles IHPS (requiert des privilèges d'administration).

Cliquez sur **Détails** en bas pour voir quelle application déclenche l'opération, quelle est la réputation du fichier ou quel type d'opération il vous est demandé d'autoriser ou de refuser.

Vous pouvez accéder aux paramètres de règle plus détaillés en cliquant sur **Options avancées**. Les options ci-dessous sont disponibles si vous choisissez **Créer une règle et se souvenir de manière permanente** :

- **Créer une règle valide seulement pour cette application** - Si vous décochez cette case, la règle sera créée pour toutes les applications source.
- **Uniquement pour l'opération** – Choisissez un fichier de règles / une application/une ou plusieurs opérations de registre. Voir les descriptions pour toutes les opérations HIPS.
- **Uniquement pour la cible** - Choisissez un fichier de règles/une application/ des cibles de registre.

> **Notifications HIPS sans fin ?**
> Pour que les notifications n'apparaissent pas, mettez le mode de filtrage sur **Mode automatique** dans Configuration avancée > **Moteur de détection** > **HIPS** > **Host Intrusion Prevention System**.



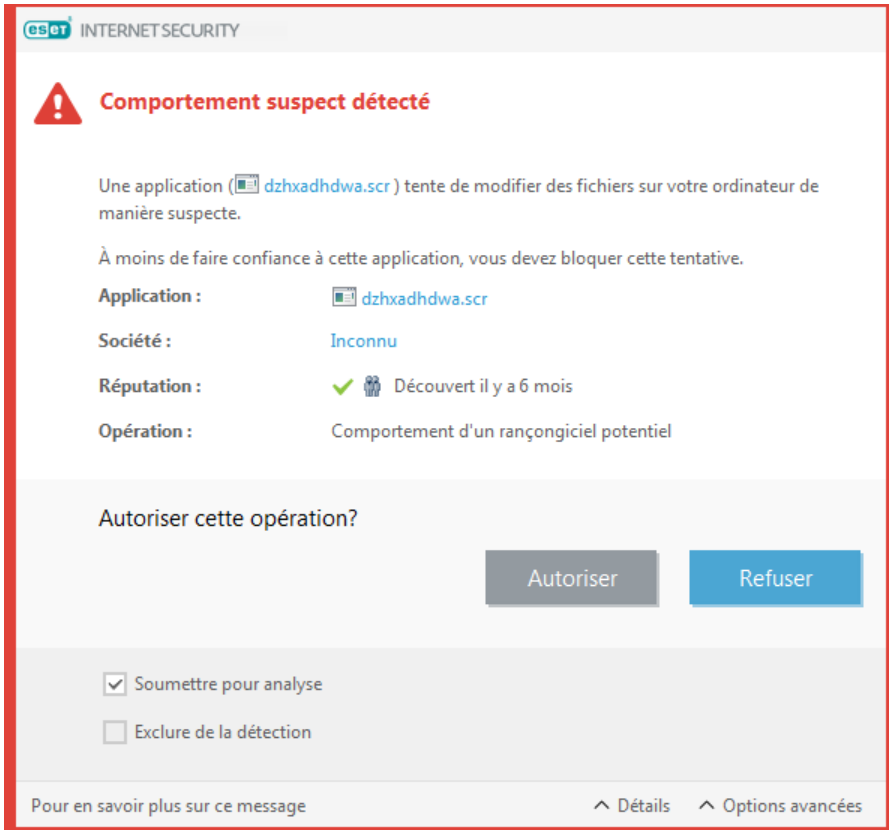
Fin du mode d’apprentissage

Le mode d’apprentissage crée et enregistre automatiquement des règles. Vous pouvez vérifier toutes les règles créées dans les paramètres de règle HIPS. Ce mode est mieux utilisé pour la configuration initiale de HIPS, mais ne doit être conservé que pendant une courte période. Aucune intervention de l'utilisateur n'est requise car ESET Internet Security enregistre les règles conformément aux paramètres prédéfinis. Passez en mode **interactif** ou **basé sur des règles personnalisées** une fois que toutes les règles pour les processus requis s’exécutant dans le système d’exploitation ont été créées pour éviter les risques à la sécurité.

Vous pouvez reporter cette décision si vous ne souhaitez pas modifier les paramètres.

Comportement d'un rançongiciel potentiel détecté

Cette fenêtre interactive apparaîtra lorsque le comportement d'un potentiel rançongiciel est détecté. Vous pouvez choisir de **Refuser** ou d'**Autoriser** l'opération.



Cliquez sur **Détails** pour afficher des paramètres de détection spécifiques. La boîte de dialogue vous permet d'**envoyer pour analyse** ou d'**exclure de la détection**.

ESET LiveGrid® doit être activé pour que la protection contre les rançongiciels fonctionne correctement.

Gestion des règles HIPS

Il s'agit d'une liste de règles définies par l'utilisateur et automatiquement ajoutées à partir du système HIPS. Plus de détails sur la création de règles et des opérations HIPS se trouvent dans le chapitre Paramètres de règle HIPS. Vous pouvez consultez aussi Principe général des HIPS.

Colonnes

Règle - Nom de la règle défini par l'utilisateur ou choisi automatiquement.

Activée : désactivez ce bouton bascule si vous voulez que la règle reste inscrite sur la liste, mais sans l'utiliser.

Action - La règle spécifie une action - **Autoriser**, **Bloquer** ou **Demander** - qui devrait être exécutée lorsque les conditions sont satisfaites.

Sources - La règle ne sera utilisée que si l'événement est déclenché par cette ou ces applications.

Cibles - La règle sera utilisée uniquement si l'opération est liée à un fichier, à une application ou à une entrée de registre spécifique.

Journalisation de la gravité - Si vous activez cette option, l'information connexe à cette règle sera inscrite dans le journal HIPS.

Notifier : une petite fenêtre de notification s'affichera dans le coin inférieur droit, lorsqu'un événement est déclenché.

Éléments de contrôle

Ajouter - Crée une nouvelle règle.

Modifier - Permet de modifier les entrées sélectionnées.

Supprimer - Supprime les entrées sélectionnées.

Priorité pour les règles HIPS

Il n'y a pas d'options pour ajuster le niveau de priorité des règles HIPS à l'aide des boutons haut/bas (comme c'est le cas pour les règles de pare-feu où les règles sont exécutées de haut en bas).

- Toutes les règles que vous créez ont la même priorité
- Plus la règle est spécifique, plus la priorité est élevée (par exemple, la règle qui s'applique à une application en particulier a une priorité supérieure à celle qui s'applique à toutes les applications).
- En interne, le système HIPS contient des règles de priorité supérieure qui ne vous sont pas accessibles (par exemple, vous ne pouvez pas écraser les règles définies pour l'autodéfense).
- Une règle que vous créez et qui pourrait geler votre système d'exploitation ne sera pas appliquée (aura la priorité la plus basse)

Modifier une règle HIPS

Voir d'abord la gestion des règles HIPS.

Nom de la règle - Nom de la règle défini par l'utilisateur ou choisi automatiquement.

Action - La règle précise une action - **Autoriser**, **Bloquer** ou **Demander** - qui doit être effectuée lorsque les conditions sont satisfaites.

Opérations concernées - Vous devez sélectionner le type d'opérations auquel s'appliquera la règle. La règle ne sera utilisée pour ce type d'opération et pour la cible sélectionnée.

Activé : désactivez ce bouton bascule si vous voulez conserver la règle dans la liste sans l'appliquer.

Journalisation de la gravité - Si vous activez cette option, l'information connexe à cette règle sera inscrite dans le journal HIPS.

Notifier l'utilisateur : une petite fenêtre de notification s'affichera dans le coin inférieur droit, lorsqu'un événement est déclenché.

La règle comporte plusieurs parties qui décrivent les conditions qui la déclenchent :

Applications sources - La règle ne sera utilisée que si l'événement est déclenché par cette ou ces applications. Sélectionnez **Applications spécifiques** dans le menu déroulant et cliquez sur **Ajoute**r pour ajouter de nouveaux

fichiers. Vous pouvez également sélectionner **Toutes les applications** dans le menu déroulant pour ajouter toutes les applications.

Fichiers cibles : La règle ne sera utilisée que si l'opération est liée à cette cible. Sélectionnez **Fichiers spécifiques** dans le menu déroulant et cliquez sur **Ajouter** pour ajouter de nouveaux fichiers ou dossiers. Vous pouvez également sélectionner **Tous les fichiers** dans le menu déroulant pour ajouter tous les fichiers.

Applications - La règle ne sera utilisée que si l'opération est liée à cette cible. Sélectionnez **Applications spécifiques** dans le menu déroulant et cliquez sur **Ajouter** pour ajouter de nouveaux fichiers ou dossiers. Vous pouvez également sélectionner **Toutes les applications** dans le menu déroulant pour ajouter toutes les applications.

Entrées du régistre - La règle ne sera utilisée que si l'opération est liée à cette cible. Sélectionnez **Entrées spécifiques** dans le menu déroulant et cliquez sur **Ajouter** pour les entrer manuellement. Vous pouvez également cliquer sur **Ouvrir l'éditeur de registre** pour sélectionner une clé dans le registre. Vous pouvez également sélectionner **Toutes les entrées** dans le menu déroulant pour ajouter toutes les applications.

> Certaines opérations de règles spécifiques prédéfinies par HIPS ne peuvent pas être bloquées et sont autorisées par défaut. En plus, toutes les opérations système ne sont pas contrôlées par HIPS. HIPS contrôle les opérations qui peuvent être considérées comme dangereuses.

Description d'opérations importantes :

Opérations sur le fichier

- **Supprimer le fichier** - L'application vous invite à autoriser la suppression du fichier cible.
- **Écrire dans le fichier** - L'application vous invite à autoriser l'écriture dans le fichier cible.
- **Accès direct au disque** - L'application tente de lire ou d'écrire sur le disque d'une manière non standard, qui contournera les procédures courantes de Windows. Cela peut entraîner la modification de fichiers sans application des règles correspondantes. Cette opération peut découler d'un logiciel malveillant qui tente d'éviter la détection, d'un logiciel de sauvegarde qui essaie de faire une copie exacte d'un disque ou d'un gestionnaire de partitions qui tente de réorganiser des volumes de disque.
- **Installer le crochet global** - Se réfère à l'appel de la fonctionSetWindowsHookEx de la bibliothèque MSDN.
- **Charger pilote** - Installation et chargement de pilotes dans le système.

Activités de l'application

- **Déboguer une autre application** - Joindre un débogueur au processus. Lors du débogage d'une application, de nombreux détails de son comportement peuvent être affichés et modifiés et ses données deviennent accessibles.
- **Intercepter des événements à partir d'une autre application** - L'application source tente d'intercepter des événements destinés à une application spécifique (par exemple un enregistreur de frappe qui tente de capturer les événements d'un navigateur).
- **Mettre fin à une autre application/la suspendre** - Suspendre, reprendre ou arrêter un processus (accès direct par l'explorateur de processus ou le volet Processus).

• **Lancer une nouvelle application** - Lancement de nouvelles applications ou de nouveaux processus.

• **Modifier l'état d'une autre application** - L'application source tente d'écrire dans la mémoire de l'application cible ou d'exécuter du code en son nom. Cette fonctionnalité peut être utile pour protéger une application essentielle en la configurant comme application cible dans une règle qui bloque l'utilisation de cette opération.

Opérations sur le registre

• **Modifier les paramètres de démarrage** - Toutes les modifications des paramètres qui définissent quelles applications seront exécutées au démarrage de Windows. Il est possible de les trouver, par exemple, en recherchant la cléRun dans le registre de Windows.

• **Supprimer du registre** - Supprimer une clé de registre ou sa valeur.

• **Renommer la clé de registre** - Renomme les clés de registre.

• **Modifier le registre** - Créer de nouvelles valeurs de clés de registre, modifier des valeurs existantes, déplacer des données dans l'arborescence de la base de données ou définir les droits du groupe ou de l'utilisateur à l'égard de clés de registre.

Vous pouvez utiliser des caractères génériques avec certaines restrictions au moment d'entrer une cible. Plutôt qu'une clé particulière, vous pouvez utiliser un symbole * (astérisque) dans les chemins d'accès du registre. Par exemple, *HKEY_USERS*\software* peut vouloir dire *HKEY_USER\.default\software*, mais non *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*.
*HKEY_LOCAL_MACHINE\system\ControlSet** n'est pas un chemin d'accès à la clé du registre valide. Un chemin d'accès à la clé du registre contenant * définit « ce chemin d'accès, sur tout niveau, après ce symbole ». C'est la seule façon d'utiliser les caractères génériques pour les fichiers cibles. La partie spécifique d'un chemin sera la première à être évaluée, puis elle sera suivie du chemin se trouvant après le caractère générique (*).

Si vous créez une règle très générique, l'avertissement sur ce type de règle s'affiche.

Dans l'exemple suivant, nous allons illustrer comment limiter le comportement indésirable d'une application précise :

1. Nommez la règle et sélectionnez **Bloquer** (ou **Demander** si vous désirez choisir plus tard) dans le menu déroulant **Action**.

2. Activez le bouton bascule situé à côté de **Avertir l'utilisateur** pour afficher une notification chaque fois qu'une règle est appliquée.

3. Sélectionnez au moins une opération dans la section **Opérations concernées** pour laquelle la règle sera appliquée.

4. Cliquez sur **Suivant**.

5. Dans la fenêtre **Applications sources**, sélectionnez **Applications précises** dans le menu déroulant pour appliquer la nouvelle règle à toutes les applications qui tentent d'effectuer l'une des opérations sélectionnées parmi celles spécifiées.

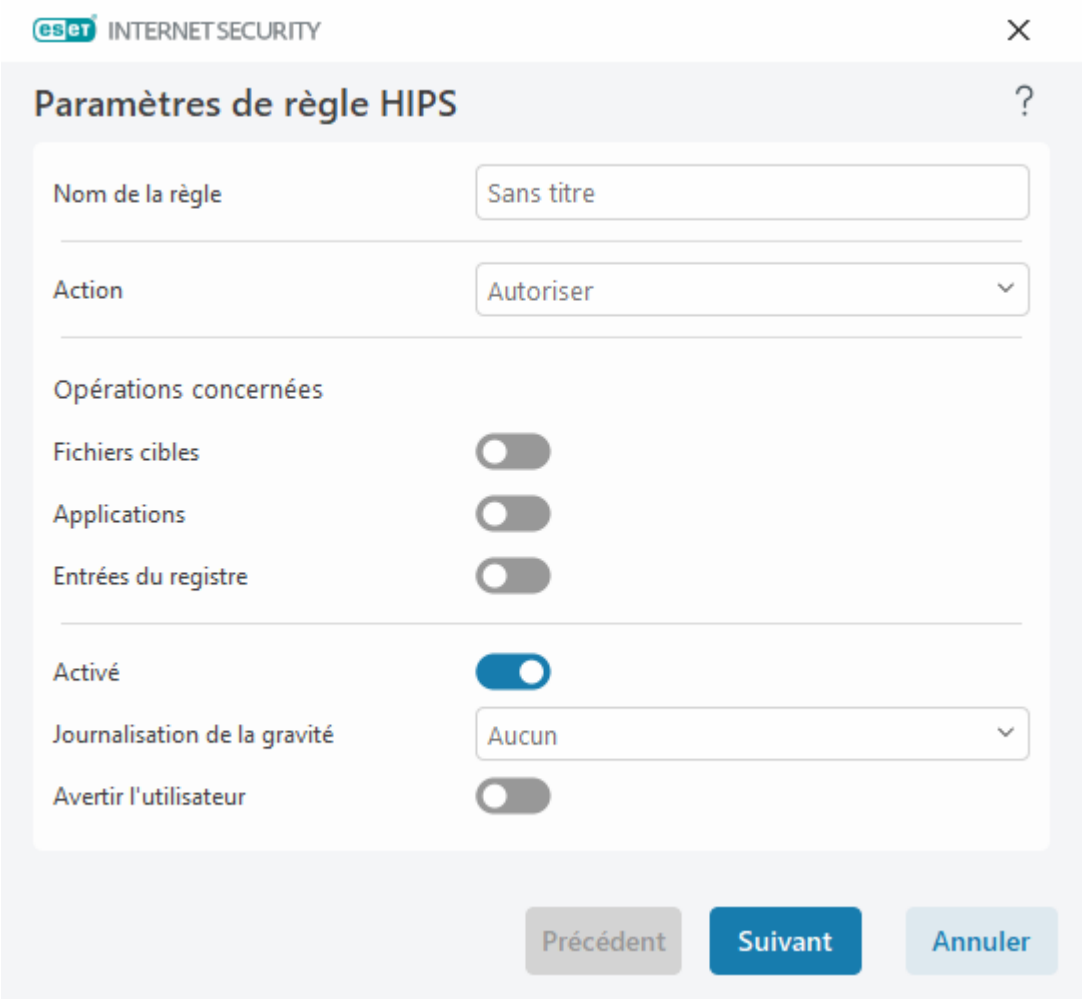
6. Cliquez sur **Ajouter** puis sur **...** pour choisir le chemin d'accès à une application spécifique et appuyez sur

OK. Ajoutez d'autres applications si vous le souhaitez.
Par exemple : *C:\Program Files (x86)\Untrusted application\application.exe*

7. Sélectionnez l'opération**Écrire dans un fichier**

8. Sélectionnez **Tous les fichiers** dans le menu déroulant. Cela bloquera toute tentative d'écriture dans un fichier par l'application ou les applications sélectionnées à l'étape précédente.

9. Cliquez sur **Terminer** pour enregistrer la nouvelle règle.



Ajout d'application/chemin d'accès au registre pour HIPS

Sélectionnez un chemin d'accès à l'application en cliquant sur l'option **...**. Lorsque vous sélectionnez un dossier, toutes les applications situées dans ce dossier sont incluses.

L'option **Ouvrir l'éditeur de registre** ouvrira le l'éditeur du Registre de Windows (regedit.exe). Lorsque vous ajoutez un chemin d'accès au registre, assurez-vous d'entrer l'emplacement approprié dans le champ **Valeur**.

Exemples d'un chemin d'accès au fichier ou au registre :

- *C:\Program Files\Internet Explorer\iexplore.exe*

- *HKEY_LOCAL_MACHINE\system\ControlSet*

Mettre à jour

Les options de configuration de mise à jour sont disponibles dans Configuration avancée > **Mettre à jour**. Cette section permet de préciser l'information sur les sources des mises à jour, comme les serveurs de mise à jour utilisés et les données d'authentification donnant accès à ces serveurs.

Mettre à jour

Le profil de mise à jour actuellement utilisé s'affiche dans le menu déroulant **Sélectionner le profil de mise à jour par défaut**.

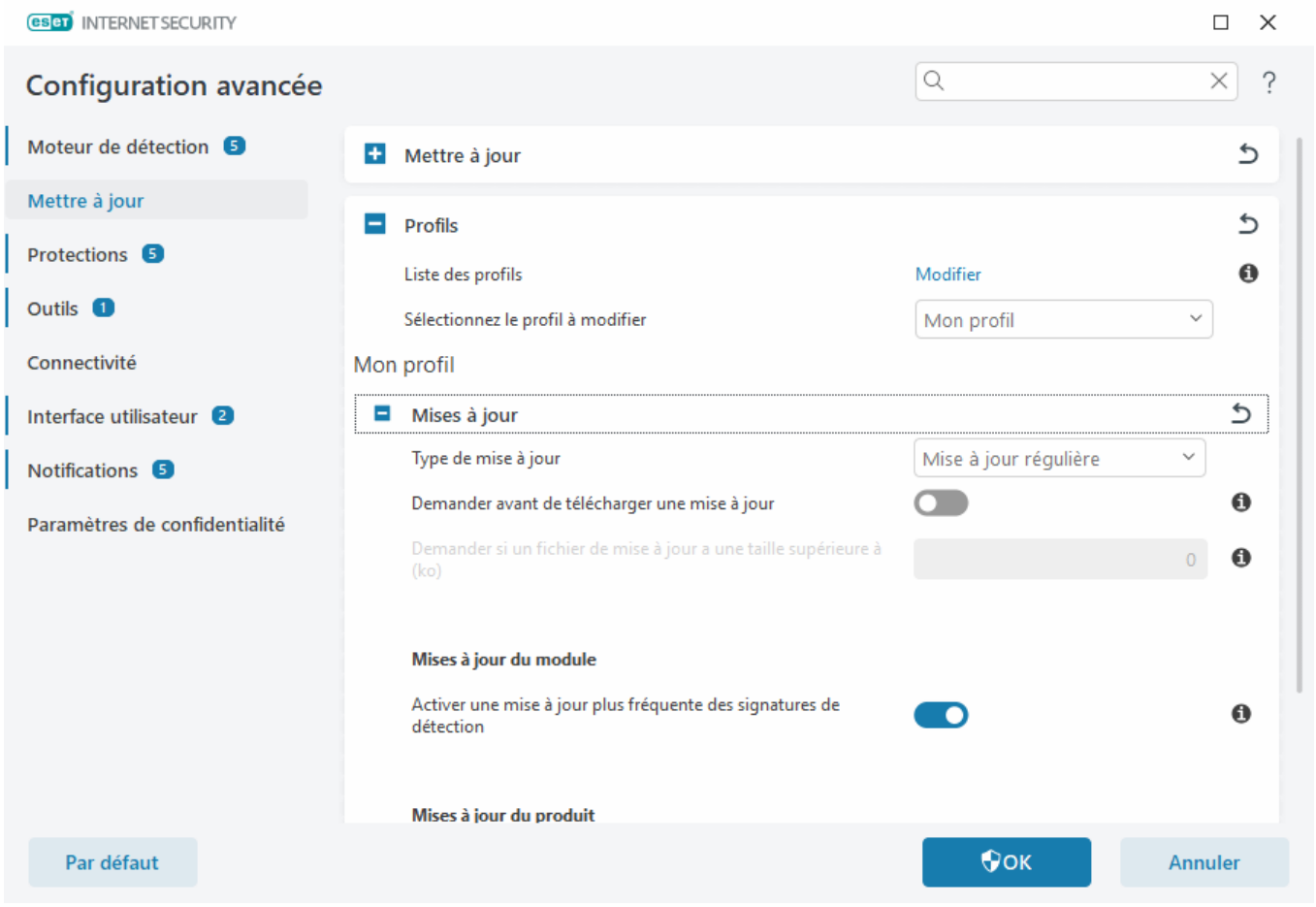
Pour créer un nouveau profil, consultez la section Profils de mise à jour.

Commutation automatique de profil : cette option vous permet d'affecter un profil de mise à jour à un profil de connexion réseau spécifique.

Si vous éprouvez des difficultés à télécharger les mises à jour du moteur de détection ou d'un module, cliquez sur **Supprimer** situé à côté de **Effacer le cache de mise à jour** pour supprimer les fichiers temporaires ou le cache de mise à jour.

Annuler les modifications du module

Si vous soupçonnez qu'une nouvelle mise à jour du moteur de détection et/ou des modules du programme peut être instable ou endommagée, vous pouvez retourner à la version antérieure et désactiver toutes les mises à jour pour une durée choisie.



Il est essentiel d'inscrire correctement tous les paramètres de mise à jour afin de télécharger correctement les mises à jour. Si un pare-feu est utilisé, assurez-vous que le programme ESET est autorisé à accéder à Internet (par exemple. communication HTTP).

Profils

Les profils de mise à jour peuvent être créés pour différentes configurations et tâches de mise à jour. Les propriétés des connexions Internet étant variables, la création de profils de mise à jour est particulièrement utile pour les utilisateurs mobiles.

Le menu déroulant **Sélectionner le profil à modifier** affiche le profil actuellement sélectionné et est réglé par défaut à **Mon profil**. Pour créer un nouveau profil, cliquez sur **Modifier** à côté de **Liste des profils**, entrez votre propre **nom de profil**, puis cliquez sur **Ajouter**.

Mises à jour

Par défaut, le menu **Type de mises à jour** est réglé à **Mise à jour régulière** afin de s'assurer que les fichiers de mise à jour sont automatiquement téléchargés à partir du serveur ESET avec le moins de trafic réseau possible. Les préversions des mises à jour (l'option **Préversion de la mise à jour**) sont des mises à jour ayant subi des tests internes approfondis et qui seront bientôt offertes au public. Vous pouvez profiter de l'activation des préversions des mises à jour en accédant aux méthodes de détection et les solutions les plus récentes. Le mode test peut cependant ne pas toujours être assez stable et ne DOIT PAS être utilisé sur les serveurs et postes de travail de production où une disponibilité et une stabilité maximales sont requises.

Demander avant de télécharger une mise à jour – Le programme affichera une notification dans laquelle vous pouvez choisir de confirmer ou de refuser le téléchargement du fichier de mise à jour.

Demander si une taille de fichier de mise à jour est supérieure à (Ko) : Le programme affichera une boîte de dialogue de confirmation si la taille du fichier est supérieur à la valeur spécifiée. Si la taille du fichier de mise à jour est fixée à 0 ko, le programme affichera toujours une boîte de dialogue de confirmation.

Mises à jour du module

Activer une mise à jour plus fréquente des signatures de détection – Les signatures de détection seront mises à jour dans un intervalle plus court. La désactivation de ce paramètre peut avoir un impact négatif sur le taux de détection.

Mises à jour du produit

Mises à jour des fonctionnalités de l'application – Permet d'installer automatiquement les nouvelles versions de ESET Internet Security.

Option de connexion

Pour utiliser un serveur mandataire pour le téléchargement des mises à jour, consultez la section Options de connexion.

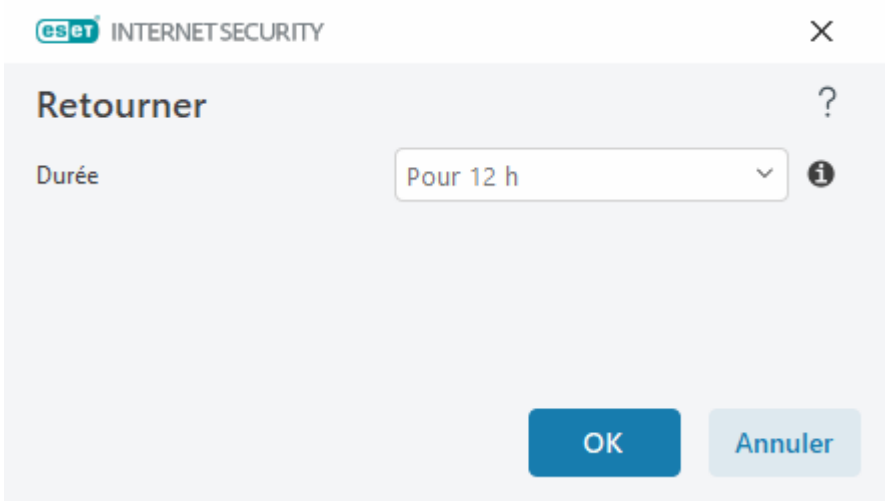
Annulation de la mise à jour

Si vous pensez qu'une nouvelle mise à jour du moteur de détection ou des modules de programme peuvent être instables ou corrompus, vous pouvez revenir à la version précédente et désactiver temporairement les mises à jour. Vous pouvez également activer les mises à jour précédemment désactivées si vous les aviez reportées indéfiniment.

ESET Internet Security enregistre des instantanés du moteur de détection et des modules de programme à utiliser avec la fonction d'annulation. Pour créer des instantanés de base de données de virus, laissez l'option **Créer des instantanés des modules** activée. Lorsque l'option **Créer des instantanés des modules** est activée, le premier instantané est créé lors de la première mise à jour. Le suivant est créé après 48 heures. Le champ **Nombre d'instantanés stockés localement** définit le nombre d'instantanés du moteur de détection stockés.

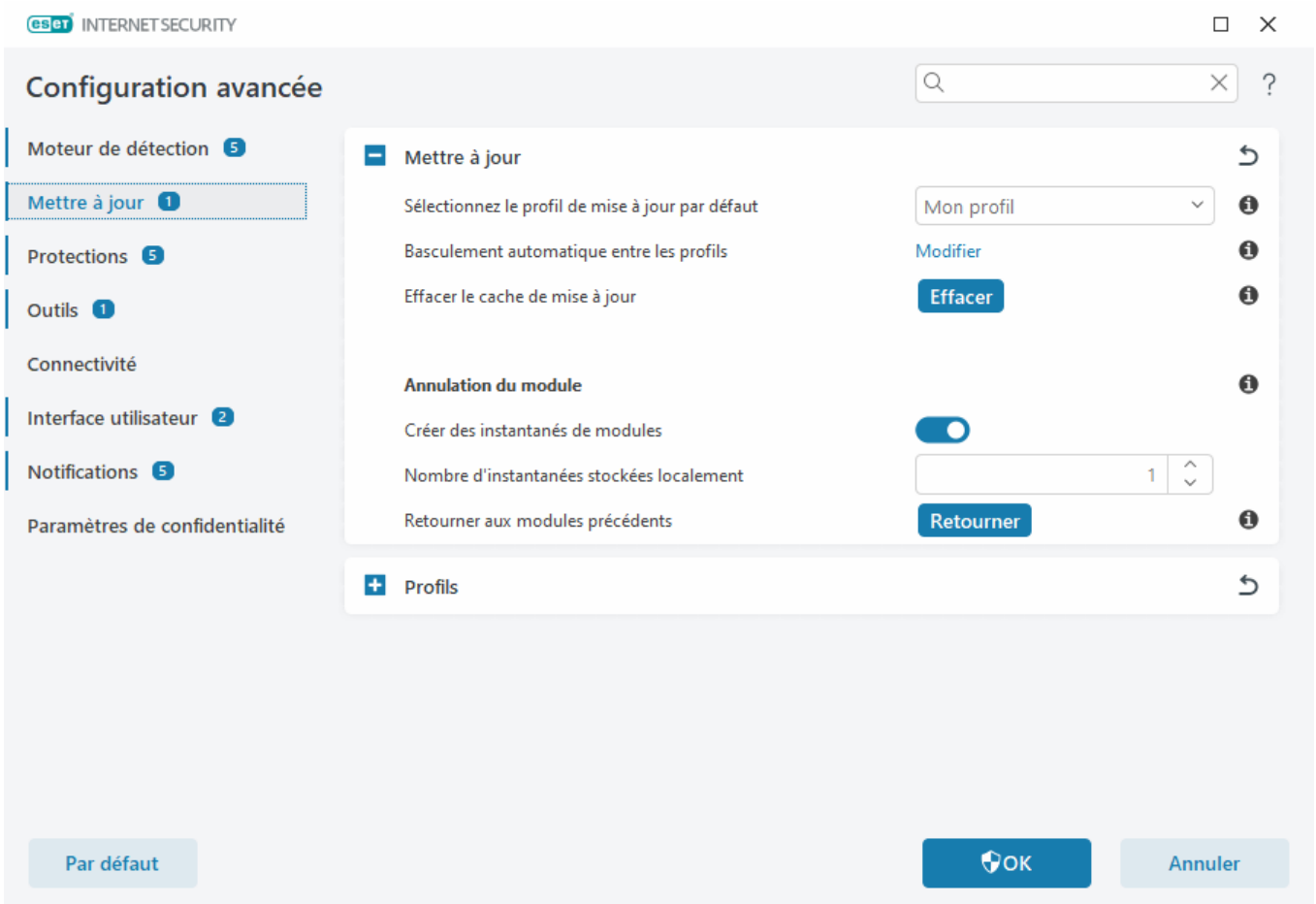
> Lorsque le nombre maximal d'instantanés est atteint (par exemple, trois), l'instantané le plus ancien est remplacé par un nouvel instantané toutes les 48 heures. ESET Internet Security rétablit les versions de mise à jour du moteur de détection et du module de programme à l'instantané le plus ancien.

Si vous cliquez sur **Annuler les modifications** dans Configuration avancée > **Mettre à jour** > **Mettre à jour**, vous devez sélectionner un intervalle dans le menu déroulant **Durée** représentant la durée pendant laquelle les mises à jour du moteur de détection et des modules du programme seront suspendues.



Sélectionnez **Jusqu'à son retrait** pour reporter indéfiniment les mises à jour régulières jusqu'à ce que vous restauriez manuellement cette fonctionnalité. ESET ne recommande pas de sélectionner cette option, puisqu'elle présente un risque potentiel au niveau de la sécurité.

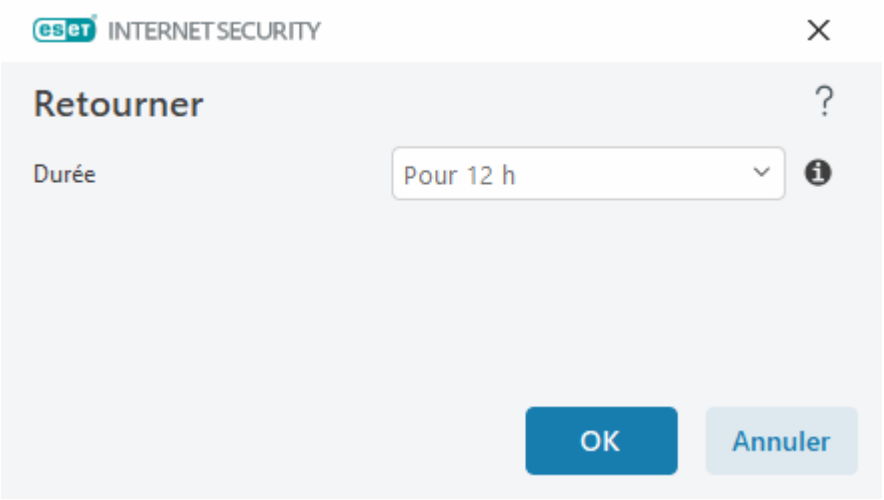
Si les annulations sont effectuées, le bouton **Annuler les modifications** passera à **Permettre les mises à jour**. Aucune mise à jour ne sera permise pendant la durée sélectionnée à partir du menu déroulant **Suspendre les mises à jour**. La version du moteur de détection sera rétablie à la plus ancienne image disponible et stockée comme image dans le système de fichiers de l'ordinateur local.



Supposons que le numéro de version du moteur de détection le plus récent est 22700, et que 22698 et 22696 sont stockés en tant qu'instantanés du moteur de détection. Notez que 22697 n'est pas disponible. Dans cet exemple, l'ordinateur a été éteint lors de la mise à jour 22697 et une mise à jour plus récente a été rendue disponible avant le téléchargement de 22697. Si le champ **Nombre d'instantanés stockés localement** est égal à deux et que vous cliquez sur **Annuler les modifications**, le moteur de détection (y compris les modules de programme) est restauré au numéro de version 22696. Ce processus peut prendre un certain temps. Vérifiez que la version du moteur de détection a été rétrogradée sur l'écran Mettre à jour.

Intervalle de temps pour la restauration

Si vous cliquez sur **Annuler les modifications** dans Configuration avancée > **Mettre à jour** > **Mettre à jour**, vous devez sélectionner un intervalle dans le menu déroulant **Durée** représentant la durée pendant laquelle les mises à jour du moteur de détection et des modules du programme seront suspendues.



Sélectionnez **Jusqu'à son retrait** pour reporter indéfiniment les mises à jour régulières jusqu'à ce que vous restauriez manuellement cette fonctionnalité. ESET ne recommande pas de sélectionner cette option, puisqu'elle présente un risque potentiel au niveau de la sécurité.

Mises à jour du produit

La section **Mises à jour du produit** vous permet d'installer automatiquement de nouvelles mises à jour des fonctionnalités lorsqu'elles sont disponibles.

Les mises à jour des fonctionnalités de l'application apportent de nouvelles fonctionnalités ou modifient celles qui existent déjà sur les versions précédentes. Elles peuvent être effectuées automatiquement sans intervention de l'utilisateur, ou vous pouvez choisir d'en être informé. Après l'installation d'une mise à jour des fonctionnalités de l'application, un redémarrage de l'ordinateur peut être nécessaire.

Mises à jour des fonctionnalités de l'application – Lorsque cette option est activée, les mises à jour des fonctionnalités de l'application s'effectuent automatiquement.

Option de connexion

Pour accéder aux options de configuration du serveur mandataire pour un profil de mise à jour spécifique, ouvrez Configuration avancée > **Mettre à jour** > **Profils** > **Mises à jour** > **Options de connexion**. Cliquez sur le menu déroulant **Mode du mandataire** et sélectionnez l'une des trois options suivantes :

- Ne pas utiliser de serveur mandataire
- Connexion par serveur mandataire
- Utiliser les paramètres globaux de serveur mandataire

Sélectionnez l'option **Utiliser les paramètres globaux de serveur mandataire** pour utiliser les options de configuration du serveur mandataire déjà indiquées dans Configuration avancée > **Connectivité** > **Serveur mandataire**.

Sélectionnez **Ne pas utiliser de serveur mandataire** pour préciser qu'aucun serveur mandataire ne sera utilisé pour mettre ESET Internet Security à jour.

L'option **Connexion par un serveur mandataire** devrait être sélectionnée si :

- Un serveur mandataire différent de celui défini dans Configuration avancée > **Connectivité** est utilisé pour mettre à jour ESET Internet Security. Dans cette configuration, les renseignements du nouveau mandataire doivent être indiqués pour l'adresse du **serveur mandataire**, le **port** de communication (3128 par défaut) ainsi que le **nom d'utilisateur** et le **mot de passe** pour le serveur mandataire si nécessaire.
- Les paramètres du serveur mandataire ne sont pas définis globalement, mais ESET Internet Security se connectera à un serveur mandataire pour les mises à jour.
- Votre ordinateur est connecté à Internet par un serveur mandataire. Les paramètres utilisés sont ceux d'Internet Explorer, pris au moment de l'installation du programme, mais s'ils sont modifiés (par exemple, si vous changez de FAI), vous devez vous assurer que les paramètres du serveur mandataire indiqués dans cette fenêtre sont exacts. En l'absence de modification, le programme ne pourra pas se connecter aux serveurs de mise à jour.

L'option par défaut pour le serveur mandataire est **Utiliser les paramètres globaux du serveur mandataire**.

Utiliser une connexion directe si le mandataire n'est pas disponible - Le serveur mandataire sera contourné pendant la mise à jour s'il n'est pas joignable.

> Les champs **Nom d'utilisateur** et **Mot de passe** dans cette section sont propres au serveur mandataire. Remplissez ces champs uniquement si un nom d'utilisateur et un mot de passe sont requis pour accéder au serveur mandataire. Ces champs ne doivent être remplis que si vous savez que vous avez besoin d'un mot de passe pour accéder à Internet par l'intermédiaire d'un serveur mandataire.

Protections

Protections protège le système contre les attaques malveillantes en contrôlant les échanges de fichiers et de courriels, ainsi que les communications Internet. Par exemple, si un objet classé comme logiciel malveillant est détecté, la correction débute immédiatement. Protections peut l'éliminer en le bloquant d'abord, puis en le

nettoyant, en le supprimant ou en le mettant en quarantaine.

Pour configurer les protections en détail, ouvrez Configuration avancée > **Protections**.

> ⚠ Seul un utilisateur d'expérience devrait apporter des modifications aux Protections. Une mauvaise configuration des paramètres du moteur de détection peut entrainer une réduction du niveau de protection.

Dans cette section :

- Réponses aux détections
- Configuration des signalements
- Configuration de la protection

Réponses aux détections

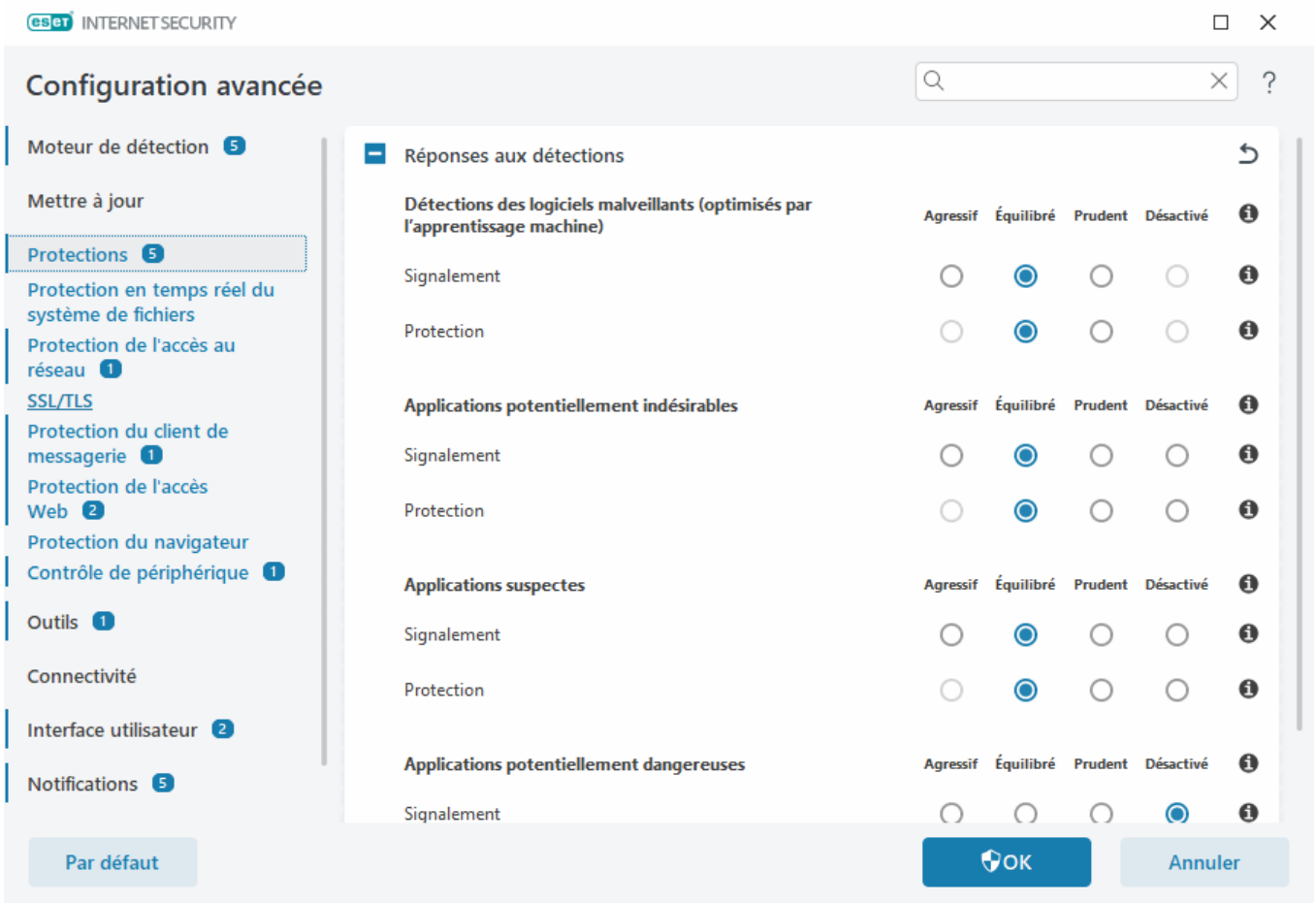
Les réponses de détection vous permettent de configurer les niveaux de protection et la création de rapports pour les catégories suivantes :

- **Détections des logiciels malveillants (optimisés par l'apprentissage machine)** - Un virus informatique est un code malveillant qui a été ajouté à des fichiers se trouvant déjà sur votre ordinateur. Cependant, le terme « virus » est souvent mal utilisé. Logiciel malveillant est une expression plus précise. La détection des logiciels malveillants est effectuée par le module du moteur de détection combiné au composant d'apprentissage automatique. Pour en savoir plus sur ces types d'application, consultez le glossaire.

- **Applications potentiellement indésirables** – Un logiciel gris ou une application potentiellement indésirable (PUA) désigne une vaste catégorie de logiciels, dont l'intention malveillante n'est pas aussi clairement établie qu'avec d'autres types de logiciels malveillants, tels que les virus ou les chevaux de Troie. Il peut cependant installer des logiciels indésirables supplémentaires, modifier le comportement ou les paramètres du périphérique numérique ou effectuer des activités non approuvées ou prévues par l'utilisateur. Pour en savoir plus sur ces types d'application, consultez le glossaire.

- **Les applications suspectes** comprennent les programmes compressés à l'aide d'un compresseur de fichiers ou d'un protecteur. Ces protecteurs sont souvent exploités par les créateurs de logiciels malveillants pour échapper à la détection.

- Les **applications potentiellement dangereuses** sont des logiciels commerciaux légitimes susceptibles d'être utilisés à des fins malveillantes. Elles comprennent des programmes comme des outils d'accès à distance, des applications de craquage de mot de passe et des enregistreurs de frappe. Pour en savoir plus sur ces types d'application, consultez le glossaire.



Protection améliorée

L'apprentissage automatique avancé fait désormais partie des protections en tant que couche de protection avancée qui améliore la détection sur la base de l'apprentissage automatique. Pour en savoir plus sur ce type de protection, consultez le glossaire.

Configuration des signalements

Lorsqu'une détection se produit (par exemple, une menace est détectée et classée comme logiciel malveillant), les informations sont enregistrées dans le journal de détection et des notifications de bureau s'affichent si elles sont configurées dans ESET Internet Security.

Le seuil de signalement est configuré pour chaque catégorie (appelée « CATÉGORIE ») :

1. Détections de logiciels malveillants
2. Applications potentiellement indésirables
3. Potentiellement dangereux
4. Applications suspectes

Signalement effectué avec le moteur de détection, y compris le composant d'apprentissage automatique. Vous pouvez fixer un seuil de signalement plus élevé que le seuil actuel de protection. Ces paramètres de signalement n'influencent pas le blocage, le nettoyage ou la suppression des objets.

Lisez ce qui suit avant de modifier un seuil (ou un niveau) pour le signalement de CATÉGORIE :

Seuil	Explication
Agressif	Signalement de la CATÉGORIE configurée avec une sensibilité maximale. Plus de détections sont signalées. Le paramètre **Agressif** peut identifier à tort des objets comme étant CATÉGORIE.
Équilibré	Signalement de la CATÉGORIE configurée sur Équilibré. Ce paramètre est optimisé pour équilibrer les performances et la précision des taux de détection et du nombre d'objets faux positifs.
Prudent	Signalement de la CATÉGORIE configurée pour réduire au minimum les objets faux positifs tout en maintenant un niveau de protection suffisant. Les objets ne sont signalés que lorsque la probabilité est évidente et correspond au comportement de CATÉGORIE.
Désactivé	Le signalement d'une CATÉGORIE n'est pas actif et les détections de ce type ne sont pas trouvées, signalées ou nettoyées. Par conséquent, ce paramètre désactive la protection de ce type de détection. Désactivé n'est pas disponible pour les signalements de logiciels malveillants et c'est la valeur par défaut pour les applications potentiellement dangereuses.

Disponibilité des modules de protection de ESET Internet Security

La disponibilité (activé ou désactivé) d'un module de protection pour un seuil de CATÉGORIE sélectionné est la suivante :

	Agressif	Équilibré	Prudent	Désactivé*
Module avancé d'apprentissage machine	✓ (mode agressif)	✓ (mode conservateur)	X	X
Module du moteur de détection	✓	✓	✓	X
Autres modules de protection	✓	✓	✓	X

* Non recommandé.

Déterminer la version du produit, les versions des modules du programme et les dates de construction

1. Cliquez sur **Aide et assistance** > **À propos de ESET Internet Security**.
2. Dans la fenêtre **À propos de**, la première ligne de texte affiche le numéro de version de votre produit ESET.
3. Cliquez sur **Composants installés** pour accéder à des informations sur des modules particuliers.

Conseils

Quelques conseils pour établir un seuil approprié à votre environnement :

- Le seuil **Équilibré** est recommandé pour la plupart des configurations.
- Plus le seuil de signalement est élevé, plus le taux de détection est élevé, mais plus il y a de chances que des objets soient faussement identifiés.
- En pratique, il n'est pas possible de garantir un taux de détection de 100 %. De même il n'est pas possible d'éviter toute classification erronée des objets propres comme logiciels malveillants.
- Conservez ESET Internet Security et ses modules à jour pour optimiser l'équilibre entre les performances et la précision des taux de détection et le nombre de faux positifs.

Configuration de la protection

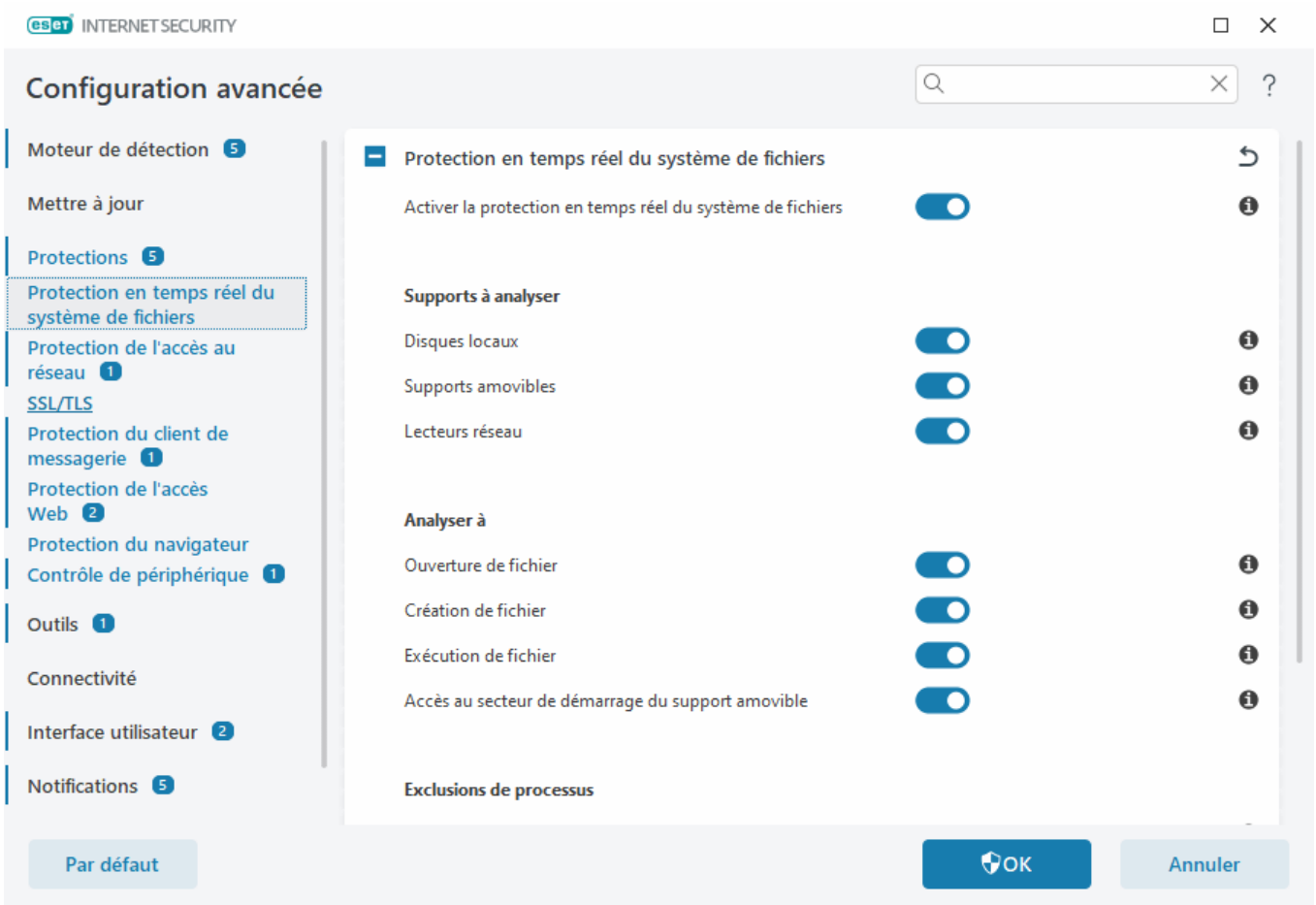
Si un objet classé comme CATÉGORIE est signalé, le programme bloque l'objet, puis le nettoie, le supprime ou le déplace vers la quarantaine.

Lisez ce qui suit avant de modifier un seuil (ou un niveau) pour la protection contre les CATÉGORIE :

Seuil	Explication
Agressif	Les détections de niveau agressif (ou inférieur) signalées sont bloquées et la correction automatique (c'est-à-dire le nettoyage) est lancée. Ce paramètre est recommandé lorsque tous les terminaux ont été analysés avec des paramètres agressifs et que des objets faussement signalés ont été ajoutés aux exclusions de détection.
Équilibré	Les détections de niveau équilibré (ou inférieur) signalées sont bloquées et la correction automatique (c'est-à-dire le nettoyage) est lancée.
Prudent	Les détections de niveau prudent signalées sont bloquées et la correction automatique (c'est-à-dire le nettoyage) est lancée.
Désactivé	Cette option est utile pour identifier et exclure les objets faussement signalés. Désactivé n'est pas disponible pour la protection contre les logiciels malveillants et c'est la valeur par défaut pour les applications potentiellement dangereuses.

Protection en temps réel du système de fichiers

La protection en temps réel du système de fichiers contrôle tous les fichiers du système pour détecter les codes malveillants lorsqu'ils sont ouverts, créés ou exécutés.



Par défaut, la protection en temps réel du système de fichier est lancée au démarrage du système d'exploitation et assure une analyse ininterrompue. Nous recommandons de ne pas désactiver **Activer la protection en temps réel du système de fichiers** dans Configuration avancée > **Protections** > **Protection en temps réel du système de fichiers** > **Protection en temps réel du système de fichiers**.

Supports à analyser

Par défaut, tous les types de supports sont analysés pour y détecter la présence potentielle de menaces :

- **Disques locaux** – Analyse tous les disques durs système et fixes (exemple : *C:*\, *D:*\).
- **Supports amovibles** – Analyse les CD/DVDs, les mémoires USB, les cartes mémoires, etc.
- **Lecteurs réseau** – Analyse tous les lecteurs réseau mappés (exemple : *H:*\ en tant que *store04*) ou des lecteurs réseau d'accès direct (exemple : *store08*).

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

Date de l'analyse

Par défaut, tous les fichiers sont analysés lorsqu'ils sont ouverts, créés ou exécutés. Il est recommandé de conserver ces paramètres par défaut, car ils offrent le niveau maximum de protection en temps réel pour votre ordinateur :

- **Ouverture de fichier** – Effectue un analyse lorsqu'un fichier est ouvert.
- **Création de fichier** - Analyse un fichier créé ou modifié.
- **Exécution de fichier** – Effectue une analyse lorsqu'un fichier est exécuté ou en cours d'exécution.
- **Accès au secteur de démarrage du support amovible** - Lorsqu'un support amovible contenant un secteur de démarrage est inséré dans le périphérique, celui-ci est immédiatement analysé. Cette option n'active pas l'analyse du fichier de média amovible. L'analyse des fichiers de support amovible se trouve dans **Support à analyser** > **Supports amovibles**. Pour que l'**accès au secteur d'amorçage du support amovible** fonctionne correctement, laissez **Secteurs d'amorçage/UEFI** activé dans ThreatSense.

Exclusions de processus

Voir Exclusions de processus.

ThreatSense

La protection en temps réel du système de fichiers vérifie tous les types de supports et est déclenchée par différents événements comme tenter d'accéder à un fichier. Grâce aux méthodes de détection de la technologie **ThreatSense** (décrites dans ThreatSense), la protection en temps réel du système de fichiers peut être configurée afin de traiter différemment les fichiers nouvellement créés et les fichiers existants. Par exemple, vous pouvez configurer la protection en temps réel du système de fichiers afin qu'elle surveille plus attentivement les fichiers nouvellement créés.

Pour assurer le minimum d'empreinte système lorsque la protection en temps réel est utilisée, les fichiers ayant

déjà été analysés ne seront pas analysés de nouveau (à moins qu'ils n'aient été modifiés). Les fichiers sont analysés immédiatement après chaque mise à jour du moteur de détection. Ce comportement est contrôlé grâce à l'**optimisation intelligente**. Si la fonction d'**optimisation intelligente** est désactivée, tous les fichiers seront analysés chaque fois que l'ordinateur y accédera. Pour modifier ce paramètre, ouvrez Configuration avancée > **Protections** > **Protection en temps réel du système de fichiers**. Cliquez sur **ThreatSense** > **Autres** et sélectionnez ou désélectionnez **Activer l'optimisation intelligente**.

La protection en temps réel du système de fichiers vous permet également de configurer des paramètres supplémentaires de ThreatSense.

Exclusions de processus

La fonctionnalité Exclusions de processus vous permet d'exclure des processus d'application de la protection en temps réel du système de fichiers. Pour améliorer la vitesse de sauvegarde, l'intégrité des processus et la disponibilité du service, certaines techniques connues pour entrer en conflit avec la protection contre les logiciels malveillants au niveau du fichier sont utilisées pendant la sauvegarde. Le seul moyen efficace d'éviter les deux situations est de désactiver l'anti-logiciel malveillant. En excluant des processus spécifiques (par exemple ceux de la solution de sauvegarde), toutes les opérations sur les fichiers attribuées à ce processus exclu sont ignorées et considérées comme sûres, minimisant ainsi les interférences avec le processus de sauvegarde. Nous vous recommandons de faire preuve de prudence lors de la création d'exclusions - un outil de sauvegarde exclu peut accéder aux fichiers infectés sans déclencher une alerte. C'est pourquoi les autorisations étendues ne sont autorisées que dans le module de protection en temps réel.

Vous ne devez pas les confondre avec les extensions de fichiers exclues, les exclusions HIPS, les exclusions de détection ou les exclusions de performance.

Les exclusions de processus aident à minimiser le risque de conflits potentiels et à améliorer les performances des applications exclues, ce qui a un effet positif sur les performances globales et la stabilité du système d'exploitation. L'exclusion d'un processus ou d'une application est une exclusion de son fichier exécutable (*.exe*).

Vous pouvez ajouter des fichiers exécutables dans la liste des processus exclus dans Configuration avancée > **Protections** > **Protection en temps réel du système de fichiers** > **Protection en temps réel du système de fichiers** > **Exclusions de processus**.

Cette fonctionnalité a été conçue pour exclure les outils de sauvegarde. Exclure le processus de l'outil de sauvegarde de l'analyse garantit non seulement la stabilité du système, mais n'affecte pas non plus les performances de la sauvegarde car elle n'est pas ralentie pendant son exécution.

Cliquez sur **Modifier** pour ouvrir la fenêtre de gestion **Exclusions de processus**, dans laquelle vous pouvez ajouter des exclusions et rechercher un fichier exécutable (par exemple *Backup-tool.exe*), qui sera exclu de l'analyse.
Dès que le fichier *.exe* est ajouté aux exclusions, l'activité de ce processus n'est pas contrôlée par ESET Internet Security et aucune analyse n'est exécutée sur les opérations sur les fichiers effectuées par ce processus.

Si vous n'utilisez pas la fonction de navigation lors de la sélection de l'exécutable de processus, vous devez entrer manuellement le chemin complet de l'exécutable. Sinon, l'exclusion ne fonctionnera pas correctement et HIPS pourra signaler des erreurs.

Au besoin, vous pouvez également **modifier** des processus existants ou les **supprimer** des exclusions.

La protection de l'accès Web ne prend pas en compte cette exclusion. Par conséquent, si vous excluez le fichier exécutable de votre navigateur Web, les fichiers téléchargés sont toujours analysés. De cette façon, une infiltration peut toujours être détectée. Ce scénario n'est qu'un exemple et nous vous déconseillons de créer des exclusions pour les navigateurs Web.

Ajouter ou modifier des exclusions de processus

Cette boîte de dialogue vous permet **d'ajouter** des processus exclus du moteur de détection. Les exclusions de processus aident à minimiser le risque de conflits potentiels et à améliorer les performances des applications exclues, ce qui a un effet positif sur les performances globales et la stabilité du système d'exploitation. L'exclusion d'un processus ou d'une application est une exclusion de son fichier exécutable (*.exe*).

Sélectionnez le chemin du fichier d'une application qui fait partie des exceptions en cliquant sur ... (par exemple *C:\Program Files\Firefox\Firefox.exe*). Ne saisissez PAS le nom de l'application.
Dès que le fichier *.exe* est ajouté aux exclusions, l'activité de ce processus n'est pas contrôlée par ESET Internet Security et aucune analyse n'est exécutée sur les opérations sur les fichiers effectuées par ce processus.

Si vous n'utilisez pas la fonction de navigation lors de la sélection de l'exécutable de processus, vous devez entrer manuellement le chemin complet de l'exécutable. Sinon, l'exclusion ne fonctionnera pas correctement et HIPS pourra signaler des erreurs.

Au besoin, vous pouvez également **modifier** des processus existants ou les **supprimer** des exclusions.

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

La protection en temps réel est le composant le plus essentiel de la sécurisation du système. Il faut être très attentif lorsqu'on modifie les paramètres de ce module. Il est recommandé de ne changer les paramètres de ce module que dans des cas précis.

Après avoir installé ESET Internet Security, tous les paramètres sont optimisés pour garantir le niveau maximal de sécurité système pour les utilisateurs. Pour restaurer les paramètres par défaut, cliquez sur en regard de Configuration avancée > **Protections** > **Réponse aux détections**.

Vérification de la protection en temps réel

Pour s'assurer que la protection en temps réel fonctionne et détecte bien les virus, utilisez un fichier de test d'*www.eicar.com*. Ce fichier de test est un fichier inoffensif que détecteront tous les programmes antivirus. Le fichier a été créé par la société EICAR (European Institute for Computer Antivirus Research) pour tester la fonctionnalité des programmes antivirus.

Vous pouvez le télécharger sur le site http://www.eicar.org/download/eicar.com
Après avoir entré cette URL dans votre navigateur, vous devriez voir un message indiquant que la menace a été supprimée.

Que faire si la protection en temps réel ne fonctionne pas

Dans cette rubrique, nous décrivons des problèmes qui peuvent survenir avec la protection en temps réel et la façon de les résoudre.

La protection en temps réel est désactivée

Si un utilisateur désactive par inadvertance la protection en temps réel, vous devez réactiver la fonctionnalité. Pour réactiver la protection en temps réel, allez à **Paramètres** dans la fenêtre principale du programme et cliquez sur **Protection de l'ordinateur** > **Protection en temps réel du système de fichiers**.

Si la protection en temps réel n'est pas lancée au démarrage du système, cela découle généralement du fait que l'option **Activer la protection en temps réel du système de fichiers** est désélectionnée. Pour vous assurer que cette option est activée, ouvrez Configuration avancée > **Protections** > **Protection en temps réel du système de fichiers**.

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

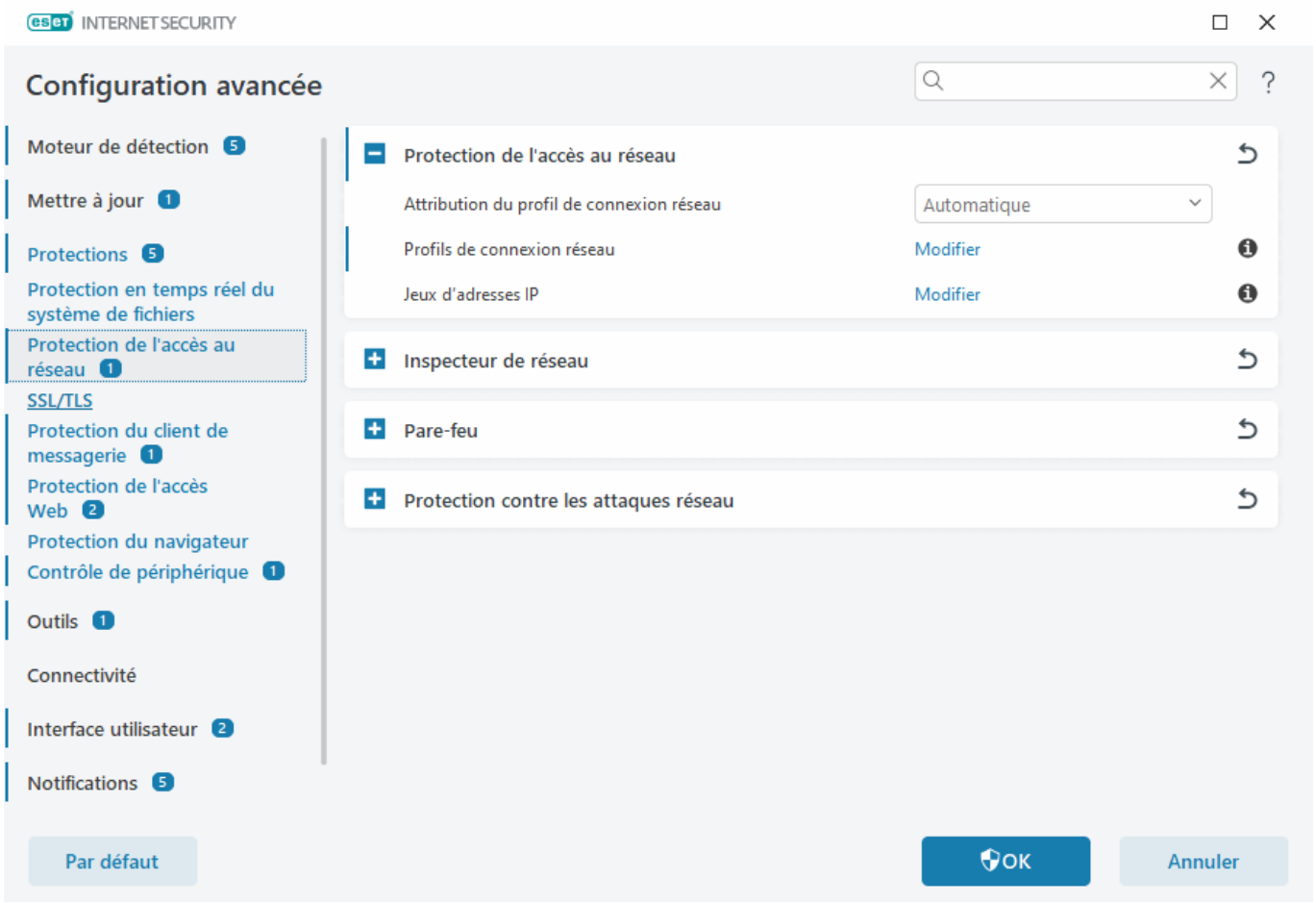
Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si deux programmes antivirus sont installés en même temps, il peut y avoir conflit entre les deux. Nous recommandons de désinstaller tout autre antivirus de votre système avant d'installer ESET.

La protection en temps réel ne démarre pas

Si la protection en temps réel n'est pas lancée au démarrage du système (et **Activer la protection en temps réel du système de fichiers** est activée), cela peut être due à des conflits avec d'autres programmes. Pour résoudre le problème, créez un journal ESET SysInspector et envoyez-le au service d'assistance technique d'ESET pour analyse.

Protection de l'accès au réseau

La protection de l'accès au réseau vous permet de configurer toutes vos connexions réseau en détail. Vous pouvez autoriser/refuser l'accès à votre ordinateur sur des réseaux spécifiques, autoriser/refuser l'accès aux périphériques réseau à partir de votre ordinateur et plus encore en fonction de la configuration. Par défaut, les règles de pare-feu et la protection de l'accès au réseau sont préconfigurées par ESET Internet Security pour offrir une sécurité maximale. Cependant, des environnements spécifiques peuvent nécessiter une configuration personnalisée. La modification des paramètres par défaut ne doit être effectuée que par un utilisateur expérimenté.



Vous pouvez configurer les paramètres suivants dans Configuration avancée > **Protections** > **Protection de l'accès au réseau** (cliquez sur les liens ci-dessous pour une description détaillée de chaque option de protection de l'accès au réseau) :

Protection de l'accès au réseau

Profils de connexion réseau : vous pouvez utiliser des profils pour contrôler le comportement du pare-feu pour des connexions réseau spécifiques.

Ensembles d'adresses :IP vous pouvez définir des ensembles d'adresses IP qui créent un groupe logique d'adresses IP, que vous pouvez utiliser pour des règles de Pare-feu.

Inspecteur de réseau

Pare-feu

Protection contre les attaques réseau

Profils de connexion réseau

Les profils peuvent être utilisés pour contrôler le comportement de la protection du réseau par ESET Internet Security pour des connexions réseau spécifiques. Lors de la création ou de la modification d'une règle de pare-feu, d'une règle d'IDS ou d'une règle de protection contre les attaques par force brute, vous pouvez l'affecter à un profil spécifique ou l'appliquer à tous les profils. Lorsqu'un profil est actif sur une connexion réseau, seules les règles globales (celles qui ne s'appliquent à aucun profil en particulier) et les règles attribuées à ce profil sont

appliquées. Vous pouvez créer plusieurs profils avec différentes règles assignées aux connexions réseau afin de modifier facilement le comportement du pare-feu.

Vous pouvez configurer des profils et des affectations de connexion réseau dans Configuration avancée > **Protections** > **Protection de l'accès au réseau** > **Protection de l'accès au réseau**.

Attribution de profil de connexion réseau : cette option vous permet de définir s'il faut attribuer automatiquement aux connexions réseau nouvellement découvertes (sélectionner **Auto** dans le menu déroulant) un profil prédéfini ou personnalisé basé sur les activateurs configurés dans les profils de connexion réseau ou s'il faut demander (sélectionner **Demander** dans le menu déroulant) avant de configurer la protection du réseau et d'attribuer un profil manuellement chaque fois qu'une nouvelle connexion réseau est détectée.

Vous pouvez également assigner manuellement un profil de connexion réseau spécifique dans la fenêtre principale du programme > **Configuration** > **Protection du réseau** > **Connexions réseau**. Passez la souris sur une connexion réseau spécifique et cliquez sur l'icône de menu ⋮ > **Modifier** pour ouvrir la fenêtre Configurer la protection réseau et sélectionner un profil.

Profils de connexion réseau : cliquez sur **Modifier** pour ajouter ou modifier des profils de connexion réseau.

Les profils suivants sont prédéfinis et ne peuvent pas être modifiés ni supprimés :

Privé : pour les réseaux fiables (réseaux domestiques ou professionnels). Votre ordinateur et les fichiers partagés stockés sur votre ordinateur sont visibles par les autres utilisateurs du réseau et les ressources système sont accessibles aux autres utilisateurs du réseau (l'accès aux fichiers et aux imprimantes partagés est activé, la communication RPC entrante est activée et le partage de bureau à distance est disponible). Nous vous recommandons d'utiliser ce paramètre lors de l'accès à un réseau local sécurisé. Ce profil est automatiquement affecté à une connexion réseau si elle est configurée en tant que domaine ou réseau privé dans Windows.

Public : pour les réseaux non fiables (réseaux publics). Les fichiers et les dossiers de votre système ne sont pas partagés ni visibles par d'autres utilisateurs du réseau et le partage des ressources système est désactivé. Nous vous recommandons d'utiliser ce paramètre lors de l'accès aux réseaux sans fil. Ce profil est automatiquement affecté à toute connexion réseau qui n'est pas configurée en tant que domaine ou réseau privé dans Windows.

Lorsque la connexion réseau passe à un autre profil, une notification s'affiche dans le coin inférieur droit de votre écran.

Ajouter ou modifier des profils de connexion réseau

Vous pouvez ajouter ou modifier des profils de connexion réseau dans Configuration avancée > **Protections** > **Protection de l'accès au réseau** > **Protection de l'accès au réseau** > **Profils de connexion réseau** > **Modifier**. Pour éditer un profil, il doit être sélectionné dans la liste de la fenêtre **Profils de connexion réseau**.

Les profils suivants sont prédéfinis et ne peuvent pas être modifiés ni supprimés :

Privé : pour les réseaux fiables (réseaux domestiques ou professionnels). Votre ordinateur et les fichiers partagés stockés sur votre ordinateur sont visibles par les autres utilisateurs du réseau et les ressources système sont accessibles aux autres utilisateurs du réseau (l'accès aux fichiers et aux imprimantes partagés est activé, la communication RPC entrante est activée et le partage de bureau à distance est disponible). Nous vous recommandons d'utiliser ce paramètre lors de l'accès à un réseau local sécurisé. Ce profil est automatiquement affecté à une connexion réseau si elle est configurée en tant que domaine ou réseau privé dans Windows.

Public : pour les réseaux non fiables (réseaux publics). Les fichiers et les dossiers de votre système ne sont pas partagés ni visibles par d'autres utilisateurs du réseau et le partage des ressources système est désactivé. Nous vous recommandons d'utiliser ce paramètre lors de l'accès aux réseaux sans fil. Ce profil est automatiquement affecté à toute connexion réseau qui n'est pas configurée en tant que domaine ou réseau privé dans Windows.

Au-dessus/Vers le haut/Vers le bas/En-dessous  vous permet d'ajuster le niveau de priorité des profils de connexion réseau (les profils de connexion réseau sont évalués et appliqués en fonction de leur priorité. Le premier profil correspondant est toujours appliqué).

Ajouter ou modifier un profil

Le profil de connexion réseau personnalisé vous permet d'appliquer des règles de pare-feu et de définir des paramètres supplémentaires pour des connexions réseau spécifiques. Vous devez spécifier à quelles connexions réseau le profil personnalisé sera affecté dans la section Activateurs.

Pour ouvrir l'éditeur de profil, accédez à la fenêtre **Profils de connexion réseau** et procédez comme suit :

- Cliquez sur **Ajouter**.
- Sélectionnez l'un des profils existants et cliquez sur **Modifier**.
- Sélectionnez l'un des profils existants et cliquez sur **Copier**.

Nom : nom personnalisé de votre profil.

Description : description du profil pour aider à identifier celui-ci.

Adresses approuvées supplémentaires : les adresses définies ici sont ajoutées à la zone de confiance de la connexion réseau à laquelle ce profil est appliqué (quel que soit le type de protection du réseau).

Connexion fiable : votre ordinateur et les fichiers partagés stockés sur votre ordinateur sont visibles par les autres utilisateurs du réseau et les ressources système sont accessibles aux autres utilisateurs du réseau. (l'accès aux fichiers et aux imprimantes partagés est activé, la communication RPC entrante est activée et le partage de bureau à distance est disponible). Nous vous recommandons d'utiliser ce paramètre lors de la création d'un profil pour une connexion au réseau local sécurisée. Tous les sous-réseaux de réseau directement connectés sont également 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, alors le sous-réseau 192.168.1.0/24 est ajouté à la zone de confiance de cette connexion réseau. Si la carte possède plus d'adresses/sous-réseaux, ils seront tous pris en compte.

Avertir lorsque le chiffrement du Wi-Fi est faible : ESET Internet Security affichera une notification sur le bureau lorsque vous vous connectez à un réseau sans fil non protégé ou à un réseau avec une protection faible.

Activateurs : conditions personnalisées qui doivent être remplies pour affecter ce profil de connexion réseau à une connexion réseau. Voir la rubrique Activateurs pour une explication détaillée.

Activateurs

Les activateurs sont des conditions personnalisées qui doivent être remplies pour qu'un profil de connexion réseau soit affecté à une connexion réseau. Si le réseau connecté possède les mêmes attributs que ceux définis dans les activateurs d'un profil de réseau connecté, le profil sera appliqué au réseau. Un profil de connexion

réseau peut avoir un ou plusieurs activateurs. S'il y a plusieurs activateurs, la logique OU s'applique (au moins une condition doit être remplie). Vous pouvez définir des activateurs dans l'éditeur de profil de connexion réseau. La création de profils de connexion réseau personnalisés doit être effectuée par un utilisateur expérimenté.

Les activateurs suivants sont disponibles (si vous souhaitez connaître les détails de votre réseau actuel, consultez la rubrique Connexions réseau) :

Adaptateur

Type de carte : appliquez le profil si la connexion réseau est établie sur le type de carte sélectionné.
Nom de la carte : appliquez le profil s'il y a correspondance avec le nom de la carte réseau.
IP de la carte : appliquez le profil s'il y a correspondance avec l'adresse IP de votre carte réseau.

DNS

Suffixe DNS : appliquez le profil s'il y a correspondance avec le nom de domaine.
IP de DNS : appliquez le profil s'il y a correspondance avec l'adresse IP du serveur DNS.

WINS

Appliquez le profil s'il y a correspondance avec l'adresse IP mappée de Windows Internet Name Service (WINS).

DHCP

IP DHCP : correspondance avec l'adresse IP de serveur DHCP.

Passerelle par défaut

IP : appliquez le profil s'il y a correspondance avec l'adresse IP de la passerelle par défaut.
Adresse MAC : appliquez le profil s'il y a correspondance avec l'adresse MAC de la passerelle par défaut.

Wi-Fi

SSID : appliquez le profil s'il y a correspondance avec le SSID (nom du Wi-Fi).
Nom du profil : appliquez le profil s'il y a correspondance avec le nom de profil Wi-Fi.
Type de sécurité : appliquez le profil s'il y a correspondance entre le type de sécurité et celui sélectionné dans le menu déroulant. Si vous souhaitez qu'il y ait plus d'une correspondance, créez un autre activateur.
Type de chiffrement : appliquez le profil s'il y a correspondance entre le type de chiffrement et celui sélectionné dans menu déroulant. Si vous souhaitez qu'il y ait plus d'une correspondance, créez un autre activateur.
Sécurité réseau : appliquez le profil si le réseau est **Ouvert**/**Sécurisé**.

Profil Windows

Appliquez le profil si le réseau est configuré dans Windows en tant que **Domaine**/**Privé**/**Public**.

Authentification

L'authentification réseau recherche un serveur spécifique sur le réseau et utilise le chiffrement asymétrique (RSA) pour l'authentifier. Le nom du réseau authentifié doit correspondre au nom défini dans les paramètres du serveur d'authentification. Le chemin est sensible à la casse. Le nom du serveur peut être entré comme une adresse IP, un nom DNS ou NetBios.
Téléchargez ESET Authentication Server.
La clé publique peut être importée en utilisant l'un des types de fichiers suivants :
• clé publique chiffrée PEM (.pem); vous pouvez générer cette clé à l'aide du serveur d'authentification d'ESET
• Clé publique chiffrée
• Certificat de clé publique (.crt)
Cliquez sur **Tester** pour tester vos paramètres. Si l'authentification réussit, l'authentification du serveur a réussi est affichée. Si l'authentification n'a pas été correctement configurée, l'un des messages d'erreur suivants s'affichera :
L'authentification auprès du serveur a échoué. Signature non valide ou incompatible.
La signature du serveur ne correspond pas à la clé publique indiquée.
L'authentification auprès du serveur a échoué. Le nom du réseau est erroné.
Le nom du réseau configurée ne correspond pas à celui du nom du réseau du serveur d'authentification. Vérifiez les deux noms et assurez-vous qu'ils sont identiques.
L'authentification auprès du serveur a échoué. Non valide ou aucune réponse du serveur.
Aucune réponse n'est reçue si le serveur ne fonctionne pas ou est inaccessible. Une réponse non valide peut être reçue si un autre serveur HTTP fonctionne sur l'adresse indiquée.
La clé publique entrée n'est pas valide.
Vérifiez que le fichier de clé publique que vous avez entré n'est pas corrompu.

Jeux d'adresses IP

Un jeu d'adresses IP est une collection d'adresses IP qui créent un groupe logique d'adresses IP. Cela est utile lors de la réutilisation du même jeu d'adresses dans plusieurs règles de pare-feu ou règles de protection contre les attaques par force brute. ESET Internet Security contient également des jeux d'adresses IP prédéfinis pour lesquels des règles internes sont appliquées. Un exemple d'un tel groupe est une **zone de confiance**. La zone de confiance représente un groupe d'adresses réseau où votre ordinateur et les fichiers partagés stockés sur votre ordinateur sont visibles par les autres utilisateurs du réseau et les ressources système sont accessibles aux autres utilisateurs du réseau.

Pour ajouter un jeu d'adresses IP :

1. Ouvrez Configuration avancée > **Protections** > **Protection de l'accès au réseau** > **Jeux d'adresses IP** > **Modifier**.

2. Cliquez sur **Ajouter**, entrez un **nom** et une **description** pour la zone, puis tapez une adresse IP distante dans le champ **Adresse de l'ordinateur distant (IPv4/IPv6, plage, masque)**.

3. Cliquez sur **OK**.

Pour plus d'informations, voir Modifier les jeux d'adresses IP.

Modifier les jeux d'adresses IP

Pour plus d'informations sur les jeux d'adresses IP, consultez la rubrique Jeux d'adresses IP.

Colonnes

Nom - Nom d'un groupe d'ordinateurs distants.

Description - Une description générale du groupe.

Adresses IP : adresses IP distantes qui appartiennent à un jeu d'adresses IP.

Éléments de contrôle

Lorsque vous **ajoutez** ou **modifiez** un jeu d'adresses IP, les champs suivants sont disponibles :

Nom - Nom d'un groupe d'ordinateurs distants.

Description - Une description générale du groupe.

Adresse de l'ordinateur distant (IPv4/IPv6, plage, masque) - permet d'ajouter une adresse distante, une plage d'adresses ou un sous-réseau.

Supprimer - Supprime une zone de la liste.

Les jeux d'adresses IP prédéfinis ne peuvent pas être supprimés.

Exemples d'adresses IP

Ajouter une adresse IPv4:
Adresse unique : ajoute l'adresse IP d'un seul ordinateur (par exemple, *192.168.0.10*).
Plage d'adresses : entrez la première et la dernière adresse IP pour préciser une plage d'adresse IP (de plusieurs ordinateurs) à laquelle appliquer la règle (par exemple, de *192.168.0.1 à 192.168.0.99*).
Sous-réseau - Sous-réseau (groupe d'ordinateurs) défini par une adresse IP et un masque. Par exemple, 255.255.255.0 est le masque de réseau pour le sous-réseau 192.168.1.0. Pour exclure le type de sous-réseau entier dans *192.168.1.0/24*.
Ajouter une adresse IPv6:
Adresse unique : ajoute l'adresse IP d'un seul ordinateur (par exemple, *2001:718:1c01:16:214:22ff:fec9:ca5*).
Sous-réseau - Sous-réseau (groupe d'ordinateurs) défini par une adresse IP et un masque (par exemple, *2002:c0a8:6301:1::1/64*).

Inspecteur de réseau

Inspecteur de réseau peut aider à identifier les vulnérabilités de votre réseau de confiance (domestique ou professionnel), par exemple, des ports ouverts ou un mot de passe de routeur faible. Il fournit également une liste de périphériques connectés, classés par type de périphériques (par exemple, imprimante, routeur, périphérique mobile, etc.) pour vous montrer ce qui est connecté à votre réseau (par exemple, console de jeu, IdO ou autres périphériques domestiques intelligents). Vous pouvez configurer l'inspecteur de réseau dans Configuration avancée > **Protections** > **Protection de l'accès au réseau** > **Inspecteur de réseau**.

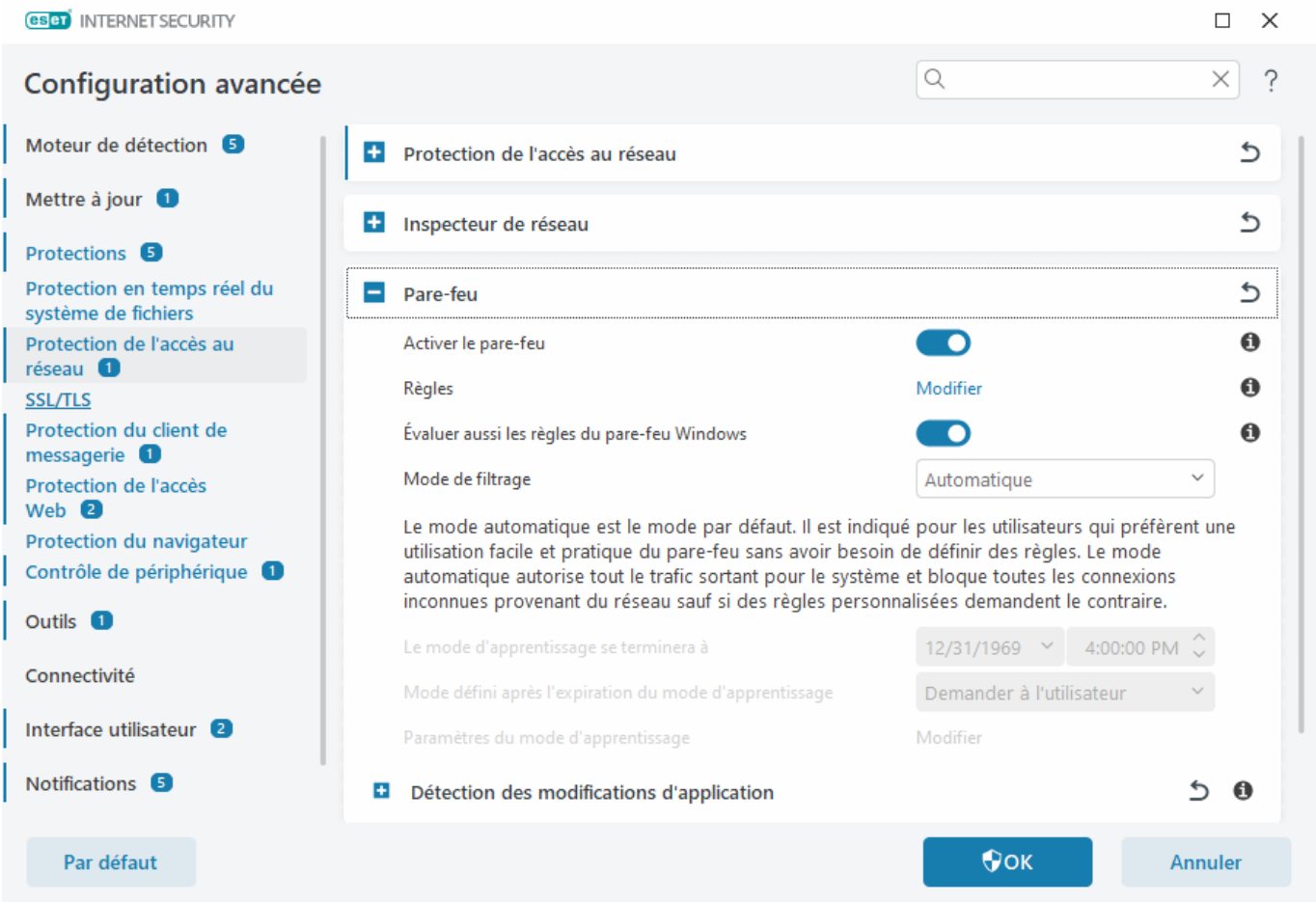
Activer l'inspecteur de réseau – Inspecteur de réseau aide à repérer les vulnérabilités du réseau domestique, comme les ports ouverts ou un mot de passe de routeur faible. Il fournit également une liste de périphériques connectés, classés par type de périphériques.

Aviser lorsque de nouveaux périphériques réseau sont découverts - Vous envoie une notification lorsqu'un nouveau périphérique est détecté sur votre réseau.

Pare-feu

Le pare-feu contrôle tout le trafic réseau entrant et sortant sur votre ordinateur en fonction des règles internes et des règles que vous avez définies. Cela se fait en autorisant ou en refusant des connexions individuelles au réseau. Le pare-feu fournit une protection contre les attaques en provenance de périphériques distants et peut bloquer certains services potentiellement dangereux.

Pour configurer le pare-feu, ouvrez Configuration avancée > **Protections** > **Protection de l'accès au réseau** > **Pare-feu**.



Pare-feu

Activer le pare-feu

Il est recommandé de laisser cette fonctionnalité activée afin de garantir la sécurité de votre système. Lorsque le pare-feu est activé, le trafic réseau est analysé dans les deux sens.

Règles

La configuration des règles permet de voir et de modifier toutes les règles de pare-feu appliquées au trafic généré par des applications individuelles, au sein des connexions et sur Internet.

Vous pouvez créer une règle IDS lorsqu'un réseau de zombies attaque votre ordinateur. Une règle peut être modifiée dans Configuration avancée > **Protections** > **Protection de l'accès réseau** > **Protection contre les attaques réseau** > **Règles IDS** en cliquant sur **Modifier**.

Évaluer aussi les règles du pare-feu Windows

En mode de filtrage automatique, le trafic entrant autorisé par les règles du pare-feu Windows est également autorisé, sauf s'il est explicitement bloqué par les règles d'ESET.

Mode de filtrage

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.

Les modes de filtrage suivants sont offerts avec le pare-feu d'ESET Internet Security :

Mode de filtrage	Description
Mode automatique	Le mode par défaut. Ce mode convient pour les utilisateurs qui préfèrent un usage facile et pratique du pare-feu sans avoir à définir de règles. Les règles personnalisées, définies par l'utilisateur peuvent être créées, mais ne sont pas obligatoires en **mode automatique**. Le mode automatique autorise tout le trafic sortant pour un système donné et bloque la majorité du trafic entrant à l'exception du trafic de la zone de confiance, (comme autorisé dans Options IDS et avancées/Services autorisés) et le trafic entrant en réponse à la communication sortante récente.
Mode interactif	Mode interactif – Permet de créer une configuration personnalisée pour le pare-feu. Lors de la détection d'une communication pour laquelle il n'existe aucune règle qui s'y 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 mémorisée comme nouvelle règle pour le pare-feu. Si vous choisissez de créer une nouvelle règle, toutes les connexions futures de ce type seront autorisées ou refusées conformément à cette règle.
Mode basé sur des règles personnalisées	Bloque toute connexion ne faisant pas l'objet d'une règle précise l'autorisant. Ce mode permet aux utilisateurs expérimentés de définir des règles qui n'autorisent que des connexions souhaitées et sûres. Toute autre connexion non précisée sera bloquée par le pare-feu.
Mode d'apprentissage	Crée automatiquement et enregistre les règles. Ce mode est indiqué pour la configuration initiale du pare-feu, mais ne doit pas être utilisé pendant de longues périodes. Aucune intervention de l'utilisateur n'est requise car ESET Internet Security enregistre les règles conformément aux paramètres prédéfinis. Le mode d'apprentissage ne devrait être utilisé que jusqu'à ce que toutes les règles aient été créées pour les communications requises afin d'éviter tout risque.

Le mode d'apprentissage se termine le : définissez la date et l'heure auxquelles le mode d'apprentissage se termine automatiquement. Vous pouvez également désactiver le mode d'apprentissage manuellement quand vous le souhaitez.

Mode défini après l'expiration du mode d'apprentissage – Définissez le mode de filtrage auquel reviendra le pare-feu de une fois le mode d'apprentissage terminé. Pour en savoir plus sur les modes de filtrage, consultez le tableau ci-dessus. Une fois que le mode d'apprentissage a pris fin, l'option **Demander à l'utilisateur** exige des privilèges d'administrateur pour effectuer une modification du mode de filtrage du pare-feu.

Paramètres du mode d'apprentissage : cliquez sur **Modifier** pour configurer les paramètres d'enregistrement des règles créées dans le mode d'apprentissage.

Détection des modifications d'application

La fonction de détection des modifications d'applications affiche des notifications si les applications modifiées, pour lesquels il existe une règle de pare-feu, tentent d'établir des connexions.

Paramètres du mode d'apprentissage

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

Ce mode peut exposer votre système à des risques; il n'est donc recommandé que pour la configuration initiale du pare-feu.

Sélectionnez **Apprentissage** dans le menu déroulant de Configuration avancée > **Protections** > **Protection de l'accès au réseau** > **Pare-feu** > **Pare-feu** > **Mode de filtrage** pour activer les options du mode d'apprentissage. Cliquez sur **Modifier** en regard de **Paramètres du mode d'apprentissage** pour configurer les options suivantes :

> ⚠ En mode d'apprentissage, le pare-feu ne filtre pas les communications. Toutes les communications entrantes et sortantes sont alors autorisées. Dans ce mode, le pare-feu ne protège pas totalement l'ordinateur.

Trafic entrant à partir de la zone de confiance - Un exemple d'une connexion entrante serait un périphérique distant qui, dans la zone fiable, tente d'établir une communication avec une application locale fonctionnant sur votre ordinateur.

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

Trafic Internet entrant - Un périphérique distant tente de communiquer avec une application fonctionnant sur cet ordinateur.

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

Chaque section vous permet de définir les 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 particulier associé à un numéro de port standard (HTTP - 80, POP3 - 110, etc.).

Ajouter une adresse IP distante/Zone fiable - Vous pouvez utiliser une adresse IP ou une zone 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 périphérique ou un groupe de périphériques en réseau.

Nombre maximal de règles pour une application - Si une application communique, par plusieurs ports, avec différentes 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.

Règles du pare-feu

Les règles du pare-feu représentent un ensemble de conditions utilisées pour tester de façon significative toutes les connexions réseau ainsi que toutes les actions affectées à ces conditions. L'utilisation des règles du pare-feu permet de définir l'action qui est effectuée lorsque différents types de connexions réseau sont établies.

Les règles sont évaluées de haut en bas et vous pouvez voir leur priorité dans la première colonne. L'action de la première règle correspondante est utilisée pour chaque connexion au réseau en cours d'évaluation.

Les connexions peuvent être divisées en connexions entrantes et sortantes. Les connexions entrantes se font à l'initiative d'un périphérique distant qui tente d'établir une connexion avec le système local. Les connexions sortantes fonctionnent dans le sens opposé – le système local communique avec le périphérique distant.

Si une nouvelle communication inconnue est détectée, il faut faire preuve de prudence au moment de décider de l'autoriser ou de la rejeter. Les connexions non sollicitées, non sécurisées ou inconnues posent un risque pour la sécurité du système. Si une telle connexion est établie, il est recommandé de faire très attention à le périphérique distant et aux applications qui tentent de se connecter à votre ordinateur. Beaucoup d'infiltrations essaient d'obtenir et d'envoyer des données personnelles ou de télécharger d'autres applications malveillantes sur les postes de travail hôtes. Le pare-feu vous permet de détecter et de mettre fin à de telles connexions.

Vous pouvez afficher et modifier les règles de pare-feu dans Configuration avancée > **Protections** > **Protection de l'accès au réseau** > **Pare-feu** > **Règles** > **Modifier**.

Si vous avez de nombreuses règles de pare-feu, vous pouvez utiliser un filtre pour afficher uniquement des règles spécifiques. Pour filtrer les règles de pare-feu, cliquez sur **Plus de filtres** au-dessus de la liste Règles de pare-feu. Vous pouvez filtrer les règles en fonction des critères suivants :

- Origine
- Direction
- Action
- Disponibilité

Par défaut, les règles de pare-feu prédéfinies sont masquées. Pour afficher toutes les règles prédéfinies, désactivez le bouton bascule en regard de **Masquer les règles intégrées (prédéfinies).** Vous pouvez désactiver ces règles, mais vous ne pouvez pas supprimer une règle prédéfinie.

Cliquez sur l'icône de recherche en haut à droite pour rechercher une ou plusieurs règles.

Colonnes

Priorité : les règles sont évaluées de haut en bas et vous pouvez voir leur priorité dans la première colonne.

Activé - Indique si les règles sont activées ou désactivées; la case correspondante doit être cochée pour activer une règle.

Application - Indique l'application à laquelle la règle s'applique.

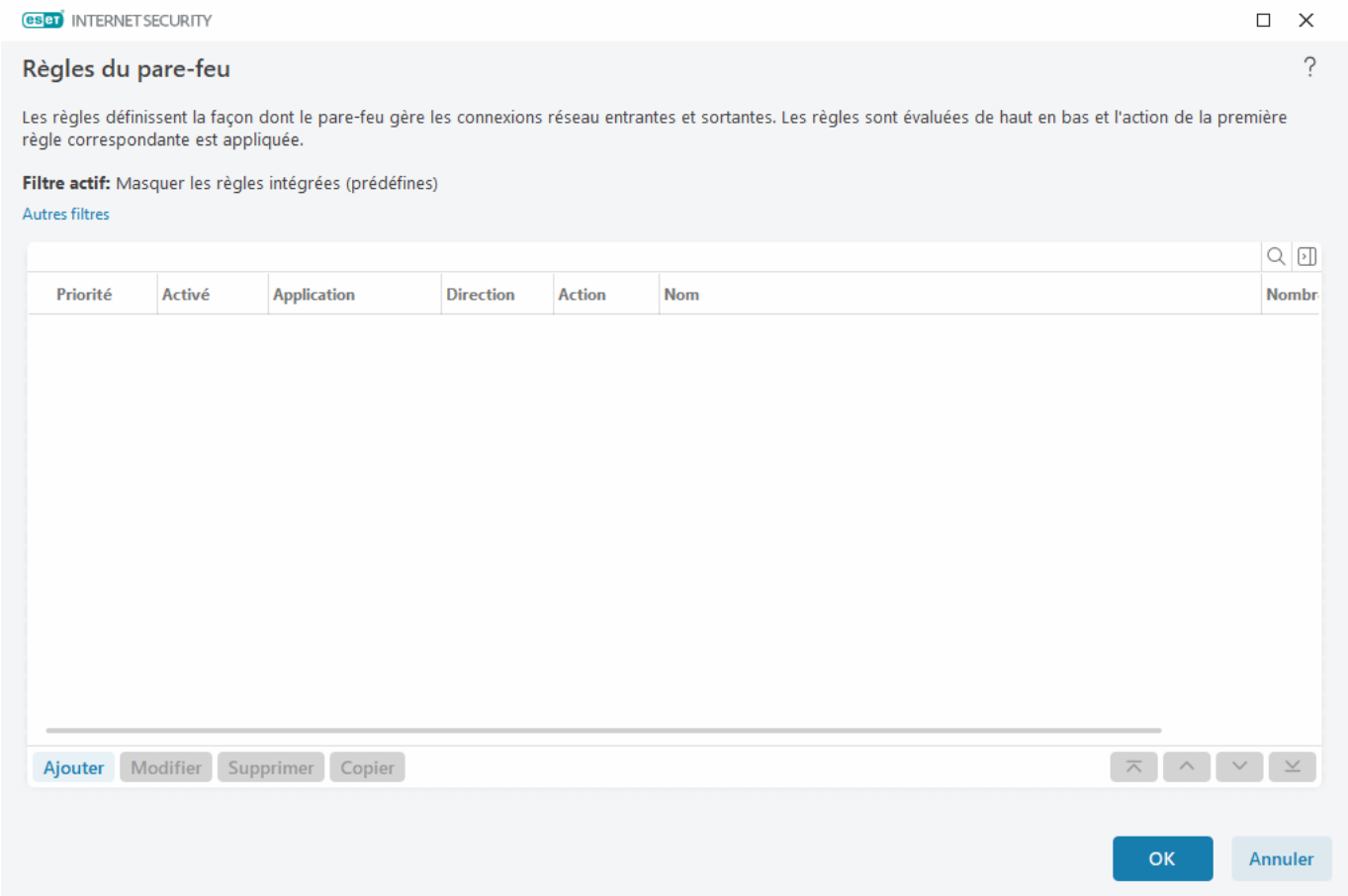
Direction - Direction de la communication (entrante/sortante/les deux).

Action - Indique l'état de la communication (bloquer/autoriser/demander).

Nom : le nom du règle. L'icône d'ESET représente une règle prédéfinie.

Nombre d'applications : nombre total de fois où la règle a été appliquée.

Cliquez sur l'icône Développer pour afficher les détails de la règle.



Éléments de contrôle

Ajouter - Crée une nouvelle règle.

Modifier – Modifier une règle existante.

Retirer – Supprimer une règle existante.

Copier - Créer une copie d'une règle sélectionnée.

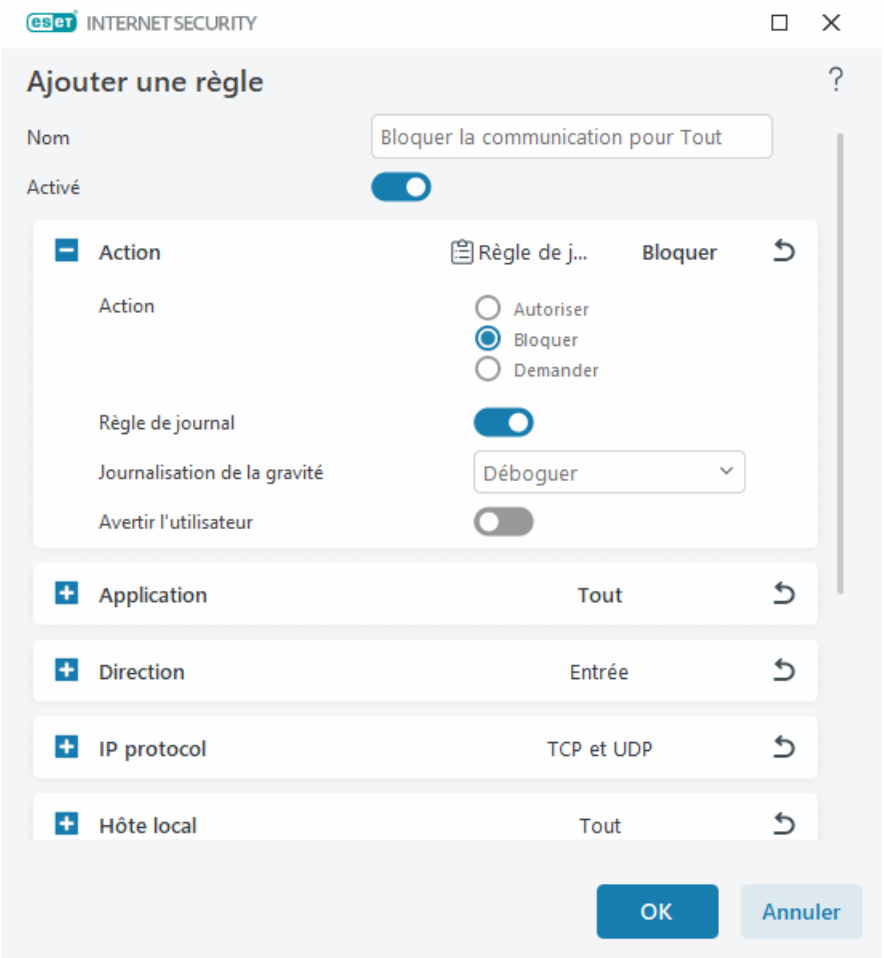
Première/Vers le haut/Vers le bas/Dernière - Permet de définir le niveau de priorité des règles (les règles sont exécutées du haut vers le bas).

Ajout ou modification de règles de pare-feu

Les règles du pare-feu représentent les conditions utilisées pour tester de façon significative toutes les connexions réseau ainsi que toutes les actions affectées à ces conditions. La modification ou l'ajout de règles de pare-feu peuvent être nécessaires lors de la modification des paramètres réseau (par exemple, l'adresse réseau ou le numéro de port a été modifié du côté distant) pour garantir le fonctionnement approprié d'une application concernée par une règle. Les règles de pare-feu personnalisées doivent être créées par un utilisateur expérimenté.

> **Instructions illustrées**
> Les articles suivants de la base de connaissances ESET peuvent n'être disponibles qu'en anglais :
> - Ouvrir ou fermer (autoriser ou refuser) un port spécifique dans le pare-feu ESET
> - Créer une règle de pare-feu depuis les fichiers journaux dans ESET Internet Security

Pour ajouter ou modifier une règle de pare-feu, ouvrez Configuration avancée > **Protections** > **Protection de l'accès au réseau** > **Pare-feu** > **Règles** > **Modifier**. Dans la fenêtre Règles de pare-feu, cliquez sur **Ajouter** ou **Modifier**.



Nom : saisissez un nom pour la règle.

Activé : cliquez sur le bouton bascule pour rendre la règle active.

Ajoutez des actions et des conditions pour la règle de pare-feu :

Action

Action : sélectionnez si vous souhaitez **autoriser/bloquer** la communication qui correspond aux conditions définies dans cette règle ou si vous souhaitez que ESET Internet Security envoie une **demande** à l'utilisateur chaque fois que la communication s'établit.
Règle de journal : si la règle est appliquée, elle sera enregistrée dans les fichiers journaux.
Consigner la gravité : sélectionnez la sévérité de l'enregistrement de journal pour cette règle.
Avertir l'utilisateur affiche une notification lorsque la règle est appliquée.

Application

Spécifiez une application dans laquelle cette règle sera appliquée.
Chemin d'accès de l'application : cliquez sur **...** et accédez à une application ou tapez le chemin d'accès complet de l'application (par exemple C:\Program Files\Firefox\Firefox.exe). Ne saisissez PAS uniquement le nom de l'application.
Signature de l'application : vous pouvez appliquer la règle aux applications basées sur leurs signatures (nom de l'éditeur). Sélectionnez dans le menu déroulant si vous souhaitez appliquer la règle à toutes les applications ayant une **signature valide** ou aux applications **signées par un signataire spécifique**. Si vous sélectionnez les applications **signées par un signataire spécifique**, vous devez définir le signataire dans le champ **Nom du signataire**.
Application de Microsoft Store : sélectionnez une application installée à partir de Microsoft Store dans le menu déroulant.
Service : vous pouvez sélectionner un service système au lieu d'une application. Ouvrez le menu déroulant pour sélectionner un service.
Appliquer aux processus enfants : certaines applications peuvent exécuter plusieurs processus même si vous ne voyez qu'une seule fenêtre d'application. Cliquez sur le bouton bascule pour activer la règle pour chaque processus de l'application spécifiée.

Direction

Sélectionnez la **direction** de la communication pour cette règle :
- **Deux sens :** communication entrante et sortante
- **Entrante :** communication entrante uniquement
- **Sortante :** communication sortante uniquement

Protocole IP

Sélectionnez un **protocole** dans le menu déroulant si vous souhaitez que cette règle s'applique seulement à un protocole spécifique.

Hôte local

Adresses locales, plage d'adresses ou sous-réseau où cette règle est appliquée. Si aucune adresse n'est spécifiée, la règle s'appliquera à toutes les communications avec les hôtes locaux. Vous pouvez ajouter des adresses IP, des plages d'adresses ou des sous-réseaux directement dans le champ de texte **IP** ou sélectionner parmi les jeux d'adresses IP existants en cliquant sur **Modifier** en regard **Jeux d'adresses IP**.

Port local

Numéro(s) de **port** locaux. Si aucun numéro n'est fourni, la règle s'appliquera à n'importe quel port. Vous pouvez ajouter un seul port de communication ou une plage de ports de communication.

Hôte distant

Adresse distante, plage d’adresses ou sous-réseau où cette règle est appliquée. Si aucune adresse n’est spécifiée, la règle s’appliquera à toutes les communications avec des hôtes distants. Vous pouvez ajouter des adresses IP, des plages d’adresses ou des sous-réseaux directement dans le champ de texte **IP** ou sélectionner parmi les jeux d’adresses IP existants en cliquant sur **Modifier** en regard **Jeux d’adresses IP**.

Port distant

Numéro(s) de **port** distant. Si aucun numéro n’est fourni, la règle s’appliquera à n’importe quel port. Vous pouvez ajouter un seul port de communication ou une plage de ports de communication.

Profil

Une règle de pare-feu peut être appliquée à des profils de connexion réseau spécifiques.
Tous : La règle sera appliquée à toute connexion réseau indépendamment du profil utilisé.
Sélectionné : la règle sera appliquée à une connexion réseau spécifique selon le profil sélectionné. Cochez la case en regard des profils que vous souhaitez sélectionner.

Voici un exemple dans lequel nous créons une nouvelle règle pour permettre à l'application du navigateur Web Firefox d'accéder à Internet ou aux sites Web du réseau local.
1. Dans la section **Action**, sélectionnez **Action** > **Autoriser**.
2. Dans la section **Application**, spécifiez le **chemin d’accès de l’application** du navigateur Web (par exemple C:\Program Files\Firefox\Firefox.exe). Ne saisissez PAS uniquement le nom de l'application.
3. Dans la section **Direction**, sélectionnez **Direction** > **Sortante**.
4. Dans la section **Protocole IP**, sélectionnez **TCP et UDP** dans le menu déroulant de **Protocole**.
5. Dans la section **Port distant**, ajoutez les numéros de **Port** : *80,443* pour permettre une navigation standard.

Détection des modifications d'application

La fonction de détection de modification d'application affiche des notifications si des applications modifiées, pour lesquelles une règle de pare-feu existe, tentent d'établir des connexions. La modification d'application est un mécanisme de remplacement temporaire ou permanent d'une application d'origine par une autre application par un exécutable différent (protection contre les abus de règles de pare-feu).

Veuillez prendre note que cette fonctionnalité n'est pas destinée à détecter des modifications sur n'importe quelle application en général. Le but est plutôt d'éviter une utilisation abusive des règles de pare-feu existantes, et seules les applications pour lesquelles des règles de pare-feu spécifiques existent sont surveillés.

Pour modifier la **détection des modifications d’application**, ouvrez Configuration avancée > **Protections** > **Protection de l'accès au réseau** > **Pare-feu** > **Détection des modifications d’application**.

Activer la détection des modifications d'applications - Si cette option est cochée, le programme surveille les modifications apportées aux applications (mises à jour, infections ou autres modifications). Quand une application modifiée tentera d'établir une connexion, vous serez averti par le pare-feu.

Autoriser la modification des applications signées (fiables) - Ne pas notifier si l'application possède la même signature numérique valide avant et après la modification.

Liste des applications exclues de la détection : Cette fenêtre vous permet d'ajouter ou de supprimer des applications individuelles pour lesquelles des modifications sont autorisées sans notification.

Liste des applications exclues de la détection

Le pare-feu dans ESET Internet Security détecte les modifications sur les applications pour lesquelles des règles existent (voir Détection des modifications à l'applications).

Dans certains cas, vous pouvez décider de ne pas utiliser cette fonctionnalité pour certaines applications et exclure celles-ci du contrôle par le pare-feu.

Ajouter - Ouvre une fenêtre dans laquelle vous pouvez sélectionner une application à ajouter à la liste des applications exclues de la détection des modifications. Vous pouvez choisir dans une liste d'applications en cours d'exécution avec une communication réseau ouverte, pour lesquelles il existe une règle de pare-feu ou ajouter une application spécifique.

Modifier - Ouvre une fenêtre dans laquelle vous pouvez modifier l'emplacement d'une application qui se trouve sur la liste des applications exclues de la détection des modifications. Vous pouvez choisir dans une liste d'applications en cours d'exécution avec une communication réseau ouverte, pour lesquelles il existe une règle de pare-feu ou de modifier l'emplacement maniellement.

Retirer - Supprime les entrées de la liste des applications exclues de la détection des modifications.

Protection contre les attaques sur le réseau (IDS)

La protection contre les attaques du réseau (IDS) améliore la détection des failles pour les vulnérabilités connues. Pour en savoir plus sur la protection contre les attaques de réseau, consultez le glossaire. Pour configurer la protection contre les attaques réseau, ouvrez Configuration avancée > **Protections** > **Protection de l'accès au réseau** > **Protection contre les attaques réseau**.

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

Activer la protection de réseaux de zombies - Détecte et bloque les communications avec les commandes malveillantes et les serveurs de contrôle en se basant sur les modèles types lorsque l'ordinateur est infecté et qu'un bot tente d'établir une communication. Pour en savoir plus sur la protection contre les réseaux de zombies, consultez le glossaire.

Règles IDS : cette option permet de configurer les options de filtrage avancées pour détecter plusieurs types d'attaques et de codes malveillants exploitant une faille de sécurité pouvant être utilisés pour nuire à votre ordinateur.

> **Instructions illustrées**
> Les articles suivants de la base de connaissances ESET peuvent n'être disponibles qu'en anglais :
> - Exclure une adresse IP de l'IDS dans ESET Internet Security

Tous les événements importants détectés par la protection du réseau sont enregistrés dans un fichier journal. Voir Journal de protection du réseau pour plus d'informations.

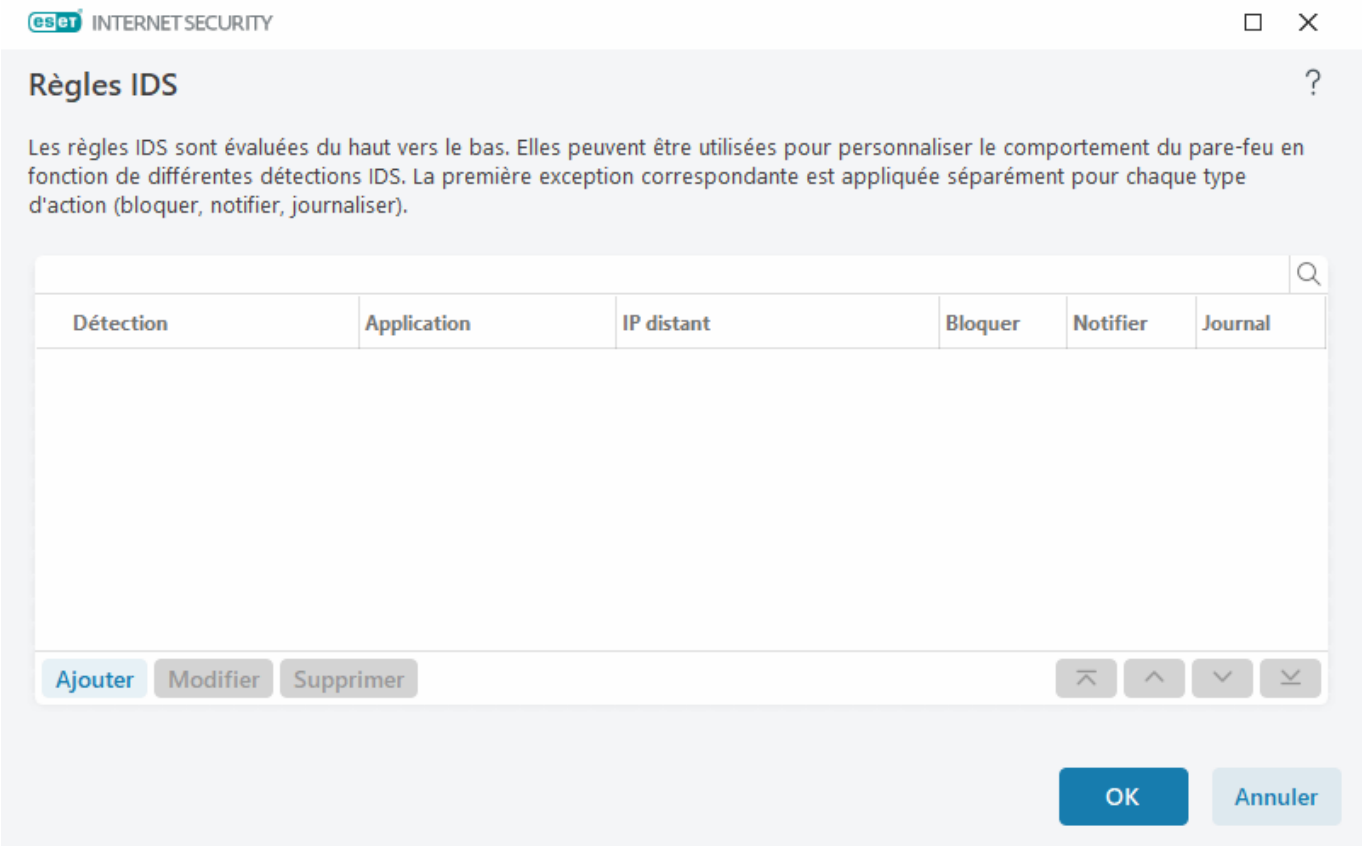
IDS règles

Dans certaines situations, l'Intrusion Detection Service (service de détection d'intrusion) (IDS) peut détecter la communication entre les routeurs ou d'autres périphériques réseau internes comme une attaque potentielle. Par exemple, vous pouvez ajouter une adresse connue, sans danger, aux adresses exclues de la zone IDS pour contourner l'IDS.

> **Instructions illustrées**
> Les articles suivants de la base de connaissances ESET peuvent n'être disponibles qu'en anglais :
> - Exclure une adresse IP de l'IDS dans ESET Internet Security

Gestion des règles IDS

- **Ajouter** - Cliquez pour créer une nouvelle règle IDS.
- **Modifier** - Cliquez pour modifier une règle IDS existante.
- **Supprimer** - Sélectionnez et cliquez si vous voulez retirer une règle IDS de la liste des règles IDS.
- **Au dessus/Vers le haut/Vers le bas/En dessous** - Permet de définir le niveau de priorité des règles (les exceptions sont évaluées du haut vers le bas).



Éditeur de règle

Détection – Types de détection.

Nom de la menace : vous pouvez spécifier un nom de menace pour certaines des détections disponibles.

Application – Sélectionnez le chemin du fichier d'une application qui fait partie des exceptions en cliquant sur ... (par exemple *C:\Program Files\Firefox\Firefox.exe*). Ne saisissez PAS le nom de l'application.

Adresse IP distante - Liste d'adresses, de plages d'adresses ou de sous-réseaux IPv4 ou IPv6 distants. Les adresses multiples doivent être séparées par une virgule.

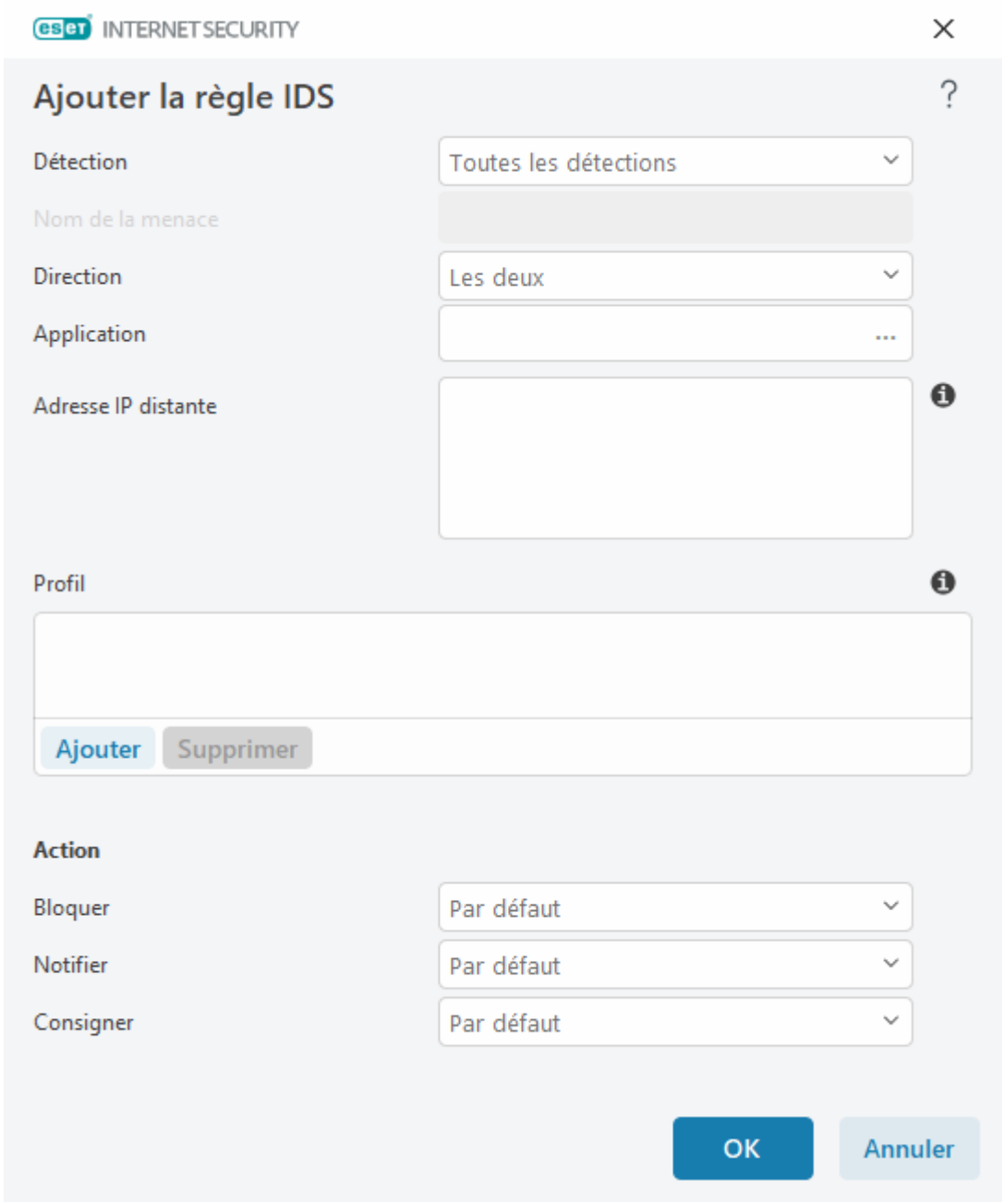
Profil : vous pouvez choisir un profil de connexion réseau auquel cette règle s'appliquera.

Action

Bloquer - Chaque processus du système a son propre comportement par défaut et sa propre action attribuée (bloquer ou autoriser). Pour écraser le comportement par défaut de ESET Internet Security, vous pouvez choisir de la bloquer ou de l'autoriser à partir du menu déroulant.

Notifier – Sélectionnez Oui pour afficher Notifications sur le bureau sur votre ordinateur. Sélectionnez Non si vous ne voulez pas de notifications sur le bureau. Les valeurs disponibles sont Par défaut/Oui/Non.

Journaliser – Sélectionnez **Oui** pour enregistrer les événements dans les fichiers journaux. Sélectionnez **Non**si vous ne voulez pas enregistrer les événements. Les valeurs disponibles sont **par défaut**/**Oui**/**Non**.



Si vous souhaitez afficher une notification et faire une inscription au journal chaque fois que l'événement se produit :

1.Cliquez sur **Ajouter** pour ajouter une nouvelle règle IDS.

2.Sélectionnez une détection particulière dans le menu déroulant **Détection**.

3.Choisissez un chemin d'application pour lequel vous souhaitez appliquer cette notification en cliquant sur **...**.

4.Laissez la **valeur par défaut** dans le menu déroulant **Bloquer**. L'action par défaut appliquée par ESET Internet Security sera alors héritée.

5.Mettez les menus déroulants **Notifier** et **Journaliser** à **Oui**.

6.Cliquez sur **OK** pour enregistrer cette notification.

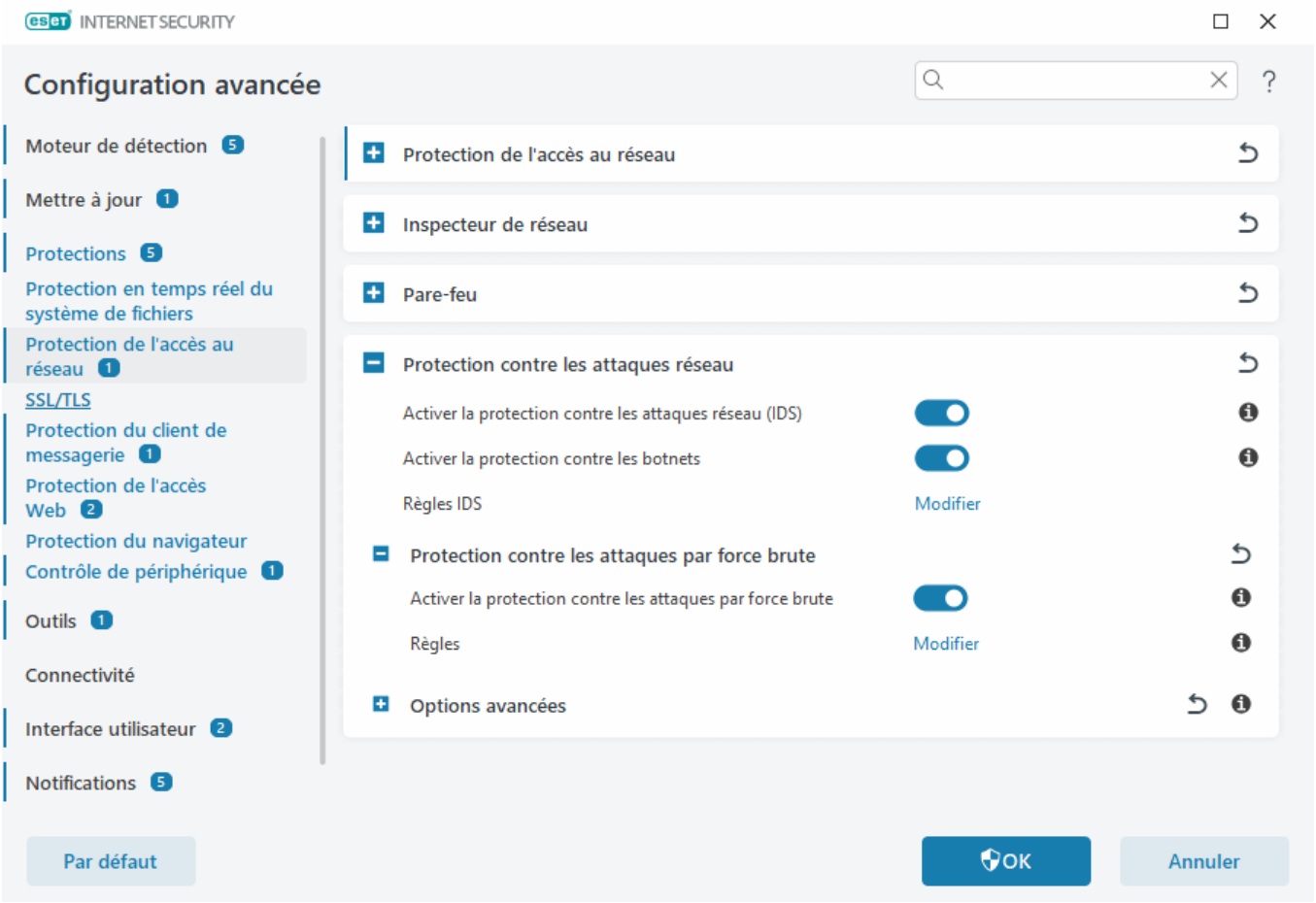
Si vous ne souhaitez pas afficher une notification récurrente d'une menace que vous ne considérez pas comme étant d'un type particulier de **détection** :
1.Cliquez sur **Ajouter** pour ajouter une nouvelle règle IDS.
2.Sélectionnez une détection particulière dans le menu déroulant **Détection**, par exemple, **Session SMB sans extension de sécurité** ou **Attaque par balayage de ports TCP**.
3.Sélectionnez **Entrant** dans le menu déroulant de direction dans le cas où il s'agit d'une communication entrante.
4.Mettez le menu déroulant **Notifier** sur **Non**.
5.Mettez le menu déroulant **Journaliser** sur **Oui**.
6.Laissez**Application** vide.
7.Si la communication ne provient pas d'une adresse IP particulière, laissez **Adresse IP distante** vide.
8.Cliquez sur **OK** pour enregistrer cette notification.

Protection contre les attaques par force brute

La protection contre les attaques par force brute bloque les attaques visant à deviner le mot de passe pour les services RDP et SMB. Une attaque par force brute est une méthode permettant de deviner un mot de passe ciblé en essayant systématiquement toutes les combinaisons de lettres, de chiffres et de symboles. Pour configurer la protection contre les attaques par force brute, ouvrez Configuration avancée > **Protections** > **Protection de l'accès au réseau** > **Protection contre les attaques réseau (IDS)** > **Protection contre les attaques par force brute**.

Activer la protection contre les attaques par force brute - ESET Internet Security inspecte le contenu du trafic réseau et bloque les tentatives d'attaques par devinette du mot de passe.

Règles : vous permettent de créer, de modifier et d'afficher des règles pour les connexions réseau entrantes et sortantes. Pour plus d'informations, consultez le chapitre Règles.



Règles

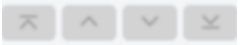
Les règles de protection contre les attaques par force brute vous permettent de créer, de modifier et d'afficher des règles pour les connexions réseau entrantes et sortantes. Les règles prédéfinies ne peuvent pas être modifiées ni supprimées.

Gestion des règles de protection contre les attaques par force brute

Ajouter - Crée une nouvelle règle.

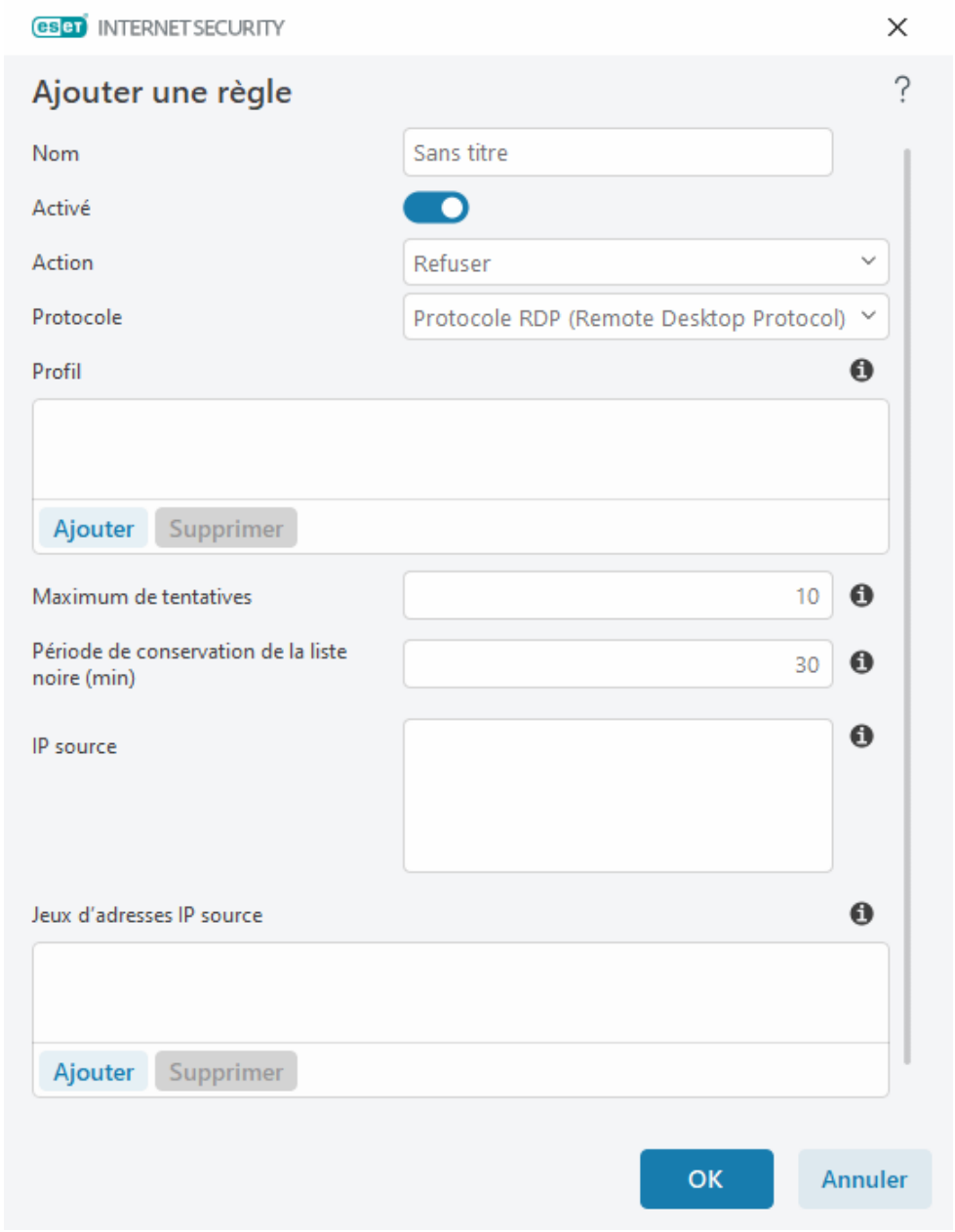
Modifier – Modifier une règle existante.

Supprimer permet de supprimer une règle existante de la liste des règles.

 **Première/Vers le haut/Vers le bas/Dernière** permet de définir le niveau de priorité des règles.

> Pour assurer la protection la plus élevée possible, la règle de blocage dont la valeur **Tentatives max** est la plus faible est appliquée même si la règle se situe plus bas dans la liste des règles dans le cas où plusieurs règles de blocage correspondent aux conditions de détection.

Éditeur de règle



Nom : le nom du règle.

Activé : désactivez ce bouton bascule si vous voulez conserver la règle dans la liste sans l'appliquer.

Action permet de choisir s'il faut **refuser** ou **autoriser** la connexion si les paramètres de règle sont respectés.

Protocole : il s'agit du protocole de communication que cette règle examinera.

Profil : des règles personnalisées peuvent être définies et appliquées pour des profils particuliers.

Maximum de tentatives : Le nombre maximal de tentatives d'attaque avant que l'adresse IP ne soit bloquée et ajoutée à la liste noire.

Période de rétention de la liste noire (min) : définit l'heure à laquelle l'adresse de la liste noire expire.

Adresse IP de source : liste d'adresses IP, de plages ou de sous-réseaux. Les adresses multiples doivent être séparées par une virgule.

Ensembles d'adresses IP source : ensembles d'adresses IP que vous avez déjà définies dans des ensembles

d’adresses IP.

Options avancées

Dans Configuration avancée > **Protections** > **Protection de l'accès au réseau** > **Protection contre les attaques réseau (IDS)** > **Options avancées**, vous pouvez activer ou désactiver la détection de plusieurs types d’attaques et d’exploits qui peuvent endommager votre ordinateur.

Dans certains cas, vous ne recevrez pas de notification de menace sur les communications bloquées. Voir la section Journalisation et création de règles ou d'exceptions à partir du journal pour des instructions sur la consultation de toutes les communications bloquées dans le journal de pare-feu.

Certaines options spécifiques de cette fenêtre peuvent varier selon le type ou la version de votre produit ESET et du module de pare-feu ainsi que de la version de votre système d'exploitation.

Détection d'intrusion

La détection d'intrusion surveille la communication avec les périphériques réseau pour y déceler toute activité malveillante.

- **ProtocoleSMB** - Détecte et bloque les divers problèmes de sécurité dans le protocole SMB.
- **Protocole RPC** - Détecte et bloque divers CVE dans le système d'appel de la procédure distante développé pour le Distributed Computing Environment (DCE).
- **Protocole RDP** - Détecte et bloque divers CVE dans le protocole RDP (voir ci-dessus).
- **ARP Détection des attaques par empoisonnement ARP** - Détection des attaques par empoisonnement ARP causées par des attaques de type « l'homme du milieu » (man-in-the-middle) ou par la détection du reniflage au niveau du commutateur de réseau. Le protocole ARP (Protocole de résolution d'adresse) est utilisé par l'application réseau ou le périphérique pour déterminer l'adresse Ethernet.
- Détection des attaques de balayage des ports **TCP/UDP** - Détecte les attaques des logiciels de balayage de ports - une application conçue pour sonder un hôte afin d'y détecter des ports ouverts. Il envoie, pour ce faire, des requêtes client à un vaste éventail d'adresses de port dans l'objectif de trouver des ports actifs et d'exploiter les vulnérabilités du service. Pour en savoir plus sur ce type d'attaque, consultez le glossaire. Pour en savoir plus sur ce type d'attaque, consultez le glossaire.
- **Bloquer l'adresse dangereuse après la détection d'une attaque** - Les adresses IP ayant été détectées comme des sources d'attaque sont ajoutées à la liste noire pour éviter toute connexion pendant un certain temps. Vous pouvez définir la **période de rétention de la liste noire**, qui détermine la durée pendant laquelle l'adresse sera bloquée après la détection d'une attaque.
- **Afficher une notification à la détection d'une attaque** – Active la notification de la zone de notification de Windows dans le coin inférieur droit de l'écran.
- **Afficher également des notifications à la détection d'une attaque sur des failles de sécurité** - Vous averti lorsque des attaques sur des failles de sécurité sont détectées ou si une menace tente d'entrer dans le système en utilisant des failles de sécurité.

Inspection des paquets

Un type d'analyse de paquet qui filtre les données qui transitent par le réseau.

- **Autoriser les connexions entrantes sur les partages admin dans le protocole SMB**- Les partages d'administration constituent les partages réseau par défaut qui partagent par défaut les partitions du disque dur (*C$*, *D$*, ...) du système, et du dossier de fichiers (ADMIN$*ADMIN$*). Désactiver la connexion aux partages d'administration devrait réduire bon nombre de risques pour la sécurité. Par exemple, le ver Conficker utilise les attaques par dictionnaire pour se connecter aux partages d'administration.

- **Refuser les anciens dialectes SMB (non pris en charge)** - Refuser des sessions SMB utilisant un ancien dialecte SMB, non pris en charge par IDS. Les systèmes d'exploitation Windows modernes prennent en charge les anciens dialectes SMB en raison de la rétrocompatibilité avec les anciens systèmes d'exploitation comme Windows 95. Le pirate peut utiliser un ancien dialecte dans une session SMB pour éviter l'inspection. Refusez les anciens dialectes SMB si votre ordinateur n'a pas à partager de fichiers (ou à utiliser la communication SMB en général) avec un ordinateur utilisant une version antérieure de Windows.

- **Refuser les sessions SMB sans sécurité étendue** - La sécurité étendue peut être utilisée pendant la négociation de session SMB afin de fournir un mécanisme d'authentification plus sécurisé que l'authentification par question/réponse du gestionnaire du réseau local (LM). Le schéma LM est jugé faible et son utilisation n'est pas recommandée.

- **Refuser l'ouverture de fichiers exécutables sur un serveur hors de la zone de confiance dans le protocole SMB** - Refuse la connexion lorsque vous tentez d'ouvrir un fichier exécutable (.exe, .dll, etc.) à partir d'un dossier partagé sur le serveur qui n'appartient pas à la zone de confiance du pare-feu. Notez que la copie de fichiers exécutables provenant de sources fiables peut être légitime. Veuillez prendre note que copier des fichiers exécutables à partir de sources fiables peut être légitime, mais cette détection devrait atténuer les risques de l'ouverture non désirée d'un fichier sur un serveur malveillant (par exemple, un fichier ouvert en cliquant sur un lien hypertexte vers un fichier exécutable malveillant commun).

- **Refuser l'authentification NTLM dans le protocole SMB pour la connexion à un serveur à l'intérieur ou à l'extérieur de la zone de confiance** - Les protocoles qui utilisent les schémas d'authentification NTLM (dans ses deux versions) sont sujets à une attaque avec transfert d'identifiants (appelée attaque par relais SMB dans le cas du protocole SMB). Refuser l'authentification NTLM à un serveur à l'extérieur de la zone de confiance devrait réduire les risques d'attaques avec transferts d'identifiants effectuée par un serveur malveillant se trouvant en dehors de la zone de confiance. Vous pouvez également refuser l'authentification NTLM aux serveurs se trouvant dans la zone de confiance.

- **Autoriser les communications avec le service Security Account Manager** - Pour de plus amples renseignements sur ces services, voir [MS-SAMR].

- **Autoriser les communications avec le service Local Security Authority** - Pour de plus amples renseignements sur ces services, voir [MS-LSAD] et [MS-LSAT].

- **Autoriser les communications avec le service Remote Registry** - Pour de plus amples renseignements sur ces services, voir [MS-RRP].

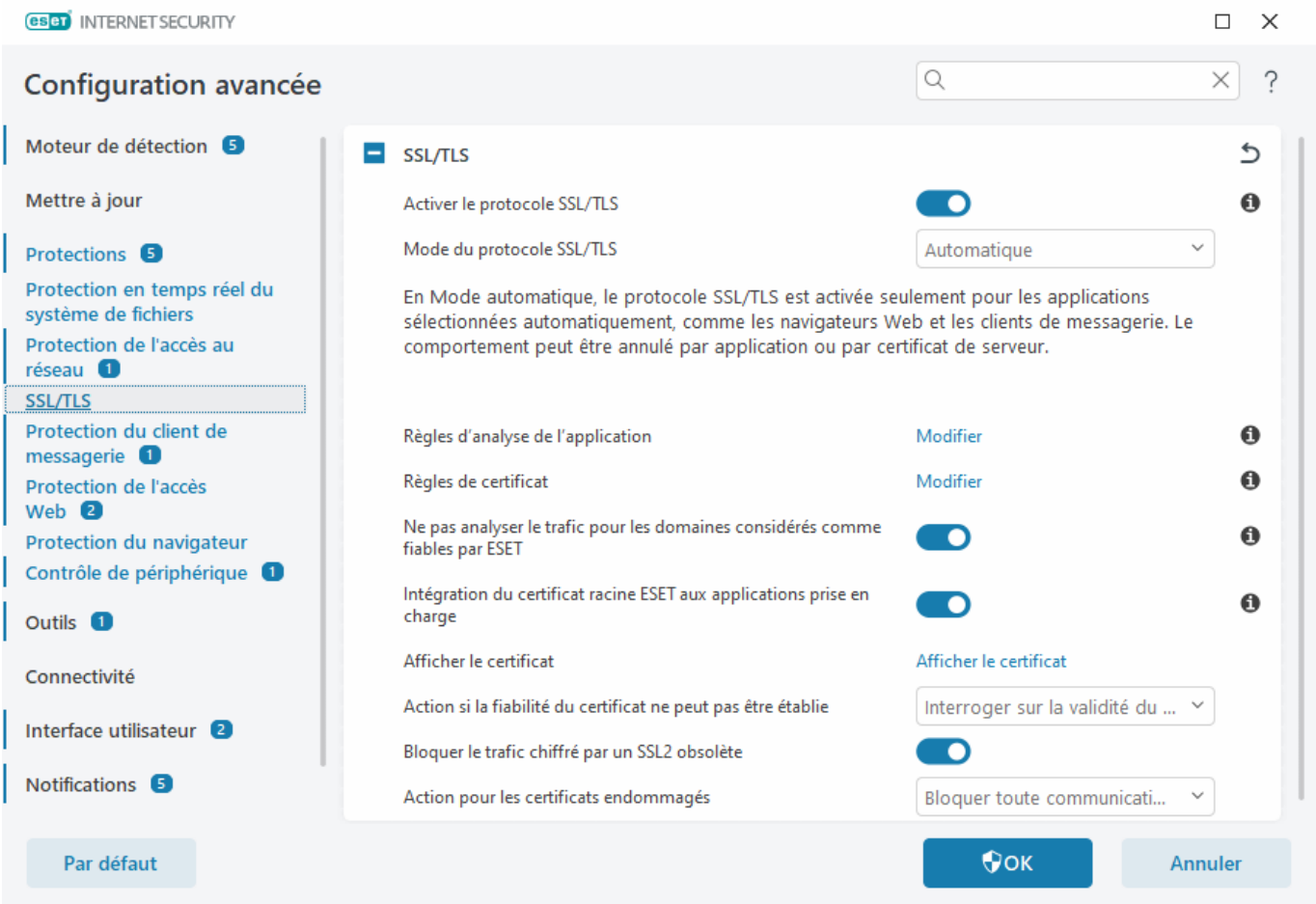
- **Autoriser les communications avec le service Service Control Manager** - Pour de plus amples renseignements sur ces services, voir [MS-SCMR].

- **Autoriser les communications avec le service Server** - Pour de plus amples renseignements sur ces services, voir [MS-SRVS].

- **Autoriser les communications avec les autres services** - Autres services MSRPC. MSRPC est la version Microsoft du mécanisme DCE RPC. MSRPC peut également utiliser des canaux nommés intégrés dans le protocole SMB (partage de fichiers réseau) pour le transport (ncacn_np transport). Les services MSRPC fournissent les interfaces permettant d'accéder à distance à vos systèmes Windows et de les gérer. Plusieurs vulnérabilités connexes à la sécurité ont été découvertes dans le système MSRPC de Windows puis utilisées à mauvais escient (vers Conficker, Sasser, etc.). Désactiver la communication avec les services MSRPC dont vous n'avez pas besoin peut permettre de réduire bon nombre de risques pour la sécurité (comme l'exécution de code à distance ou des attaques par déni de service).

SSL/TLS

ESET Internet Security peut vérifier les menaces de communication qui utilisent le protocole SSL. Vous pouvez utiliser différents modes de filtrage pour les communications protégées par SSL à l'aide des certificats fiables, des certificats inconnus ou des certificats exclus de la vérification des communications protégées par SSL. Pour modifier les paramètres SSL/TLS, ouvrez Configuration avancée > **Protections** > **SSL/TLS**.



Activer SSL/TLS : si cette option est désactivée, ESET Internet Security n'analysera pas les communications utilisant SSL/TLS.

Le mode **SSL/TLS** est disponible dans les options suivantes :

Mode de filtrage	Description
Automatique	Le mode par défaut qui n'analysera que les applications appropriées comme les navigateurs Web et les clients de messagerie. Vous pouvez l'ignorer en sélectionnant les applications dans lesquelles la communication est numérisée.

Mode de filtrage	Description
Interactif	Si vous entrez un nouveau site protégé par SSL (avec un certificat inconnu), une boite de dialogue de sélection d'action s'affiche. Ce mode permet de créer une liste de certificats ou d'applications SSL qui seront exclus de l'analyse.
Basé sur des règles personnalisées	Sélectionnez cette option pour analyser toutes les communications protégées par SSL à l'exception des communications protégées par des certificats exclus de la vérification. Si une nouvelle communication utilisant un certificat signé, mais inconnu est établie, vous n'en serez pas avisé et la communication sera automatiquement filtrée. Lorsque vous accédez à un serveur en utilisant un certificat non fiable indiqué comme étant fiable (ajouté à la liste des certificats fiables), la communication avec le serveur est permise et le contenu du canal de communication est filtré.

Règles d'analyse des applications : vous permet de personnaliser le comportement de ESET Internet Security pour des applications spécifiques.

Règles des certificats : vous permet de personnaliser le comportement de ESET Internet Security pour des certificats SSL spécifiques.

Ne pas analyser le trafic pour les domaines considérés comme fiables par ESET : lorsque cette option est activée, la communication avec des domaines considérés comme fiables est exclue de l'analyse. Une liste blanche intégrée gérée par ESET détermine la fiabilité d'un domaine.

Intégrer le certificat racine ESET dans les applications prises en charge : 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). Lorsque cette option est activée, ESET Internet Security ajoutera automatiquement le certificat racine ESET SSL Filter CA aux navigateurs connus (par exemple, Opera). Pour les navigateurs utilisant le magasin de certification du système, le certificat est ajouté automatiquement. Par exemple, Firefox est automatiquement configuré pour faire confiance aux autorités Racine dans le magasin de certification du système.

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.

Action si la fiabilité du certificat ne peut pas être établie : dans certains cas, un certificat de site Web ne peut pas être vérifié à l'aide du magasin TRCA (Trusted Root Certification Authorities). C'est le cas par exemple d'un certificat expiré, d'un certificat non approuvé, d'un certificat non valide pour le domaine ou d'une signature spécifique pouvant être analysé, mais ne signant pas le certificat correctement. Les sites Web légitimes utiliseront toujours des certificats approuvés. S'ils n'en fournissent pas, cela pourrait signifier qu'un pirate déchiffre votre communication ou que le site Web rencontre des difficultés techniques.

Si l'option **Interroger sur la validité du certificat** (valeur par défaut) est sélectionnée, vous serez invité à sélectionner une action à prendre lorsqu'une communication chiffrée est établie. Une boîte de dialogue de sélection d'une action dans laquelle vous pouvez marquer le certificat comme fiable ou exclus s'affichera. Dans les cas où le certificat ne fait pas partie de la liste TRCA, la fenêtre sera rouge. Si le certificat fait partie de la liste TRCA, la fenêtre sera verte.

Vous pouvez sélectionner **Bloquer toute communication utilisant le certificat** pour qu'elle mette toujours fin à une connexion chiffrée à un site qui utilise un certificat non approuvé.

Bloquer le trafic chiffré par un SSL2 obsolète : les communications utilisant une version antérieure du protocole SSL seront automatiquement bloquées.

Action pour les certificats endommagés : un certificat endommagé indique que le certificat utilise un format non reconnu par ESET Internet Security ou qu'il a été endommagé (par exemple, écrasé par des données aléatoires). Dans ce cas, nous vous recommandons de laisser l'option **Bloquer toute communication utilisant le certificat** sélectionnée. Si l'option **Interroger sur la validité du certificat** est sélectionnée, l'utilisateur est invité à sélectionner une action à entreprendre lorsque la communication chiffrée est établie.

> **Exemples illustrés**
> Les articles suivants de la base de connaissances ESET peuvent n'être disponibles qu'en anglais :
> - Avis de certificat dans les produits ESET Windows Home
> - « Trafic réseau chiffré : Certificat non approuvé » s'affiche lors de la visite de pages Web

Règles d'analyse de l'application

Les **règles d'analyse de l'application** peuvent être utilisées pour personnaliser le comportement de ESET Internet Security pour des applications spécifiques et mémoriser les actions choisies lorsque le **mode SSL/TLS** est en **mode Interactif**. La liste peut être affichée et modifiée dans Configuration avancée > **Protections** > **SSL/TLS** > **Règles d'analyse de l'application** > **Modifier**.

La fenêtre **Règles d'analyse de l'application** se compose de :

Colonnes

Application - Choisissez un fichier exécutable dans l'arborescence de répertoire, cliquez sur l'option **...** ou entrez manuellement le chemin d'accès.

Action d'analyse - Sélectionnez **Analyser** ou **Ignorer** pour procéder à l'analyse ou ignorer la communication. Sélectionnez **Auto** pour activer le mode d'analyse automatique et demander l'action à entreprendre en mode interactif. Sélectionnez **Demander** pour toujours demander à l'utilisateur l'action à entreprendre.

Éléments de contrôle

Ajouter - Ajouter l'application filtrée.

Modifier - Sélectionnez l'application que vous voulez configurer et cliquez sur **Modifier**.

Supprimer - Sélectionnez l'application que vous voulez supprimer et cliquez sur **Supprimer**.

Importation/Exportation**–** Importez des applications à partir d'un fichier ou enregistrez votre liste actuelle d'applications dans un fichier.

OK/**Annuler** - Cliquez sur **OK** si vous souhaitez enregistrer les modifications ou cliquez sur **Annuler** si vous souhaitez quitter sans enregistrer.

Règles de certificat

Les règles de certificat peuvent être utilisées pour personnaliser le comportement de ESET Internet Security pour des certificats SSL spécifiques et pour mémoriser les actions choisies lorsque le **mode SSL/TLS** est en **mode interactif**. La liste peut être consultée et modifiée dans Configuration avancée > **Protections** > **SSL/TLS** > **Règles**

de certificat > **Modifier**.

La fenêtre **Règles de certificat** se compose de :

Colonnes

Nom - Le nom du certificat.

Émetteur du certificat - Nom du créateur du certificat.

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

Accès - Sélectionnez **Autoriser**ou **Bloquer** comme **Action d'accès** pour autoriser ou bloquer toute communication sécurisée par ce certificat indépendamment de sa fiabilité. Sélectionnez **Auto** pour autoriser les certificats fiables et demander l'action à entreprendre pour les certificats non fiables. Sélectionnez **Demander** pour toujours demander à l'utilisateur l'action à entreprendre.

Analyser - Sélectionnez **Analyser** ou **Ignorer** comme **action d'analyse** pour analyser ou ignorer toute communication sécurisée par ce certificat. Sélectionnez **Auto** pour activer le mode d'analyse automatique et demander l'action à entreprendre en mode interactif. Sélectionnez **Demander** pour toujours demander à l'utilisateur l'action à entreprendre.

Éléments de contrôle

Ajouter : Ajoutez un nouveau certificat et réglez les paramètres des options d'accès et d'analyse.

Modifier - Sélectionnez le certificat que vous voulez configurer et cliquez sur **Modifier**.

Supprimer : Sélectionnez le certificat que vous voulez supprimer et cliquez sur **Supprimer**.

OK/Annuler - Cliquez sur **OK** si vous souhaitez enregistrer les modifications ou cliquez sur **Annuler** si vous souhaitez quitter sans enregistrer.

Trafic réseau chiffré

Si votre système est configuré pour utiliser l'analyse du protocole SSL/TLS, une fenêtre de dialogue vous invitant à choisir une action s'affichera dans deux situations :

Premièrement, si un site utilise un certificat invérifiable ou non valide, et que ESET Internet Security est configuré pour demander l'avis de l'utilisateur dans de tels cas (par défaut oui pour les certificats invérifiables et non pour les certificats non valides), une boîte de dialogue vous demandera **d'autoriser** ou de **bloquer** la connexion. Si le certificat ne se trouve pas dans le Trusted Root Certification Authorities store (TRCA), il est considéré comme non approuvé.

Deuxièmement, si le **mode SSL/TLS** est réglé sur le **mode interactif**, une boîte de dialogue pour chaque site Web vous demandera si vous voulez **analyser** ou **ignorer** le trafic. Certaines applications vérifient que leur trafic SSL n'est ni modifié ni consulté par quiconque; dans de tels cas ESET Internet Security doit **ignorer** ce trafic pour que l'application continue de fonctionner.

Exemples illustrés

Les articles suivants de la base de connaissances ESET peuvent n'être disponibles qu'en anglais :

- Avis de certificat dans les produits ESET Windows Home
- « Trafic réseau chiffré : Certificat non approuvé » s'affiche lors de la visite de pages Web

Dans les deux cas, l'utilisateur peut choisir de mémoriser l'action sélectionnée. Les actions enregistrées sont stockées dans les règles de certificat.

Protection du client de messagerie

Pour configurer la protection du client de messagerie, ouvrez Configuration avancée > **Protections** > **Protection du client de messagerie** et choisissez parmi les options de configuration suivantes :

- Protection du transport de messagerie
- Protection de la boîte aux lettres
- Gestion des listes d'adresses
- ThreatSense

Protection du transport de messagerie

IMAP(S) et POP 3(S) sont les protocoles les plus couramment utilisés pour recevoir des courriels à l'aide d'une application de client de messagerie. Le protocole Internet Message Access Protocol (IMAP) est un autre protocole Internet utilisé pour la récupération des courriels. L'IMAP offre quelques avantages par rapport à POP3 : par exemple, plusieurs clients peuvent se connecter simultanément à la même boîte aux lettres et conserver l'information sur l'état des messages tel que le fait de savoir si le message a été lu ou non, si une réponse a été envoyée ou s'il a été supprimé. Le module de protection assurant ce contrôle est automatiquement lancé au démarrage du système et est alors actif en mémoire.

ESET Internet Security fournit une protection pour ces protocoles, indépendamment du client de messagerie utilisé, et sans nécessiter la reconfiguration du client de messagerie. Par défaut, toutes les communications via les protocoles POP3 et IMAP sont analysées, quels que soient les numéros de port POP3 / IMAP par défaut.
Le protocole MAPI n'est pas analysé. Cependant, la communication avec le serveur Microsoft Exchange peut être analysée par le module d'intégration dans les clients de messagerie tels que Microsoft Outlook.

ESET Internet Security prend également en charge l'analyse des protocoles IMAPS (585, 993) et POP3S (995) qui utilisent un canal chiffré pour transférer des informations entre un serveur et un client. ESET Internet Security contrôle la communication à l'aide des protocoles SSL (Secure Socket Layer) et TLS (Transport Layer Security).
Les communications chiffrées seront analysées par défaut. Pour afficher la configuration de l'analyseur, ouvrez Configuration avancée > **Protections** > SSL/TLS.

Pour configurer la protection du transport du courriel, ouvrez Configuration avancée > **Protections** > **Protection du client de messagerie** > **Protection du transport du courriel**.

Activer la protection du transport du courriel : lorsque cette option est activée, les communications de transport de courriels sont analysées par ESET Internet Security.

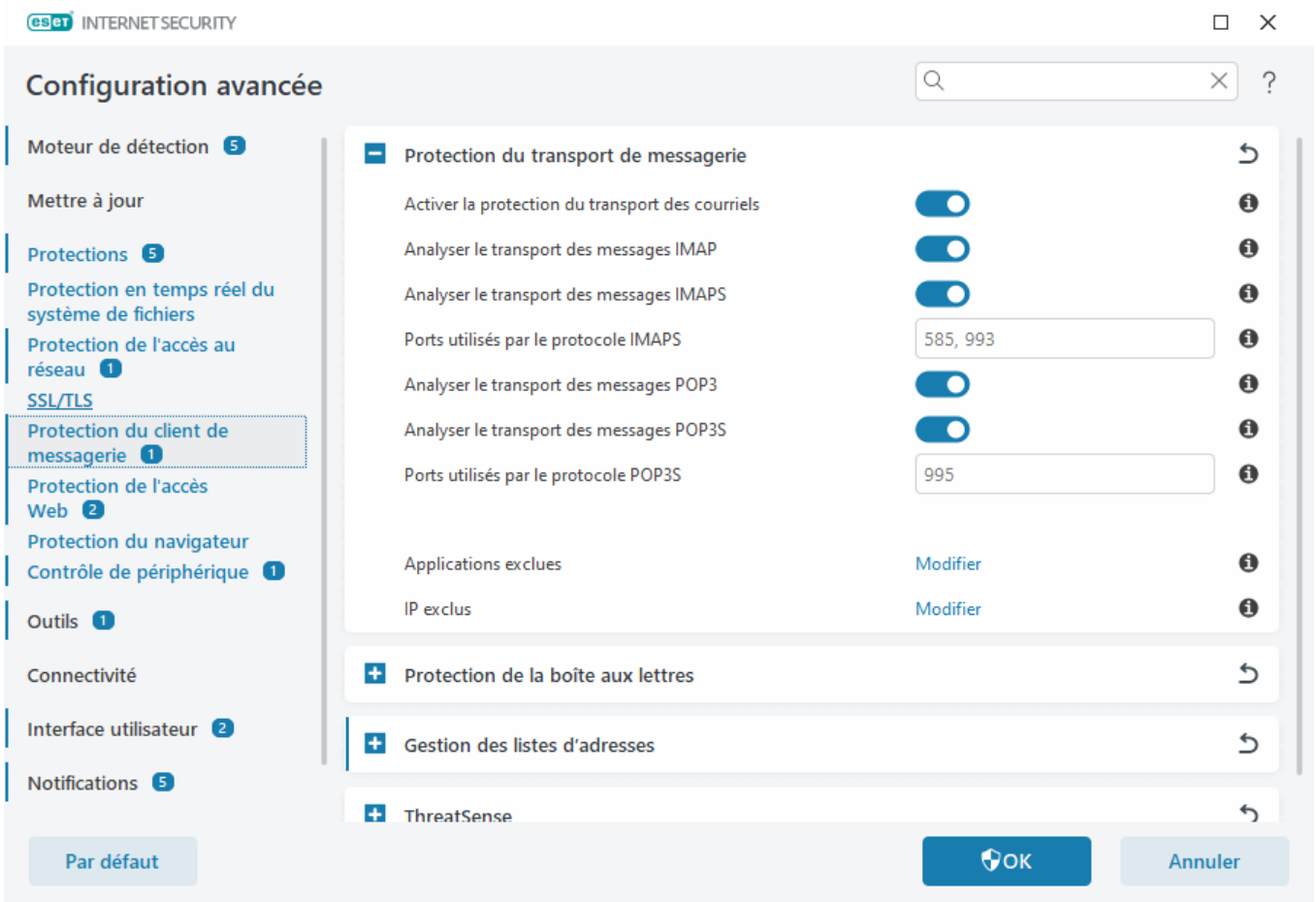
Vous pouvez choisir les protocoles de transport de courriels qui seront analysés en cliquant sur le bouton bascule en regard des options suivantes (par défaut, l'analyse de tous les protocoles est activée) :

- **Analyser le transport des messages IMAP**
- **Analyser le transport des messages IMAPS**
- **Analyser le transport des messages POP3**
- **Analyser le transport des messages POP3S**

Par défaut, ESET Internet Security analysera les communications IMAPS et POP3S sur les ports standard. Pour ajouter des ports personnalisés pour les protocoles IMAPS et POP3S, ajoutez-les au champ de texte en regard de **Ports utilisés par le protocole IMAPS** ou **Ports utilisés par le protocole POP3S**. Les numéros de ports multiples doivent être séparés par des virgules.

Applications exclues : vous permet d'exclure des applications spécifiques de l'analyse par la protection du transport du courriel. Elle est utile lorsque la protection de l'accès Web entraîne des problèmes de compatibilité.

Adresses IP exclues : vous permet d'exclure des adresses distantes spécifiques de l'analyse par la protection du transport du courriel. Elle est utile lorsque la protection de l'accès Web entraîne des problèmes de compatibilité.



Applications exclues

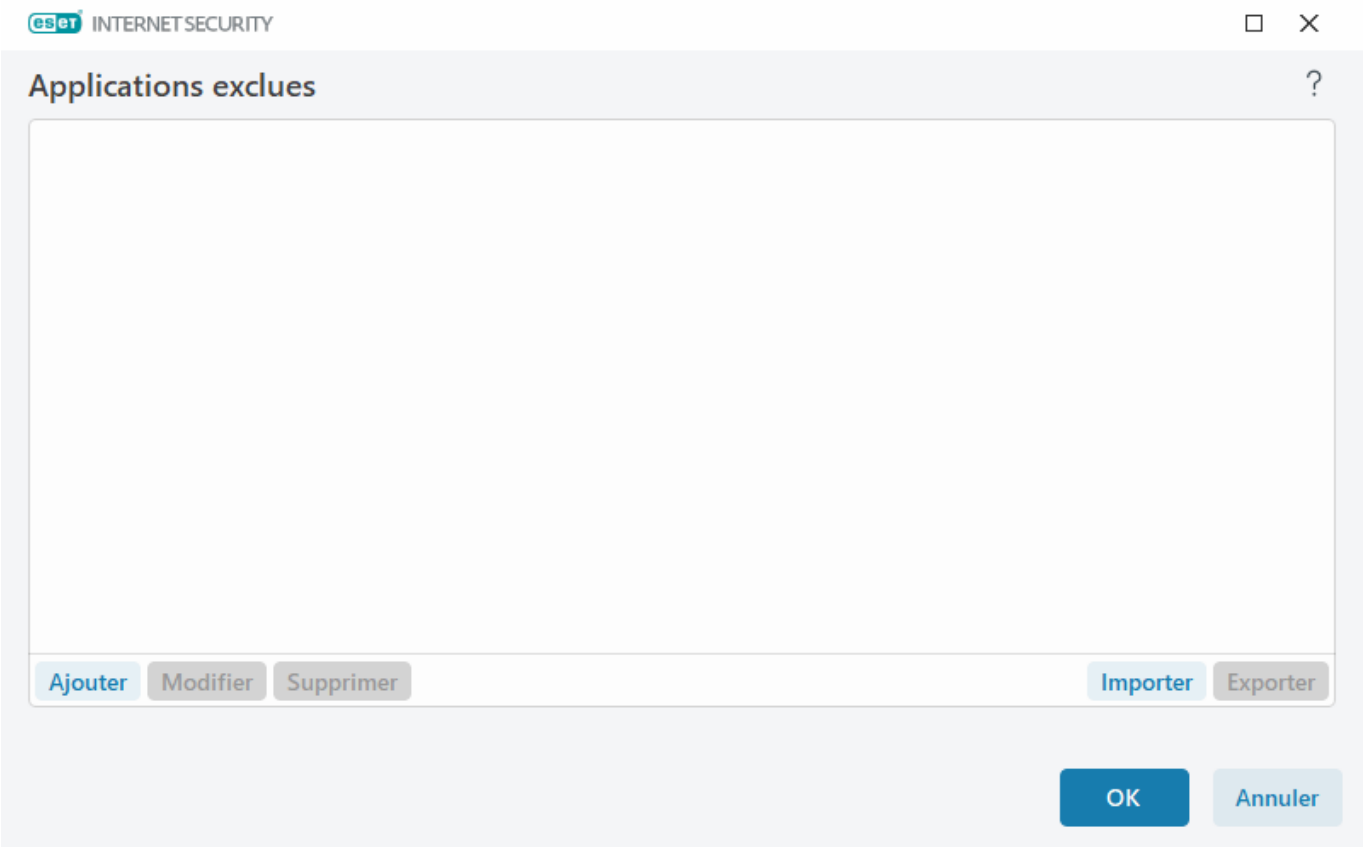
Pour exclure l'analyse des communications pour des applications spécifiques, ajoutez-les à la liste. Les communications envoyées par ces applications par les protocoles HTTP(S)/POP3(S)/IMAP(S) ne seront pas

vérifiées pour savoir si elles contiennent des menaces. Il est recommandé de n'utiliser cette option que pour les applications qui ne fonctionnent pas bien lorsque la communication fait l'objet d'une vérification.

Les applications et services en cours d'exécution seront automatiquement disponibles ici lorsque vous cliquez sur **Ajouter**. Cliquez sur **...** et accédez à une application pour ajouter l’exclusion manuellement.

Modifier - Modifie les entrées sélectionnées de la liste.

Retirer - Supprime des entrées de la liste.



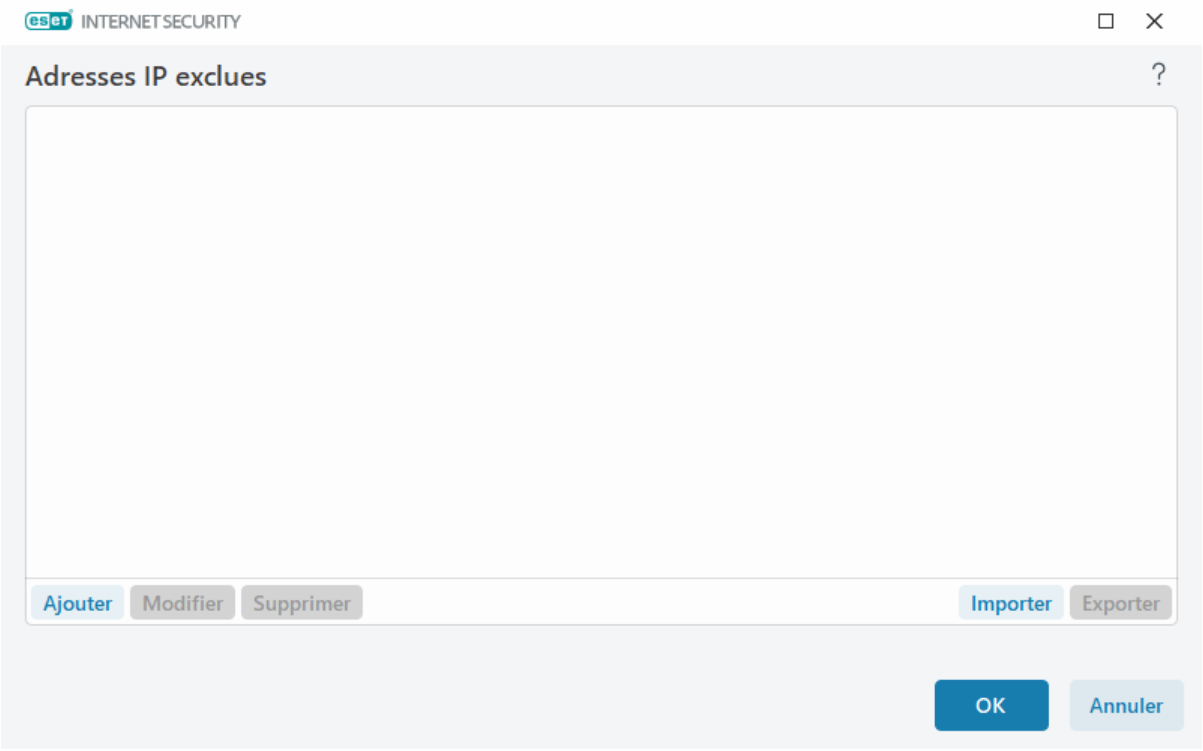
IP exclus

Les adresses inscrites dans cette liste seront exclues de l’analyse. Les communications envoyées à ces adresses ou reçues de celles-ci par les protocoles HTTP(S)/POP3(S)/IMAP(S) ne seront pas vérifiées pour savoir si elles contiennent des menaces. Il est recommandé de n'utiliser cette option que pour les adresses connues pour être fiables.

Cliquez sur **Ajouter** pour exclure une adresse IP, une plage d'adresses ou un sous-réseau d'un point distant.

Cliquez sur **Modifier** pour modifier l’adresse IP sélectionnée.

Cliquez sur **Retirer** pour supprimer les entrées sélectionnées de la liste.



Exemples d’adresses IP

Ajouter une adresse IPv4:
Adresse unique : ajoute l’adresse IP d’un seul ordinateur (par exemple, *192.168.0.10*).
Plage d’adresses : entrez la première et la dernière adresse IP pour préciser une plage d’adresse IP (de plusieurs ordinateurs) à laquelle appliquer la règle (par exemple, de *192.168.0.1 à 192.168.0.99*).
Sous-réseau - Sous-réseau (groupe d'ordinateurs) défini par une adresse IP et un masque. Par exemple, 255.255.255.0 est le masque de réseau pour le sous-réseau 192.168.1.0. Pour exclure le type de sous-réseau entier dans *192.168.1.0/24*.
Ajouter une adresse IPv6:
Adresse unique : ajoute l’adresse IP d’un seul ordinateur (par exemple, *2001:718:1c01:16:214:22ff:fec9:ca5*).
Sous-réseau - Sous-réseau (groupe d'ordinateurs) défini par une adresse IP et un masque (par exemple, *2002:c0a8:6301:1::1/64*).

Protection de la boîte aux lettres

L’intégration de ESET Internet Security avec votre boîte de messagerie augmente le niveau de protection active contre le code malveillant dans les courriels.

Pour configurer la protection des boîtes aux lettres, ouvrez Configuration avancée > **Protections** > **Protection du client de messagerie** > **Protection de la boîte aux lettres**.

Activer la protection du courriel par des modules d'extension client – Lorsque cette option est désactivée, la protection par les modules d'extension du client de messagerie est désactivée.

Sélectionnez les courriels à analyser :

- **Message reçu**
- **Message envoyé**

- **Message lu**
- **Courriel modifié**

Nous vous recommandons de conserver l'option **Activer la protection du courriel par les modules d'extension des clients** activée. Même si l'intégration n'est pas activée ni fonctionnelle, la communication par courriel est toujours protégée par le module de protection du transport du courriel (IMAP/IMAPS et POP3/POP3S).

Recherche de pourriel

Les courriels non sollicités, appelés pourriels, se classent parmi les plus grands problèmes de communication électronique. Il représente jusqu'à 30 % de toutes les communications par courriel. L'antipourriel du client de messagerie constitue une protection contre ce problème. En combinant plusieurs principes de sécurité du courriel, l'antipourriel du client de messagerie offre un meilleur filtrage pour garder votre boîte de réception propre. Un principe important de la détection des pourriels consiste à reconnaître les courriels non sollicités en fonction d'adresses fiables (autorisées) et d'adresses de pourriels (bloquées) prédéfinies.

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

Activer l'antipourriel du client de messagerie : une fois que cette option est activée, les messages reçus seront analysés à la recherche des pourriels.

Utiliser l'analyseur de pourriels avancé : des données antipourriel supplémentaires seront téléchargées périodiquement, ce qui permettra d'accroître les capacités antipourriel et d'obtenir de meilleurs résultats.

Consignation de la note attribuée au pourriel – Le moteur antipourriel de ESET Internet Security attribue une note de pourriel à tous les messages analysés. Le message sera enregistré dans le journal de protection antipourriel (Fenêtre principale du programme > **Outils** > **Fichiers journaux** > **Antipourriel du client de messagerie**).

- **Rien** - Le score de l'analyse antipourriel ne sera pas consigné au journal.
- **Reclassé et marqué comme du pourriel** - Sélectionnez cette options si vous voulez enregistrer le score des messages marqués comme SPAM.
- **Tous** - Tous les messages seront inscrits dans le journal, avec la note attribuée au pourriel.

Lorsque vous cliquez sur un message dans le dossier des pourriels, vous pouvez choisir **Reclassifier les messages sélectionnés comme n'étant pas du pourriel** et le message sera déplacé vers la boîte de réception. Lorsque vous cliquez sur un message que vous considérez comme du pourriel dans la boîte de réception, sélectionnez **Reclassifier les messages comme étant du pourriel** et le message sera déplacé vers le dossier des pourriels. Vous pouvez sélectionner plusieurs messages et les traiter tous simultanément.

Optimisation de la gestion des pièces jointes : si l'optimisation est désactivée, toutes les pièces jointes sont

analysées immédiatement. Il se peut que les performances du client de messagerie soient ralenties.

Intégrations : vous permet d'intégrer la protection des boîtes aux lettres à votre client de messagerie. Voir Intégrations pour plus d'informations.

Réponse : vous permet de personnaliser la gestion des pourriels. Voir Réponse pour plus d'informations.

Intégrations

L'intégration de ESET Internet Security avec votre client de messagerie augmente le niveau de protection active contre le code malveillant dans les courriels. Si votre client de messagerie est pris en charge, vous pouvez activer l'intégration dans ESET Internet Security. Lorsque l'intégration dans votre client de messagerie est faite, la barre d'outils de ESET Internet Security est insérée directement dans le client de messagerie, permettant une protection plus efficace des courriels. Pour modifier les paramètres d'intégration, ouvrez Configuration avancée > **Protections** > **Protection du client de messagerie** > **Protection de la boîte aux lettres** > **Intégration**.

Intégrer à Microsoft Outlook – Microsoft Outlook est actuellement le seul client de messagerie pris en charge. La protection de la messagerie fonctionne comme un plugiciel. L'avantage principal du plugiciel est qu'il est indépendant du protocole utilisé. Ainsi, quand un client de messagerie reçoit un message chiffré, il le déchiffre et l'envoie à l'analyseur de virus. Consultez cet article de la base de connaissances ESET pour obtenir la liste complète des versions de Microsoft Outlook prises en charge.

Traitement avancé du client de messagerie : traite les événements supplémentaires de Outlook Messaging API (MAPI) : Objet modifié (`fnevObjectModified`) et Objet créé (`fnevObjectCreated`). Si vous rencontrez un ralentissement du système lorsque vous utilisez votre client de messagerie, désactivez cette option.

Barre d'outils Microsoft Outlook

La protection de Microsoft Outlook fonctionne comme un plugiciel. Une fois que ESET Internet Security est installée, cette barre d'outils contenant les options de protection antivirus et d'antipourriel du client de messagerie est ajoutée à Outlook Express :

Pourriel - Marque les messages choisis comme pourriel. Après le marquage, une « empreinte » du message est envoyée à un serveur central de stockage des signatures de pourriel. Si le serveur reçoit d'autres empreintes similaires de plusieurs utilisateurs, le message sera alors classé comme pourriel.

N'est pas du pourriel - Marque les messages sélectionnés comme n'étant pas du pourriel.

Adresse de pourriel (bloquée, liste d'adresses de pourriel) : ajoute une nouvelle adresse d'expéditeur en tant qu'adresse bloquée à la liste d'adresses. Tous les messages reçus des adresses figurant sur la liste seront automatiquement classés comme pourriel.

> ⚠ Prenez garde à la mystification - l'usurpation d'adresse d'un expéditeur dans les courriels pour amener les destinataires à les lire et à y répondre.

Adresse fiable (autorisée, liste d'adresses fiables) : ajoute une adresse d'expéditeur en tant qu'adresse autorisée à la liste d'adresses. Tous les messages reçus d'adresses autorisées ne sont jamais classés comme pourriel.

ESET Internet Security – Double-cliquez sur l'icône pour ouvrir la fenêtre principale de ESET Internet Security.

Analyser à nouveau les messages - Permet de lancer une vérification manuelle du courriel. Vous pouvez préciser les messages à analyser et activer la nouvelle analyse des messages reçus. Pour plus d'informations, consultez la rubrique Protection de la boîte aux lettres.

Configuration de l'analyseur : affiche les options de configuration le la protection de la boîte aux lettres.

Configuration de l'antipourriel : affiche les options de configuration de la protection de la boîte aux lettres.

Carnets d'adresses : ouvre la fenêtre Gestion des listes d'adresses dans laquelle vous pouvez accéder à des listes d'adresses exclues, fiables et de pourriel.

Boîte de dialogue de confirmation

Cette notification permet de vérifier que l'utilisateur veut vraiment exécuter l'action sélectionnée, ce qui devrait éliminer des erreurs possibles.

Par ailleurs, la boîte de dialogue offre également la possibilité de désactiver les confirmations.

Analyser à nouveau les messages

La barre d'outils de ESET Internet Security intégrée dans les clients de messagerie permet aux utilisateurs de préciser plusieurs options pour la vérification du courriel. L'option **Analyser à nouveau les messages** offre deux modes d'analyse :

Tous les messages du dossier en cours - Analyse les messages dans le dossier actuellement affiché.

Messages sélectionnés uniquement - N'analyse que les messages marqués par l'utilisateur.

La case à cocher **Réanalyser les messages déjà analysés** offre à l'utilisateur une option permettant d'effectuer une autre analyse sur les messages ayant déjà été analysés.

Réponse

En fonction des résultats de l'analyse des messages, ESET Internet Security peut déplacer des messages analysés ou ajouter du texte personnalisé à l'objet. Vous pouvez configurer ces paramètres dans Configuration avancée > **Protections** > **Protection du client de messagerie** > **Protection de la boîte aux lettres** > **Réponse**.

L'antipourriel du client de messagerie dans ESET Internet Security vous permet de configurer les paramètres suivants pour les messages :

Ajouter un texte à l'objet des messages - Permet d'ajouter une chaîne avec préfixe personnalisée à la ligne d'objet des messages classifiés comme pourriels. Le **texte** par défaut est « [SPAM] ».

Déplacer dans le dossier des pourriels - Lorsque cette option est activée, les pourriels seront déplacés par défaut vers le dossier des pourriels et les messages reclassés comme n'étant pas du pourriel seront déplacés vers la boîte de réception. Lorsque vous cliquez avec le bouton droit de la souris sur un message et sélectionnez ESET Internet Security dans le menu contextuel, des options applicables vous sont offertes.

Déplacer vers un dossier personnalisé : lorsque cette option est activée, les pourriels sont déplacés vers un

dossier spécifié ci-dessous.

Dossier - Indiquez le dossier personnalisé dans lequel vous voulez placer les courriels infectés lorsqu'ils sont détectés.

S’il y a un message contenant la détection, ESET Internet Security tente de nettoyer le message par défaut. Si le message ne peut pas être nettoyé, vous pouvez choisir une **action à prendre si le nettoyage n’est pas possible** :

- **Aucune action** : Si cette option est activée, le programme identifiera les messages infectés, les laissera tels quels et n'effectuera aucune action.
- **Supprimer les messages** - Le programme avertit l'utilisateur à propos des infiltrations et supprime le message.
- **Déplacer le message vers le dossier Éléments supprimés** - Les messages infectés seront automatiquement déplacés vers le dossier Éléments supprimés.
- **Déplacer le message vers le dossier** (action par défaut) - Les messages infectés seront automatiquement déplacés vers le dossier indiqué.

Dossier - Indiquez le dossier personnalisé dans lequel vous voulez placer les courriels infectés lorsqu'ils sont détectés.

Marquer les pourriels comme lus - Activez cette option pour marquer automatiquement les pourriels comme lus. Vous pouvez ainsi vous concentrer sur les messages « propres ».

Marquer les pourriels comme non lus : Les messages classés au départ comme pourriels, mais marqués plus tard comme « propres », seront affichés comme comme non lus.

Après la vérification d'un courriel, une notification avec le résultat de l'analyse peut être ajoutée au message. Vous pouvez sélectionner **Ajouter une étiquette aux messages reçus et lus** ou **Ajouter une étiquette aux messages envoyés**. Sachez cependant qu'en de rares occasions, les étiquettes de messages peuvent être omises dans des messages HTML problématiques ou si le message a été falsifié par des logiciels malveillants. Les étiquettes peuvent être ajoutées tant aux messages reçus et lus que sortants (ou aux deux). Les options suivantes sont disponibles :

- **Jamais** - Aucune balise de message ne sera ajoutée.
- **Lorsqu'une détection se produit** - Seuls les messages contenant des logiciels malveillants seront marqués comme vérifiés (par défaut).
- **Tout courriel analysé** - Le programme ajoutera des messages à tout courriel analysé.

Mettre à jour l’objet du courriel reçu et lu / **Mettre à jour l’objet du courriel envoyé** : activez cette option pour ajouter le texte personnalisé spécifié ci-dessous au message.

Texte à ajouter à l'objet d'un message détecté - Modifier ce modèle si vous voulez modifier le format du préfixe d'objet d'un courriel infecté. Cette fonction remplacera l'objet du message « Hello » par une valeur au format suivant : « [detection %DETECTIONNAME%] Hello ». La variable %DETECTIONNAME% représente la menace détectée.

Gestion des listes d’adresses

La fonctionnalité Antipourriel du client de messagerie de ESET Internet Security vous permet de configurer différents paramètres pour les listes d'adresses. Pour configurer les listes d’adresses, ouvrez Configuration avancée > **Protections** > **Protection du client de messagerie** > **Gestion des listes d’adresses**.

Activer la liste d’adresses de l’utilisateur – Activez cette option pour activer la liste d’adresses de l’utilisateur.

Liste d’adresses de l’utilisateur - Liste des adresses courriels dans laquelle vous pouvez ajouter, modifier ou supprimer des adresses pour définir les règles antipourriel. Les règles de cette liste seront appliquées à l’utilisateur actuel.

Activer la liste d'adresses globale - Cette option permet d'activer le carnet d'adresses global partagé par toutes les personnes utilisant ce périphérique.

Liste d’adresses globale - Liste des adresses courriels dans laquelle vous pouvez ajouter, modifier ou supprimer des adresses pour définir les règles antipourriel. Les règles de cette liste seront appliquées à tous les utilisateurs.

Autoriser et ajouter automatiquement dans la liste d'adresses de l'utilisateur

Traiter les adresses du carnet d'adresses comme fiables : Les adresses de votre liste de contacts seront traitées comme des adresses de confiance sans être ajoutées à la liste des adresses de l'utilisateur.

Ajouter les adresses des destinataires des messages sortants - Cette option permet d'ajouter les adresses des destinataires des messages envoyés à la liste de l’utilisateur comme adresses autorisées.

Ajouter les adresses des messages reclassifiés comme n'étant PAS du pourriel - Cette option permet d'ajouter les adresses des expéditeurs des messages reclassifiés comme n'étant PAS du pourriel à la liste d’adresses de l’utilisateur comme adresses autorisées.

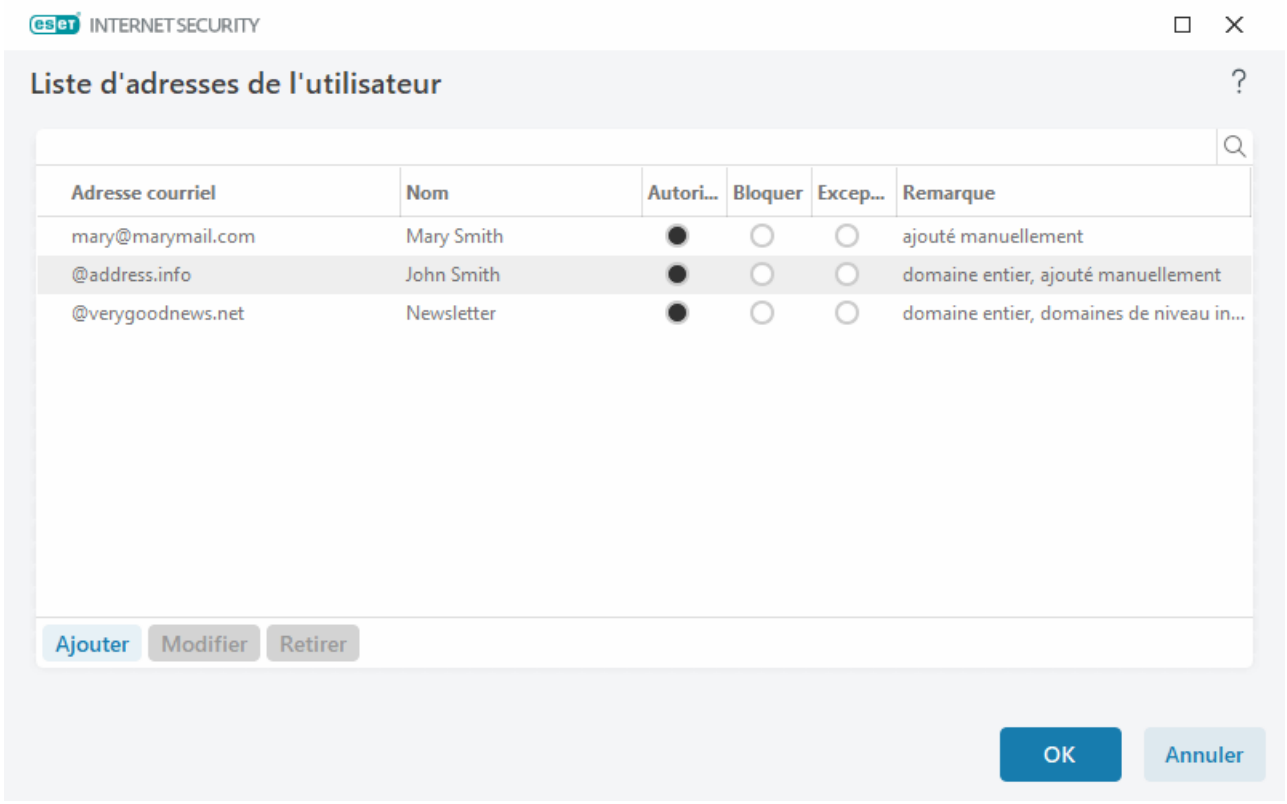
Ajouter automatiquement dans la liste d'adresses de l'utilisateur comme une exception

Ajouter les adresses de ses propres comptes - Cette option permet d'ajouter vos adresses des comptes de client de messagerie existants à la liste d’adresses de l’utilisateur comme des exceptions.

Listes d'adresses

Pour vous protéger contre les courriels non sollicités, ESET Internet Security vous permet de classer les adresses courriel dans des listes d’adresses.

Pour modifier les listes d'adresses, ouvrez Configuration avancée > **Protections** > **Protection du client de messagerie** > **Gestion des listes d'adresses**, puis cliquez sur **Modifier** située à côté de **Liste d'adresses de l'utilisateur** ou de **Liste d’adresses globale**.



Colonnes

Adresse courriel – Adresse à laquelle la règle s'appliquera. Les caractères génériques ne sont pas pris en charge.

Nom – Nom de règle personnalisé.

Autoriser/Bloquer/Exception – Boutons radio utilisés pour déterminer quelle action entreprendre pour l'adresse courriel (cliquez sur le bouton radio dans la colonne préférée pour changer rapidement l'action) :

- **Autoriser** - Adresses considérées comme sans dangers et de qui vous souhaitez recevoir des messages.
- **Bloquer** - Adresses considérées comme dangereuses ou comme source de pourriels et de qui vous ne voulez pas recevoir de messages.
- **Exception** - Adresses pour lesquelles la présence de pourriels est toujours vérifiée et qui peuvent être usurpées et utilisées pour l'envoi de pourriels.

Remarque – Informations sur la façon dont la règle a été créée et si elle s'applique à l'ensemble du domaine ou des domaines de niveau inférieur.

Gestion des adresses

- **Ajouter** – Cliquez sur cette option pour ajouter une règle pour une nouvelle adresse.
- **Modifier** – Sélectionnez cette option et cliquez dessus pour modifier une règle existante.
- **Supprimer** – Sélectionnez cette option et cliquez dessus si vous souhaitez supprimer une règle de la liste d'adresses.

Ajouter/modifier une adresse

Cette fenêtre vous permet d'ajouter ou de modifier une adresse dans la gestion des listes d'adresses et de configurer l'action entreprise :

Adresse courriel – Adresse à laquelle la règle s'appliquera.

Nom – Nom de règle personnalisé.

Action – Action à entreprendre si l'adresse courriel du contact correspond à l'adresse spécifiée dans le champ **Adresse courriel** :

- **Autoriser** - Adresses considérées comme sans dangers et de qui vous souhaitez recevoir des messages.
- **Bloquer** - Adresses considérées comme dangereuses ou comme source de pourriels et de qui vous ne voulez pas recevoir de messages.
- **Exception** - Adresses pour lesquelles la présence de pourriels est toujours vérifiée et qui peuvent être usurpées et utilisées pour l'envoi de pourriels.

Domaine entier - Sélectionnez cette option pour que le règle soit appliquée à l'ensemble du domaine du contact (pas seulement à l'adresse précisée dans le champ **Adresse courriel**, mais à toutes les adresses courriel du domaine *address.info*).

Domaines de niveau inférieur - Sélectionnez cette option pour que le règle soit appliquée au domaine de niveau inférieur du contact. (*address.info* représente le domaine alors que *my.address.info* représente le sous-domaine).

Résultat du traitement des adresses

Lorsque vous ajoutez de nouvelles adresses ou modifiez l'action entreprise pour l'adresse courriel, ESET Internet Security affiche des messages de notification. Le contenu de ces messages varie en fonction de l'action que vous tentez d'exécuter.

Cochez la case **Ne plus demander** pour exécuter l'action automatiquement sans que le message ne soit affiché.

ThreatSense

ThreatSense combine de nombreuses méthodes de détection de menaces complexes. Cette technologie proactive fournit également une protection durant les premières heures de 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 simultanément plusieurs flux de données, maximisant ainsi l'efficacité et le taux de détection. La technologie ThreatSense élimine également avec succès les rootkits.

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

- les types de fichiers et extensions à analyser

- la combinaison de plusieurs méthodes de détection;
- les niveaux de nettoyage, etc.

Pour accéder à la fenêtre de configuration, cliquez sur **ThreatSense** dans Configuration avancée pour tout module qui utilise la technologie ThreatSense (voir ci-dessous). Différents scénarios de sécurité peuvent nécessiter des configurations différentes. Dans cet esprit, ThreatSense est configurable individuellement pour les modules de protection suivants :

- Protection en temps réel du système de fichiers
- Analyse en état inactif
- Analyse au démarrage
- Protection des documents
- Protection du client de messagerie
- Protection de l'accès Web
- Analyse de l'ordinateur

Les paramètres de ThreatSense sont hautement optimisés pour chaque module et leur modification peut grandement affecter le fonctionnement du système. Par exemple, en modifiant les paramètres afin d'analyser à chaque fois les compacteurs exécutables ou d'autoriser l'heuristique avancée dans la protection en temps réel du système de fichiers, vous pouvez diminuer les performances du système (normalement, seuls les fichiers nouvellement créés sont analysés par ces méthodes). Il est recommandé de laisser inchangés les paramètres par défaut de ThreatSense pour tous les modules, à l'exception du module Analyse de l'ordinateur.

Objets à analyser

Cette section vous permet de définir quels éléments et fichiers de l'ordinateur seront analysés à la recherche des infiltrations.

Mémoire vive - Activez cette option pour détecter les menaces qui s'attaquent à la mémoire vive du système.

Secteurs d'amorçage/UEFI - Analyse les secteurs d'amorçage à la recherche des logiciels malveillants dans l'enregistrement de démarrage principal. Pour en savoir plus sur l'UEFI, consultez le glossaire.

Fichiers courriel - 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 beaucoup d'autres.

Archives à extraction automatique - Les archives à extraction automatique (SFX) sont des archives qui peuvent s'extraire toutes seules.

Compresseurs d'exécutable - Après avoir été exécutés, les compresseurs d'exécutables (contrairement aux types d'archives standard) se décompressent en mémoire. En plus des compacteurs statiques standards (UPX, yoda, ASPack, FSG, etc.), l'analyseur est capable der reconnaitre beaucoup d'autres types de compacteurs grâce à l'utilisation de l'émulation de code.

Options d'analyse

Sélectionnez les méthodes utilisées lors de l'analyse du système à la recherche d'infiltrations. Les options suivantes sont disponibles :

Heuristiques - La méthode heuristique utilise un algorithme d'analyse de l'activité (malveillante) des programmes. Le principal avantage de cette technologie est sa capacité à identifier un code malveillant qui n'existait pas ou n'était pas connu par le moteur de détection. L'inconvénient de cette méthode est la probabilité (très faible) de fausses alarmes.

Heuristique avancée/Signatures ADN - La méthode heuristique avancée utilise un algorithme heuristique développé par ESET, optimisé pour la détection des vers d'ordinateur et les chevaux de Troie et écrit dans un langage de programmation de haut niveau. L'utilisation de l'heuristique avancée augmente considérablement les capacités de détection de menaces des produits ESET. Les signatures peuvent détecter et identifier les virus de façon fiable. Grâce au système de mise à jour automatique, de nouvelles signatures peuvent être disponibles dans les quelques heures de la découverte d'une menace. L'inconvénient des signatures est qu'elles ne détectent que les virus qu'elles connaissent (ou une version légèrement modifiée de ces virus).

Nettoyage

Les paramètres de nettoyage déterminent le comportement de ESET Internet Security lors du nettoyage des objets. Quatre niveaux de nettoyage sont possibles :

ThreatSense possède les niveaux de correction (c'est-à-dire de nettoyage) suivants :

Correction dans ESET Internet Security

Niveau de nettoyage	Description
Toujours corriger la détection	Cette option permet de tenter de corriger la détection lors du nettoyage des objets sans aucune intervention de l'utilisateur final. Dans de rares cas (fichiers système, par exemple), si la détection ne peut pas être corrigée, l'objet signalé est laissé à son emplacement d'origine.
Corriger la détection si cela ne présente pas de danger, conserver sinon	Cette option permet de tenter de corriger la détection lors du nettoyage des objets sans aucune intervention de l'utilisateur final. Dans certains cas (fichiers système ou archives contenant à la fois des fichiers propres et des fichiers infectés), si la détection ne peut pas être corrigée, l'objet signalé est laissé à son emplacement d'origine.
Corriger la détection si cela ne présente pas de danger, demander sinon	Cette option permet de tenter de corriger la détection lors du nettoyage des objets. Dans certains cas, si aucune action ne peut être effectuée, l'utilisateur final reçoit une alerte interactive et doit sélectionner une action de correction (par exemple, supprimer ou ignorer). Ce paramètre est recommandé dans la plupart des cas.
Toujours demander à l'utilisateur final	Lors du nettoyage des objets, une fenêtre interactive s'ouvre et l'utilisateur final doit sélectionner une action de correction (par exemple, supprimer ou ignorer). Ce niveau est conçu pour les utilisateurs plus avancés qui savent quelles mesures prendre lorsqu'une détection se produit.

Exclusions

Une extension est la partie d'un nom de fichier délimitée par un point. Elle définit le type et le contenu du fichier. Cette section de la configuration de ThreatSense vous permet de définir les types de fichiers à analyser.

Autre

Au moment de configurer les paramètres du moteur ThreatSense pour une analyse de l'ordinateur à la demande, les options suivantes dans la section **Autres** seront aussi offertes :

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 beaucoup de ressources système, vous pouvez activer l'analyse en arrière-plan à faible priorité de manière à réserver des ressources pour vos applications.

Consigner tous les objets – Le journal d'analyse affichera tous les fichiers analysés dans des archives auto-extractibles, même ceux qui ne sont pas infectés (peut générer beaucoup de données de journal d'analyse et augmenter la taille du fichier journal d'analyse).

Activer l'optimisation intelligente - Lorsque la fonction Optimisation intelligente est activée, les paramètres les plus optimaux sont utilisés pour assurer le niveau d'analyse le plus efficient tout en conservant la vitesse d'analyse la plus élevée. Les différents modules de protection effectuent une analyse intelligente, utilisant pour ce faire différentes méthodes d'analyse et les appliquant à différents types de fichiers. Si l'optimisation Smart est activée, seuls les paramètres définis par l'utilisateur dans le moteur ThreatSense utilisé pour ces modules particuliers seront appliqués au moment de l'analyse.

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

Limites

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

Paramètres de l'objet

Taille maximale de l'objet - Définit la taille maximale des objets à analyser. Le module antivirus donné n'analysera alors que les objets d'une taille inférieure à celle indiquée. Cette option ne devrait être modifiée que par des utilisateurs expérimentés ayant des raisons précises d'exclure de l'analyse des objets de plus grande taille. Valeur par défaut : illimité.

Durée maximale d'analyse de l'objet (sec.) : définit la valeur de temps maximale pour l'analyse des fichiers dans un objet conteneur (tel qu'une archive RAR/ZIP ou un courriel avec plusieurs pièces jointes). Ce paramètre ne s'applique pas aux fichiers autonomes. Si une valeur définie par l'utilisateur a été entrée et que ce temps s'est écoulé, l'analyse s'arrête dès que possible, que cette analyse de fichier d'un objet conteneur soit terminée ou non.
Dans le cas d'une archive avec des fichiers volumineux, l'analyse s'arrêtera au plus tôt lorsqu'un fichier de l'archive est extrait (par exemple, lorsqu'une variable définie par l'utilisateur dure 3 secondes, mais que l'extraction d'un fichier prend 5 secondes). Le reste des fichiers de l'archive ne sera pas analysé lorsque ce temps sera écoulé.

Pour limiter le temps d'analyse, y compris les archives plus grandes, utilisez **Taille maximale de l'objet** et **Taille maximale du fichier dans l'archive** (non recommandé en raison de risques de sécurité possibles).
Valeur par défaut : ilimité.

Configuration de l'analyse d'archive

Niveau d'imbrication des archives - Précise la profondeur maximale de l'analyse des archives. Valeur par défaut : 10.

Taille maximale du fichier dans l'archive - Cette option permet de préciser la taille maximale des fichiers (après extraction) à analyser, contenus dans les archives. La valeur maximale est **3 Go**.

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

Protection de l'accès Web

La protection de l'accès Web vous permet de configurer les paramètres avancés du module de protection Internet. Les options suivantes sont disponibles dans Configuration avancée > **Protections** > **Protection de l'accès Web** > **Protection de l'accès Web** :

Activer la protection de l'accès Web : Lorsque cette option est désactivée, la protection de l'accès Web et la protection antihameçonnage ne fonctionnent pas.

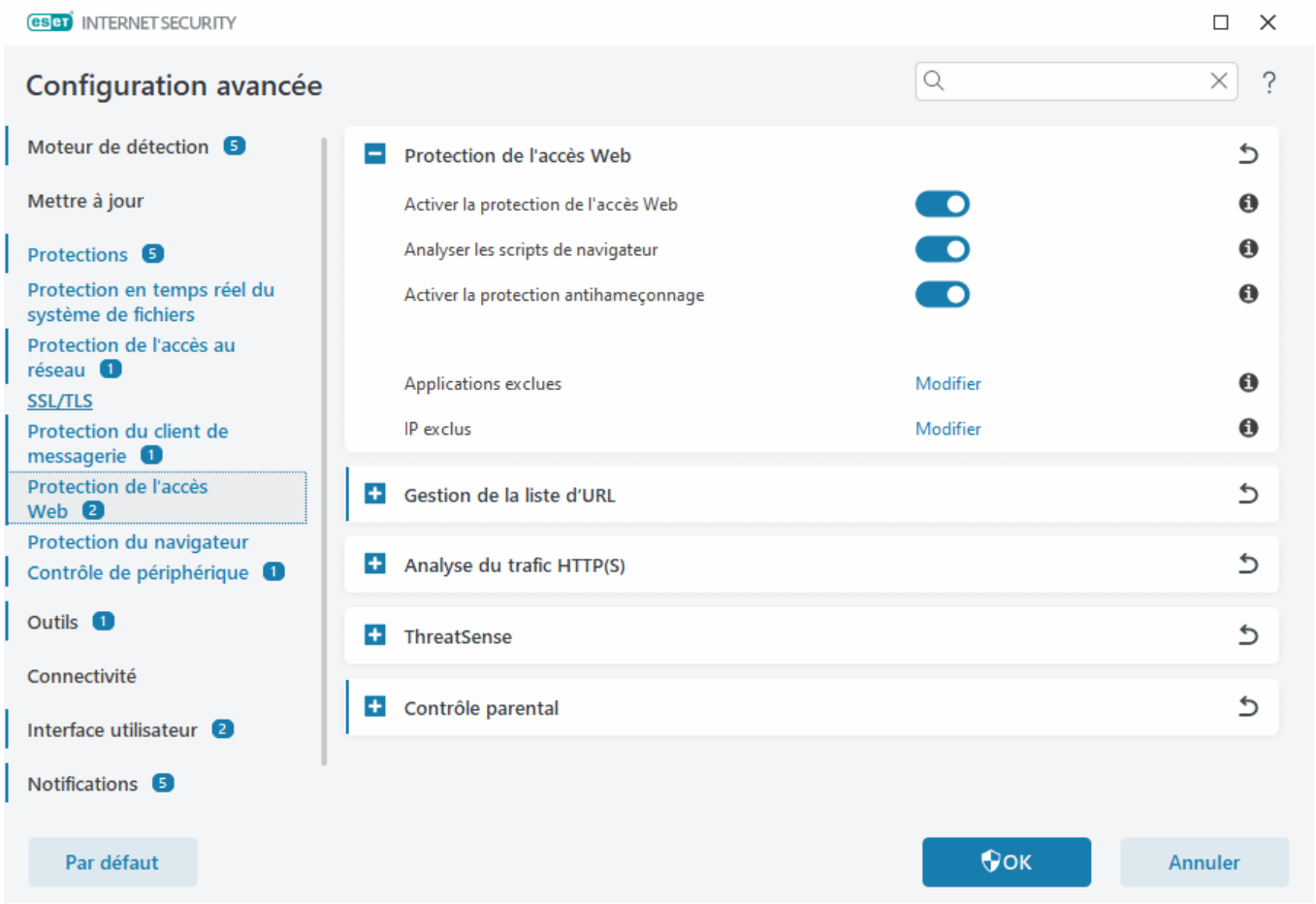
> i Nous vous recommandons fortement de laisser la protection de l'accès Web activée et de ne pas exclure des applications ou des adresses IP par défaut.

Analyser les scripts du navigateur : lorsque cette option est activée, le moteur de détection vérifie tous les programmes JavaScript exécutés par les navigateurs Web.

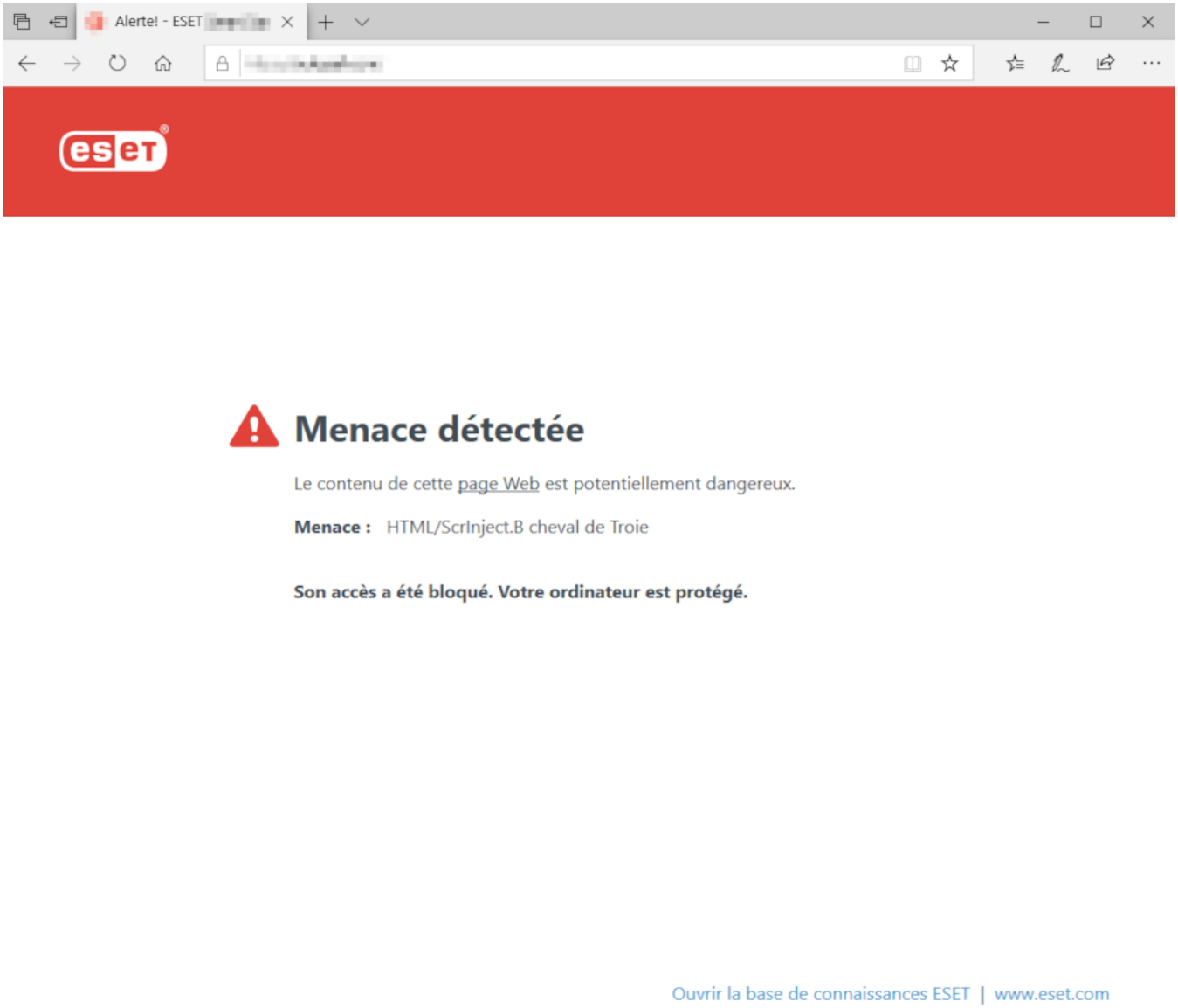
Activer la protection antihameçonnage : lorsque cette option est activée, les pages Web d'hameçonnage sont bloquées. Voir Anti-Phishing protection pour de plus amples renseignements.

Applications exclues : cette option vous permet d'exclure des applications spécifiques de l'analyse par la protection de l'accès Web. Elle est utile lorsque la protection de l'accès Web entraîne des problèmes de compatibilité.

Adresses IP exclues : cette option vous permet d'exclure des adresses distantes spécifiques de l'analyse par la protection de l'accès Web. Elle est utile lorsque la protection de l'accès Web entraîne des problèmes de compatibilité.



La protection de l'accès Web affiche le message suivant dans votre navigateur lorsque le site Web est bloqué :



Instructions illustrées

Les articles suivants de la base de connaissances ESET peuvent n'être disponibles qu'en anglais :

- Exclure un site Web sécurisé du blocage par la protection de l'accès Web
- Bloquer un site Web à l'aide de ESET Internet Security

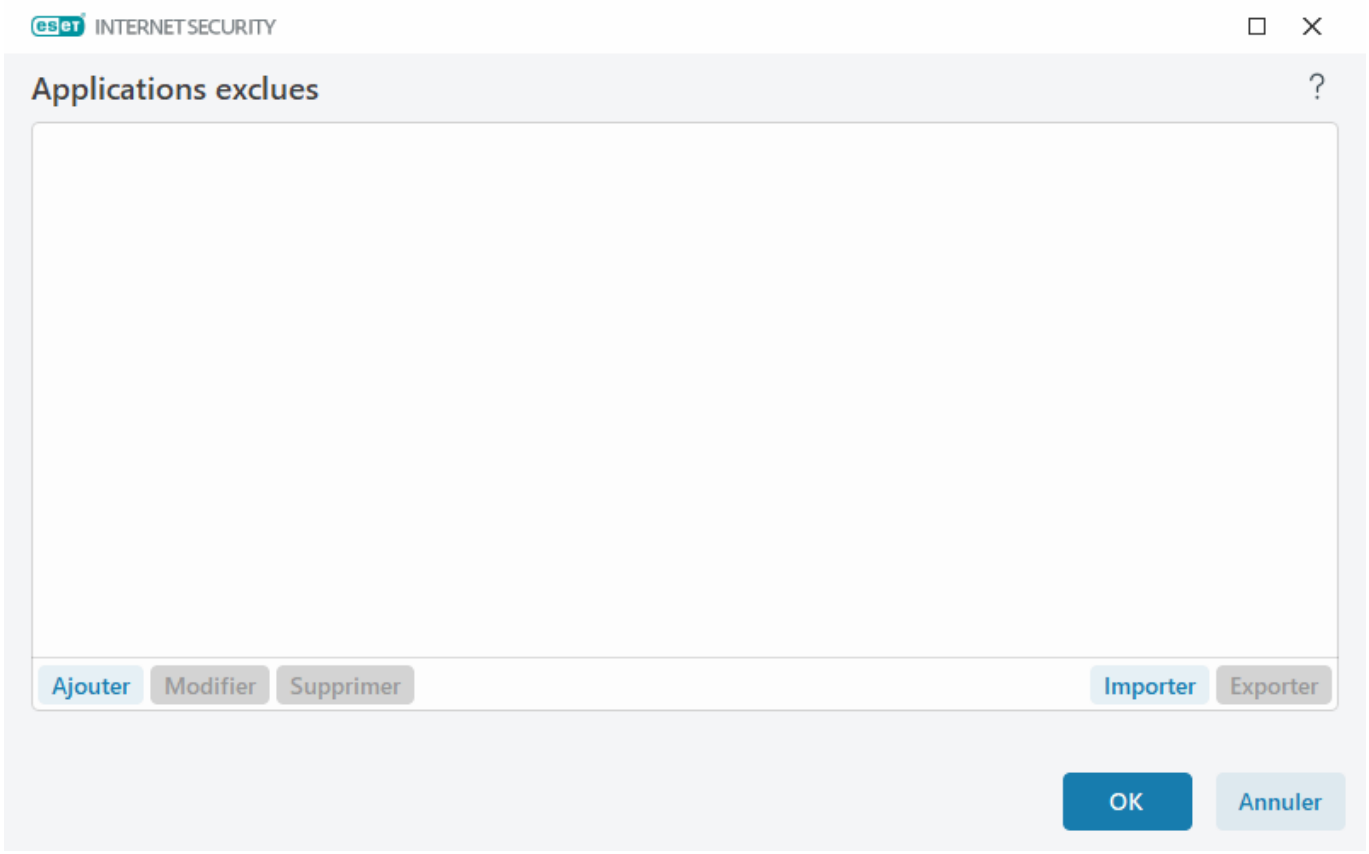
Applications exclues

Pour exclure l'analyse des communications pour des applications spécifiques, ajoutez-les à la liste. Les communications envoyées par ces applications par les protocoles HTTP(S)/POP3(S)/IMAP(S) ne seront pas vérifiées pour savoir si elles contiennent des menaces. Il est recommandé de n'utiliser cette option que pour les applications qui ne fonctionnent pas bien lorsque la communication fait l'objet d'une vérification.

Les applications et services en cours d'exécution seront automatiquement disponibles ici lorsque vous cliquez sur **Ajouter**. Cliquez sur **...** et accédez à une application pour ajouter l'exclusion manuellement.

Modifier - Modifie les entrées sélectionnées de la liste.

Retirer - Supprime des entrées de la liste.



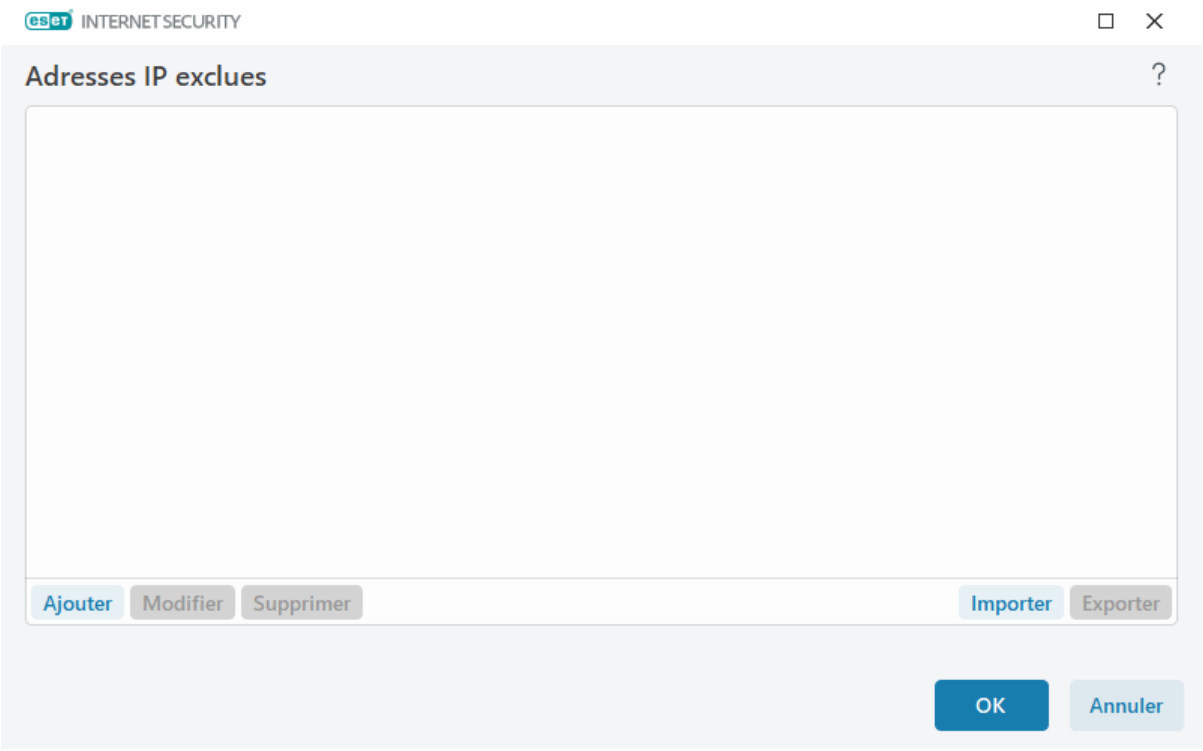
IP exclus

Les adresses inscrites dans cette liste seront exclues de l'analyse. Les communications envoyées à ces adresses ou reçues de celles-ci par les protocoles HTTP(S)/POP3(S)/IMAP(S) ne seront pas vérifiées pour savoir si elles contiennent des menaces. Il est recommandé de n'utiliser cette option que pour les adresses connues pour être fiables.

Cliquez sur **Ajouter** pour exclure une adresse IP, une plage d'adresses ou un sous-réseau d'un point distant.

Cliquez sur **Modifier** pour modifier l'adresse IP sélectionnée.

Cliquez sur **Retirer** pour supprimer les entrées sélectionnées de la liste.



Exemples d’adresses IP

Ajouter une adresse IPv4:
Adresse unique : ajoute l’adresse IP d’un seul ordinateur (par exemple, *192.168.0.10*).
Plage d’adresses : entrez la première et la dernière adresse IP pour préciser une plage d’adresse IP (de plusieurs ordinateurs) à laquelle appliquer la règle (par exemple, de *192.168.0.1 à 192.168.0.99*).
Sous-réseau - Sous-réseau (groupe d'ordinateurs) défini par une adresse IP et un masque. Par exemple, 255.255.255.0 est le masque de réseau pour le sous-réseau 192.168.1.0. Pour exclure le type de sous-réseau entier dans *192.168.1.0/24*.
Ajouter une adresse IPv6:
Adresse unique : ajoute l’adresse IP d’un seul ordinateur (par exemple, *2001:718:1c01:16:214:22ff:fec9:ca5*).
Sous-réseau - Sous-réseau (groupe d'ordinateurs) défini par une adresse IP et un masque (par exemple, *2002:c0a8:6301:1::1/64*).

Gestion de la liste d’URL

La **gestion de la liste d’URL** dans Configuration avancée > **Protections** > **Protection de l'accès Web** vous permet de spécifier les adresses HTTP à bloquer, à autoriser ou à exclure de l’analyse de contenu.

SSL/TLS doit être activé si vous souhaitez filtrer les adresses HTTPS en plus des adresses HTTP. Sinon, seuls les domaines des sites HTTPS que vous avez visités seront ajoutés, l'URL complète ne le sera pas.

Les sites Web de la **liste des adresses bloquées** ne seront pas accessibles, sauf s'ils sont également inclus dans la **liste des adresses autorisées**. Les sites Web de la **liste des adresses exclues de l'analyse de contenu** ne sont pas analysés à la recherche de code malveillant lorsqu'un utilisateur y accède.

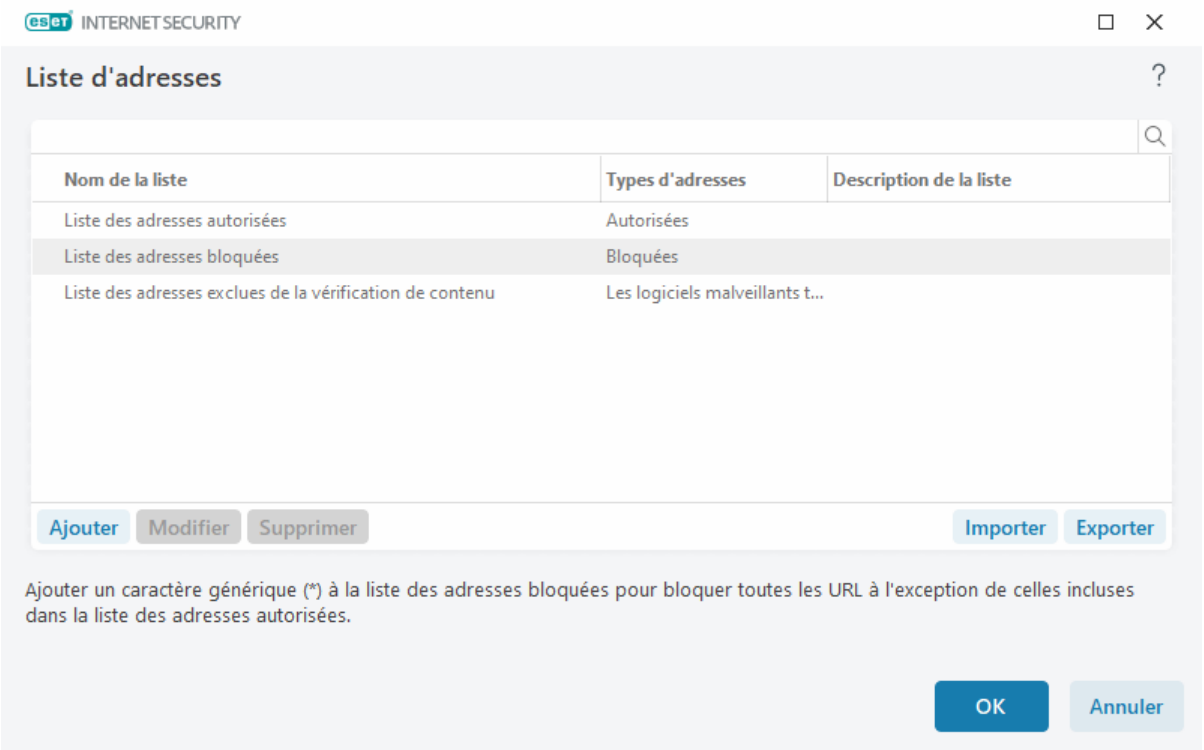
Si vous voulez bloquer toutes les adresses HTTP à l'exception des adresses indiquées dans la **Liste des adresses autorisées**, ajoutez * à la **Liste des adresses bloquées** active.

Les symboles spéciaux * (astérisque) et ? (point d'interrogation) peuvent être utilisés dans les listes. L’astérisque remplace n’importe quelle chaîne de caractères, et le point d’interrogation remplace n’importe quel symbole.

Faites attention lorsque vous spécifiez les adresses exclues, car la liste ne doit contenir que des adresses fiables et sûres. De même, assurez-vous d'employer correctement les symboles * et ? dans cette liste. Voir Ajouter des adresses/masques de domaine HTTP pour en savoir plus sur la façon dont un domaine entier incluant tous les sous-domaines peut être jumelé en toute sécurité. Pour activer une liste, sélectionnez l'option **Liste active**. Si vous voulez être notifié quand une adresse est entrée à partir de la liste actuelle, sélectionnez l'option **Notifier une fois appliqué**.

Adresses considérées comme fiables par ESET

Si l'option **Ne pas analyser le trafic avec des domaines considérés comme fiables par ESET** est activée avec SSL/TLS, les domaines de la liste blanche gérés par ESET ne seront pas affectés par la configuration de la gestion de la liste d'URL.



Éléments de contrôle

Ajouter - Permet de créer un nouvelle liste en plus de celles prédéfinies. Cette option peut être utile si vous souhaitez séparer logiquement différents groupes d'adresses. Par exemple, une liste des adresses bloquées peut contenir des adresses d'une liste noire publique externe et une seconde peut contenir votre propre liste noire, ce qui rend plus facile la mise à jour de la liste externe tout en gardant la vôtre intact.

Modifier - Permet de modifier les listes existantes. Utilisez cette option pour ajouter ou retirer des adresses.

Supprimer - Permet de supprimer des listes existantes. Disponible uniquement pour des listes créées avec l'option **Ajouter**, non pour les listes par défaut.

Liste d'adresses

Cette section permet de préciser des listes d'adresses HTTP(S) qui seront bloquées, autorisées ou exclues de la vérification.

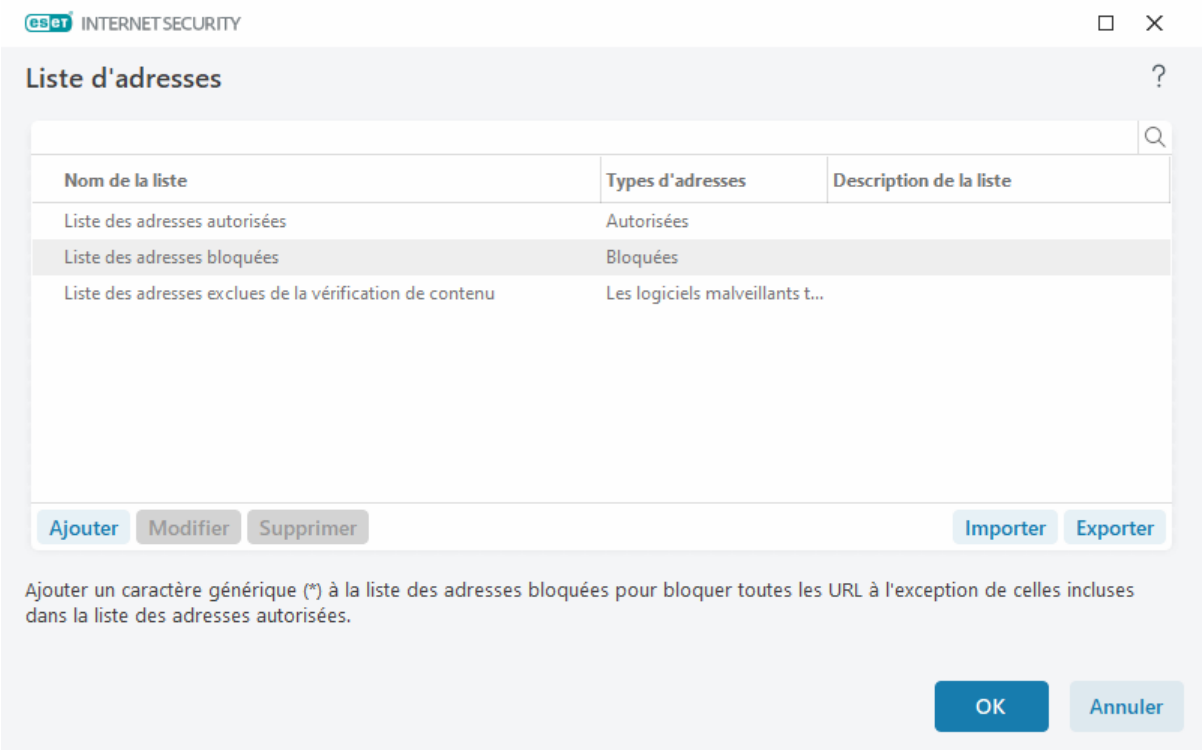
Par défaut, les trois listes suivantes sont disponibles :

• **Liste des adresses exclues de l'analyse de contenu** - Aucune vérification de la présence de programmes malveillants n'est effectuée pour les adresses indiquées dans la liste.

• **Liste des adresses autorisées** - Si l'option N'autoriser l'accès qu'aux adresses HTTP figurant dans la liste des adresses autorisées est activée et que la liste des adresses bloquées contient * (correspond à tout), l'utilisateur n'est autorisé à accéder qu'aux adresses indiquées dans cette liste. Les adresses de cette liste sont autorisées même si elle sont incluses dans la liste des adresses bloquées.

• **Liste des adresses bloquées**- L'utilisateur n'est pas autorisé à accéder aux adresses indiquées dans cette liste.

Cliquez sur **Ajouter** pour créer une liste. Pour supprimer les listes sélectionnées, cliquez sur **Supprimer**.



Instructions illustrées

Les articles suivants de la base de connaissances ESET peuvent n'être disponibles qu'en anglais :

- Exclure un site Web sécurisé du blocage par la protection de l'accès Web
- Bloquer un site Web à l'aide de produits ESET Windows Home

Pour plus d'informations, voir Gestion de la liste des URL.

Créer une nouvelle liste d'adresses

Cette boîte de dialogue vous permet de configurer une nouvelle liste d'adresses URL/masques qui seront bloqués, autorisés ou exclus de la vérification.

Vous pouvez configurer les options suivantes :

Type de liste d'adresse - Trois types de listes dont disponibles :

• **Les logiciels malveillants trouvés sont ignorés** - Aucune vérification de la présence de programmes

malveillants n'est effectuée pour toutes les adresses indiquées dans la liste.

- **Bloqué** – L'accès aux adresses spécifiées dans cette liste est bloqué.

- **Autorisé** – L'accès aux adresses spécifiées dans cette liste est autorisé. Les adresses de cette liste sont autorisées même si elle sont incluses dans la liste des adresses bloquées.

Nom de la liste - Précisez le nom de la liste. Ce champ n'est pas disponible lors de la modification de l'une des listes prédéfinies.

Description de la liste - Entrez une brève description de la liste (facultatif). Elle n'est pas disponible lors de la modification de l'une des listes prédéfinies.

Pour activer la liste, sélectionnez l'option **Activer la liste** située à coté de la liste. Si vous souhaitez être averti lorsqu'une liste spécifique est utilisée lors de l'accès à des sites Web, sélectionnez **Notifier lors de l'application**. Par exemple, vous recevrez une notification si un site est bloqué ou autorisé parce qu'il est inclus dans la liste des adresses bloquées ou autorisées. La notification contient le nom de la liste.

Niveau de gravité de la journalisation : les informations sur la liste spécifique utilisée lors de l'accès aux sites Web peuvent être inscrites dans les fichiers journaux.

Éléments de contrôle

Ajouter - Ajouter une nouvelle adresse URL à la liste (entrez plusieurs valeurs avec des séparateurs).

Modifier - Modifie les adresses existantes dans la liste. Disponible uniquement pour les adresses créées avec **Ajouter**.

Retirer - Supprime les adresses existantes dans la liste. Disponible uniquement pour les adresses créées avec **Ajouter**.

Importer - Importer un fichier avec des adresses URL (valeurs séparées avec un saut de ligne, par exemple *.txt en utilisant l'encodage UTF-8).

Comment ajouter un masque URL

Veuillez vous reporter aux instructions de cette boîte de dialogue avant d'entrer l'adresse ou le masque de domaine souhaité.

ESET Internet Security permet de bloquer l'accès à des sites Web particuliers et d'empêcher le navigateur Internet d'en afficher le contenu. Qui plus est, il permet à l'utilisateur de préciser des adresses à exclure de la vérification. Si l'utilisateur ignore le nom complet du serveur distant ou s'il souhaite préciser un groupe de serveurs distants, il peut aussi utiliser des « masques ». Ces masques peuvent contenir les symboles « ? » et « * » :

- utiliser ? pour représenter un caractère quelconque

- utiliser * pour représenter une chaîne de caractères.

Ainsi, *.c?m désigne toutes les adresses dont la dernière partie commence par la lettre c et se termine par la lettre m, avec un caractère inconnu entre les deux (.com, .cam, etc.)

Une séquence de début « *. » est traitée spécialement si elle est utilisée au début du nom de domaine. Tout d'abord, le caractère générique « * » ne correspond pas au caractère de barre oblique (« / ») dans ce cas. Cela permet d'éviter le contournement du masque, par exemple le masque **.domain.com* ne correspondra pas à *http://anydomain.com/anypath#.domain.com* (un tel suffixe peut être ajouté à n'importe quel URL sans incidence sur le téléchargement). Et deuxièmement, le caractère « *. » correspond également à une chaîne vide dans ce cas particulier. Il s'agit de permettre de faire correspondre un domaine entier, y compris tous les sous-domaines à l'aide d'un seul masque. Par exemple le masque **.domain.com* correspond aussi à *http://domain.com*. L'utilisation de **domain.com* serait incorrect, puisqu'il correspondrait aussi à *http://anotherdomain.com*.

Analyse du trafic HTTP(S)

Par défaut, ESET Internet Security est configuré pour analyser le trafic HTTP et HTTPS qui est utilisé par les navigateurs Internet et d'autres applications. Vous devriez désactiver l'analyse du trafic seulement si vous rencontrez des problèmes avec un logiciel tiers et voulez savoir si le problème est provoqué par ESET Internet Security.

Activer l'analyse du trafic HTTP – Le trafic HTTP est toujours surveillé sur tous les ports pour toutes les applications.

Activer l'analyse du trafic HTTPS : le trafic HTTPS utilise un canal chiffré pour transférer des informations entre le serveur et le client. ESET Internet Security vérifie les communications à l'aide des méthodes de chiffrement SSL (Secure Socket Layer) et TLS (Transport Layer Security). Le programme analysera uniquement le trafic sur les ports définis dans **Ports utilisés par le protocole HTTPS**, indépendamment de la version du système d'exploitation (vous pouvez ajouter des ports aux ports prédéfinis 443 et 0 à 65535).

ThreatSense

ThreatSense combine de nombreuses méthodes de détection de menaces complexes. Cette technologie proactive fournit également une protection durant les premières heures de 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 simultanément plusieurs flux de données, maximisant ainsi l'efficacité et le taux de détection. La technologie ThreatSense élimine également avec succès les rootkits.

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

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

Pour accéder à la fenêtre de configuration, cliquez sur **ThreatSense** dans Configuration avancée pour tout module qui utilise la technologie ThreatSense (voir ci-dessous). Différents scénarios de sécurité peuvent nécessiter des configurations différentes. Dans cet esprit, ThreatSense est configurable individuellement pour les modules de protection suivants :

- Protection en temps réel du système de fichiers

- Analyse en état inactif
- Analyse au démarrage
- Protection des documents
- Protection du client de messagerie
- Protection de l'accès Web
- Analyse de l'ordinateur

Les paramètres de ThreatSense sont hautement optimisés pour chaque module et leur modification peut grandement affecter le fonctionnement du système. Par exemple, en modifiant les paramètres afin d'analyser à chaque fois les compacteurs exécutables ou d'autoriser l'heuristique avancée dans la protection en temps réel du système de fichiers, vous pouvez diminuer les performances du système (normalement, seuls les fichiers nouvellement créés sont analysés par ces méthodes). Il est recommandé de laisser inchangés les paramètres par défaut de ThreatSense pour tous les modules, à l'exception du module Analyse de l'ordinateur.

Objets à analyser

Cette section vous permet de définir quels éléments et fichiers de l'ordinateur seront analysés à la recherche des infiltrations.

Mémoire vive - Activez cette option pour détecter les menaces qui s'attaquent à la mémoire vive du système.

Secteurs d'amorçage/UEFI - Analyse les secteurs d'amorçage à la recherche des logiciels malveillants dans l'enregistrement de démarrage principal. Pour en savoir plus sur l'UEFI, consultez le glossaire.

Fichiers courriel - 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 beaucoup d'autres.

Archives à extraction automatique - Les archives à extraction automatique (SFX) sont des archives qui peuvent s'extraire toutes seules.

Compresseurs d'exécutable - Après avoir été exécutés, les compresseurs d'exécutables (contrairement aux types d'archives standard) se décompressent en mémoire. En plus des compacteurs statiques standards (UPX, yoda, ASPack, FSG, etc.), l'analyseur est capable der reconnaitre beaucoup d'autres types de compacteurs grâce à l'utilisation de l'émulation de code.

Options d'analyse

Sélectionnez les méthodes utilisées lors de l'analyse du système à la recherche d'infiltrations. Les options suivantes sont disponibles :

Heuristiques - La méthode heuristique utilise un algorithme d'analyse de l'activité (malveillante) des programmes. Le principal avantage de cette technologie est sa capacité à identifier un code malveillant qui n'existait pas ou n'était pas connu par le moteur de détection. L'inconvénient de cette méthode est la probabilité (très faible) de fausses alarmes.

Heuristique avancée/Signatures ADN - La méthode heuristique avancée utilise un algorithme heuristique développé par ESET, optimisé pour la détection des vers d'ordinateur et les chevaux de Troie et écrit dans un langage de programmation de haut niveau. L'utilisation de l'heuristique avancée augmente considérablement les capacités de détection de menaces des produits ESET. Les signatures peuvent détecter et identifier les virus de façon fiable. Grâce au système de mise à jour automatique, de nouvelles signatures peuvent être disponibles dans les quelques heures de la découverte d'une menace. L'inconvénient des signatures est qu'elles ne détectent que les virus qu'elles connaissent (ou une version légèrement modifiée de ces virus).

Nettoyage

Les paramètres de nettoyage déterminent le comportement de ESET Internet Security lors du nettoyage des objets. Quatre niveaux de nettoyage sont possibles :

ThreatSense possède les niveaux de correction (c'est-à-dire de nettoyage) suivants :

Correction dans ESET Internet Security

Niveau de nettoyage	Description
Toujours corriger la détection	Cette option permet de tenter de corriger la détection lors du nettoyage des objets sans aucune intervention de l'utilisateur final. Dans de rares cas (fichiers système, par exemple), si la détection ne peut pas être corrigée, l'objet signalé est laissé à son emplacement d'origine.
Corriger la détection si cela ne présente pas de danger, conserver sinon	Cette option permet de tenter de corriger la détection lors du nettoyage des objets sans aucune intervention de l'utilisateur final. Dans certains cas (fichiers système ou archives contenant à la fois des fichiers propres et des fichiers infectés), si la détection ne peut pas être corrigée, l'objet signalé est laissé à son emplacement d'origine.
Corriger la détection si cela ne présente pas de danger, demander sinon	Cette option permet de tenter de corriger la détection lors du nettoyage des objets. Dans certains cas, si aucune action ne peut être effectuée, l'utilisateur final reçoit une alerte interactive et doit sélectionner une action de correction (par exemple, supprimer ou ignorer). Ce paramètre est recommandé dans la plupart des cas.
Toujours demander à l'utilisateur final	Lors du nettoyage des objets, une fenêtre interactive s'ouvre et l'utilisateur final doit sélectionner une action de correction (par exemple, supprimer ou ignorer). Ce niveau est conçu pour les utilisateurs plus avancés qui savent quelles mesures prendre lorsqu'une détection se produit.

Exclusions

Une extension est la partie d'un nom de fichier délimitée par un point. Elle définit le type et le contenu du fichier. Cette section de la configuration de ThreatSense vous permet de définir les types de fichiers à analyser.

Autre

Au moment de configurer les paramètres du moteur ThreatSense pour une analyse de l'ordinateur à la demande, les options suivantes dans la section **Autres** seront aussi offertes :

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 beaucoup de ressources système, vous pouvez activer l'analyse en arrière-plan à faible priorité de manière à réserver des ressources pour vos applications.

Consigner tous les objets – Le journal d'analyse affichera tous les fichiers analysés dans des archives auto-extractibles, même ceux qui ne sont pas infectés (peut générer beaucoup de données de journal d'analyse et augmenter la taille du fichier journal d'analyse).

Activer l'optimisation intelligente - Lorsque la fonction Optimisation intelligente est activée, les paramètres les plus optimaux sont utilisés pour assurer le niveau d'analyse le plus efficient tout en conservant la vitesse d'analyse la plus élevée. Les différents modules de protection effectuent une analyse intelligente, utilisant pour ce faire différentes méthodes d'analyse et les appliquant à différents types de fichiers. Si l'optimisation Smart est activée, seuls les paramètres définis par l'utilisateur dans le moteur ThreatSense utilisé pour ces modules particuliers seront appliqués au moment de l'analyse.

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

Limites

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

Paramètres de l'objet

Taille maximale de l'objet - Définit la taille maximale des objets à analyser. Le module antivirus donné n'analysera alors que les objets d'une taille inférieure à celle indiquée. Cette option ne devrait être modifiée que par des utilisateurs expérimentés ayant des raisons précises d'exclure de l'analyse des objets de plus grande taille. Valeur par défaut : illimité.

Durée maximale d'analyse de l'objet (sec.) : définit la valeur de temps maximale pour l'analyse des fichiers dans un objet conteneur (tel qu'une archive RAR/ZIP ou un courriel avec plusieurs pièces jointes). Ce paramètre ne s'applique pas aux fichiers autonomes. Si une valeur définie par l'utilisateur a été entrée et que ce temps s'est écoulé, l'analyse s'arrête dès que possible, que cette analyse de fichier d'un objet conteneur soit terminée ou non.
Dans le cas d'une archive avec des fichiers volumineux, l'analyse s'arrêtera au plus tôt lorsqu'un fichier de l'archive est extrait (par exemple, lorsqu'une variable définie par l'utilisateur dure 3 secondes, mais que l'extraction d'un fichier prend 5 secondes). Le reste des fichiers de l'archive ne sera pas analysé lorsque ce temps sera écoulé.
Pour limiter le temps d'analyse, y compris les archives plus grandes, utilisez **Taille maximale de l'objet** et **Taille maximale du fichier dans l'archive** (non recommandé en raison de risques de sécurité possibles).
Valeur par défaut : ilimité.

Configuration de l'analyse d'archive

Niveau d'imbrication des archives - Précise la profondeur maximale de l'analyse des archives. Valeur par défaut : 10.

Taille maximale du fichier dans l'archive - Cette option permet de préciser la taille maximale des fichiers (après

extraction) à analyser, contenus dans les archives. La valeur maximale est **3 Go**.

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

Contrôle parental

L'option **Activer le contrôle parental** intègre le contrôle parental dans ESET Internet Security. Cliquez sur **Modifier** en regard de Compte utilisateur pour associer des comptes utilisateur Windows utilisés par le contrôle parental à des utilisateurs précis afin de les empêcher d'accéder à des contenus Internet inappropriés ou nuisibles.

Comptes utilisateur

Dans Configuration avancée > **Protections** > **Protection de l'accès Web** > **Contrôle parental** > **Compte utilisateur** > **Modifier**, vous pouvez associer des comptes utilisateur Windows utilisés par le contrôle parental afin de protéger des utilisateurs précis et les empêcher d'accéder à des contenus Internet inappropriés ou nuisibles.

Colonnes

Compte Windows - Le nom de l'utilisateur.

Activé - Lorsque cette option est activée, le contrôle parental pour un compte utilisateur en particulier est activé.

Domaine - Le nom du domaine auquel appartient un utilisateur.

Date de naissance - Âge de l'utilisateur à qui appartient ce compte.

Éléments de contrôle

Ajouter - Le dialogue Utilisation de comptes utilisateur s'affiche.

Modifier : cette option vous permet de modifier les comptes sélectionnés.

Supprimer - Supprimer le compte sélectionné.

Actualiser - Si vous avez ajouté un compte utilisateur, ESET Internet Security peut actualiser la liste des comptes utilisateur, sans avoir à rouvrir cette fenêtre.

Paramètres du compte d'utilisateur

La fenêtre comporte trois onglets :

Généralités

Cliquez sur le bouton bascule en regard de **Activé** pour activer le contrôle parental pour le compte Windows sélectionné ci-dessous.

Tout d'abord, **Sélectionnez** un compte Windows sur votre ordinateur. Les restrictions définies dans le contrôle

parental n'affectent que les comptes Windows standards. Les comptes Administrateur peuvent modifier des restrictions.

Si le compte est utilisé par un parent, sélectionnez **Compte parent**.

Définissez la **date de naissance de l'enfant** pour le compte afin de déterminer son niveau d'accès et définir des règles d'accès pour des pages Web adaptées à son âge.

Journalisation de la gravité

ESET Internet Security enregistre tous les événements importants dans un fichier journal, accessible directement à partir du menu principal. Cliquez sur **Outils** > **Fichiers journaux**, puis sélectionnez **Contrôle parental** dans le menu déroulant **Journal**.

- **Diagnostic** - Consigne les données requises pour affiner le programme.
- **Information** : Enregistre les messages informatifs, y compris les exceptions autorisées et bloquées, ainsi que tous les enregistrements ci-dessus.
- **Avertissement** - Enregistre les erreurs critiques et les messages d'avertissement.
- **Aucun** - Aucune journalisation ne sera faite.

Exceptions

Créer une exception peut autoriser ou refuser l'accès à un utilisateur à des sites Web qui ne se trouvent pas sur la liste d'exceptions. Cela est utile lorsque vous voulez contrôler l'accès à des sites Web spécifiques plutôt que d'utiliser des catégories. Les exceptions créées pour un compte peuvent être copiées et utilisées pour un autre compte. Cela est utile lorsque vous voulez créer des règles identiques pour des enfants d'un même âge.

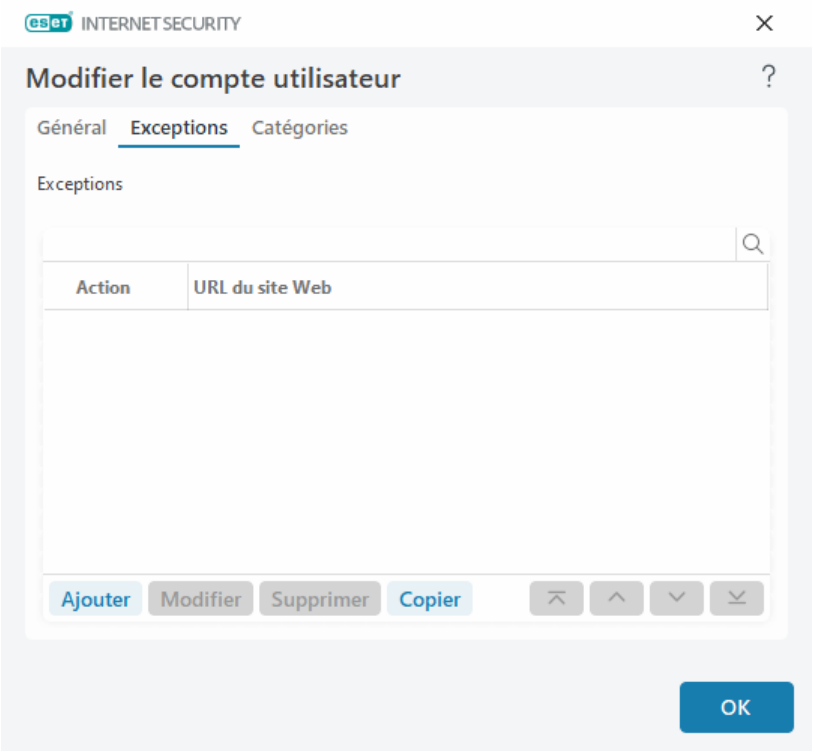
Cliquez sur **Ajouter** pour créer une nouvelle exception. Spécifiez l'**Action** (par exemple, **Bloquer**) à l'aide du menu déroulant, tapez l'**URL du site Web** à laquelle cette exception s'applique, puis cliquez sur **OK**. L'exception sera ajoutée à la liste des exceptions existantes en affichant son état.

Ajouter - Crée une nouvelle exception.

Modifier - Vous pouvez modifier l'**URL du site Web** ou l'**Action** de l'exception sélectionnée.

Supprimer - Supprime l'exception sélectionnée.

Copier - Sélectionnez un utilisateur dans le menu déroulant à partir duquel vous voulez copier l'exception créée.

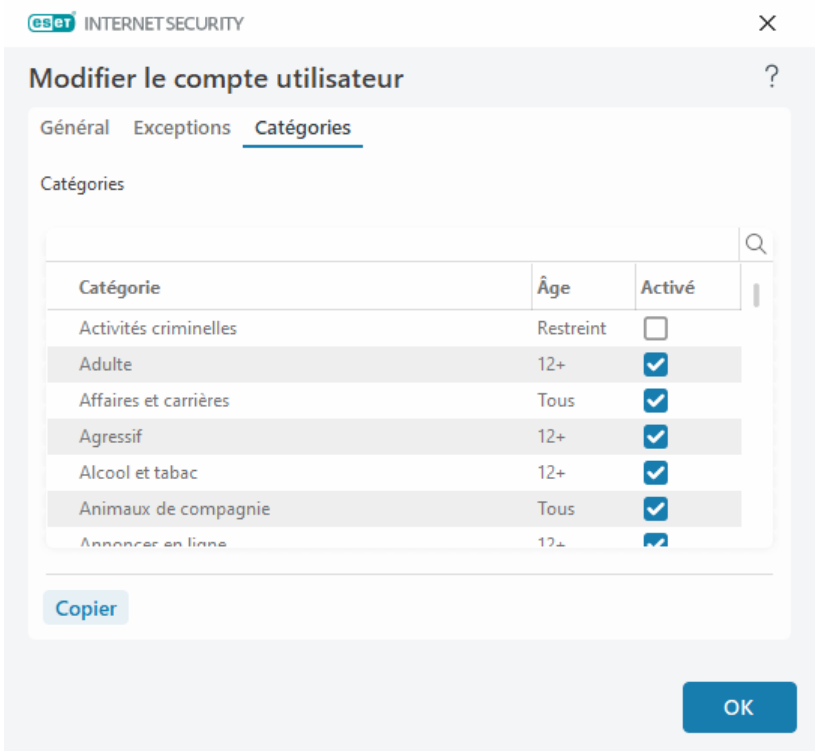


Les exceptions définies ont priorité sur les catégories définies pour le ou les comptes sélectionnés. Par exemple, si la catégorie **Actualités** est bloquée pour un compte, mais que vous avez défini comme exception une page Web autorisée présentant des actualités, ce compte pourra accéder à cette page Web. Vous pouvez voir toutes les modifications apportées dans la section Exceptions.

Catégories

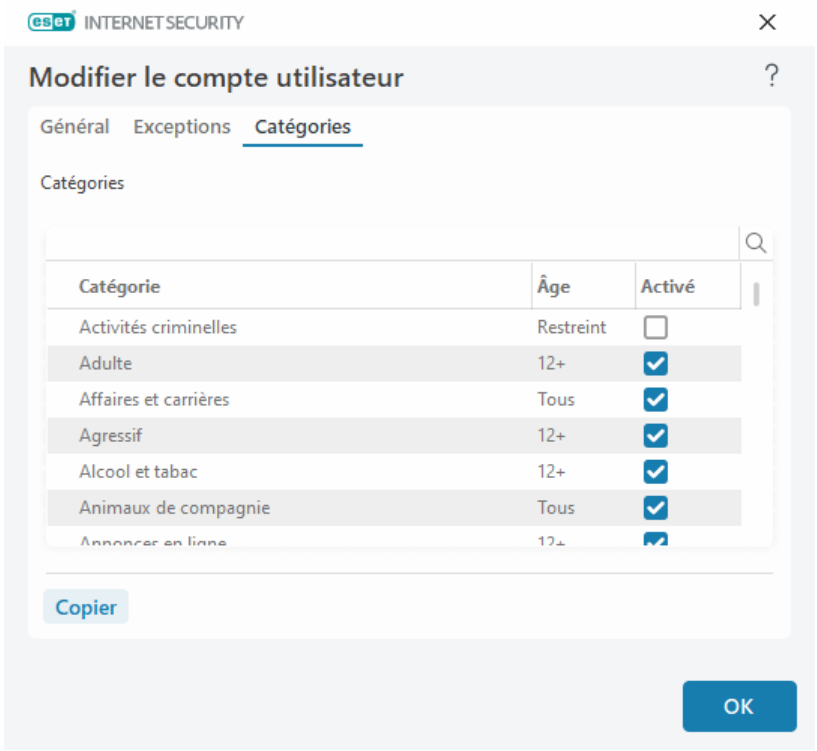
Dans l'onglet **Catégories**, vous pouvez définir les catégories générales des pages Web que vous voulez bloquer ou autoriser, pour chaque compte. Cochez la case située à côté d'une catégorie pour l'autoriser. Si vous laissez la case non cochée, la catégorie ne sera pas autorisé pour ce compte.

Copier - Vous permet de copier une liste des catégories bloquées ou autorisées à partir d'un compte existant modifié.



Catégories

Cochez la case dans la colonne **Activé** à côté d'une catégorie pour l'autoriser. Si vous laissez la case vide, la catégorie ne sera pas autorisée pour ce compte.



Voici quelques exemples de catégories (groupes) qui ne sont pas forcément bien connues des utilisateurs :

- **Divers** - En général, des adresses IP privées (locales) comme l'intranet, 127.0.0.0/8, 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 comprend des pages Web qui ne sont pas résolues en raison d'une erreur de connexion au moteur de base de données du contrôle parental.
- **Non catégorisé** - Pages Web inconnues non répertoriées dans la base de données du contrôle parental.
- **Dynamique** – Pages Web redirigeant vers d'autres pages sur d'autres sites Web.

Protection du navigateur

La protection du navigateur est une autre couche de protection pour votre sécurité et la confidentialité de vos renseignements qui protège la mémoire du navigateur contre l'inspection par d'autres processus, augmente la protection contre les enregistreurs de frappe et empêche de coller toutes les données de paiement en ligne modifiées par des logiciels malveillants du presse-papiers dans le navigateur sécurisé. Pour configurer la protection du navigateur, ouvrez Configuration avancée > **Protections** > **Protection du navigateur** et choisissez l'une des options de configuration suivantes :

- Opérations bancaires et navigation sécurisées
- Liste d'autorisation de la protection du navigateur
- Cadre du navigateur

Opérations bancaires et navigation sécurisées

Vous pouvez configurer Opérations bancaires et navigation sécurisées dans Configuration avancée > **Protections** > **Protection du navigateur** > **Opérations bancaires et navigation sécurisées**.

Opérations bancaires et navigation sécurisées

Activer Opérations bancaires et navigation sécurisées – Lorsque Opérations bancaires et navigation sécurisées est activé, tous les navigateurs Web pris en charge démarrent en mode sécurisé par défaut.

Protection du navigateur

Sécuriser tous les navigateurs pour lancer tous les navigateurs pris en charge en mode sécurisé.

Mode d'installation de l'extension : Dans le menu déroulant, vous pouvez sélectionner les extensions qui seront autorisées à être installées sur un navigateur sécurisé par ESET :

- **Extensions essentielles :** Seules les extensions les plus essentielles développées par un fabricant de navigateur particulier.
- **Toutes les extensions :** Les extensions prises en charge par un navigateur en particulier.

> La modification du mode d'installation de l'extension n'affecte pas les extensions de navigateur déjà installées :

Navigateur sécurisé

La protection améliorée de la mémoire - Si cette option est activée, la mémoire du navigateur sécurisé sera protégée contre l'inspection par d'autres processus.

Protection du clavier – Si cette option est activée, les informations saisies au moyen du clavier dans le navigateur sécurisé seront masquées pour les autres applications. Cela augmente la protection contre les enregistreurs de frappe.

Protection du presse-papiers – Si cette option est activée, ESET Internet Security empêche de coller toutes les données relatives au paiement en ligne modifiées par des logiciels malveillants du presse-papiers dans le navigateur sécurisé. Cela garantit une protection contre les modifications potentielles apportées par des logiciels malveillants.

Cadre du navigateur : Personnalisez les paramètres d'affichage du cadre du navigateur dans les navigateurs protégés.

Liste d'autorisation de la protection du navigateur : Gérez les fichiers ajoutés à la liste d'autorisation de la protection du navigateur.

Sécurité et confidentialité du navigateur

Activer Sécurité et confidentialité du navigateur – En désactivant cette fonctionnalité, l'extension Sécurité et confidentialité du navigateur sera désinstallée de tous les navigateurs pris en charge sur tous les comptes Windows.

Afficher les notifications Sécurité et confidentialité du navigateur – Si cette option est activée, ESET Internet Security affichera les notifications de Sécurité et confidentialité du navigateur.

Analyseur de scripts de navigateur

Activer l'analyse avancée des scripts de navigateur – Si cette option est activée, l'analyseur antivirus vérifiera tous les programmes JavaScript exécutés par les navigateurs Internet.

00

Contrôle de périphérique

ESET Internet Security offre la possibilité de commande automatique du périphérique (CD/DVD/USB/etc.). Vous bloquer ou de régler les filtres ou permissions étendus et de définir la capacité d'un utilisateur d'accéder à un périphérique donné et travailler avec celui-ci. Cela peut être utile si l'administrateur de l'ordinateur veut empêcher l'utilisation de périphériques comportant un contenu non sollicité par des utilisateurs.

Périphériques externes pris en charge :

- Stockage sur disque (Disque dur, Disque USB amovible)
- CD/DVD
- USB Imprimante

- FireWire Stockage
- Bluetooth Périphérique
- Lecteur de carte à puce
- Périphérique d'acquisition d'images
- Modem
- LPT/COM port
- Périphérique portable (périphériques alimentés par batterie tels que les lecteurs multimédias, les téléphones intelligents, les périphériques prêts à l'emploi, etc.)
- Tous les types de périphériques

Les options de contrôle de périphérique peuvent être modifiées dans Configuration avancée > **Protections** > **Contrôle de périphérique**.

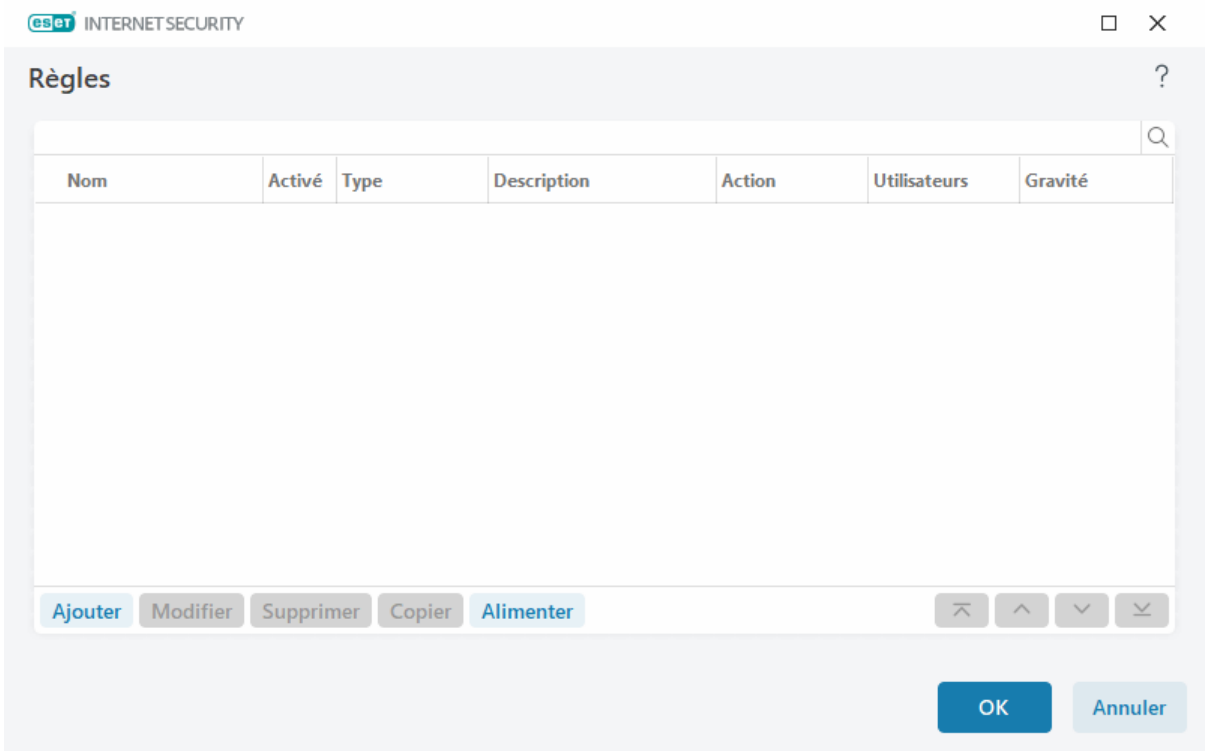
Cliquez sur le bouton bascule **Activer la commande du périphérique** pour activer la fonctionnalité de commande du périphérique dans ESET Internet Security; vous devez redémarrer votre ordinateur pour que cette modification prenne effet. Une fois le contrôle de périphérique activé, vous pouvez définir les **règles** dans la fenêtre Éditeur de règles.

> Vous pouvez créer différents groupes de périphériques pour lesquels des règles différentes seront appliquées. Vous pouvez également créer un seul groupe de périphériques pour lesquels la règle avec l'action **Autoriser** ou **Blocage d'écriture** sera appliquée. Cela garantit le blocage des périphériques non reconnus par le contrôle des périphériques lorsqu'il est connecté à votre ordinateur.

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

Éditeur des règles du contrôle de périphérique

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



Des périphériques particuliers peuvent être autorisés ou bloqués par utilisateur ou groupe d'utilisateurs, ainsi qu'en fonction de paramètres supplémentaires qui peuvent être précisés dans la configuration de la règle. La liste de règles contient plusieurs éléments descriptifs d'une règle comme le nom, le type de périphérique externe, l'action à effectuer après la connexion d'un périphérique externe à l'ordinateur et la gravité, tels que consignés dans le journal. Consultez également Ajouter des règles de contrôle de périphérique.

Cliquez sur **Ajouter** ou **Modifier** pour gérer une règle. Cliquez sur **Copier** pour créer une nouvelle règle avec les options prédéfinies utilisées pour une autre règle sélectionnée. Les chaînes en XML qui s'affichent lorsque vous cliquez sur une règle peuvent être copiées dans le Bloc-notes pour aider les administrateurs de système à exporter ou à importer ces données et à les utiliser, par exemple dans .

En tenant la touche **CTRL** enfoncée et en cliquant simultanément sur les règles, vous pourrez en sélectionner plusieurs et effectuer des actions sur celles-ci, comme les supprimer ou les monter ou descendre dans la liste. La case **Activé** active ou désactive une règle, ce qui peut être utile si vous ne voulez pas supprimer définitivement la règle.

Cliquez sur l'option **Alimenter** pour remplir automatiquement les paramètres du support amovible connecté à votre ordinateur.

Les règles sont classées par ordre de priorité; les règles ayant une priorité plus élevée sont plus près du sommet. Les règles peuvent être déplacées en cliquant sur **Au dessus/Vers le haut/Vers le bas/En dessous** et peuvent être déplacées individuellement ou en groupes.

Les entrées de journal peuvent être consultées dans la fenêtre principale du programme en cliquant sur **Outils** > Fichiers journaux.

Le journal de contrôle des périphériques enregistre toutes les occurrences où le contrôle de périphérique est déclenché.

Périphériques détectés

Le bouton **Alimenter** donne un aperçu de tous les périphériques actuellement connectés avec les informations sur : le type de périphérique, le fournisseur du périphérique, le modèle et le numéro de série (si disponible). Si vous souhaitez voir tous les périphériques masqués, sélectionnez **Afficher les périphériques masqués**.

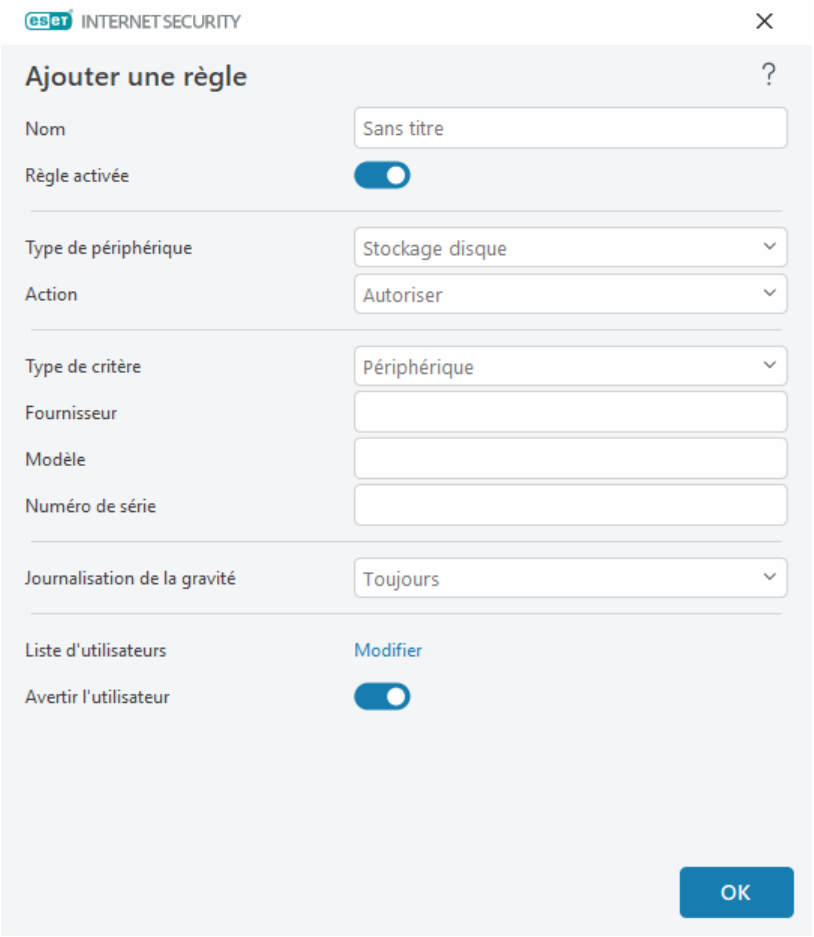
Sélectionnez un périphérique dans la liste des périphériques détectés et cliquez sur **OK** pour ajouter une règle de contrôle de périphérique avec des informations prédéfinies (tous les paramètres peuvent être ajustés).

Les périphériques en mode faible consommation (veille) sont marqués d'une icône d'avertissement . Pour activer le bouton **OK** et ajouter une règle pour ce périphérique :

- Reconnectez le périphérique
- Utilisez le périphérique (par exemple, démarrez l'application Appareil photo dans Windows pour réveiller une webcam)

Ajout de règles du contrôle de périphérique

Une règle de contrôle de périphériques définit l'action à entreprendre lorsqu'un périphérique conforme aux critères énoncés dans la règle est branché à l'ordinateur.



Entrez une description de la règle dans le champ **Nom** pour pouvoir l'identifier plus facilement. Cliquez sur le bouton bascule à côté de **Règle activée** pour activer ou désactiver cette règle, ce qui peut être utile si vous ne

voulez pas supprimer définitivement la règle.

Type de périphérique

Choisissez le type de périphérique externe dans le menu déroulant (Stockage sur disque/Dispositif portable/Bluetooth/FireWire/etc.). Les renseignements de types de périphériques sont tirés du système d'exploitation et peuvent être affichés dans le Gestionnaire de périphériques lorsqu'un périphérique est branché à l'ordinateur. Les périphériques de stockage incluent les disques externes ou les lecteurs conventionnels de cartes mémoires branchés à un port USB ou FireWire. Les lecteurs de cartes à puce comprennent les lecteurs de cartes à puce avec circuit intégré, comme les cartes SIM ou les cartes d'authentification. Les numériseurs ou les appareils photos sont des exemples de périphériques d'acquisition d'images. Parce que ces périphériques ne fournissent que des renseignements sur leurs actions et ne fournissent pas de renseignements sur les utilisateurs, ils ne peuvent être bloqués que globalement.

Action

L'accès aux appareils autres que de stockage peut être autorisé ou bloqué. À l'inverse, les règles connexes aux périphériques de stockage permettent de sélectionner l'un des droits suivants :

- **Permettre** : L'accès complet au périphérique sera autorisé.
- **Bloquer** - L'accès au périphérique sera bloqué.
- **Blocage d'écriture** - Seule l'accès en lecture à partir du périphérique sera autorisée.
- **Avertir** - Chaque fois qu'un périphérique est connecté, l'utilisateur sera informé s'il est autorisé ou bloqué, et une entrée de journal sera effectuée. Les périphériques ne sont pas mémorisés; une notification sera toujours affichée pour les connexions ultérieures du même périphérique.

À noter que seules certaines actions (autorisations) sont disponibles pour tous les types de périphériques. Si c'est un périphérique de stockage, toutes les quatre actions sont disponibles. Pour les périphériques autres que de stockage, seules trois actions sont disponibles (par exemple, l'action **Blocage d'écriture** n'est pas disponible pour Bluetooth ne peuvent qu'être autorisés, bloqués ou avertis).

Type de critère

Sélectionnez **Groupe de périphériques** ou **Périphérique**.

D'autres paramètres présentés ci-dessous peuvent être utilisés pour affiner les règles pour différents périphériques. Tous les paramètres sont sensibles à la casse et prennent en charge les caractères génériques (*, ?) :

- **Fournisseur** - Filtrer par nom de fournisseur ou par identifiant.
- **Modèle** - Nom donné au périphérique.
- **Numéro de série** - Les périphériques externes ont généralement leur propre numéro de série. Dans le cas des CD/DVD, il s'agit du numéro de série du périphérique, non du lecteur de CD.

> Si ces paramètres ne sont pas définis, la règle ignorera ces champs lors de la recherche de correspondance. Les paramètres de filtrage dans tous les champs de texte sont sensibles à la casse et prennent en charge les caractères génériques; un point d'interrogation (?) représente un seul caractère, tandis qu'un astérisque (*) représente une chaîne de zéro ou plusieurs caractères.

Pour afficher des informations sur un périphérique, créez une règle pour ce type de périphérique, connectez-le à votre ordinateur, puis vérifiez les détails le concernant dans le journal de contrôle du périphérique.

Journalisation de la gravité

ESET Internet Security enregistre tous les événements importants dans un fichier journal, accessible directement à partir du menu principal. Cliquez sur **Outils** > **Fichiers journaux**, puis sélectionnez **Contrôle de périphérique** dans le menu déroulant **Journal**.

- **Toujours** - Consigne tous les événements.
- **Diagnostic** - Consigne les données requises pour affiner le programme.
- **Information** - Enregistre des messages informatifs, y compris les messages de mise à jour réussie, ainsi que toutes les entrées préalables.
- **Avertissement** - Enregistre les erreurs critiques et les messages d'avertissement.
- **Aucun** - Aucune journalisation ne sera faite.

Liste de l'utilisateur

Les règles peuvent être restreintes à certains utilisateurs ou groupes d'utilisateurs en les ajoutant dans la liste des utilisateurs. Pour ce faire, cliquez sur **Modifier** à côté de **Liste des utilisateurs**.

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

Limitations de la liste des utilisateurs

La liste des utilisateurs ne peut pas être définie pour les règles avec des types de périphérique spécifiques :

- Imprimante USB
- Périphérique Bluetooth
- Lecteur de carte à puce
- Périphérique d'acquisition d'images
- Modem
- Port LPT/COM

Notifier l'utilisateur : Si un périphérique bloqué par une règle existante est inséré, une fenêtre de notification s'affiche.

Groupes d'appareils

Le périphérique connecté à votre ordinateur peut présenter un risque pour la sécurité.

La fenêtre Groupes de périphériques est divisée en deux sections. La partie droite de la fenêtre contient une liste des périphériques appartenant au groupe respectif et la partie gauche contient des groupes créés. Sélectionnez un groupe pour afficher les périphériques dans le volet droit.

Lorsque vous ouvrez la fenêtre Groupes de périphériques et sélectionnez un groupe, vous pouvez ajouter ou supprimer des périphériques dans la liste. Une autre façon d'ajouter des périphériques au groupe est de les importer depuis un fichier. Vous pouvez aussi cliquer sur le bouton **Remplir** et tous les périphériques connectés à votre ordinateur apparaitront dans la fenêtre **Périphériques détectés**. Sélectionnez les périphériques dans la liste alimentée pour les ajouter au groupe en cliquant sur **OK**.

Éléments de contrôle

Ajouter : vous pouvez ajouter un groupe en entrant son nom ou un périphérique à un groupe existant selon la section de la fenêtre à partir de laquelle vous avez cliquez sur le bouton.

Modifier - Vous permet de modifier le nom du groupe sélectionné ou les paramètres du périphérique (fournisseur, modèle, numéro de série).

Supprimer : Supprime le groupe ou le périphérique sélectionné en fonction de la partie de la fenêtre ou vous avez cliqué sur le bouton.

Importer – Permet d'importer une liste de périphériques à partir d'un fichier texte. L'importation de périphériques à partir d'un fichier texte nécessite un formatage correct :

- Chaque périphérique commence à la nouvelle ligne.
- Les renseignements sur le **fournisseur**, le **modèle** et le **numéro de série** doivent être présents pour chaque périphérique et séparés par une virgule.

Voici un exemple du contenu d'un fichier texte :

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Exporter – Permet d'exporter une liste de périphériques vers un fichier.

Le bouton **Alimenter** donne un aperçu de tous les périphériques actuellement connectés avec les informations sur : le type de périphérique, le fournisseur du périphérique, le modèle et le numéro de série (si disponible).

Ajouter un périphérique

Cliquez sur **Ajouter** dans la fenêtre de droite pour ajouter un périphérique à un groupe existant. D'autres paramètres présentés ci-dessous peuvent être utilisés pour affiner les règles pour différents périphériques. Tous les paramètres sont sensibles à la casse et prennent en charge les caractères génériques (*, ?) :

- **Fournisseur** - Filtrer par nom de fournisseur ou par ID.
- **Modèle** - Nom donné au périphérique.
- **Numéro de série** - Les périphériques externes ont généralement leur propre numéro de série. Dans le cas des CD/DVD, il s'agit du numéro de série du périphérique, non du lecteur de CD.
- **Description :** il s’agit de votre description du périphérique pour une meilleure organisation.

Si ces paramètres ne sont pas définis, la règle ignorera ces champs lors de la recherche de correspondance. Les paramètres de filtrage dans tous les champs de texte sont sensibles à la casse et prennent en charge les caractères génériques; un point d'interrogation (?) représente un seul caractère, tandis qu'un astérisque (*) représente une chaîne de zéro ou plusieurs caractères.

Cliquez sur **OK** pour enregistrer les modifications. Cliquez sur **Annuler** pour quitter la fenêtre **Groupes de périphériques** sans enregistrer les modifications.

Une fois le groupe de périphériques créé, vous devez ajouter une nouvelle règle de contrôle de périphérique pour le groupe de périphériques créé et sélectionner l'action à réaliser.

À noter que seules certaines actions (autorisations) sont disponibles pour tous les types de périphériques. Toutes les quatre actions sont disponibles s'il s'agit d'un périphérique de stockage. Pour les périphériques autres que de stockage, seules trois actions sont disponibles (par exemple, l'action **Blocage d'écriture** n'est pas disponible pour Bluetooth, ce qui signifie que les périphériques Bluetooth ne peuvent qu'être autorisés, bloqués ou avertis).

Protection de la caméra Web

Protection de la caméra Web vous signale les processus et les applications qui accèdent à la caméra Web de votre ordinateur. Lorsqu'une application tente d'accéder à votre caméra, vous recevez une notification. Vous pouvez alors **autoriser** ou **bloquer** l'accès de ces processus ou de ces applications indésirables à votre caméra. La couleur de la fenêtre d'alerte dépend de la réputation de l'application.

Les options de protection de la webcam peuvent être modifiées dans Configuration avancée > **Protections** > **Contrôle de périphérique** > **Protection de la webcam**.

Pour activer la fonctionnalité de protection de la webcam dans ESET Internet Security, activez le bouton bascule en regard de **Activer la protection de la webcam**.

Une fois la protection de la webcam activée, l'option **Règles** est activée, ce qui vous permet d'ouvrir la fenêtre Éditeur des règles.

Pour désactiver les alertes pour les applications qui possèdent une règle qui a été modifiée, mais qui dispose toujours d'une signature numérique valide (par exemple, une mise à jour de l'application), activez le bouton bascule en regard de **Désactiver les alertes d'accès à la webcam pour les applications modifiées.**

Éditeur des règles de protection de caméra Web

Cette fenêtre affiche les règles existantes et permet un contrôle des applications et des processus qui accèdent à la caméra Web de votre ordinateur en fonction de l'action que vous avez prise.

Les actions suivants sont disponibles :

- **Autoriser l\\'accès**
- **Bloquer l'accès**

- **Demander** (Requiert l'avis de l'utilisateur chaque fois qu'une application tente d'accéder à la webcam)

Décochez la case de la colonne **Notifier** pour ne plus recevoir de notifications lorsqu'une application accède à la webcam.

Instructions illustrées
Comment créer et modifier des règles de webcam dans ESET Internet Security.

ThreatSense

ThreatSense combine de nombreuses méthodes de détection de menaces complexes. Cette technologie proactive fournit également une protection durant les premières heures de 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 simultanément plusieurs flux de données, maximisant ainsi l'efficacité et le taux de détection. La technologie ThreatSense élimine également avec succès les rootkits.

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

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

Pour accéder à la fenêtre de configuration, cliquez sur **ThreatSense** dans Configuration avancée pour tout module qui utilise la technologie ThreatSense (voir ci-dessous). Différents scénarios de sécurité peuvent nécessiter des configurations différentes. Dans cet esprit, ThreatSense est configurable individuellement pour les modules de protection suivants :

- Protection en temps réel du système de fichiers
- Analyse en état inactif
- Analyse au démarrage
- Protection des documents
- Protection du client de messagerie
- Protection de l'accès Web
- Analyse de l'ordinateur

Les paramètres de ThreatSense sont hautement optimisés pour chaque module et leur modification peut grandement affecter le fonctionnement du système. Par exemple, en modifiant les paramètres afin d'analyser à chaque fois les compacteurs exécutables ou d'autoriser l'heuristique avancée dans la protection en temps réel du système de fichiers, vous pouvez diminuer les performances du système (normalement, seuls les fichiers nouvellement créés sont analysés par ces méthodes). Il est recommandé de laisser inchangés les paramètres par défaut de ThreatSense pour tous les modules, à l'exception du module Analyse de l'ordinateur.

Objets à analyser

Cette section vous permet de définir quels éléments et fichiers de l'ordinateur seront analysés à la recherche des infiltrations.

Mémoire vive - Activez cette option pour détecter les menaces qui s'attaquent à la mémoire vive du système.

Secteurs d'amorçage/UEFI - Analyse les secteurs d'amorçage à la recherche des logiciels malveillants dans l'enregistrement de démarrage principal. Pour en savoir plus sur l'UEFI, consultez le glossaire.

Fichiers courriel - 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 beaucoup d'autres.

Archives à extraction automatique - Les archives à extraction automatique (SFX) sont des archives qui peuvent s'extraire toutes seules.

Compresseurs d'exécutable - Après avoir été exécutés, les compresseurs d'exécutables (contrairement aux types d'archives standard) se décompressent en mémoire. En plus des compacteurs statiques standards (UPX, yoda, ASPack, FSG, etc.), l'analyseur est capable der reconnaitre beaucoup d'autres types de compacteurs grâce à l'utilisation de l'émulation de code.

Options d'analyse

Sélectionnez les méthodes utilisées lors de l'analyse du système à la recherche d'infiltrations. Les options suivantes sont disponibles :

Heuristiques - La méthode heuristique utilise un algorithme d'analyse de l'activité (malveillante) des programmes. Le principal avantage de cette technologie est sa capacité à identifier un code malveillant qui n'existait pas ou n'était pas connu par le moteur de détection. L'inconvénient de cette méthode est la probabilité (très faible) de fausses alarmes.

Heuristique avancée/Signatures ADN - La méthode heuristique avancée utilise un algorithme heuristique développé par ESET, optimisé pour la détection des vers d'ordinateur et les chevaux de Troie et écrit dans un langage de programmation de haut niveau. L'utilisation de l'heuristique avancée augmente considérablement les capacités de détection de menaces des produits ESET. Les signatures peuvent détecter et identifier les virus de façon fiable. Grâce au système de mise à jour automatique, de nouvelles signatures peuvent être disponibles dans les quelques heures de la découverte d'une menace. L'inconvénient des signatures est qu'elles ne détectent que les virus qu'elles connaissent (ou une version légèrement modifiée de ces virus).

Nettoyage

Les paramètres de nettoyage déterminent le comportement de ESET Internet Security lors du nettoyage des objets. Quatre niveaux de nettoyage sont possibles :

ThreatSense possède les niveaux de correction (c'est-à-dire de nettoyage) suivants :

Correction dans ESET Internet Security

Niveau de nettoyage	Description
Toujours corriger la détection	Cette option permet de tenter de corriger la détection lors du nettoyage des objets sans aucune intervention de l'utilisateur final. Dans de rares cas (fichiers système, par exemple), si la détection ne peut pas être corrigée, l'objet signalé est laissé à son emplacement d'origine.

Niveau de nettoyage	Description
Corriger la détection si cela ne présente pas de danger, conserver sinon	Cette option permet de tenter de corriger la détection lors du nettoyage des objets sans aucune intervention de l'utilisateur final. Dans certains cas (fichiers système ou archives contenant à la fois des fichiers propres et des fichiers infectés), si la détection ne peut pas être corrigée, l'objet signalé est laissé à son emplacement d'origine.
Corriger la détection si cela ne présente pas de danger, demander sinon	Cette option permet de tenter de corriger la détection lors du nettoyage des objets. Dans certains cas, si aucune action ne peut être effectuée, l'utilisateur final reçoit une alerte interactive et doit sélectionner une action de correction (par exemple, supprimer ou ignorer). Ce paramètre est recommandé dans la plupart des cas.
Toujours demander à l'utilisateur final	Lors du nettoyage des objets, une fenêtre interactive s'ouvre et l'utilisateur final doit sélectionner une action de correction (par exemple, supprimer ou ignorer). Ce niveau est conçu pour les utilisateurs plus avancés qui savent quelles mesures prendre lorsqu'une détection se produit.

Exclusions

Une extension est la partie d'un nom de fichier délimitée par un point. Elle définit le type et le contenu du fichier. Cette section de la configuration de ThreatSense vous permet de définir les types de fichiers à analyser.

Autre

Au moment de configurer les paramètres du moteur ThreatSense pour une analyse de l'ordinateur à la demande, les options suivantes dans la section **Autres** seront aussi offertes :

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 beaucoup de ressources système, vous pouvez activer l'analyse en arrière-plan à faible priorité de manière à réserver des ressources pour vos applications.

Consigner tous les objets – Le journal d'analyse affichera tous les fichiers analysés dans des archives auto-extractibles, même ceux qui ne sont pas infectés (peut générer beaucoup de données de journal d'analyse et augmenter la taille du fichier journal d'analyse).

Activer l'optimisation intelligente - Lorsque la fonction Optimisation intelligente est activée, les paramètres les plus optimaux sont utilisés pour assurer le niveau d'analyse le plus efficient tout en conservant la vitesse d'analyse la plus élevée. Les différents modules de protection effectuent une analyse intelligente, utilisant pour ce faire différentes méthodes d'analyse et les appliquant à différents types de fichiers. Si l'optimisation Smart est activée, seuls les paramètres définis par l'utilisateur dans le moteur ThreatSense utilisé pour ces modules particuliers seront appliqués au moment de l'analyse.

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

Limites

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

Paramètres de l'objet

Taille maximale de l'objet - Définit la taille maximale des objets à analyser. Le module antivirus donné n'analysera alors que les objets d'une taille inférieure à celle indiquée. Cette option ne devrait être modifiée que par des utilisateurs expérimentés ayant des raisons précises d'exclure de l'analyse des objets de plus grande taille. Valeur par défaut : illimité.

Durée maximale d'analyse de l'objet (sec.) : définit la valeur de temps maximale pour l'analyse des fichiers dans un objet conteneur (tel qu'une archive RAR/ZIP ou un courriel avec plusieurs pièces jointes). Ce paramètre ne s'applique pas aux fichiers autonomes. Si une valeur définie par l'utilisateur a été entrée et que ce temps s'est écoulé, l'analyse s'arrête dès que possible, que cette analyse de fichier d'un objet conteneur soit terminée ou non.
Dans le cas d'une archive avec des fichiers volumineux, l'analyse s'arrêtera au plus tôt lorsqu'un fichier de l'archive est extrait (par exemple, lorsqu'une variable définie par l'utilisateur dure 3 secondes, mais que l'extraction d'un fichier prend 5 secondes). Le reste des fichiers de l'archive ne sera pas analysé lorsque ce temps sera écoulé.
Pour limiter le temps d'analyse, y compris les archives plus grandes, utilisez **Taille maximale de l'objet** et **Taille maximale du fichier dans l'archive** (non recommandé en raison de risques de sécurité possibles).
Valeur par défaut : ilimité.

Configuration de l'analyse d'archive

Niveau d'imbrication des archives - Précise la profondeur maximale de l'analyse des archives. Valeur par défaut : 10.

Taille maximale du fichier dans l'archive - Cette option permet de préciser la taille maximale des fichiers (après extraction) à analyser, contenus dans les archives. La valeur maximale est **3 Go**.

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

Niveaux de nettoyage

Pour modifier les paramètres du niveau de nettoyage pour un module de protection donné, développez **ThreatSense** (par exemple, **Protection en temps réel du système de fichiers**), puis choisissez un **niveau de nettoyage** dans le menu déroulant.

ThreatSense possède les niveaux de correction (c'est-à-dire de nettoyage) suivants :

Correction dans ESET Internet Security

Niveau de nettoyage	Description
Toujours corriger la détection	Cette option permet de tenter de corriger la détection lors du nettoyage des objets sans aucune intervention de l'utilisateur final. Dans de rares cas (fichiers système, par exemple), si la détection ne peut pas être corrigée, l'objet signalé est laissé à son emplacement d'origine.
Corriger la détection si cela ne présente pas de danger, conserver sinon	Cette option permet de tenter de corriger la détection lors du nettoyage des objets sans aucune intervention de l'utilisateur final. Dans certains cas (fichiers système ou archives contenant à la fois des fichiers propres et des fichiers infectés), si la détection ne peut pas être corrigée, l'objet signalé est laissé à son emplacement d'origine.
Corriger la détection si cela ne présente pas de danger, demander sinon	Cette option permet de tenter de corriger la détection lors du nettoyage des objets. Dans certains cas, si aucune action ne peut être effectuée, l'utilisateur final reçoit une alerte interactive et doit sélectionner une action de correction (par exemple, supprimer ou ignorer). Ce paramètre est recommandé dans la plupart des cas.
Toujours demander à l'utilisateur final	Lors du nettoyage des objets, une fenêtre interactive s'ouvre et l'utilisateur final doit sélectionner une action de correction (par exemple, supprimer ou ignorer). Ce niveau est conçu pour les utilisateurs plus avancés qui savent quelles mesures prendre lorsqu'une détection se produit.

Extension de fichiers exclus de l'analyse

Les extensions de fichier exclues font partie de ThreatSense. Pour configurer les extensions de fichier exclues, cliquez sur **ThreatSense** dans Configuration avancée pour tout module qui utilise la technologie ThreatSense.

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 de ThreatSense vous permet de définir les types de fichiers à analyser.

Ne confondez pas avec les exclusions de processus, les exclusions HIPS ou les exclusions de fichier/dossier.

Par défaut, les fichiers sont analysés. N'importe quelle extension peut être ajoutée à la liste des fichiers exclus de l'analyse.

L'exclusion de fichiers peut parfois être utile lorsque l'analyse de certains types de fichiers empêche le fonctionnement approprié du programme utilisant ces extensions. Par exemple, il peut être judicieux d'exclure les extensions `.edb`, `.eml` et `.tmp` lorsque vous utilisez les serveurs Microsoft Exchange.

Pour ajouter une nouvelle extension à la liste, cliquez sur **Ajouter**. Puis entrez l'extension dans le champ vide, (par exemple, tmp); cliquez ensuite sur **OK**.) puis cliquez sur OK. Lorsque vous sélectionnez **Entrez plusieurs valeurs**, vous pouvez ajouter plusieurs extensions de fichier séparées par des lignes, des virgules ou des points-virgules. Par exemple, choisissez **Points-virgules** dans le menu déroulant comme séparateur et tapez `edb;eml;tmp`
Vous pouvez utiliser le symbole spécial ? (point d'interrogation). Le point d'interrogation représente n'importe quel symbole (par exemple `?db`).

Pour voir l'extension exacte (le cas échéant) d'un fichier dans un système d'exploitation Windows, vous devez cocher la case **Extensions de nom de fichier** dans **Explorateur Windows** > **Afficher** (onglet).

Paramètres supplémentaires ThreatSense

Pour modifier ces paramètres, ouvrez Configuration avancée > **Protections** > **Protection en temps réel du système de fichiers** > **Paramètres supplémentaires de ThreatSense**.

Paramètres supplémentaires ThreatSense pour des fichiers nouvellement créés et modifiés

Les fichiers nouvellement créés ou les fichiers modifiés ont une probabilité d'infection relativement plus élevée que celle des fichiers existants. C'est pour cette raison que le programme utilise des paramètres d'analyse supplémentaires pour vérifier ces fichiers. ESET Internet Security utilise une heuristique avancée qui peut détecter les nouvelles menaces avant la diffusion de la mise à jour du moteur de détection, en plus des méthodes d'analyse basées sur les signatures.

En plus des fichiers nouvellement créés, l'analyse est aussi effectuée sur les **archives à extraction automatique** (.sfx) et les **fichiers exécutables compressés par un compresseur d'exécutables** (interne). Par défaut, les archives sont analysées jusqu'au dixième niveau d'imbrication et vérifiées indépendamment de leur taille réelle. Désactivez l'option **Paramètres d'analyse d'archive par défaut** pour modifier les paramètres d'analyse de l'archive.

Autres paramètres ThreatSense pour les fichiers exécutés

Heuristique avancée sur l'exécution du fichier - Par défaut, l'heuristique avancée est utilisée lorsque les fichiers sont exécutés. Lorsque cette option est activée, nous vous recommandons fortement de conserver l'optimisation intelligente et ESET LiveGrid® activés afin de réduire l'incidence sur la performance du système.

Heuristique avancée à l'exécution de fichiers à partir de supports amovibles - L'heuristique avancée fait l'émulation du code dans un environnement virtuel et évalue son comportement avant d'autoriser l'exécution du code à partir d'un support amovible.

Outils

Vous pouvez configurer des paramètres avancés pour les fonctionnalités qui offrent une sécurité supplémentaire et aident à simplifier l'administration de ESET Internet Security dans Configuration avancée > **Outils**.

- Mise à jour Microsoft Windows®
- ESET CMD
- Fichiers journaux
- Mode jeu
- Diagnostic

Mise à jour Microsoft Windows®

La fonctionnalité Windows Update est un élément important de la protection des utilisateurs contre les logiciels malveillants. C'est pourquoi il est essentiel que vous installiez les mises à jour de Microsoft Windows dès qu'elles sont disponibles. ESET Internet Security vous informe des mises à jour manquantes en fonction du niveau indiqué dans Configuration avancée > **Outils**. Les niveaux suivants sont disponibles :

- **Aucune mise à jour** - Aucune mise à jour du système ne pourra être téléchargée.
- **Mises à jour facultatives** - Les mises à jour de faible priorité pourront minimalement être téléchargées.
- **Mises à jour recommandées** - Les mises à jour courantes pourront minimalement être téléchargées.
- **Mises à jour importantes** - Les mises à jour importantes pourront minimalement être téléchargées.
- **Mises à jour critiques** - Seules les mises à jour critiques pourront être téléchargées.

Fenêtre de dialogue - Mises à jour système

Si des mises à jour sont disponibles pour votre système d'exploitation, ESET Internet Security affiche une notification dans la fenêtre principale du programme sous **Vue d'ensemble**. Cliquez sur **Plus d'information** pour ouvrir la fenêtre des mises à jour du système.

La fenêtre Mises à jour système affiche la liste des mises à jour disponibles, prêtes pour téléchargement et installation. Le type de chaque mise à jour s'affiche à côté de son nom.

Double cliquez sur n'importe quelle ligne de mise à jour pour afficher la fenêtre Informations sur les mises à jour contenant des informations supplémentaires.

Cliquez sur **Exécuter une mise à jour système** pour télécharger et installer toutes les mises à jour du système d'exploitation répertoriées.

Mettre à jour les informations

La fenêtre Mises à jour système affiche la liste des mises à jour disponibles, prêtes pour téléchargement et installation. Le niveau de priorité de chaque mise à jour s'affiche à côté de son nom.

Cliquez sur **Exécuter une mise à jour système** pour lancer le téléchargement et l'installation des mises à jour du système d'exploitation.

Cliquez à droite sur toute rangée de mise à jour puis sur **Afficher l'information** pour afficher une nouvelle fenêtre avec de l'information supplémentaire.

ESET CMD

Il s'agit d'une fonctionnalité qui permet des commandes avancées ecmd. Elle vous permet d'exporter et d'importer des paramètres en utilisant la ligne de commande (ecmd.exe). Jusqu'à présent, il était possible d'exporter et d'importer des paramètres uniquement à l'aide de l'IUG. La configuration de ESET Internet Security

peut être exportée à l'aide d'un fichier *.xml*.

Lorsque ESET CMD est activé, deux méthodes d'autorisation vous sont offertes :

- **Aucune** – aucune autorisation. Nous ne recommandons pas cette méthode car elle permet l'importation de toute configuration non signée, ce qui comporte un risque.

- **Mot de passe de configuration avancée** – un mot de passe est requis lors de l'importation de la configuration d'un fichier .xml; le fichier doit être signé (voir signature de la configuration .xml plus bas). Le mot de passe spécifié dans Configuration de l'accès doit être fourni avant qu'une nouvelle configuration puisse être importée. Si la configuration de l'accès n'est pas activée, le mot de passe ne correspond pas ou le fichier de configuration .xml n'est pas signé, la configuration ne sera pas importée.

Une fois qu'ESET CMD est activé, vous pouvez utiliser la ligne de commande pour importer ou exporter les configurations de ESET Internet Security. Vous pouvez le faire manuellement ou créer un script pour l'automatiser.

Pour utiliser les commandes avancées d'ecmd, vous devez les exécuter avec des privilèges d'administrateur ou ouvrir l'invite de commandes (cmd) de Windows en utilisant **Exécuter en tant qu'administrateur**. Sinon, vous obtiendrez le message **Error executing command**. En outre, lors de l'exportation de la configuration, le dossier de destination doit exister. La commande Export fonctionne même lorsque le paramètre ESET CMD est désactivé.

Commande d'exportation des paramètres :
`ecmd /getcfg c:\config\settings.xml`

Commande d'importation des paramètres :
`ecmd /setcfg c:\config\settings.xml`

Les commandes ecmd avancées ne peuvent être exécutées que localement.

Signature d'un fichier de configuration *.xml* :

1. Téléchargez l'exécutable XmlSignTool.

2. Ouvrez l'invite de commande Windows (cmd) en utilisant l'option **Exécuter en tant qu'administrateur**.

3. Accédez à l'emplacement de sauvegarde de `xmlsigntool.exe`

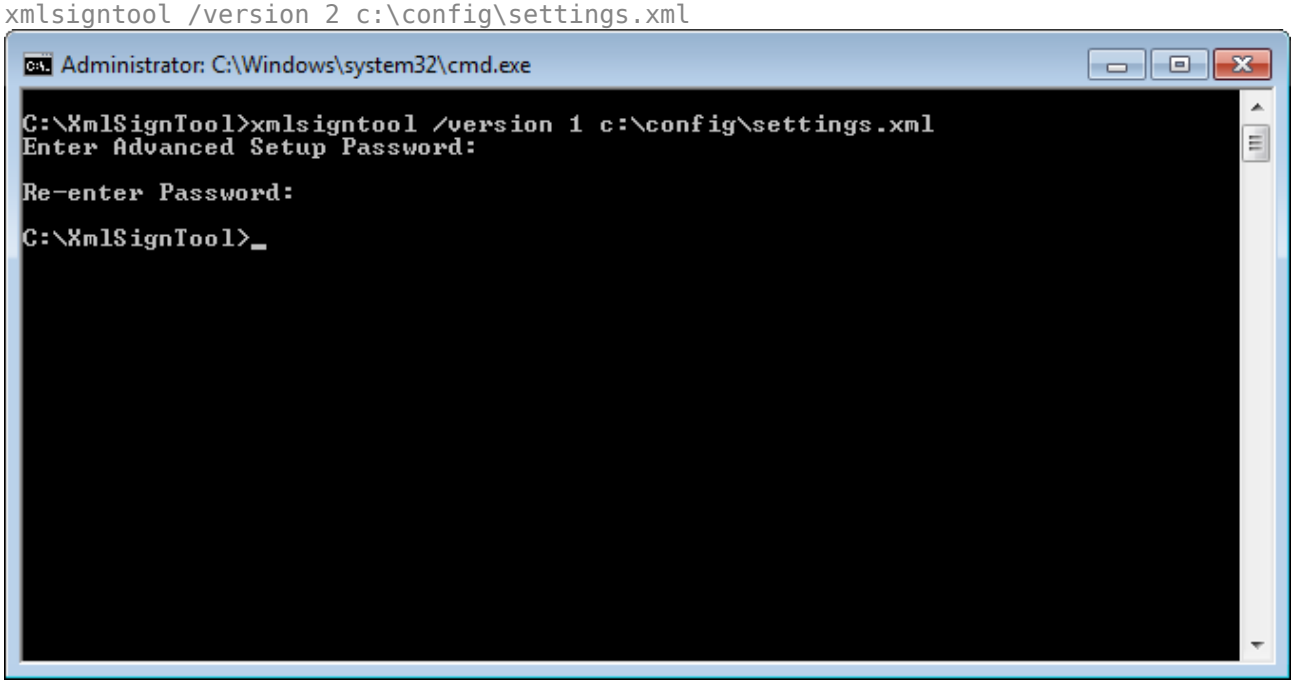
4. Exécutez la commande pour signer le fichier de configuration *.xml* : `xmlsigntool /version 1|2 <xml_file_path>`

La valeur du paramètre `/version` dépend de la version de ESET Internet Security. Utilisez `/version 1` pour les anciennes version de ESET Internet Security au lieu de 11.1. Utilisez `/version 2` pour la version actuelle de ESET Internet Security.

5. Entrez deux fois le mot de passe de la configuration avancée lorsque XmlSignTool le demande. Votre fichier de configuration *.xml* est maintenant signé et peut être utilisé pour l'importation sur une autre instance de ESET Internet Security avec ESET CMD en utilisant la méthode d'autorisation de mot de passe de configuration avancée.

Commande de signature de fichier de configuration exportée :

```
xmlsigntool /version 2 c:\config\settings.xml
```



Si le mot de passe de la configuration d'accès change et que vous souhaitez importer la configuration qui a été signée précédemment avec un ancien mot de passe, vous devez signer le fichier de configuration *.xml* à nouveau à l'aide du mot de passe actuel. Cela vous permet d'utiliser un fichier de configuration plus ancien sans avoir besoin de l'exporter sur une autre machine exécutant ESET Internet Security avant l'importation.

L'activation d'ESET CMD sans une autorisation n'est pas recommandé, car cela permettra l'importation de toute configuration non signée. Définissez le mot de passe dans Configuration avancée > **Interface utilisateur** > **Configuration de l'accès** pour empêcher des modifications non autorisées par les utilisateurs.

Fichiers journaux

Pour accéder à la configuration de journalisation de ESET Internet Security, cliquez sur Configuration avancée > **Outils** > **Fichiers journaux**. La section journaux permet de définir la manière dont les journaux sont gérés. Le programme supprime automatiquement les anciens fichiers journaux pour gagner de l'espace disque. Vous pouvez préciser les options suivantes pour les fichiers journaux :

Verbosité minimale de journalisation - Précise le niveau minimal de verbosité des événements à consigner :

- **Diagnostic** - Consigne l'information requise pour mettre au point le programme et tous les enregistrements préalables.
- **Informative** - Enregistre des messages informatifs, y compris les messages de mise à jour réussie, ainsi que toutes les entrées préalables.
- **Avertissements** - Enregistre les erreurs critiques et les messages d'avertissement.
- **Erreurs** - Des erreurs comme « Erreur de téléchargement de fichier » et les erreurs critiques seront enregistrées.
- **Critique** - Ne consigne que les erreurs critiques (échec de démarrage de la protection antivirus, pare-feu, etc...).

Toutes les connexions bloquées seront enregistrées lors de la sélection du niveau de verbosité du diagnostic.

Les entrées journal plus vieilles que le nombre de jours indiqué dans le champ **Supprimer automatiquement les entrées après (jours)** seront automatiquement supprimées.

Optimiser automatiquement les fichiers journaux - Si cette fonction est activée, les fichiers journaux seront automatiquement défragmentés si le pourcentage est supérieur à la valeur indiquée dans **Si le nombre d'entrées inutilisées dépasse (%)**.

Cliquez sur **Optimiser** pour lancer la défragmentation des journaux. Toutes les entrées journaux vides seront supprimées durant ce processus, ce qui améliorera la performance et la vitesse de traitement des journaux. Cette amélioration peut être notable, tout particulièrement lorsque les journaux contiennent un grand nombre d'entrées.

Activez l'option **Activer le protocole de texte** pour permettre le stockage des journaux dans un autre format de fichier différent des fichiers journaux :

- **Répertoire cible** - Le répertoire où les fichiers journaux seront stockés (s'applique uniquement aux fichiers texte/CSV). Chaque section du journal a son propre fichier avec un nom prédéfini (par exemple, virlog.txt pour la section **Détections** des fichiers journaux, si vous utilisez le format de fichier texte brut pour stocker les journaux).

- **Type** - Si vous sélectionnez le format de fichier **Texte**, les journaux seront stockés dans un fichier texte et les données seront séparées en onglets. La même chose s'applique au format de fichier **CSV** contenant des données séparées par des virgules. Si vous sélectionnez **Événement**, les journaux seront stockés dans le journal d'événement de Windows (peuvent être consultés à l'aide de l'observateur d'événements dans Panneau de contrôle) contrairement aux fichiers.

- **Supprimer tous les journaux** - Supprime tous les journaux stockés et sélectionnés dans le menu déroulant **Type**. Une notification s'affiche une fois la suppression des journaux effectuée.

Pour permettre une résolution plus rapide des problèmes, ESET pourrait vous demander de fournir des journaux de votre ordinateur. ESET Log Collector facilite la collecte des informations nécessaires. Pour plus de détails sur ESET Log Collector, consultez notre article de la Base de connaissances.

Mode jeu

Le mode joueur est une fonctionnalité destinée aux utilisateurs qui exigent une utilisation interrompue de leur logiciel, qui ne veulent pas être dérangés par des fenêtres de notification ou d'alerte et qui veulent minimiser la charge sur le CPU. Ce mode peut aussi être utilisé lors de présentations qui ne peuvent être interrompues par l'activité de l'antivirus. Une fois cette fonctionnalité activée, toutes les fenêtres contextuelles seront désactivées et l'activité du planificateur sera complètement arrêtée. La protection du système s'exécute toujours en arrière-plan, mais n'exige aucune interaction de l'utilisateur.

Vous pouvez activer ou désactiver le mode Joueur dans la fenêtre principale du programme sous **Configuration** > **Protection de l'ordinateur** en cliquant sur  ou  à côté de **mode Joueur**. Activer le mode Joueur entraîne un risque potentiel puisque l'icône de l'état de la protection dans la barre des tâches tournera à l'orange, en plus d'afficher un avertissement. Vous pouvez aussi voir cet avertissement dans la fenêtre principale du programme où le **mode Joueur activé** sera indiqué en orange.

Activez l'option **Activer automatiquement le mode jeu lorsque des applications s'exécutent en mode plein écran**, sous Configuration avancée > **Outils** > **Mode jeu** pour que le mode jeu démarre dès que vous lancez une application en mode plein écran et s'arrête automatiquement dès que vous quittez l'application.

Activez l'option **Désactiver le mode jeu automatiquement après** pour définir le temps en minutes après lequel le mode jeu sera automatiquement désactivé.

> Si le pare-feu est en mode interactif et que le mode joueur est activé, vous risquez de rencontrer des difficultés pour vous connecter à Internet. Cela peut se révéler problématique si vous lancez 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 joueur. Pour autoriser la communication, définissez une règle de communication pour chaque application qui pourrait rencontrer ce problème, ou utilisez un mode de filtrage différent, dans le pare-feu. N'oubliez pas que si le mode jeu est activé et que vous ouvrez une page Web ou une application pouvant poser un risque de sécurité, elle pourrait être bloquée sans aucune explication ou avertissement car l'interaction utilisateur est désactivée.

Diagnostic

Les diagnostics fournissent des vidages sur incident des processus d'ESET (par exemple, ekrn). Si une application se bloque, un fichier de vidage sera généré. Cela peut aider les développeurs à déboguer et résoudre divers ESET Internet Security problèmes.

Cliquez sur le menu déroulant à côté de **Type de vidage** et sélectionnez l'une des trois options disponibles :

- Sélectionnez **Désactiver** pour désactiver cette fonctionnalité.
- **Mini** (par défaut) - Enregistre le plus petit ensemble d'information utile pouvant aider à identifier la raison pour laquelle l'application s'est arrêtée inopinément. Ce type de fichier de vidage peut être utile lorsque l'espace est limité. Cependant, en raison de l'information limitée incluse dans ce fichier, des erreurs n'ayant pas été causées directement par la menace en cours au moment du problème pourraient ne pas être découvertes lors d'une analyse de ce fichier.
- **Complet** - Enregistre tout le contenu de la mémoire système, au moment où l'application s'est arrêtée inopinément. Un vidage complet de mémoire peut contenir des données liées aux processus en cours d'exécution au moment de la création du vidage mémoire.

Dossier cible - Répertoire où sera généré le fichier de vidage lors du plantage.

Ouvrir le dossier de diagnostic - Cliquez sur **Ouvrir** pour ouvrir ce répertoire dans une nouvelle fenêtre de l'*Explorateur Windows*.

Créer un vidage de diagnostique - Cliquez sur **Créer** pour créer des fichiers de vidage de diagnostique dans le **répertoire cible**.

Journalisation avancée

Activer la journalisation avancée dans les messages de marketing – Eenregistre tous les événements liés aux messages de marketing dans le produit.

Activer la journalisation avancée du moteur antipourriel – Enregistre tous les événements qui se produisent pendant l'analyse antipourriel. Cela peut aider les développeurs à diagnostiquer et résoudre les problèmes liés au moteur antipourriels d'ESET.

Activer la journalisation avancée du moteur anti-vol – Enregistre tous les événements qui se produisent dans Anti-vol pour permettre le diagnostic et la résolution des problèmes.

Activer la journalisation avancée de la protection du navigateur – Enregistrer tous les événements qui se produisent dans Opérations bancaires et navigation sécurisées.

Activer la journalisation avancée de l'analyseur d'ordinateur – Enregistrer tous les événements qui surviennent lors de l'analyse de fichiers et de dossiers à l'aide de l'analyse de l'ordinateur.

Activer la journalisation avancée du contrôle de périphériques – Enregistre tous les événements qui se produisent dans Contrôle de périphériques. Cela peut aider les développeurs à diagnostiquer et résoudre les problèmes liés au contrôle de périphériques.

Activer la journalisation avancée de Direct Cloud – Enregistre tous les événements qui se produisent dans ESET LiveGrid®. Cela peut aider les développeurs à diagnostiquer et résoudre les problèmes liés à ESET LiveGrid®.

Activer la journalisation avancée dans Protection des documents Protection des documents : permet d'enregistrer tous les événements qui se produisent dans le module Protection des documents afin de permettre le diagnostic et la résolution de problèmes.

Activer la journalisation avancée de la protection du client de messagerie : permet d'enregistrer tous les événements qui se produisent dans le composant Protection du client de messagerie et le plugiciel de client de messagerie pour permettre le diagnostic et la résolution des problèmes.

Activer la journalisation avancée du noyau – Enregistre tous les événements qui se produisent dans le noyau ESET (ekrn).

Activer la journalisation avancée de l'octroi de licences – Enregistre toutes les communications du produit avec l'activation ESET ou les serveurs ESET License Manager.

Activer le suivi de la mémoire - Enregistre tous les événements qui aideront les développeurs à diagnostiquer les fuites de mémoire.

Activer la journalisation avancée de la protection réseau - Enregistre toutes les données relatives au réseau traversant le pare-feu au format PCAP afin d'aider les développeurs à diagnostiquer et à résoudre les problèmes liés au pare-feu.

Activer la journalisation avancée de l'analyseur de trafic réseau : enregistre toutes les données passant par l'analyseur de trafic réseau au format PCAP afin d'aider les développeurs à diagnostiquer et à résoudre les problèmes liés à l'analyseur du trafic réseau.

Activer la journalisation avancée du système d'exploitation - Enregistre des renseignements supplémentaires sur le système d'exploitation, tels que les processus en cours, l'activité du processeur et les opérations sur le disque. Cela peut aider les développeurs à diagnostiquer et réparer les problèmes liés au produit ESET fonctionnant sur votre système d'exploitation.

Activer la journalisation avancée du contrôle parental – Enregistre tous les événements qui se produisent dans le contrôle parental. Cela peut aider les développeurs à diagnostiquer et résoudre les problèmes liés au contrôle parental.

Activer la journalisation avancée de la messagerie poussée – Enregistre tous les événements qui se produisent pendant la messagerie poussée.

Activer la journalisation avancée de la protection en temps réel du système de fichiers – Enregistre tous les événements qui se produisent pendant l'analyse des fichiers et des dossiers grâce à la protection en temps réel du système de fichiers.

Activer la journalisation avancée du moteur de mise à jour : Enregistre tous les événements qui se produisent au cours du processus de mise à jour. Cela peut aider les développeurs à diagnostiquer et à résoudre les problèmes liés au moteur de mise à jour.

Les fichiers journaux se trouvent dans *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Assistance technique

Lorsque vous contactez le service d'assistance technique d'ESET à partir de ESET Internet Security, vous pouvez envoyer des données de configuration du système. Sélectionnez **Toujours envoyer** dans le menu déroulant **Envoyer les données de configuration du système** pour envoyer les données automatiquement, ou sélectionnez **Demander avant l'envoi** pour que votre autorisation soit sollicitée avant l'envoi des données.

Connectivité

Dans des réseaux spécifiques, un serveur mandataire peut servir de médiateur pour la communication entre votre ordinateur et Internet. Si vous utilisez un serveur mandataire, vous devez définir les paramètres suivants. Sinon, ESET Internet Security et ses modules ne peuvent pas être mis à jour automatiquement. Dans ESET Internet Security, la configuration du serveur mandataire est disponible dans deux sections différentes de la configuration avancée.

Vous pouvez configurer les paramètres globaux du serveur mandataire dans Configuration avancée > **Connectivité** > **Serveur mandataire**. La sélection du serveur mandataire à ce niveau définit les paramètres de serveur mandataire globaux pour l'ensemble de ESET Internet Security. Les paramètres définis ici seront utilisés par tous les modules exigeant une connexion Internet.

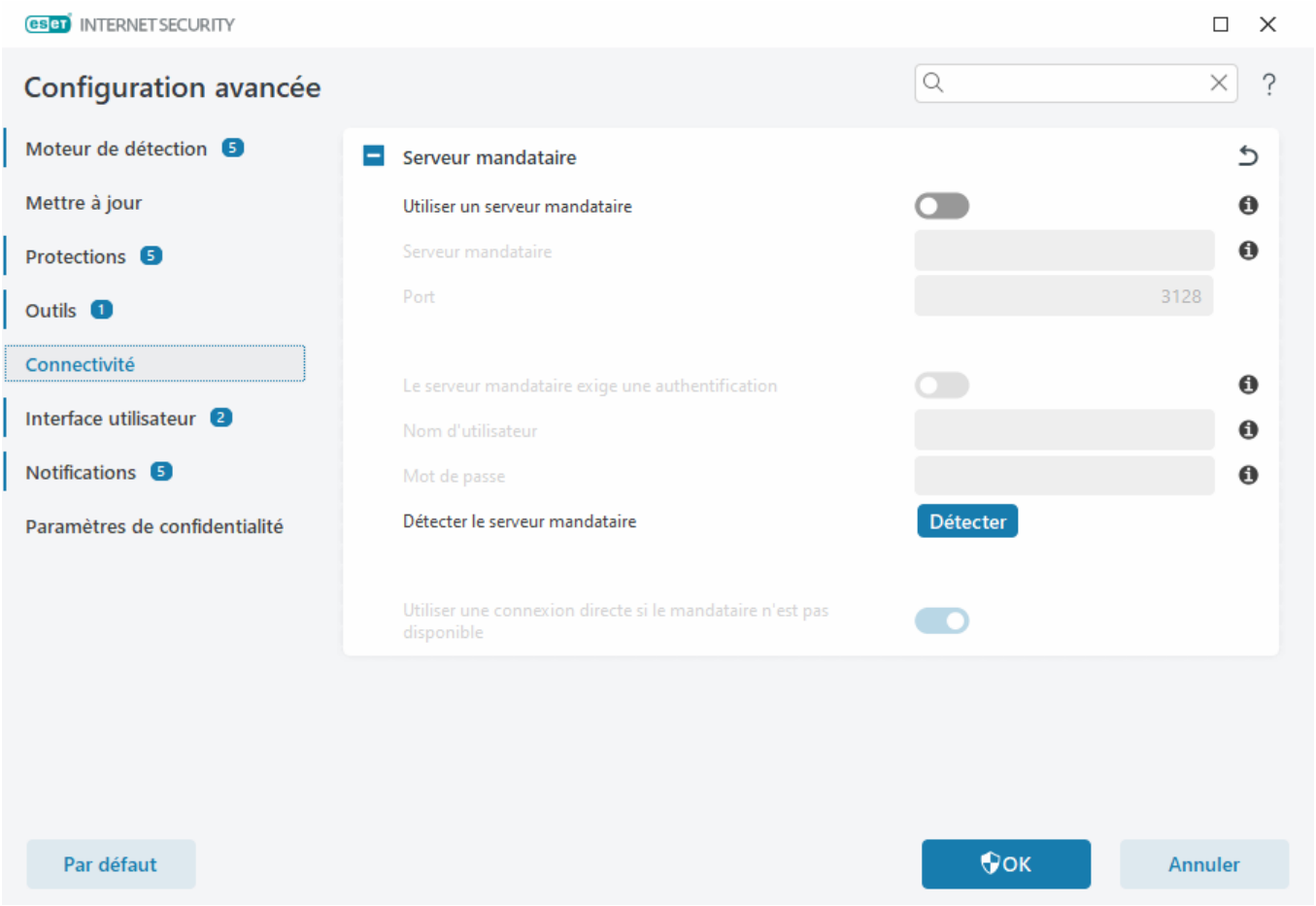
Pour spécifier les paramètres globaux du serveur mandataire, activez l'option **Utiliser le serveur mandataire** et tapez l'adresse du **serveur mandataire** ainsi que le numéro de **port** du serveur mandataire.

Si la communication avec le serveur mandataire exige une authentification, sélectionnez **Le serveur mandataire exige une authentification** et entrez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants. Cliquez sur **Détecter le serveur mandataire** pour détecter et renseigner automatiquement les paramètres du serveur mandataire. ESET Internet Security copiera les paramètres spécifiés dans les options Internet pour Internet Explorer ou Google Chrome.

> Vous devez entrer votre nom d'utilisateur et votre mot de passe manuellement dans les paramètres du **serveur mandataire**.

Utiliser une connexion directe si le mandataire n'est pas disponible - Si ESET Internet Security est configuré pour utiliser le mandataire et que ce dernier n'est pas joignable, ESET Internet Security contournera le mandataire et communiquera directement avec les serveurs d'ESET.

Les paramètres de serveur mandataire peuvent aussi être définis dans Configuration avancée > **Mettre à jour** > **Profils** > **Mises à jour** > **Options de connexion** en sélectionnant **Connexion par un serveur mandataire** dans le menu déroulant **Mode mandataire**. Cette configuration s'applique uniquement aux mises à jour et est recommandée pour les ordinateurs portables recevant des mises à jour de module à partir d'emplacements distants. Pour plus d'informations, consultez la rubrique Configuration avancée des mises à jour.



Interface utilisateur

Pour configurer le comportement de l'interface utilisateur graphique (GUI) du programme, ouvrez Configuration avancée > **Interface utilisateur**.

Vous pouvez régler l'apparence visuelle du programme et les effets utilisés dans l'écran de configuration avancée de Élément de l'interface utilisateur.

Pour que votre logiciel de sécurité offre une sécurité maximale, vous pouvez empêcher toute désinstallation ou toute modification non autorisée en protégeant les paramètres par un mot de passe à l'aide de l'outil Configuration de l'accès.

> Pour configurer le comportement des notifications système, des alertes de détection et des états d'application, consultez la section Notifications.

Éléments de l'interface utilisateur

Vous pouvez ajuster l'environnement de travail (IUG) de ESET Internet Security selon vos besoins dans Configuration avancée > **Interface utilisateur** > **Éléments de l'interface utilisateur**.

Mode de couleur : sélectionnez le jeu de couleurs de l'interface graphique de ESET Internet Security dans le menu déroulant :

- L'option **Identique à la couleur du système** définit le jeu de couleurs de ESET Internet Security selon la configuration du système d'exploitation.
- **Sombre** : ESET Internet Security utilisera un jeu de couleurs sombres (mode sombre).
- **Clair** : ESET Internet Security utilisera un jeu de couleur clair standard.

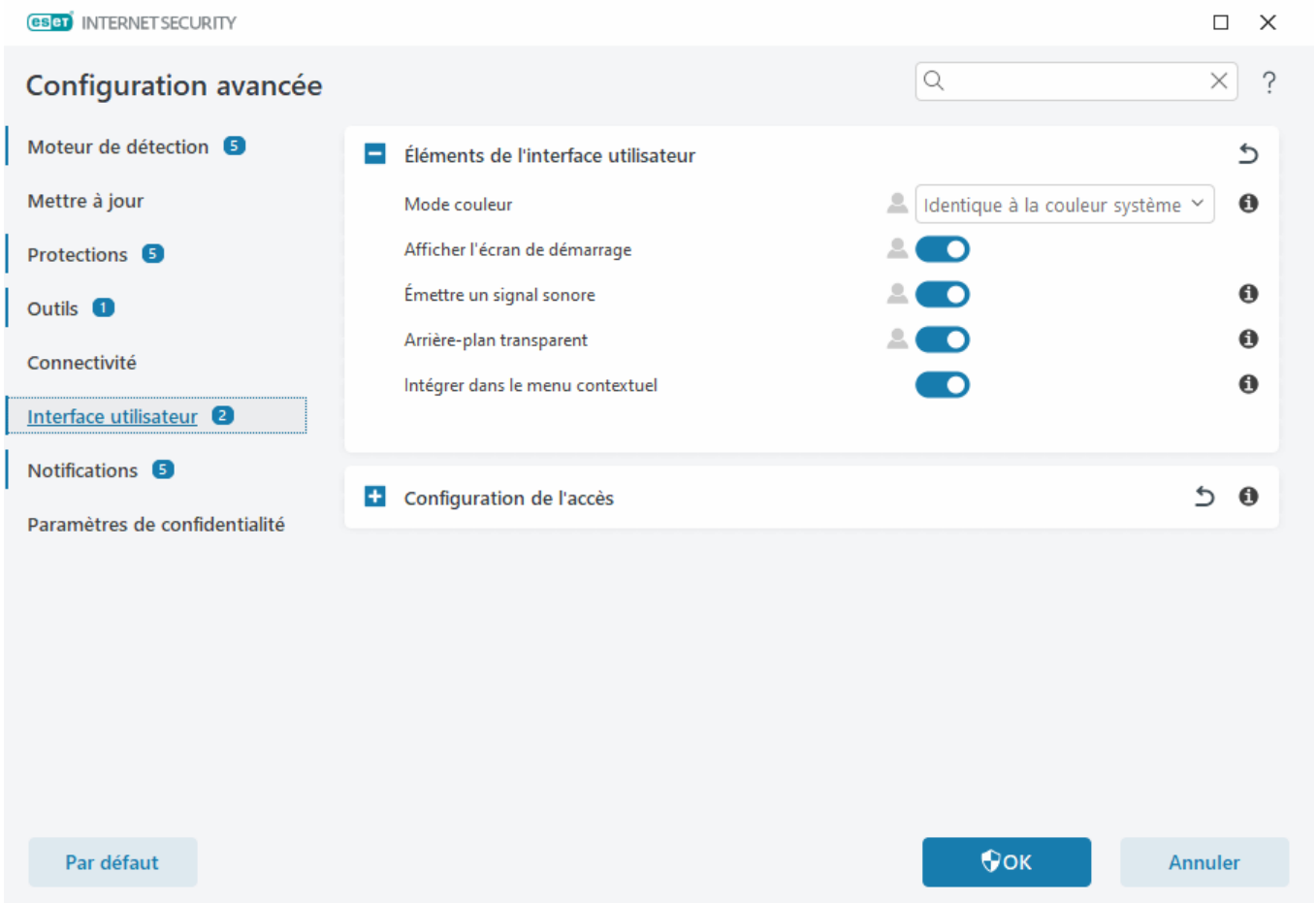
> Vous pouvez également sélectionner le jeu de couleurs de l'interface graphique de ESET Internet Security dans le coin supérieur droit de la fenêtre principale du programme.

Afficher l'écran de démarrage lors du lancement : affiche l'écran de démarrage de ESET Internet Security lors du lancement.

Émettre un signal sonore - émet un signal sonore lorsque des événements importants se produisent pendant une analyse, par exemple lorsqu'une menace est détectée ou lorsque l'analyse prend fin.

Arrière-plan transparent – Active un effet d'arrière-plan transparent pour la fenêtre principale du programme. Un arrière-plan transparent n'est disponible que pour les dernières versions de Windows (RS4 et les versions ultérieures).

Intégrer au menu contextuel - Intègre les éléments de contrôle de ESET Internet Security dans le menu contextuel.



Configuration de l'accès

Les paramètres de ESET Internet Security sont une partie essentielle de votre politique de sécurité. Des modifications non autorisées pourraient mettre en danger la stabilité et la protection de votre système. Pour éviter les modifications non autorisées, les paramètres de configuration de ESET Internet Security peuvent être protégés par mot de passe. La configuration de l'accès peut s'effectuer dans Configuration avancée > **Interface utilisateur** > **Configuration de l'accès**.

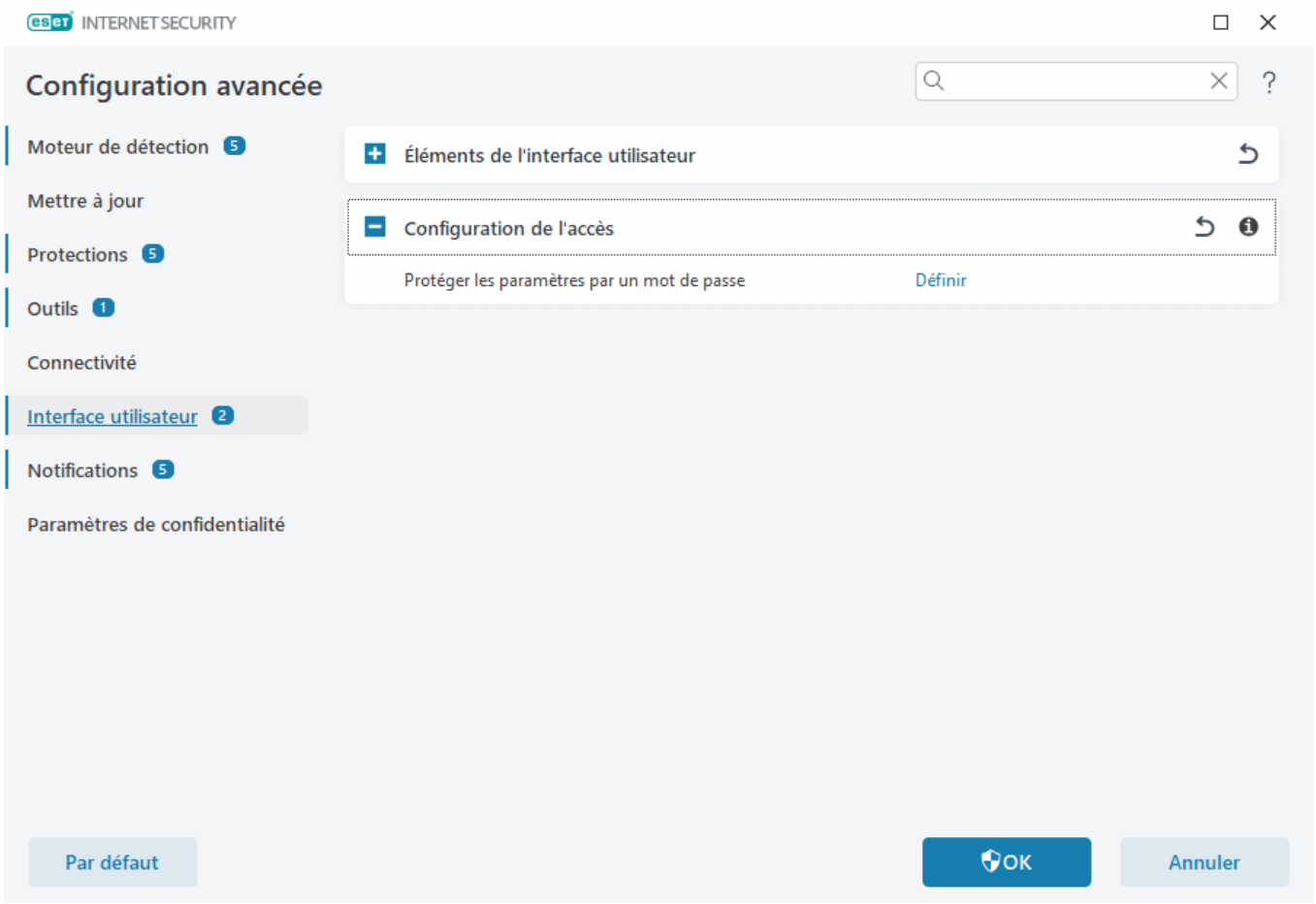
Pour définir ou modifier un mot de passe visant à protéger les paramètres de configuration et la désinstallation de ESET Internet Security, cliquez sur **Définir** à côté de **Paramètres de protection de mot de passe**.

Lorsque vous souhaitez accéder à la configuration avancée et que celle-ci est protégée par un mot de passe, la fenêtre de saisie du mot de passe s'affiche. Si vous oubliez ou perdez votre mot de passe, cliquez sur l'option **Restaurer le mot de passe** ci-dessous et entrez l'adresse de courriel que vous avez utilisée pour l'enregistrement de l'abonnement. ESET vous enverra un courriel avec le code de vérification et des instructions sur la façon de réinitialiser votre mot de passe.

- Comment déverrouiller la configuration avancée

Pour modifier votre mot de passe, cliquez sur **Modifier le mot de passe** à côté de **Paramètres de protection de mot de passe**.

Pour supprimer votre mot de passe, cliquez sur **Supprimer** à côté de **Paramètres de protection de mot de passe**.



Mot de passe pour la configuration avancée

Pour protéger la configuration avancée et éviter toute modification non autorisée de ESET Internet Security, tapez le nouveau mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**. Cliquez sur **OK**.

Lorsque vous souhaitez modifier un mot de passe existant :

1. Tapez votre ancien mot de passe dans le champ **Ancien mot de passe**.
2. Entrez votre nouveau mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**.
3. Cliquez sur **OK**.

Ce mot de passe sera exigé pour accéder à la configuration avancée.

Si vous avez oublié votre mot de passe, reportez-vous à la rubrique Déverrouiller le mot de passe de vos paramètres dans ESET home products.

Pour récupérer votre clé d'activation ESET perdue, la date d'expiration de votre abonnement ou d'autres informations d'abonnement pour ESET Internet Security, consultez la section J'ai perdu ma clé d'activation.

Prise en charge des lecteurs d'écran

ESET Internet Security peut être utilisé avec des lecteurs d'écran pour permettre aux utilisateurs d'ESET malvoyants de naviguer dans le produit ou de configurer les paramètres. Les lecteurs d'écran suivants sont pris en

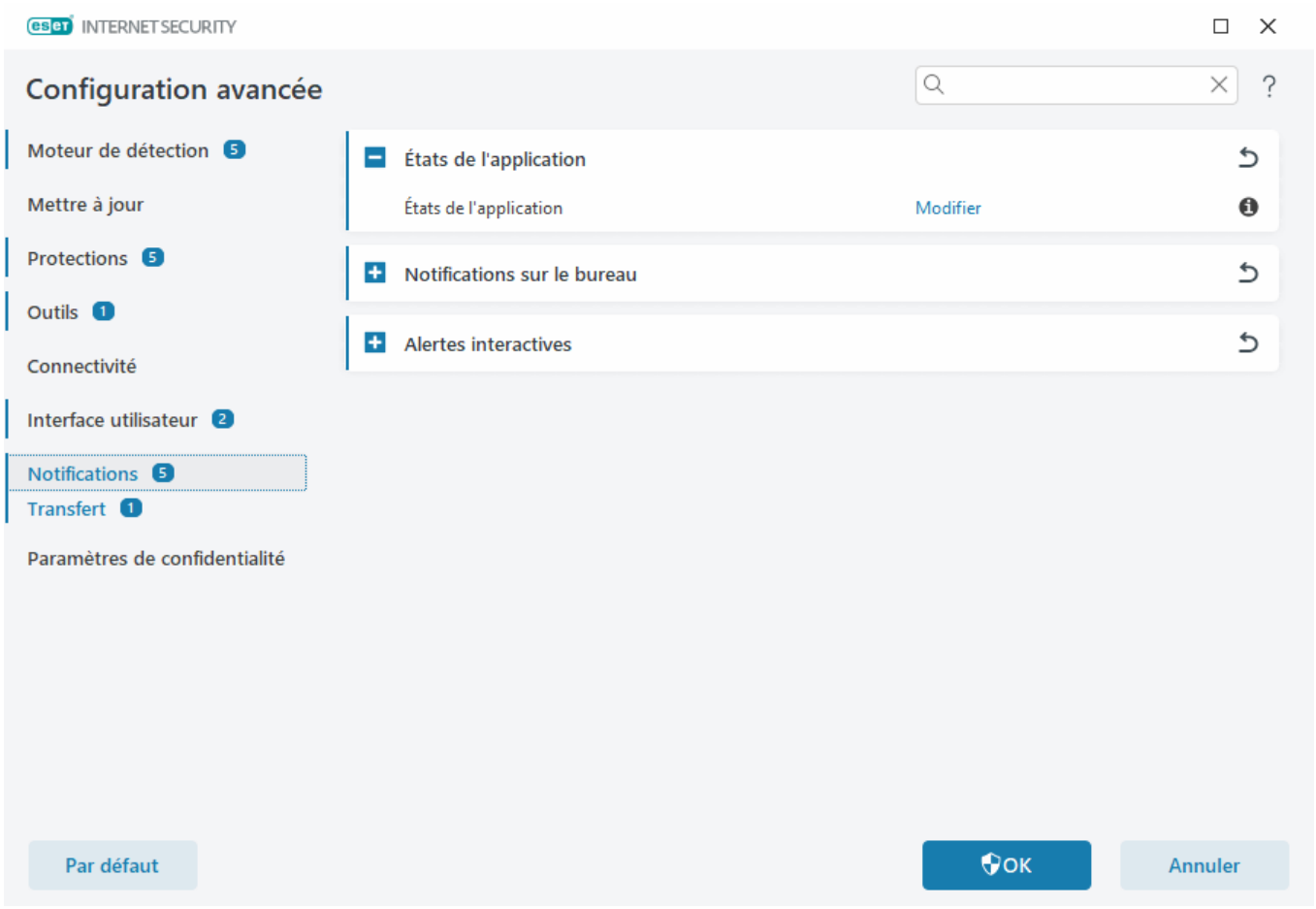
charge (JAWS, NVDA, Narrator).

Pour s'assurer que le logiciel de lecture d'écran peut accéder à l'interface utilisateur graphique de ESET Internet Security correctement, suivez les instructions contenues dans notre article de base de connaissances.

Notifications

Pour gérer les notifications de ESET Internet Security, ouvrez Configuration avancée > **Notifications**. Vous pouvez configurer les types de notifications suivants :

- États de l'application : notifications affichées dans l'onglet **Vue d'ensemble** de la fenêtre principale du programme.
- Notifications de bureau : petites fenêtres de notification à côté de la barre des tâches système.
- Alertes interactives – Fenêtres d'alerte et boîtes de message qui nécessitent une interaction de l'utilisateur.
- Transfert (notifications par courriel) – Les notifications par courriel sont envoyées à l'adresse de courriel indiquée.



États de l'application

États de l'application – Cliquez sur **Modifier** pour sélectionner les états de l'application qui seront affichés dans la section d'accueil de la fenêtre principale du programme > **Aperçu**.

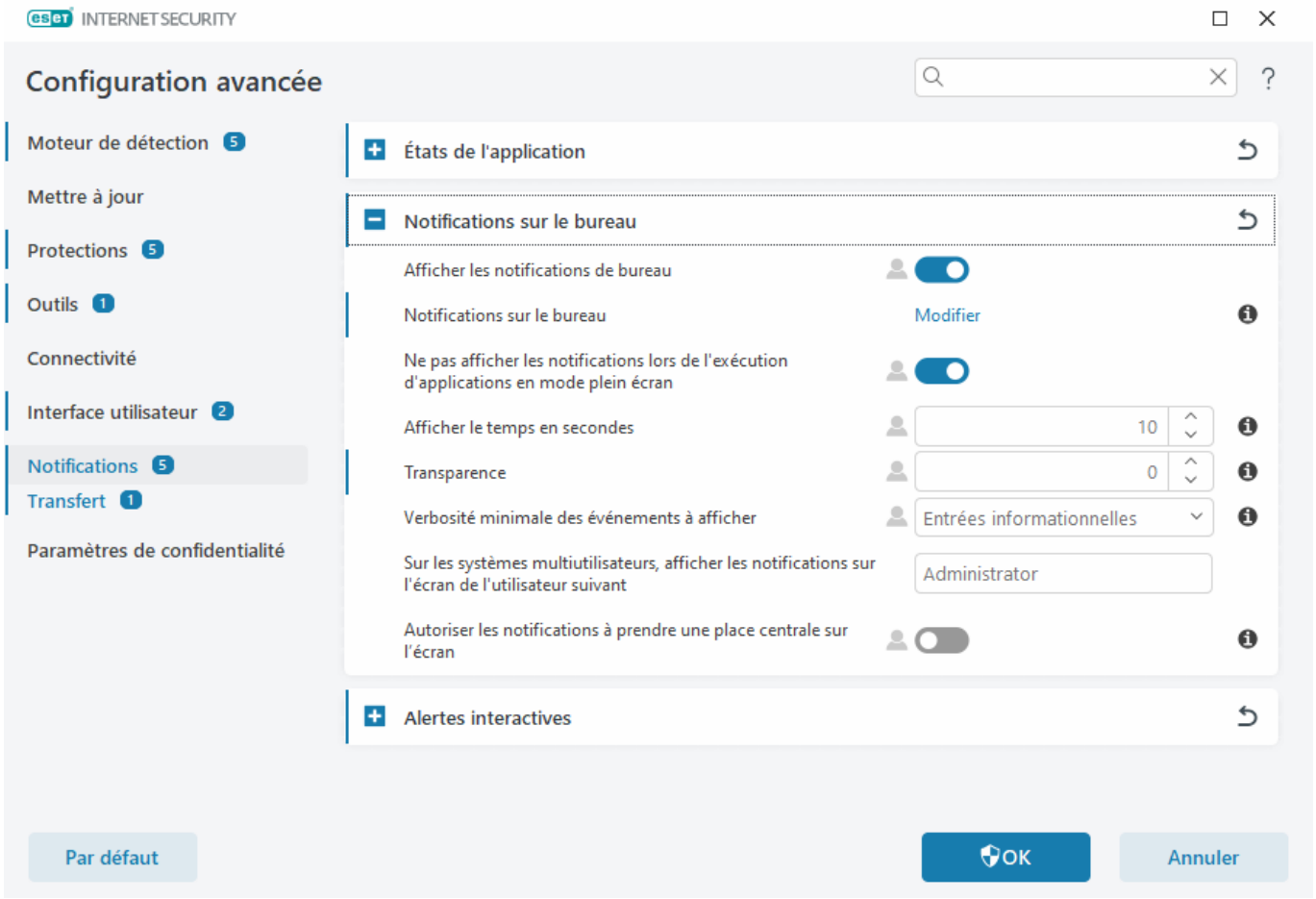
Boîte de dialogue - États de l'application

Dans cette boîte de dialogue, vous pouvez sélectionner les états de l'application qui seront affichés. Par exemple, lorsque vous mettez en pause la protection antivirus et antispyware ou que vous activez le mode Joueur.

L'état de l'application sera également affiché si votre produit n'est pas activé ou si votre abonnement a expiré.

Notifications sur le bureau

Les notifications de bureau s'affichent dans une petite fenêtre de notification à côté de la barre des tâches système. Par défaut, elles s'affichent pendant 10 secondes, puis elles disparaissent lentement. Les notifications informent l'utilisateur au sujet des mises à jour réussies des produits, des nouveaux périphériques connectés, de l'achèvement des tâches d'analyse antivirus ou de la découverte de nouvelles menaces.



Afficher les notifications sur le bureau – Nous vous recommandons de garder cette option activée afin que le produit puisse vous informer lorsqu'un nouvel événement se produit.

Notifications sur le bureau – Cliquez sur **Modifier** pour activer ou désactiver des notifications sur le bureau.

Ne pas afficher les notifications lors de l'exécution d'applications en mode plein écran – Permet de supprimer toutes les notifications non interactives lorsque vous exécutez des applications en mode plein écran.

Afficher le temps en secondes – Définissez la durée d'affichage de la notification. La valeur doit être comprise entre 3 et 30 secondes.

Transparence – Définissez le pourcentage de transparence des notifications. La plage prise en charge est de 0 (pas de transparence) à 80 (transparence très élevée).

Verbosité minimale des événements à afficher – Définissez le niveau de gravité de la notification de départ affiché. Dans le menu déroulant, sélectionnez l'une des options suivantes :

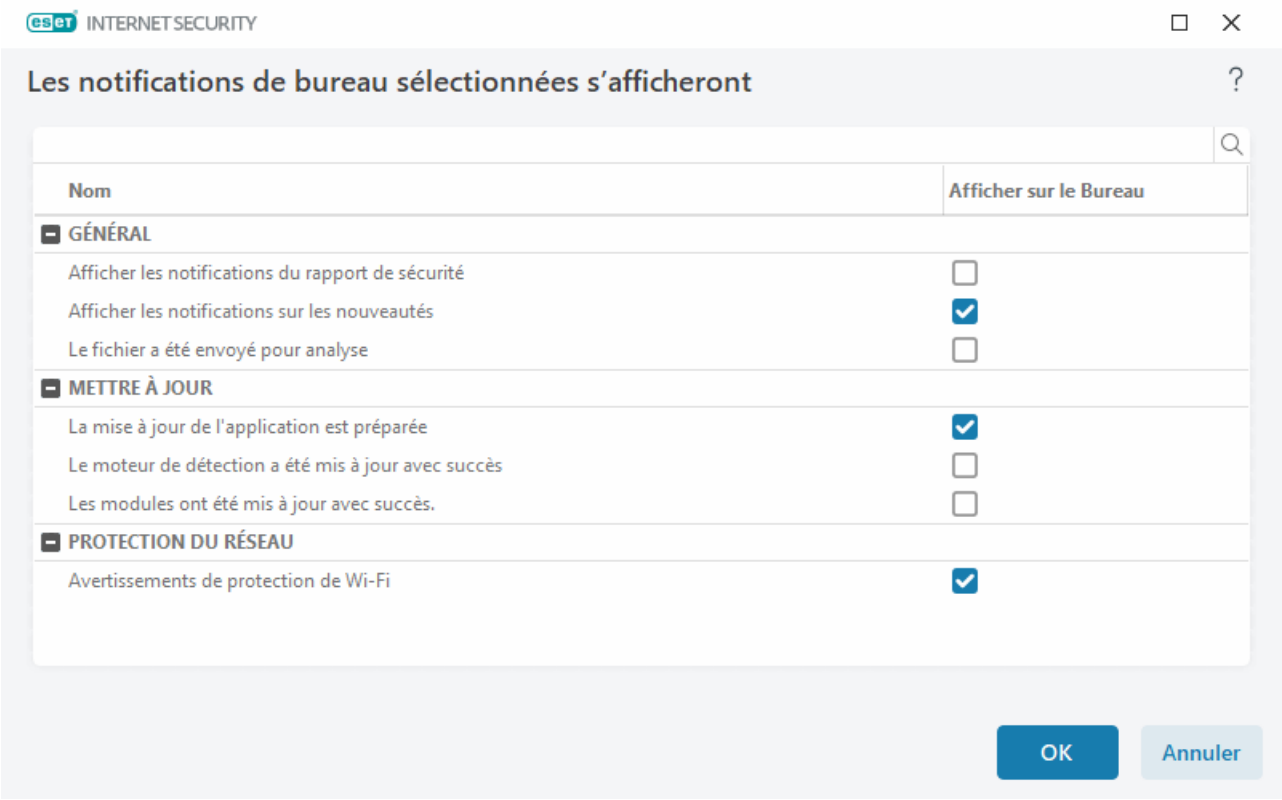
- **Diagnostic** - Consigne l'information requise pour mettre au point le programme et tous les enregistrements préalables.
- **Informative** - Affiche des messages informatifs, comme les événements de réseau non standard, y compris les messages de mise à jour réussie, ainsi que tous les enregistrements préalables.
- **Avertissements :** affiche des messages d'avertissement, des erreurs et des erreurs graves (par exemple, échec de la mise à jour).
- **Erreurs –** Affiche les erreurs (par exemple, la protection des documents n'a pas démarré) et les erreurs critiques.
- **Critique** - Affiche uniquement les erreurs critiques (échec de démarrage de la protection antivirus ou système infecté).

Sur les systèmes multi-utilisateurs, afficher les notifications sur l'écran de cet utilisateur - Permet aux comptes sélectionnés de recevoir des notifications de bureau. Par exemple, si vous n'utilisez pas le compte Administrateur, tapez le nom complet du compte et les notifications sur le bureau seront affichées pour le compte spécifié. Un seul compte utilisateur peut recevoir les notifications du bureau.

Autoriser les notifications à s'afficher en premier plan à l'écran - Permet aux notifications de s'afficher en premier plan à l'écran et à être accessibles dans le menu **ALT + Tab**.

Liste de notifications sur le bureau

Pour régler la visibilité des notifications de bureau (affichées en bas à droite de l'écran), accédez à Configuration avancée > **Notifications** > **Notifications sur le bureau**. Cliquez sur **Modifier** situé à côté de **Notifications sur le bureau** et cochez la case **Afficher** appropriée.



Généralités

Afficher les notifications du rapport de sécurité - Permet de recevoir une notification lorsqu'un nouveau rapport de sécurité est généré.

Afficher les notifications Nouveautés – Notifications sur toutes les nouvelles fonctionnalités et améliorations de la dernière version du produit.

Le fichier a été envoyé pour analyse – Recevez une notification chaque fois que ESET Internet Security envoie un fichier pour analyse.

Inspecteur de réseau

Envoyer une notification au sujet des périphériques réseau nouvellement découverts— Recevez une notification quand un nouveau périphérique est connecté au réseau.

Protection du réseau

Profil réseau modifié — Recevez une notification quand le profil réseau est changé.

Avertissements de protection Wifi : recevez une notification lorsque vous tentez de vous connecter à un réseau Wi-Fi avec un mot de passe faible ou sans mot de passe.

Mettre à jour

La mise à jour de l'application est prête – Recevez une notification lorsqu'une nouvelle version de ESET Internet Security mise à jour est prête.

Le moteur de détection a été mis à jour avec succès – Recevez une notification lorsque le produit met à jour les

modules du moteur de détection.

Les modules ont été mis à jour avec succès – Recevez une notification lorsque le produit met à jour les composants du programme.

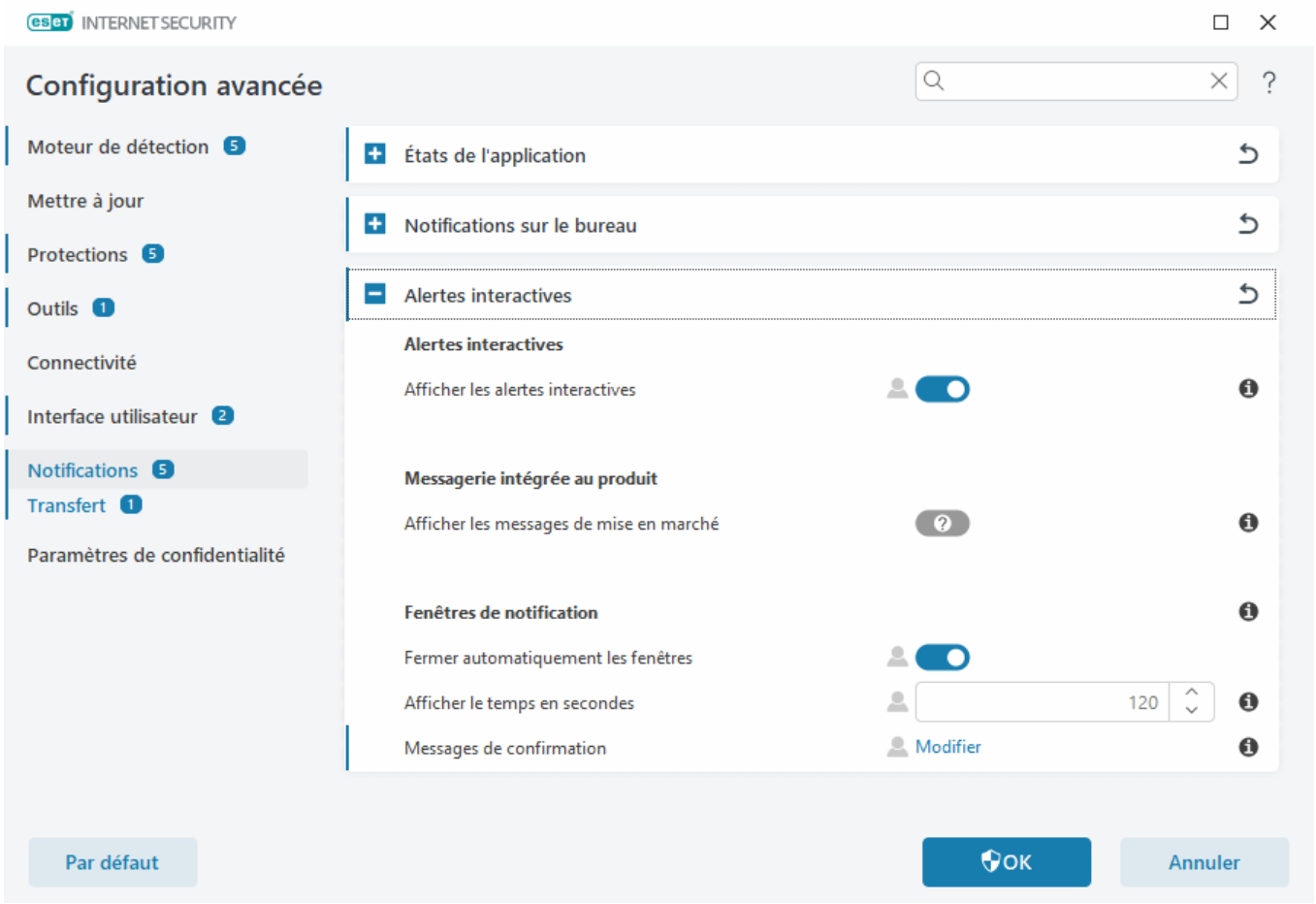
Pour définir les paramètres généraux des notifications sur le bureau, par exemple, la durée d'affichage d'un message ou la verbosité minimale des événements à afficher, consultez Notifications sur le bureau dans Configuration avancée > **Notifications**.

Alertes interactives

Vous recherchez des informations sur les alertes et les notifications courantes ?

- Menace détectée
- L'adresse a été bloquée
- Produit non activé
- Passer à un produit avec plus de fonctionnalités
- Passer à un produit avec moins de fonctionnalités
- La mise à jour est disponible
- L'information de mise à jour n'est pas cohérente
- Dépannage lorsque le message « Échec de la mise à jour des modules » s'affiche
- Résoudre les erreurs de mise à jour des modules
- Menace réseau bloquée
- Certificat du site Web révoqué

La section **Alertes interactives** dans Notifications **de configuration avancée** > vous permet de configurer la façon dont les boîtes de message et les alertes interactives relatives aux détections sont gérées par ESET Internet Security lorsqu'une décision doit être prise par un utilisateur (par exemple, un site Web d'hameçonnage potentiel).



Alertes interactives

Lorsque **Afficher les alertes interactives** est désactivée, toutes les fenêtres d'alerte et les boîtes de dialogue du navigateur sont masquées, ce qui ne convient qu'à un nombre limité de situations particulières. Nous recommandons de laisser cette option activée.

Messagerie intégrée au produit

La messagerie intégrée a été conçue afin d'informer les utilisateurs des nouvelles et des autres communications ESET. L'envoi de messages marketing requiert le consentement d'un utilisateur. Par conséquent, les messages marketing ne sont pas envoyés à un utilisateur par défaut (affichés sous la forme d'un point d'interrogation). En activant cette option, vous acceptez de recevoir des messages marketing d'ESET. Si vous ne souhaitez pas **recevoir de message marketing d'ESET**, désactivez cette option.

Fenêtres de notification

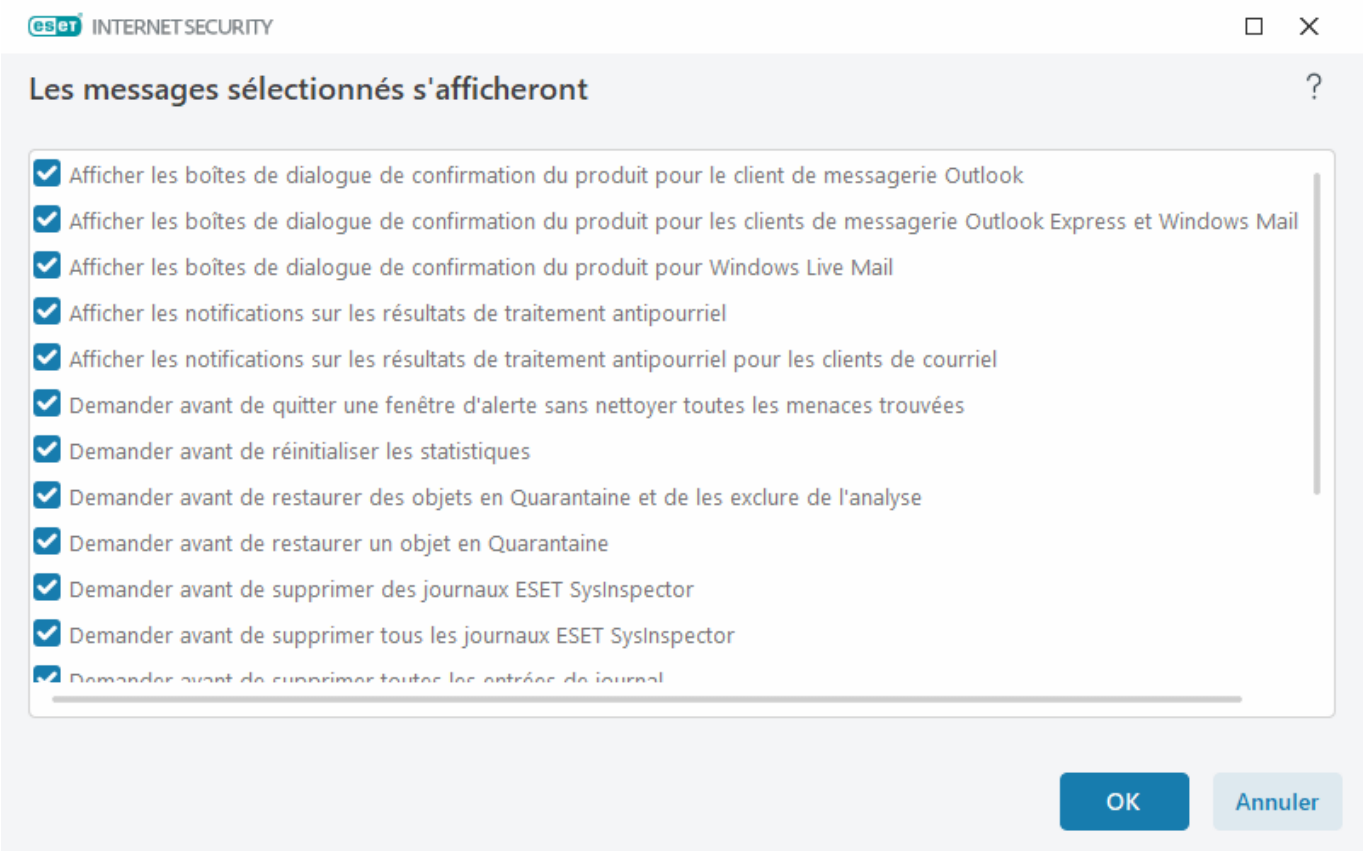
Pour fermer automatiquement les fenêtres de messages après un certain temps, sélectionnez l'option **Fermer automatiquement la boîte de message**. Si les fenêtres d'alerte ne sont pas fermées manuellement, elles le sont automatiquement, une fois le laps de temps écoulé.

Afficher le temps en secondes – Définissez la durée d'affichage de l'alerte. La valeur doit être comprise entre 10 et 999 secondes.

Messages de confirmation - Cliquez sur **Modifier** pour afficher une liste de messages de confirmation que vous pouvez choisir d'afficher ou de ne pas afficher.

Messages de confirmation

Pour régler les messages de confirmation, accédez à Configuration avancée > **Notifications** > **Alertes interactives** et cliquez sur **Modifier** située à côté de **Message de confirmation**.



Cette boîte de dialogue affiche les messages de confirmation que ESET Internet Security affiche avant qu'une action ne soit effectuée. Cochez ou décochez la case à côté de chaque message de confirmation pour autoriser ou désactiver.

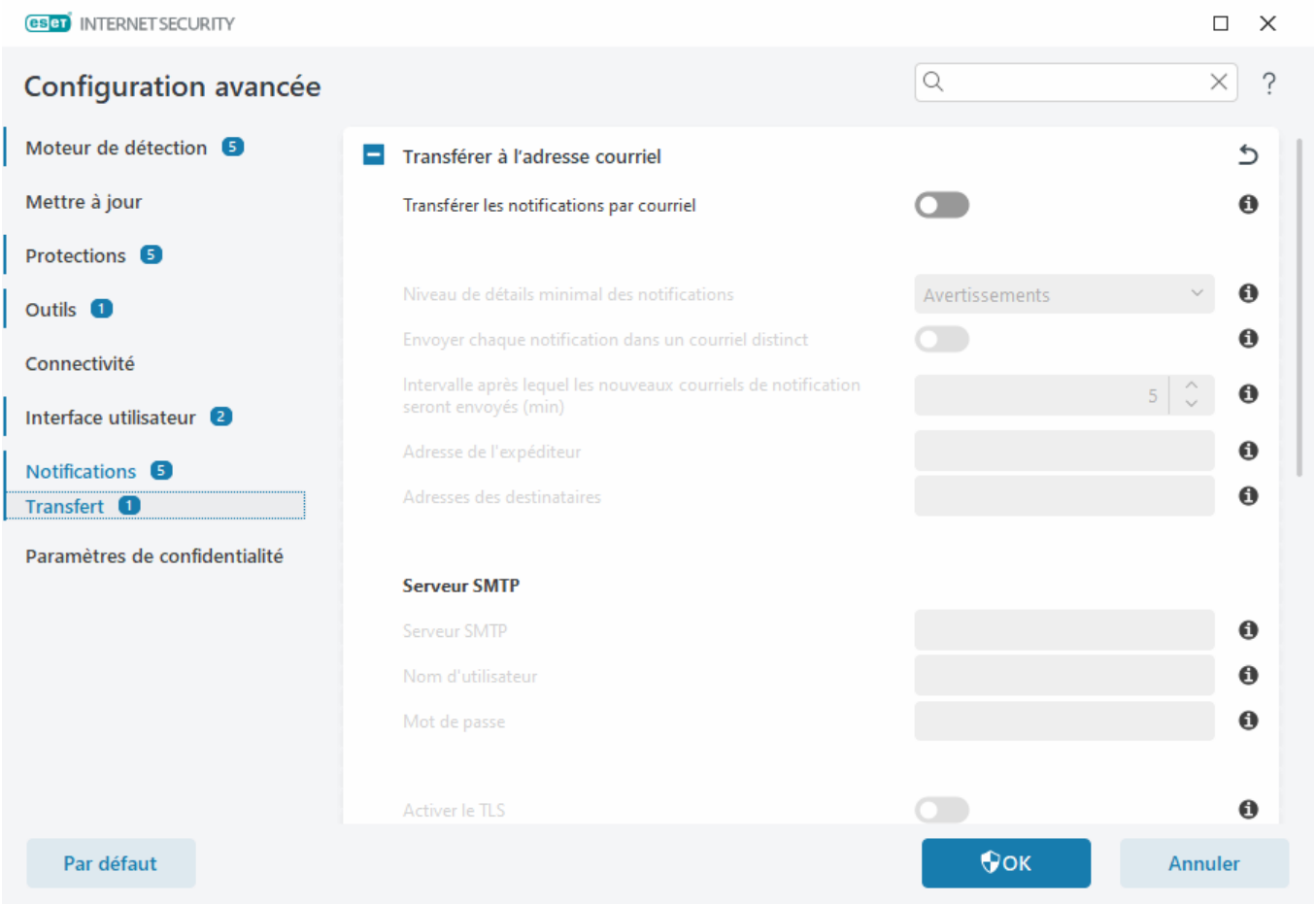
En savoir plus sur les fonctionnalités spécifiques liées aux messages de confirmation :

- Demander avant de supprimer des journaux ESET SysInspector
- Demander avant de supprimer tous les journaux ESET SysInspector
- Demander avant de supprimer un objet en Quarantaine
- Demander avant d'ignorer des paramètres dans la configuration avancée
- Demander avant de quitter une fenêtre d'alerte sans nettoyer toutes les menaces trouvées
- Demander avant de supprimer une entrée d'un journal
- Demander avant de supprimer une tâche planifiée dans le Planificateur
- Demander avant de supprimer toutes les entrées de journal
- Demander avant de réinitialiser les statistiques

- Demander avant de restaurer un objet en Quarantaine
- Demander avant de restaurer des objets en Quarantaine et de les exclure de l'analyse
- Demander avant d'exécuter une tâche planifiée dans le Planificateur
- Afficher les notifications sur les résultats de traitement antipourriel
- Afficher les notifications sur les résultats de traitement antipourriel pour les clients de courriel
- Afficher les boîtes de dialogue de confirmation du produit pour les clients de messagerie Outlook Express et Windows Mail
- Afficher les boîtes de dialogue de confirmation du produit pour Windows Live Mail
- Afficher les boîtes de dialogue de confirmation du produit pour le client de messagerie Outlook

Transfert

ESET Internet Security prend en charge l'envoi automatique de courriels d'avis, si un événement ayant le niveau de verbosité sélectionné se produit. Pour activer l'envoie de notifications par courriel, cliquez sur Configuration avancée > **Notifications** > **Transfert** et activez **Transférer les notifications par courriel**.



À partir du menu déroulant **Verbosité minimale pour les notifications**, vous pouvez sélectionner le niveau de sévérité de départ des notifications à envoyer.

• **Diagnostic** - Consigne l'information requise pour mettre au point le programme et tous les enregistrements préalables.

• **Informative** - Enregistre des messages informatifs, comme les événements de réseau non standard, y compris les messages de mise à jour réussie, ainsi que tous les enregistrements préalables.

• **Avertissements :** enregistre les erreurs critiques et les messages d'avertissement (par exemple, échec de la mise à jour).

• **Erreurs** - Des erreurs comme « La protection du document n'a pas démarrée » et autres erreurs critiques seront enregistrées.

• **Critique** – Enregistre uniquement les erreurs critiques (par exemple, Erreur de démarrage de la protection antivirus ou Menace trouvée).

Envoyer chaque notification dans un courriel distinct – Lorsque cette option est activée, le destinataire recevra un nouveau courriel pour chaque notification. Cela peut entrainer la réception d'un grand nombre de courriels dans un court laps de temps.

Intervalle après lequel les nouveaux courriels de notification seront envoyés (min) - Intervalle en minutes, après lequel de nouvelles notifications seront envoyées par courriel. Mettez cette valeur à 0 si vous souhaitez envoyer ces notifications immédiatement.

Adresse de l'expéditeur - Ce champ indique l'adresse de l'expéditeur qui sera affichée dans l'en-tête des courriels de notification.

Adresse du destinataire - Ce champ indique l'adresse du destinataire qui sera affichée dans l'en-tête des courriels de notification. Les valeurs multiples sont prises en charge. Veuillez utiliser un point-virgule comme séparateur.

serveur SMTP

Serveur **SMTP** - Le serveur SMTP utilisé pour envoyer des notifications (par ex. smtp.provider.com:587, le port prédéfini est 25).

ESET Internet Security prend en charge les serveurs SMTP avec chiffrement TLS.

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 pour accéder au serveur SMTP.

Activer le TLS – Alerte et notifications sécurisées grâce au chiffrement TLS.

Tester la connexion SMTP – Un courriel de test sera envoyé à l'adresse de courriel du destinataire. Les champs d'adresses du serveur SMTP, du nom d'utilisateur, du mot de passe, d'adresse de l'expéditeur et du destinataire doivent être remplies.

Format des messages

Les communications entre le programme et l'utilisateur ou l'administrateur de système distant se font par la messagerie ou le réseau local (au moyen du service de messagerie Windows). Le **format par défaut des messages** d'alerte et des notifications est optimal dans la plupart des situations. Dans certaines situations, le format des messages d'événement doit être changé.

Format des messages d'événement - Format des messages d'événements qui s'affichent sur les ordinateurs distants.

Format des messages d'avertissement de menace - Les messages d'alerte de menace et de notification ont un format par défaut prédéfini. Nous recommandons de conserver le format prédéfini. Toutefois, dans certaines circonstances (par exemple, si vous avez un système automatisé de traitement de courriels), vous serez peut-être amené à modifier le format des messages.

Jeu de caractères – Convertit un courriel en un codage de caractères ANSI basé sur les paramètres régionaux de Windows (par exemple, windows-1250, Unicode (UTF-8), ACSII 7-bit, ou japonais (ISO-2022-JP)). En conséquence, "á" sera changé en "a" et un symbole inconnu en "?".

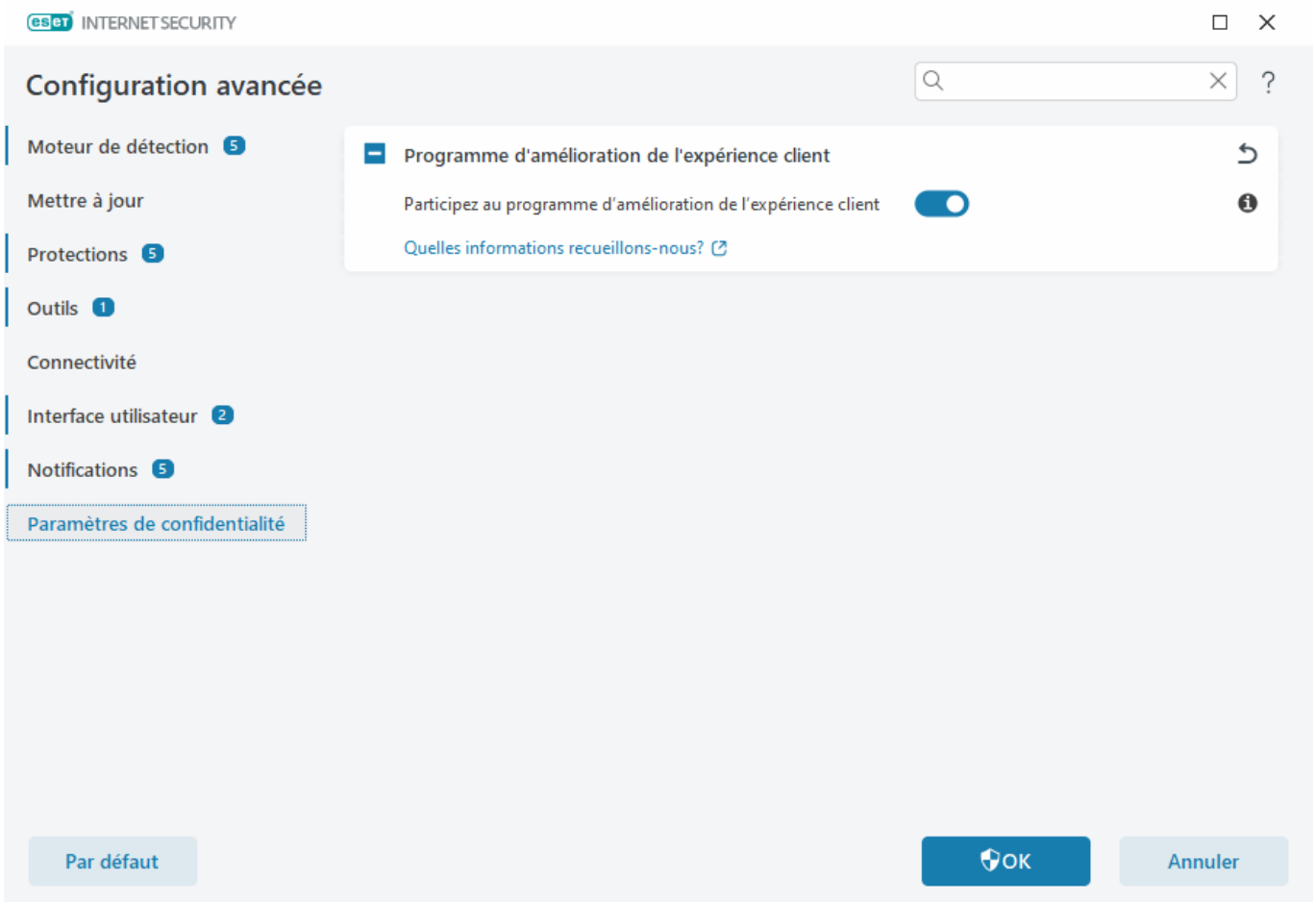
Utiliser l'encodage Quoted-Printable – Le courriel source sera encodé au format Quoted-Printable (QP) qui utilise les caractères ASCII et peut transmettre correctement par courriel les caractères nationaux spéciaux en format 8 bits (áéíóú).

- **%TimeStamp%** - Date et heure de l'événement
- **%Scanner%** - Module concerné
- **%ComputerName%** - Nom de l'ordinateur où l'alerte s'est produite
- **%ProgramName%** - Module ayant généré l'alerte
- **%InfectedObject%** - Nom du fichier ou message infecté, etc.
- **%VirusName%** - Identification de l'infection
- **%Action%** – Mesures prises contre l'infiltration
- **%ErrorDescription%** - Description d'un événement autre qu'un virus

Les mots-clés **%InfectedObject%** et **%VirusName%** ne sont utilisés que dans les messages d'alerte de menace, tandis que le mot-clé **%ErrorDescription%** n'est utilisé que dans les messages d'événement.

Paramètres de confidentialité

Ouvrez Configuration avancée > **Paramètres de confidentialité**.



Programme d\'amélioration de l\'expérience client

Activez le bouton bascule en regard de **Participer au programme d'amélioration de l'expérience client** pour rejoindre le programme d'amélioration de l'expérience client. En y adhérant, vous fournissez à ESET des informations anonymes relatives à l'utilisation des produits ESET. Les données collectées nous aideront à améliorer votre expérience et ne seront jamais partagées avec des tiers. Quelles informations recueillons-nous ?

Rétablir les paramètres par défaut

Cliquez sur **Par défaut** dans Configuration avancée pour rétablir tous les paramètres du programme, pour tous les modules. Tous les paramètres du programme, pour tous les modules, seront réinitialisés à l'état qu'ils devraient avoir après une nouvelle installation.

Consultez également Importer et exporter les paramètres.

Rétablir tous les paramètres dans la section en cours

Cliquez sur la flèche incurvée pour rétablir tous les paramètres de la section actuelle aux paramètres par défaut définis par ESET.

Veuillez noter que tous les changements qui ont été effectués seront perdus après que vous aurez cliquez sur **Revenir aux paramètres par défaut**.

Rétablir le contenu des tableaux - Lorsque cette option est activée, les règles, les tâches ou les profils qui ont été

ajoutés manuellement ou automatiquement seront perdus.

Consultez également Importer et exporter les paramètres.

Erreur lors de l’enregistrement de la configuration

Ce message d'erreur indique qu'en raison d'une erreur, les paramètres n'ont pas été enregistrés correctement.

Cela signifie généralement que l'utilisateur qui a tenté de modifier les paramètres du programme :

- dispose de droits d'accès insuffisants ou ne dispose pas des privilèges système nécessaires pour modifier les fichiers de configuration et le registre du système.
  > Pour effectuer les modifications souhaitées, l'administrateur système doit se connecter.

- a récemment activé le mode d’apprentissage dans HIPS ou le pare-feu et a tenté d’apporter des modifications à la configuration avancée.
  > Pour enregistrer la configuration et éviter le conflit de configuration, fermez la configuration avancée sans enregistrer et essayez à nouveau d'effectuer les modifications souhaitées.

La deuxième cause la plus commune est peut-être que le programme ne fonctionne plus correctement, est corrompu et doit donc être réinstallé.

Analyseur de ligne de commande

Le module antivirus de ESET Internet Security peut être lancé en utilisant la ligne de commande - manuellement (avec la commande « ecls ») ou avec un fichier de commandes (« bat »).

Utilisation de l'analyseur de ligne de commande d'ESET :

```
ecls [OPTIONS..] FILES..
```

Les paramètres et commutateurs suivants peuvent être utilisés lors de l'exécution de l'analyseur à la demande à partir de la ligne de commande :

Options

/base-dir=DOSSIER	charger les modules du DOSSIER
/quar-dir=DOSSIER	DOSSIER de quarantaine
/exclude=MASK	exclure les fichiers correspondants à MASQUE de l'analyse
/subdir	analyser les sous-dossiers (valeur par défaut)
/no-subdir	ne pas analyser les sous-dossiers
/max-subdir-level=NIVEAU	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=FICHIER	consigner les résultats dans le FICHIER

/log-rewrite	Écraser le fichier de sortie (par défaut - ajouter)
/log-console	consigner les résultats dans la console (valeur par défaut)
/no-log-console	ne pas consigner les résultats dans la console
/log-all	consigner également les fichiers nettoyés
/no-log-all	ne pas consigner 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=TAILLE	analyser uniquement les fichiers plus petits que TAILLE Mo (valeur par défaut 0 = illimité)
/max-arch-level=NIVEAU	sous-niveau maximal d'archives à analyser dans les archives (archives imbriquées)
/scan-timeout=LIMITE	analyser les archives pendant un maximum de LIMITE secondes
/max-arch-size=TAILLE	n'analyser les fichiers contenus dans une archive que s'ils sont plus petits que TAILLE (valeur par défaut 0 = illimité)
/max-sfx-size=TAILLE	n'analyser les fichiers d'une archive à extraction automatique que s'ils sont plus petits que TAILLE Mo (valeur par défaut 0 = illimité)
/mail	analyser les fichiers courriel (valeur par défaut)
/no-mail	ne pas analyser les fichiers courriel
/mailbox	analyser les boîtes aux lettres (valeur par défaut)
/no-mailbox	ne pas analyser les boîtes aux lettres
/sfx	analyser les archives à extraction automatique (valeur par défaut)
/no-sfx	ne pas analyser les archives à extraction automatique
/rtp	analyser les fichiers exécutables compressés (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	analyser pour déceler la présence d'applications suspectes (par défaut)
/no-suspicious	ne pas analyser pour déceler la présence d'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-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 suivantes sont disponibles : • `none` (par défaut) - aucun nettoyage automatique n'est effectué. • `standard` - ecls.exe tentera de nettoyer ou de supprimer automatiquement les fichiers infectés. • `strict` - ecls.exe tentera de nettoyer ou de supprimer automatiquement les fichiers infectés sans l'intervention de l'utilisateur (vous ne recevrez aucune invite avant la suppression des fichiers). • `rigoureux` - ecls.exe supprimera les fichiers sans aucune tentative de nettoyage quel que soit le fichier en question. • `supprimer` - ecls.exe supprimera les fichiers sans aucune tentative de nettoyage, mais ne supprimera pas les fichiers sensibles comme les fichiers systèmes de Windows.
/quarantine	copier les fichiers infectés (si nettoyés) vers Quarantaine (complète l'action effectuée pendant le nettoyage)
/no-quarantine	ne pas copier les fichiers infectés dans la quarantaine

Options générales

/help	afficher l'aide et quitter
/version	afficher l'information sur la 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 ne peuvent pas être analysés (peuvent être des menaces)
50	menace trouvée
100	erreur

Un code de sortie supérieur à 100 indique un fichier non analysé, qui peut donc être infecté.

Foire aux questions

Vous trouverez ci-dessous quelques-unes des questions les plus fréquemment posées et les problèmes rencontrés. Cliquez sur l'intitulé d'une rubrique pour apprendre comment résoudre le problème :

- Comment effectuer la mise à jour de ESET Internet Security

- ESET Internet Security a détecté une menace
- Comment éliminer un virus de mon ordinateur
- Comment autoriser la communication pour une certaine application
- Comment activer le contrôle parental pour un compte
- Comment créer une nouvelle tâche dans le Planificateur
- Comment programmer une tâche d'analyse (hebdomadaire)
- Comment déverrouiller la configuration avancée
- Comment résoudre la désactivation du produit à partir de ESET HOME

Si votre problème n'est pas abordé dans la liste ci-dessus, essayez de faire une recherche dans les pages d'aide en ligne de ESET Internet Security.

Si vous ne trouvez pas la solution à votre problème/question dans les pages d'aide en ligne de ESET Internet Security, consultez la base de connaissances ESET en ligne qui est régulièrement mise à jour. Vous trouverez ci-dessous des liens vers les articles les plus populaires de notre base de connaissances :

- Comment renouveler mon abonnement?
- Je reçois une erreur d'activation lorsque j'installe le produit ESET. Qu'est-ce que ça signifie ?
- Activer mon produit ESET Windows pour les particuliers à l'aide de la clé d'activation
- Désinstaler ou réinstaller mon produit ESET pour particuliers
- Je reçois un message selon lequel mon installation d'ESET s'est arrêtée prématurément
- Que dois-je faire après avoir renouvelé mon abonnement? (utilisateurs de la version résidentielle)
- Et si je change d'adresse courriel ?
- Transférer mon produit ESET sur un nouvel ordinateur ou périphérique
- Comment démarrer Windows en Mode sans échec ou Mode sans échec avec prise en charge réseau ?
- Exclure un site web sûr du blocage
- Autoriser l'accès des logiciels de lecture d'écran à ESET GUI

Au besoin, vous pouvez communiquer avec notre service d'assistance technique pour soumettre vos questions ou problèmes. Le formulaire se trouve dans l'onglet Aide et assistance de .

Comment effectuer la mise à jour de ESET Internet

Security

La mise à jour de ESET Internet Security peut être effectuée manuellement ou automatiquement. Pour la déclencher, cliquez sur **Mettre à jour** dans la fenêtre principale du programme, puis sur **Vérifier les mises à jour**.

L'installation par défaut crée une tâche de mise à jour automatique qui s'exécute chaque heure. Si vous devez modifier l'intervalle, il faut aller dans **Outils** > Planificateur.

Comment éliminer un virus de mon ordinateur

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

1. De la fenêtre principale du programme, cliquez sur **Analyse de l'ordinateur**.

2. Cliquez sur **Analyse de votre ordinateur** pour lancer l'analyse de votre système.

3. Une fois l'analyse terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés.

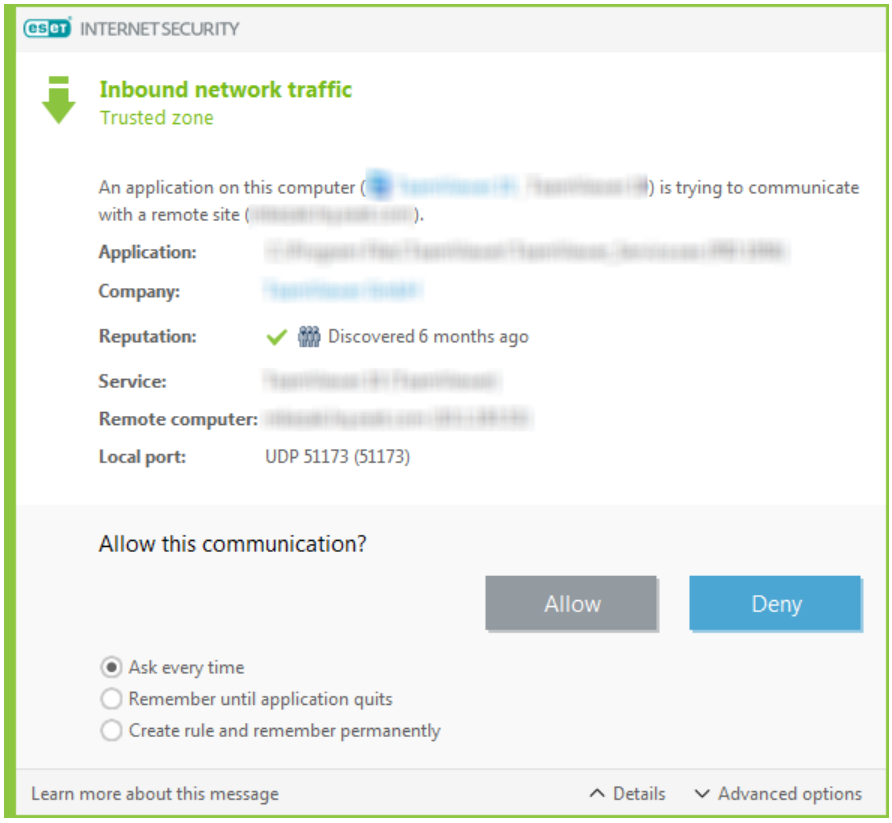
4. Si vous ne voulez analyser qu'une certaine partie de votre disque, cliquez sur **Analyse personnalisée** et sélectionnez les cibles à analyser.

Pour obtenir plus d’informations, consultez les documents suivants :

- Article de la base de connaissances ESET
- Quarantaine

Comment autoriser la communication pour une certaine application

Si une nouvelle connexion est détectée en mode interactif et qu'aucune règle ne correspond à la communication, une boîte de dialogue vous demandera **d'autoriser** ou de **refuser** la connexion. Si vous voulez que ESET Internet Security exécute la même action chaque fois que l'application tente d'établir une connexion, cochez la case **Créer la règle et mémoriser de manière permanente**.



Dans la configuration du pare-feu, vous pouvez créer de nouvelles règles de pare-feu pour les applications avant leur détection par ESET Internet Security. Ouvrez la fenêtre principale du programme, puis **Configuration** > **Protection du réseau** > **Pare-feu** > **Configurer** > **Avancée** > **Règles** > **Modifier**.

Cliquez sur **Ajouter** et dans l'onglet **Général**, entrez le nom, le sens et le protocole de communication de la règle. La fenêtre vous permet de définir l'action à prendre lorsqu'une règle est appliquée.

Dans l'onglet **Local**, entrez le chemin de l'exécutable de l'application ainsi que le port local de communication. Dans l'onglet **Distant**, entrez l'adresse et le port distants (le cas échéant). La règle nouvellement créée sera appliquée dès que l'application tentera de communiquer de nouveau.

Comment activer le contrôle parental pour un compte

Pour activer le contrôle parental pour un compte utilisateur particulier, effectuez les étapes ci-dessous :

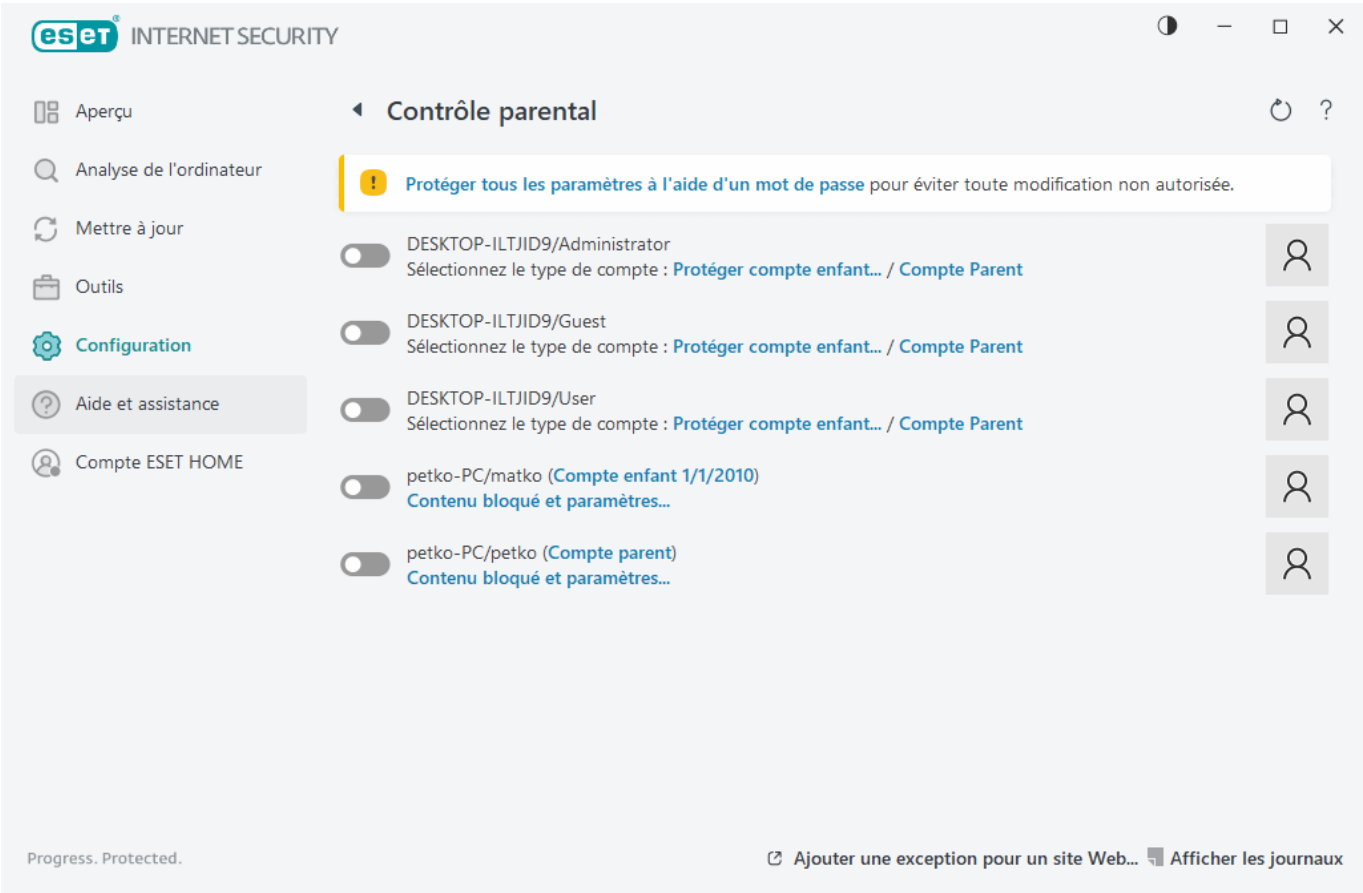
1. Par défaut, le contrôle parental est désactivé dans ESET Internet Security. Deux méthodes permettent d'activer le contrôle parental :

   • Cliquez sur l'icône du bouton bascule dans **Configuration** > **Protection Internet** > **Contrôle parental** à partir de la fenêtre principale du programme et faites passer l'état du contrôle parental à activé.

   • Ouvrez Configuration avancée > **Protections** > **Protection de l'accès Web Contrôle parental**, puis activez le bouton bascule en regard de **Activer le contrôle parental**.

2. Cliquez sur **Configuration** > **Protection internet** > **Contrôle parental** à partir de la fenêtre principale du programme. Même si **Activé** s'affiche à côté de **Contrôle parental**, vous devez configurer le contrôle parental pour le compte souhaité. Pour cela, cliquez sur le symbole de la flèche, puis dans la fenêtre suivante, sélectionnez **Protéger ce compte enfant** ou ce **Compte parent**. Dans la fenêtre suivante, sélectionnez la date

de naissance afin de déterminer le niveau d'accès et les pages Web adaptées à l'âge qui sont recommandées. Le contrôle parental est désormais activé pour le compte spécifié. Cliquez sur **Contenu bloqué et paramètres** sous un nom de compte pour personnaliser les catégories que vous souhaitez autoriser ou bloquer dans l'onglet Catégories. Pour autoriser ou bloquer des pages Web personnalisées ne correspondant à aucune catégorie, cliquez sur l'onglet Exceptions.



Comment créer une nouvelle tâche dans le Planificateur

Pour créer une nouvelle tâche dans **Outils** > **Planificateur**, cliquez sur **Ajouter une tâche** ou cliquez à l'aide du bouton droit et sélectionnez **Ajouter** dans le menu contextuel. Cinq types de tâches planifiées sont disponibles :

- **Exécuter une application externe** - Planifie l'exécution d'une application externe.
- **Maintenance des journaux** - Les fichiers journaux contiennent les restes des enregistrements supprimés. Cette tâche optimise les enregistrements dans les fichiers journaux de façon régulière, afin qu'ils puissent fonctionner de façon efficace.
- **Contrôle des fichiers de démarrage du système** - Vérifier les fichiers qui peuvent être exécutés au démarrage du système ou lors de l'ouverture de session.
- **Créer un instantané de l'état de l'ordinateur** - Crée un instantané de l'ordinateur ESET SysInspector - recueille de l'information détaillée sur les composants système (pilotes, applications, par ex.) et évalue le niveau de risque de chacun des composants.
- **Analyse de l'ordinateur à la demande** - Effectue l'analyse des fichiers et dossiers de votre ordinateur.

- **Mise à jour** – Planifie une tâche de mise à jour en mettant à jour les modules.

Puisque la **mise à jour** est l'une des tâches planifiées les plus souvent utilisées, nous expliquerons ci-après comment ajouter une nouvelle tâche de mise à jour :

Dans le menu déroulant **Tâche planifiée**, sélectionnez **Mise à jour**. Entrez le nom de la tâche dans le champ **Nom de la tâche** puis cliquez sur **Suivant**. Sélectionnez la fréquence de la tâche. Les options suivantes sont disponibles : **Une fois**, **Plusieurs fois**, **Quotidiennement**, **Chaque semaine** et **Déclenchée par un événement**. Sélectionnez **Ignorer la tâche lors du fonctionnement sur batterie** afin de minimiser les ressources systèmes lorsqu'un portable est alimenté par batterie. La tâche sera exécutée à la date et à l'heure indiquées dans les champs **Exécution de la tâche**. On peut ensuite définir l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée. Les options suivantes sont disponibles :

- **À la prochaine heure planifiée**
- **Dès que possible**
- **Immédiatement, si le temps écoulé depuis la dernière exécution dépasse une valeur spécifique** (l'intervalle peut être défini à l'aide de la case de défilement **Heure depuis la dernière exécution (en heures)**)

Dans l'étape suivante, une fenêtre de résumé des informations sur la tâche planifiée en cours s'affiche. Cliquez sur **Terminer** une fois les modifications terminées.

Une boîte de dialogue s'ouvre pour permettre de choisir les profils à utiliser pour la tâche planifiée. Ici, vous pouvez définir le profil principal et le profil secondaire. Le profil secondaire est utilisé lors que la tâche ne peut pas se terminer en utilisant le profil principal. Confirmez en cliquant sur **Terminer** et la nouvelle tâche planifiée sera ajoutée à la liste des tâches actuellement planifiées.

Comment planifier une analyse hebdomadaire d'un ordinateur

Pour planifier une tâche régulière, ouvrez la fenêtre principale du programme et cliquez sur **Outils** > **Planificateur**. Vous trouverez ci-dessous un guide abrégé sur la manière de programmer une tâche qui lancera l'analyse des disques locaux toutes les semaines. Reportez-vous à cet article de la base de connaissances ESET pour obtenir des instructions plus détaillées.

Pour programmer une tâche :

1. cliquez sur **Ajouter** dans la fenêtre principale du Planificateur.

2. Entrez un nom pour la tâche et sélectionnez **Analyse de l'ordinateur à la demande** dans le menu déroulant **Type de tâche**.

3. Sélectionnez **Hebdomadaire** comme fréquence des tâches.

4. Réglez le jour et l'heure auxquels la tâche sera déclenchée.

5. Sélectionnez **Exécuter la tâche dès que possible** pour exécuter la tâche plus tard dans le cas où l'exécution d'une tâche planifiée ne démarre pas pour une raison quelconque (par exemple, l'ordinateur était éteint).

6. Passez en revue le résumé de la tâche programmée, puis cliquez sur **Terminer**.

7. Dans le menu déroulant **Cibles**, sélectionnez **Disques locaux**.

8. Cliquez sur **Terminer** pour appliquer la tâche.

Comment déverrouiller la configuration avancée lorsqu'elle est protégée par un mot de passe

Lorsque vous souhaitez accéder à la configuration avancée et que celle-ci est protégée par un mot de passe, la fenêtre de saisie du mot de passe s'affiche. Si vous oubliez ou perdez votre mot de passe, cliquez sur l'option **Restaurer le mot de passe** et entrez l'adresse de courriel que vous avez utilisée pour l'enregistrement de l'abonnement. ESET vous enverra un courriel avec un code de vérification. Entrez le code de vérification, puis écrivez et confirmez le nouveau mot de passe. Le code de vérification est valide pendant 7 jours.

Restaurer le mot de passe via votre compte ESET HOME : utilisez cette option si l'abonnement utilisé pour l'activation est associé à votre compte ESET HOME. Tapez l'adresse courriel que vous utilisez pour vous connecter à votre compte ESET HOME.

Si vous ne vous souvenez pas de votre adresse courriel ou si vous avez des difficultés à restaurer le mot de passe, cliquez sur **Contacter l'assistance technique**. Vous êtes redirigé vers le site Web d'ESET pour contacter notre service d'assistance technique.

Générer le code pour le service d'assistance technique : cette option génère le code à fournir au service d'assistance technique. Copiez le code fourni par le service d'assistance technique et cliquez sur **J'ai un code de vérification**. Entrez le code de vérification, puis écrivez et confirmez le nouveau mot de passe. Le code de vérification est valide pendant 7 jours.

Pour plus d'informations, reportez-vous à la rubrique Déverrouiller le mot de passe de vos paramètres dans ESET Windows Home Products.

Comment résoudre la désactivation du produit à partir de ESET HOME

Produit non activé

Ce message d'erreur s'affiche lorsque le propriétaire de l'abonnement désactive votre ESET Internet Security dans le portail ESET HOME ou que l'abonnement partagé avec votre compte ESET HOME n'est l'est plus. Pour résoudre ce problème :

- Cliquez sur **Activer** et utilisez l'une des méthodes d'activation pour activer ESET Internet Security.

- Informez le propriétaire de l'abonnement que votre ESET Internet Security a été désactivée par lui ou que l'abonnement n'est plus partagé avec vous. Le propriétaire peut résoudre le problème dans le ESET HOME.

Produit désactivé, périphérique déconnecté

Ce message d’erreur apparaît après la suppression d'un périphérique du ESET HOME. Pour résoudre ce problème :

- Cliquez sur **Activer** et utilisez l’une des méthodes d’activation pour activer ESET Internet Security.
- Informez le propriétaire de l’abonnement que votre ESET Internet Security a été désactivé et que le périphérique a été déconnecté de ESET HOME.
- Si vous êtes le propriétaire de l’abonnement et que vous n’êtes pas au courant de ces modifications, consultez le flux d’activités de votre ESET HOME. Si vous trouvez une activité suspecte, changez le mot de passe de votre compte ESET HOME et contactez le service d'assistance technique d'ESET.

Produit désactivé, périphérique déconnecté

Ce message d’erreur apparaît après la suppression d'un périphérique du ESET HOME. Pour résoudre ce problème :

- Cliquez sur **Activer** et utilisez l’une des méthodes d’activation pour activer ESET Internet Security.
- Informez le propriétaire de l’abonnement que votre ESET Internet Security a été désactivé et que le périphérique a été déconnecté de ESET HOME.
- Si vous êtes le propriétaire de l’abonnement et que vous n’êtes pas au courant de ces modifications, consultez le flux d’activités de votre ESET HOME. Si vous trouvez une activité suspecte, changez le mot de passe de votre compte ESET HOME et contactez le service d'assistance technique d'ESET.

Produit non activé

Ce message d’erreur s’affiche lorsque le propriétaire de l’abonnement désactive votre ESET Internet Security dans le portail ESET HOME ou que l’abonnement partagé avec votre compte ESET HOME n’est l'est plus. Pour résoudre ce problème :

- Cliquez sur **Activer** et utilisez l’une des méthodes d’activation pour activer ESET Internet Security.
- Informez le propriétaire de l’abonnement que votre ESET Internet Security a été désactivée par lui ou que l’abonnement n’est plus partagé avec vous. Le propriétaire peut résoudre le problème dans le ESET HOME.

0

Programme d\'amélioration de l\'expérience client

En adhérant au programme d'amélioration de l'expérience client, vous fournissez à ESET des informations anonymes relatives à l'utilisation de nos produits. Plus d'informations sur le traitement des données sont disponibles dans notre Politique de confidentialité.

Votre consentement

La participation au programme est volontaire et conditionnelle à votre consentement. Après l'adhésion, la

participation est passive, ce qui signifie que vous n'avez pas besoin de prendre d'autres mesures. Vous pouvez révoquer votre consentement en modifiant les paramètres du produit à tout moment. Cela nous empêchera de poursuivre le traitement de vos données anonymes.

Vous pouvez révoquer votre consentement en modifiant les paramètres du produit à tout moment:

- Modifier les paramètres du programme d'amélioration de l'expérience client pour les produits ESET Windows Home

Quelles types d'informations recueillons-nous?

Données sur l'interaction avec le produit

Ces informations nous en disent plus sur l'utilisation de nos produits. Grâce à cela, nous savons, par exemple, quelles fonctionnalités sont souvent utilisées, quels paramètres les utilisateurs modifient ou combien de temps ils passent à utiliser le produit.

Données sur les appareils

Nous recueillons ces informations pour comprendre où et sur quels appareils nos produits sont utilisés. Des exemples typiques sont le modèle d'appareil, le pays, la version et le nom du système d'exploitation.

Données de diagnostic d'erreur

Des informations sur les situations d'erreur et de plantage sont également collectées. Par exemple, quelle erreur s'est produite et quelles actions l'ont provoquée.

Pourquoi recueillons-nous ces informations?

Ces informations anonymes nous permettent d'améliorer nos produits pour vous, notre utilisateur. Elles nous aident à les rendre plus pertinentes, faciles à utiliser et aussi exempts de défauts que possible.

Qui contrôle ces informations?

ESET, spol. s r.o. est le seul responsable du traitement des données collectées dans le cadre du Programme. Ces informations ne sont pas partagées avec des tiers.

Contrat de licence d'utilisateur final

En vigueur à partir du 19 octobre 2021.

IMPORTANT : Veuillez lire soigneusement les conditions d’application du produit stipulées ci-dessous avant de télécharger, d’installer, de copier ou d’utiliser le produit. **EN TÉLÉCHARGEANT, EN INSTALLANT, EN COPIANT OU EN UTILISANT LE LOGICIEL, VOUS ACCEPTEZ CES CONDITIONS AINSI QUE LA POLITIQUE DE CONFIDENTIALITÉ.**

Contrat de licence de l'utilisateur final

Selon les conditions du présent Contrat de licence d’utilisateur final (« Contrat ») signé par et entre ESET, spol. s r. o., dont le siège social se situe au Einsteinova 24, 85101 Bratislava, Slovak Republic, inscrite au Registre du Commerce du tribunal régional de Bratislava I, Section Sro, Insertion No 3586/B, numéro d’inscription des

entreprises : 31333532 (« ESET » ou « Fournisseur ») et vous, personne physique ou morale, (ci-après appelé « vous » ou « Utilisateur final »), vous êtes autorisé à utiliser le Logiciel défini à l'Article 1 du présent Contrat. Le Logiciel défini à l'article 1 du présent Contrat peut être enregistré sur un support de données, envoyé par courriel, téléchargé sur Internet, téléchargé à partir de serveurs du Fournisseur ou obtenu à partir d'autres sources, sous réserve des modalités et conditions précisées ci-dessous.

CE DOCUMENT N'EST PAS UN CONTRAT D'ACHAT, MAIS UN ACCORD LIÉ AUX DROITS DE L'UTILISATEUR FINAL. Le Fournisseur reste le propriétaire de la copie du Logiciel et du support physique fourni dans l'emballage commercial, et de toutes les copies du Logiciel que l'Utilisateur final est autorisé à faire dans le cadre du présent Contrat.

En cliquant sur « J'accepte » ou « J'accepte... » lorsque vous téléchargez, copiez ou utilisez le Logiciel, vous acceptez les conditions du présent Contrat et reconnaissez la Politique de confidentialité. Si vous n'acceptez pas toutes les conditions du présent Contrat et/ou de la Politique de confidentialité, cliquez immédiatement sur l'option d'annulation, annulez l'installation ou le téléchargement, ou détruisez ou renvoyez le Logiciel, le support d'installation, la documentation qui l'accompagne et le reçu de vente au Fournisseur ou au point de vente auprès duquel vous avez acquis le Logiciel.

VOUS RECONNAISSEZ QUE VOTRE UTILISATION DU LOGICIEL INDIQUE QUE VOUS AVEZ LU ET COMPRIS LE PRÉSENT CONTRAT ET ACCEPTÉ D'EN RESPECTER LES CONDITIONS.

1. **Logiciel.** Dans le présent Contrat, le terme « Logiciel » désigne : (i) le programme informatique accompagné du présent Contrat et de toutes ses composantes; (ii) tous les contenus sur les disques, CD-ROM, DVD, courriels ou tout autre fichier joint, ou sur tout autre support avec lequel ce Contrat est fourni, incluant la forme du code objet du Logiciel fourni sur un support de données, par courriel ou téléchargement sur Internet; (iii) tout matériel d'explication écrit ou toute autre documentation éventuelle en lien avec le logiciel, surtout toute description du Logiciel, ses spécifications, toute description des propriétés ou de l'opération du Logiciel, toute description de l'environnement d'exécution dans lequel le Logiciel est utilisé, les instructions d'utilisation ou d'installation du Logiciel ou toute description sur la manière d'utiliser le Logiciel (« Documentation »); (iv) les copies du Logiciel, les retouches d'erreur possibles dans le Logiciel, les ajouts au Logiciel, les extensions au Logiciel, les versions modifiées du Logiciel et les mises à jour des composants du Logiciel, s'il y a lieu, pour lesquels vous avez obtenu une licence du Fournisseur, en vertu de l'Article 3 de ce Contrat. Le Logiciel doit être fourni exclusivement sous forme de code objet exécutable.

2. **Installation, ordinateur et clé de licence**. Les logiciels fournis sur un support de données, envoyés par courrier électronique, téléchargés à partir d'Internet, téléchargés à partir des serveurs du fournisseur ou obtenus à partir d'autres sources nécessitent une installation. Vous devez installer le logiciel sur un ordinateur correctement configuré, en respectant au moins les exigences définies dans la documentation. La méthodologie d'installation est décrite dans la documentation. Aucun programme informatique ou matériel pouvant avoir un effet négatif sur le logiciel ne peut être installé sur l'ordinateur sur lequel vous installez le logiciel. Ordinateur désigne le matériel, y compris mais sans se limiter aux ordinateurs personnels, aux ordinateurs portables, aux postes de travail, aux ordinateurs de poche, aux téléphones intelligents, aux appareils électroniques portatifs ou à d'autres appareils électroniques pour lesquels le Logiciel est conçu, sur lequel il sera installé et/ou utilisé. Clé de licence désigne la séquence unique de symboles, de lettres, de chiffres ou de signes spéciaux fournie à l'utilisateur final afin de permettre l'utilisation légale du logiciel, sa version spécifique ou l'extension de la durée de la licence conformément au présent contrat.

3. **Licence**. Sous réserve du fait que vous ayez accepté les conditions du présent Contrat et que vous respectiez toutes les modalités stipulées dans le présent Contrat, le Fournisseur vous accorde les droits suivants (« Licence ») :

a) **Installation et utilisation.** Vous détenez un droit non exclusif et non transférable d'installer le Logiciel sur le disque dur d'un ordinateur ou sur un support similaire de stockage permanent de données, d'installer et de

stocker le Logiciel dans la mémoire d'un système informatique et d'exécuter, de stocker et d'afficher le Logiciel.

b) **Précision du nombre de licences.** Le droit d'utiliser le Logiciel est lié au nombre d'Utilisateurs finaux. On entend par « un Utilisateur final » : (i) l'installation du Logiciel sur un seul système informatique, ou (ii) si l'étendue de la Licence est liée au nombre de boîtes aux lettres, un Utilisateur final désigne un utilisateur d'ordinateur qui reçoit du courriel par le biais d'un agent d'utilisateur (« AU »). Si l'AU accepte du courriel et le distribue automatiquement par la suite à plusieurs utilisateurs, le nombre d'Utilisateurs finaux doit être déterminé en fonction du nombre réel d'utilisateurs auxquels le courriel est distribué. Si un serveur de messagerie joue le rôle de passerelle de courriel, le nombre d'Utilisateurs finaux est égal au nombre d'utilisateurs du serveur de messagerie pour lesquels la passerelle fournit des services. Si un certain nombre d'adresses de messagerie sont affectées à un seul et même utilisateur (par l'intermédiaire d'alias) et que ce dernier les accepte et si les courriels ne sont pas distribués automatiquement du côté du client à d'autres utilisateurs, la Licence n'est requise que pour un seul ordinateur. Vous ne devez pas utiliser la même Licence au même moment sur plusieurs ordinateurs. L'utilisateur final est autorisé à entrer la clé de licence du logiciel uniquement dans la mesure où il a le droit d'utiliser le logiciel conformément à la limitation découlant du nombre de licences accordées par le fournisseur. La clé de licence est réputée confidentielle. Vous ne devez pas partager la licence avec des tiers ni permettre à des tiers d'utiliser la clé de licence, sauf autorisation du présent accord ou du fournisseur. Si votre clé de licence est compromise, informez le fournisseur immédiatement.

c) **Version Home/Business Edition.** Une version Home Edition du Logiciel doit être utilisée exclusivement dans un environnement privé et/ou non commercial à des fins personnelles et familiales seulement. Une version Business Edition du Logiciel doit être obtenue pour toute utilisation dans un environnement commercial ainsi que pour utiliser le Logiciel sur des serveurs de messagerie, des relais de messagerie, des passerelles de messagerie ou des passerelles Internet.

d) **Durée de la Licence.** Le droit d'utiliser le Logiciel est limité dans le temps.

e) **Logiciel acheté à un fabricant d'équipement informatique.** Les logiciels classés comme « OEM » sont limités à l'ordinateur avec lequel vous les avez obtenus. Elle ne peut pas être transférée à un autre ordinateur.

f) **Version d'évaluation ou non destinée à la revente.** Un Logiciel classé comme non destiné à la revente ou comme version d'évaluation ne peut pas être vendu et ne doit être utilisé qu'aux fins de démonstration ou d'évaluation des caractéristiques du Logiciel.

g) **Résiliation de la Licence.** La Licence expire automatiquement à la fin de la période pour laquelle elle a été accordée. Si vous ne respectez pas les dispositions du présent Contrat, le Fournisseur est en droit de mettre fin au Contrat, sans renoncer à tout droit ou recours juridique ouvert au Fournisseur dans de tels cas. En cas d'annulation du présent Contrat, vous devez immédiatement supprimer, détruire ou renvoyer à vos frais le Logiciel et toutes les copies de sauvegarde à ESET ou à l'endroit où vous avez obtenu le Logiciel. Lors de la résiliation de la licence, le fournisseur aura également le droit d'annuler le droit de l'utilisateur final d'utiliser les fonctions du logiciel, qui nécessitent une connexion aux serveurs du fournisseur ou à des serveurs tiers.

4. **Fonctions avec collecte de données et nécessitant une connexion Internet.** Pour fonctionner correctement, le logiciel nécessite une connexion à Internet et doit se connecter à intervalles réguliers aux serveurs du fournisseur ou à des serveurs tiers aux fins de collecte de données applicables conformément à la politique de confidentialité. La connexion à Internet et aux fins de collecte de données applicable sont nécessaires pour les fonctions suivantes du Logiciel :

a) **Mises à jour du Logiciel.** Le Fournisseur est autorisé à émettre des mises à jour ou mises à niveau du Logiciel (« Mises à jour ») de temps à autre, mais n'en a pas l'obligation. Cette fonction est activée dans la configuration standard du Logiciel; les Mises à jour sont donc installées automatiquement, sauf si l'Utilisateur final a désactivé l'installation automatique des Mises à jour. Aux fins de fourniture des mises à jour, la vérification de l'authenticité

de la Licence est requise, y compris les informations sur l'ordinateur et/ou la plateforme sur laquelle le Logiciel est installé tout en respectant la Politique de confidentialité.

La fourniture de toute mise à jour peut être soumise à la politique de fin de vie (« politique de fin de vie »), qui est disponible sur https://go.eset.com/eol_home. Aucune mise à jour ne sera fournie après que le Logiciel ou l'une de ses fonctionnalités a atteint la date de fin de vie telle que définie dans la politique de fin de vie.

b) **Réacheminement des infiltrations et des données au Fournisseur.** Le Logiciel contient des fonctions qui recueillent des échantillons de virus informatiques et d'autres programmes informatiques malveillants, ainsi que des objets suspects, problématiques, potentiellement indésirables ou potentiellement dangereux comme des fichiers, des adresses URL, des datagrammes IP et des secteurs Ethernet (« Infiltrations ») et les envoie par la suite au Fournisseur. Les données envoyées incluent, mais sans s'y limiter des renseignements sur le processus d'installation, l'ordinateur et/ou la plateforme sur laquelle le Logiciel est installé, les renseignements sur les opérations et la fonctionnalité du Logiciel (« Renseignements »). Les Renseignements et les Infiltrations pourraient contenir des données (incluant des données personnelles obtenues aléatoirement ou accidentellement) sur l'Utilisateur final ou d'autres utilisateurs de l'ordinateur sur lequel le Logiciel est installé ainsi que les fichiers visés par les Infiltrations avec les métadonnées associées.

Les Renseignements et les Infiltrations pourraient être recueillies par les fonctions du Logiciel suivantes :

i. La fonction LiveGrid Reputation System inclut la collecte et l'envoi de hachage à sens unique lié aux Infiltrations au Fournisseur. Cette fonction est activée sous les paramètres standard du Logiciel.

ii. La fonction LiveGrid Feedback System inclut la collecte et l'envoi d'infiltrations avec les métadonnées associées et les informations au Fournisseur. Cette fonction peut être activée par l'utilisateur final pendant le processus d'installation du logiciel.

Le Fournisseur utilisera les Informations et les Infiltrations reçues uniquement à des fins d'analyse et de recherche d'infiltrations, d'amélioration du Logiciel et de vérification de l'authenticité des Licences et prendra les mesures appropriées pour s'assurer que les Infiltrations et les Informations reçues restent sécurisées. En activant cette fonction du Logiciel, les Infiltrations et les Informations peuvent être collectées et traitées par le Fournisseur comme spécifié dans la Politique de Confidentialité et en conformité avec les réglementations légales pertinentes. Vous pouvez désactiver ces fonctions à tout moment.

Aux fins du présent contrat, il est nécessaire de collecter, de traiter et de stocker les données permettant au fournisseur de vous identifier conformément à la politique de confidentialité. Vous reconnaissez par la présente que le Fournisseur vérifie, en utilisant ses propres moyens, si vous utilisez le Logiciel conformément aux dispositions du présent Contrat. Vous reconnaissez par la présente qu'aux fins du présent Contrat, il est nécessaire que vos données soient transférées pendant la communication entre le Logiciel et les systèmes informatiques du Fournisseur ou de ses partenaires commerciaux dans le cadre du réseau de distribution et d'asssitance du Fournisseur afin d'assurer le bon fonctionnement du logiciel et l'autorisation d'utiliser le logiciel ainsi que la protection des droits du fournisseur.

Après la conclusion du présent accord, le Fournisseur ou l'un de ses partenaires faisant partie du réseau de distribution et d'assistance du Fournisseur aura le droit de transférer, de traiter et de stocker les données essentielles vous identifiant à des fins de facturation, d'exécution du contrat et de transmission de notifications.

Vous trouverez des informations détaillées sur la confidentialité, la protection des données personnelles et vos droits en tant que personne concernée dans la politique de confidentialité, disponible sur le site Web du Fournisseur et accessible directement depuis le processus d'installation. Vous pouvez également le visiter à partir de la section d'aide du logiciel.

5. **Exercice des droits de l'Utilisateur final**. Vous devez exercer les droits de l'Utilisateur final en personne ou par

l’intermédiaire de vos employés. Vous n’êtes autorisé à utiliser le Logiciel que pour assurer la sécurité de vos opérations et protéger les systèmes informatiques pour lesquels vous avez obtenu une Licence.

6. **Limitations aux droits.** Vous ne pouvez pas copier, distribuer, extraire des composants ou créer des travaux dérivés basés sur le Logiciel. Vous devez respecter les restrictions suivantes lorsque vous utilisez le Logiciel :

a) Vous pouvez effectuer une copie de sauvegarde archivée du Logiciel sur un support de stockage permanent, à condition que cette copie de sauvegarde archivée ne soit pas installée ni utilisée sur un autre ordinateur. Toutes les autres copies que vous pourriez faire du Logiciel seront considérées comme une violation du présent Contrat.

b) Vous n’êtes pas autorisé à utiliser, à modifier, à traduire, à reproduire ou à transférer les droits d’utilisation du Logiciel ou des copies du Logiciel d’aucune manière autre que celles prévues dans le présent Contrat.

c) Vous ne pouvez pas vendre, concéder en sous-licence, louer à bail ou louer le Logiciel ou utiliser le Logiciel pour offrir des services commerciaux.

d) Vous ne pouvez pas désosser, décompiler ou désassembler le Logiciel ni tenter de toute autre façon de découvrir le code source du Logiciel, sauf dans la mesure où cette restriction est expressément interdite par la loi.

e) Vous acceptez de n’utiliser le Logiciel que de façon conforme à toutes les lois applicables de la juridiction dans laquelle vous utilisez le Logiciel, notamment les restrictions applicables relatives aux droits d’auteur et aux droits de propriété intellectuelle.

f) Vous convenez de n’utiliser le logiciel et ses fonctionnalités que de façon à ne pas limiter la possibilité, pour les autres utilisateurs finaux, d’accéder à ces services. Le Fournisseur se réserve le droit de limiter la portée des services fournis à certains utilisateurs finaux pour en permettre l’utilisation par le plus grand nombre possible d’utilisateurs finaux. Limiter la portée des services fournis signifie aussi pouvoir mettre fin à la possibilité d’utiliser l’une des fonctionnalités du logiciel et supprimer les données et informations stockées sur les serveurs du Fournisseur ou de tiers relativement à une fonctionnalité spécifique du logiciel.

g) Vous acceptez de ne pas exercer d'activités impliquant l'utilisation de la clé de licence, contrairement aux termes du présent Contrat ou conduisant à fournir une clé de licence à toute personne qui n'a pas le droit d'utiliser le logiciel, comme le transfert de clé de licence sous quelque forme que ce soit, ainsi que la reproduction non autorisée ou la distribution de clés de licence dupliquées ou générées ou l'utilisation du logiciel suite à l'utilisation d'une clé de licence obtenue d'une source autre que le fournisseur.

7. **Droits d’auteur**. Le Logiciel et tous les droits inclus, notamment les droits d’auteur et les droits de propriété intellectuelle sont la propriété d’ESET et/ou de ses concédants de licence. Ils sont protégés par les dispositions des traités internationaux et par toutes les lois nationales applicables dans le pays où le Logiciel est utilisé. La structure, l’organisation et le code du Logiciel sont des secrets commerciaux importants et des informations confidentielles appartenant à ESET et/ou à ses concédants de licence. Vous n’êtes pas autorisé à copier le Logiciel, sauf dans les exceptions précisées en 6 (a). Toutes les copies que vous êtes autorisé à faire en vertu du présent Contrat doivent contenir les mentions relatives aux droits d’auteur et de propriété qui apparaissent sur le Logiciel. Si vous désossez, décompilez ou désassemblez le Logiciel ou tentez de toute autre façon de découvrir le code source du Logiciel, en violation des dispositions du présent Contrat, vous acceptez que les données ainsi obtenues doivent être automatiquement et irrévocablement transférées au Fournisseur dans leur totalité, dès que de telles données sont connues, indépendamment des droits du Fournisseur relativement à la violation du présent Contrat.

8. **Réservation de droits**. Le Fournisseur se réserve tous les droits sur le Logiciel, à l’exception des droits qui vous sont expressément garantis en vertu des conditions du présent Contrat en tant qu’Utilisateur final du Logiciel.

9. **Versions multilingues, logiciel sur plusieurs supports, multiples copies**. Si le Logiciel est utilisé sur plusieurs

plateformes et en plusieurs langues, ou si vous recevez plusieurs copies du Logiciel, vous ne pouvez utiliser le Logiciel que pour le nombre de systèmes informatiques ou de versions pour lesquels vous avez obtenu une Licence. Vous ne pouvez pas vendre, louer à bail, louer, concéder en sous-licence, prêter ou transférer des versions ou des copies du Logiciel que vous n'utilisez pas.

10. **Début et fin du Contrat.** Ce Contrat entre en vigueur à partir du jour où vous en acceptez les modalités. Vous pouvez résilier ce Contrat à tout moment en désinstallant de façon permanente, détruisant et renvoyant, à vos frais, le Logiciel, toutes les copies de sauvegarde et toute la documentation associée fournie par le Fournisseur ou ses partenaires commerciaux. Votre droit d'utiliser le Logiciel et l'une de ses fonctionnalités peut être soumis à la Politique de fin de vie. Une fois que le Logiciel ou l'une de ses fonctionnalités a atteint la date de fin de vie définie dans la Politique de fin de vie, votre droit d'utiliser le Logiciel prendra fin. Quelle que soit la façon dont ce Contrat se termine, les dispositions énoncées aux articles 7, 8, 11, 13, 19 et 21 continuent de s'appliquer pour une durée illimitée.

11. **DÉCLARATIONS DE L'UTILISATEUR FINAL**. EN TANT QU'UTILISATEUR FINAL, VOUS RECONNAISSEZ QUE LE LOGICIEL EST FOURNI « EN L'ÉTAT », SANS AUCUNE GARANTIE D'AUCUNE SORTE, QU'ELLE SOIT EXPRESSE OU IMPLICITE, DANS LA LIMITE PRÉVUE PAR LA LOI APPLICABLE. NI LE FOURNISSEUR, NI SES CONCÉDANTS DE LICENCE, NI SES FILIALES, NI LES DÉTENTEURS DE DROIT D'AUTEUR NE FONT UNE QUELCONQUE DÉCLARATION OU N'ACCORDENT DE GARANTIE EXPRESSE OU IMPLICITE QUELCONQUE, NOTAMMENT DES GARANTIES DE VENTE, DE CONFORMITÉ À UN OBJECTIF PARTICULIER OU SUR LE FAIT QUE LE LOGICIEL NE PORTE PAS ATTEINTE À DES BREVETS, DROITS D'AUTEURS, MARQUES OU AUTRES DROITS DÉTENUS PAR UN TIERS. NI LE FOURNISSEUR NI AUCUN AUTRE TIERS NE GARANTIT QUE LES FONCTIONS DU LOGICIEL RÉPONDRONT À VOS ATTENTES OU QUE LE FONCTIONNEMENT DU LOGICIEL SERA CONTINU ET EXEMPT D'ERREURS. VOUS ASSUMEZ L'ENTIÈRE RESPONSABILITÉ ET LES RISQUES LIÉS AU CHOIX DU LOGICIEL POUR L'OBTENTION DES RÉSULTATS ESCOMPTÉS ET POUR L'INSTALLATION, L'UTILISATION ET LES RÉSULTATS OBTENUS.

12. **Aucune obligation supplémentaire**. À l'exception des obligations mentionnées explicitement dans le présent Contrat, aucune obligation supplémentaire n'est imposée au Fournisseur et à ses concédants de licence.

13. **LIMITATION DE GARANTIE**. DANS LA LIMITE MAXIMALE PRÉVUE PAR LES LOIS APPLICABLES, LE FOURNISSEUR, SES EMPLOYÉS OU SES CONCÉDANTS DE LICENCE NE SERONT EN AUCUN CAS TENUS POUR RESPONSABLES D'UNE QUELCONQUE PERTE DE PROFIT, REVENUS, VENTES, DONNÉES, OU DES FRAIS D'OBTENTION DE BIENS OU SERVICES DE SUBSTITUTION, DE DOMMAGE MATÉRIEL, DOMMAGE PHYSIQUE, INTERRUPTION D'ACTIVITÉ, PERTE DE DONNÉES COMMERCIALES, OU DE TOUT DOMMAGE DIRECT, INDIRECT, FORTUIT, ÉCONOMIQUE, DE GARANTIE, PUNITIF, SPÉCIAL OU CORRÉLATIF, QUELLE QU'EN SOIT LA CAUSE ET QUE CE DOMMAGE DÉCOULE D'UNE RESPONSABILITÉ CONTRACTUELLE, DÉLICTUELLE OU D'UNE NÉGLIGENCE OU DE TOUTE AUTRE THÉORIE DE RESPONSABILITÉ, LIÉE À L'INSTALLATION, À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISER LE LOGICIEL, MÊME SI LE FOURNISSEUR OU SES CONCÉDANTS DE LICENCE ONT ÉTÉ AVERTIS DE L'ÉVENTUALITÉ D'UN TEL DOMMAGE. CERTAINS PAYS ET CERTAINES LOIS N'AUTORISANT PAS L'EXCLUSION DE RESPONSABILITÉ, MAIS AUTORISANT LA LIMITATION DE RESPONSABILITÉ, LA RESPONSABILITÉ DU FOURNISSEUR, DE SES EMPLOYÉS OU DE SES CONCÉDANTS DE LICENCE SERA LIMITÉE AU MONTANT QUE VOUS AVEZ PAYÉ POUR LA LICENCE.

14. Aucune disposition du présent Contrat ne porte atteinte aux droits accordés par la loi de toute partie agissant comme client si l'exécution y est contraire.

15. **Assistance technique**. ESET ou des tiers mandatés par ESET fourniront une assistance technique à leur discrétion, sans garantie ni déclaration solennelle. Aucune assistance technique ne sera fournie après que le Logiciel ou l'une de ses fonctionnalités a atteint la date de fin de vie telle que définie dans la politique de fin de vie. L'Utilisateur final devra peut-être sauvegarder toutes les données, logiciels et programmes existants avant que l'assistance technique ne soit fournie. ESET et/ou les tiers mandatés par ESET ne seront en aucun cas tenus responsables d'un quelconque dommage ou d'une quelconque perte de données, de biens, de logiciels ou de matériel, ou d'une quelconque perte de profit en raison de la fourniture de l'assistance technique. ESET et/ou les

tiers mandatés par ESET se réservent le droit de décider si l'assistance technique couvre la résolution du problème. ESET se réserve le droit de refuser, de suspendre l'assistance technique ou d'y mettre fin à sa discrétion. Des informations de licence ainsi que des informations et d'autres données conformes à la politique de confidentialité peuvent être exigées aux fins de l'assistance technique.

16. **Transfert de Licence**. Le Logiciel ne peut pas être transféré d'un système informatique à un autre, à moins d'une précision contraire dans les modalités du présent Contrat. L'Utilisateur final n'est autorisé qu'à transférer de façon définitive la Licence et tous les droits accordés par le présent Contrat à un autre Utilisateur final avec l'accord du Fournisseur, si cela ne s'oppose pas aux modalités du présent Contrat et dans la mesure où (i) l'Utilisateur final d'origine ne conserve aucune copie du Logiciel; (ii) le transfert des droits est direct, c'est-à-dire qu'il s'effectue directement de l'Utilisateur final original au nouvel Utilisateur final; (iii) le nouvel Utilisateur final assume tous les droits et devoirs de l'Utilisateur final d'origine en vertu du présent Contrat; (iv) l'Utilisateur final d'origine transmet au nouvel Utilisateur final toute la documentation permettant de vérifier l'authenticité du Logiciel, conformément à l'article 17.

17. **Vérification de l'authenticité du Logiciel.** L'Utilisateur final peut démontrer son droit d'utilisation du Logiciel de l'une des façons suivantes : (i) au moyen d'un certificat de Licence émis par le Fournisseur ou un tiers mandaté par le Fournisseur; (ii) au moyen d'un Contrat de Licence écrit, si un tel contrat a été conclu; (iii) en soumettant un courriel envoyé par le Fournisseur contenant les renseignements sur la Licence (nom d'utilisateur et mot de passe). Les informations de licence et les données d'identification de l'utilisateur final peuvent être requises conformément à la politique de confidentialité aux fins de vérification de l'authenticité du logiciel.

18. **Licence pour les pouvoirs publics et le gouvernement des États-Unis**. Le Logiciel est fourni aux pouvoirs publics, y compris le gouvernement des États-Unis, avec les droits de Licence et les restrictions mentionnés dans le présent Contrat.

19. **Conformité aux contrôles à l'exportation**.

a) Vous ne devez pas, directement ou indirectement, exporter, réexporter, transférer ni donner accès au logiciel de quelque manière que ce soit à toute personne, ni l'utiliser de quelque manière que ce soit, ni être impliqué dans un acte qui pourrait avoir pour conséquence qu'ESET ou ses sociétés holding, ses filiales et les filiales de ses sociétés holding, ainsi que les entités contrôlées par ses sociétés holding (« affiliés ») violent les lois sur le contrôle à l'exportation ou en subissent des conséquences négatives, ce qui comprend :

i. toute loi qui contrôle, restreint ou impose des exigences de licence pour l'exportation, la réexportation ou le transfert de biens, de logiciels, de technologies ou de services, émise ou adoptée par un gouvernement, un État ou un organisme de réglementation des États-Unis d'Amérique, de Singapour, du Royaume-Uni, de l'Union européenne ou de l'un de ses États membres, ou de tout pays dans lequel des obligations au titre de l'accord doivent être exécutées, ou dans lequel ESET ou l'une de ses sociétés affiliées sont constituées ou exercent leurs activités et

ii. toute sanction, restriction, embargo, interdiction d'importation ou d'exportation, interdiction de transfert de fonds ou d'actifs ou de prestation de services, ou mesure équivalente imposée par un gouvernement, un État ou un organisme de réglementation des États-Unis d'Amérique, de Singapour, du Royaume-Uni, de l'Union européenne ou de l'un de ses États membres, ou de tout pays dans lequel des obligations au titre de l'accord doivent être exécutées, ou dans lequel ESET ou l'une de ses sociétés affiliées sont constituées ou exercent leurs activités (« lois de sanction »), de nature économique, financière, commerciale ou autre.

(actes juridiques mentionnés aux points i et ii ci-dessus, ensemble, les « Lois sur le contrôle du commerce »).

b) ESET a le droit de suspendre ses obligations au titre des présentes conditions, ou de les résilier avec effet immédiat dans le cas où :

i. ESET détermine que, selon son avis raisonnable, l'utilisateur a violé ou est susceptible de violer la disposition de l'article 19 a) de l'accord; ou

ii. l'utilisateur final et/ou le logiciel deviennent soumis aux lois sur le contrôle des exportations et, en conséquence, ESET détermine que, selon son opinion raisonnable, l'exécution continue de ses obligations en vertu de l'accord pourrait avoir pour conséquence qu'ESET ou ses affiliés violent les lois de contrôle du commerce ou en subissent des conséquences négatives.

c) Rien dans l'accord n'est destiné, et rien ne doit être interprété ni compris comme étant destiné à inciter ou à obliger l'une ou l'autre des parties à agir ou à s'abstenir d'agir (ou à accepter d'agir ou de s'abstenir d'agir) d'une manière qui soit incompatible avec les lois de contrôle du commerce applicables, réprimée ou interdite.

20. **Avis**. Tous les avis et les retours du Logiciel et de la Documentation doivent être adressés à ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, sans préjudice du droit d'ESET de Vous communiquer toute modification du présent Contrat, des Politiques de confidentialité, de la Politique de fin de vie et de la Documentation conformément à l'article 22 du Contrat. ESET peut vous envoyer des courriels, des notifications dans l'application par le biais du logiciel ou publier la communication sur son site Web. Vous acceptez de recevoir des communications légales d'ESET sous forme électronique, y compris toute communication sur la modification des Conditions, des Conditions spéciales ou des Politiques de confidentialité, toute proposition/acceptation de contrat ou invitation à négocier, avis ou autres communications légales. Cette communication électronique sera considérée comme reçue par écrit, à moins qu'une forme différente de communication soit spécifiquement requise par les lois applicables.

21. **Loi applicable**. Le présent Contrat est régi par la loi de la République Slovaque et interprété conformément à celle-ci. L'Utilisateur final et le Fournisseur conviennent que les principes relatifs aux conflits de la loi applicable et la Convention des Nations Unies sur les contrats pour la Vente internationale de marchandises ne s'appliquent pas. Vous acceptez expressément que le tribunal de Bratislava I., Slovaquie, arbitre tout litige ou conflit avec le Fournisseur ou en relation avec votre utilisation du Logiciel, et vous reconnaissez expressément que le tribunal a la juridiction pour de tels litiges ou conflits.

22. **Dispositions générales**. Si une disposition du présent Contrat s'avère nulle et inopposable, cela n'affectera pas la validité des autres dispositions du présent Contrat. Ces dispositions resteront valables et opposables en vertu des conditions stipulées dans le présent Contrat. Le présent Contrat a été signé en anglais. Dans le cas où une traduction du présent Contrat est préparée pour des raisons de commodité ou pour toute autre raison, ou dans le cas d'une divergence entre les versions linguistiques du présent Contrat, la version anglaise prévaudra.

ESET se réserve le droit d'apporter des modifications au Logiciel ainsi que de réviser les conditions du présent Contrat, de ses Annexes, des Addenda, de la Politique de Confidentialité, de la Politique de fin de vie et de la Documentation ou toute partie de ceux-ci à tout moment en mettant à jour le document concerné (i) pour refléter les modifications apportées au Logiciel ou à la façon dont ESET fait des affaires, (ii) pour des raisons légales, réglementaires ou de sécurité, ou (iii) pour prévenir les abus ou les dommages. Vous serez informé de toute révision du Contrat par courriel, par notification dans l'application ou par d'autres moyens électroniques. Si vous n'êtes pas d'accord avec les modifications proposées au Contrat, vous pouvez le résilier conformément à l'article 10 dans les 30 jours suivant la réception d'un avis de modification. À moins que vous ne résiliiez le Contrat dans ce délai, les modifications proposées seront réputées acceptées et entreront en vigueur à votre égard à la date à laquelle vous avez reçu un avis de changement.

Ceci constitue le Contrat total entre le Fournisseur et vous relativement au Logiciel et remplace l'ensemble des précédentes déclarations, discussions, promesses, communications ou publicités concernant le Logiciel.

ADDENDA À L'ACCORD

Évaluation de la sécurité des périphériques connectés au réseau. Des dispositions complémentaires s'appliquent

à l'évaluation de la sécurité des périphériques connectés au réseau comme suit :

Le logiciel contient une fonction de contrôle de la sécurité du réseau local de l'utilisateur final et des périphériques du réseau local, qui requiert le nom du réseau local et des informations sur les périphériques du réseau local, telles que la présence, le type, le nom, l'adresse IP et l'adresse MAC du périphérique du réseau local en relation avec les renseignements de licence. Les informations incluent également le type de sécurité pour sans fil et le type de chiffrement pour sans fil des périphériques de routeur. Cette fonction peut également fournir des informations sur la disponibilité de la solution logicielle de sécurité pour sécuriser les périphériques du réseau local.

Protection contre l'utilisation abusive des données. Des dispositions complémentaires s'appliquent à la protection contre l'utilisation abusive des données comme suit :

Le logiciel contient une fonction qui empêche la perte ou une mauvaise utilisation des données confidentielles en lien direct avec le vol d'un ordinateur. Cette fonction est désactivée dans les paramètres par défaut du logiciel. Le compte ESET HOME doit être créé pour que la fonction soit activée, ce qui permet la collecte de données en cas de vol de l'ordinateur. Si vous avez choisi d'activer cette fonction du logiciel, les données sur l'ordinateur volé seront collectées et envoyées au fournisseur; ces données peuvent inclure des données sur l'emplacement réseau de l'ordinateur, des données sur le contenu affiché sur l'écran de l'ordinateur, des données sur la configuration de l'ordinateur et/ou des données enregistrées par une caméra connectée à l'ordinateur (ci-après dénommé « données »). L'utilisateur final est autorisé à utiliser les données obtenues par cette fonction et fournies par l'intermédiaire du compte ESET HOME exclusivement pour remédier à une situation défavorable causée par le vol d'un ordinateur. C'est dans le seul but de fournir cette fonction, que le Fournisseur traite les données comme indiqué dans la politique de confidentialité et en conformité avec les réglementations légales pertinentes. Le Fournisseur doit permettre à l'utilisateur final d'accéder aux données pendant la période requise pour atteindre l'objectif pour lequel les données ont été obtenues et qui ne doit pas dépasser la période de conservation spécifiée dans la politique de confidentialité. La protection contre la mauvaise utilisation des données doit être utilisée exclusivement avec les ordinateurs et les comptes auxquels l'utilisateur final a légitimement accès. Toute utilisation illégale sera signalée à l'autorité compétente. Le Fournisseur se conformera aux lois pertinentes et assistera les autorités chargées de l'application de la loi en cas de mauvaise utilisation des données. Vous acceptez et reconnaissez que vous êtes responsable de la protection du mot de passe pour accéder au compte ESET HOME et vous acceptez de ne pas divulguer votre mot de passe à un tiers. L'utilisateur final est responsable de toute activité impliquant la fonction de protection contre la mauvaise utilisation des données et le compte ESET HOME, que cette activité soit autorisée ou non. Si le compte ESET HOME est compromis, informez le fournisseur immédiatement. Les dispositions complémentaires relatives à la protection contre l'utilisation abusive des données s'appliquent exclusivement aux utilisateurs finaux de ESET Internet Security et de ESET Smart Security Premium.

ESET Secure Data. Des dispositions complémentaires s'appliquent à ESET Secure Data comme suit :

1. Définitions. Dans ces dispositions complémentaires de ESET Secure Data, les mots suivants ont les significations correspondantes ci-après :

a) « Information » toute information ou donnée chiffrée ou déchiffrée à l'aide du logiciel;

b) « Produits »le logiciel ESET Secure Data et la documentation;

c) « ESET Secure Data » le(s) logiciel(s) utilisé(s) pour le chiffrement et le déchiffrement des données électroniques;

Toutes les références au pluriel incluent le singulier et toutes les références au masculin incluent le féminin et le neutre et vice versa. Les mots sans définition spécifique doivent être utilisés conformément aux définitions stipulées dans le Contrat.

2. Déclaration supplémentaire de l'utilisateur final. Vous reconnaissez et acceptez que :

a) il est de votre responsabilité de protéger, de conserver et de sauvegarder les Informations;

b) vous devez sauvegarder entièrement toutes les Informations et les données (incluant, sans toutefois s'y limiter, toutes les données et tous les renseignements essentiels) sur votre ordinateur avant l'installation de ESET Secure Data;

c) vous devez conserver en lieu sûr les mots de passe ou d'autres renseignements utilisés pour la configuration et l'utilisation d'ESET Secure Data; vous devez également faire des copies de sauvegarde de toutes les clés de chiffrement, des codes de licence, des clés de fichiers et d'autres données générées sur un support de stockage séparé;

d) vous êtes responsable de l'utilisation des produits. Le Fournisseur ne pourra en aucun cas être tenu responsable des pertes, des réclamations ou des dommages résultants du chiffrement ou du déchiffrement non autorisé ou erroné des informations ou des données (incluant, sans toutefois s'y limiter, des informations) quel que soit le lieu ou la façon dont ces informations ou données sont stockées;

e) s'il est vrai que le Fournisseur a pris toutes les mesures raisonnables pour assurer l'intégrité et la sécurité d'ESET Secure Data, les produits (ou l'un d'eux) ne doivent pas être utilisés dans une zone qui dépend d'un système à sécurité intégrée, qui est potentiellement dangereuse ou qui comporte des risques, incluant, sans toutefois s'y limiter, des installations nucléaires, des systèmes de navigation, de contrôle ou de communication aériens, des systèmes d'armes et de défense ainsi que des systèmes de soutien ou de surveillance de vie;

f) il est de votre responsabilité de veiller à ce que le niveau de sécurité et de chiffrement fourni par les produits soit suffisant pour vos besoins;

g) vous êtes responsable de votre utilisation des produits (ou de l'un d'eux), incluant, sans toutefois s'y limiter, le fait de veiller à ce que cette utilisation soit conforme à toutes les lois et à tous les règlements en vigueur de la République slovaque ou de tout autre pays, de toute autre région ou de tout autre état où le produit est utilisé. Vous devez vous assurer avant toute utilisation des produits que cette utilisation ne viole aucun embargo gouvernemental (en République slovaque ou ailleurs);

h) ESET Secure Data peut communiquer avec les serveurs du Fournisseur de temps en temps pour vérifier les informations de licence, les correctifs disponibles, les ensembles de modifications provisoires et d'autres mises à jour susceptibles d'améliorer, de maintenir, de modifier ou d'améliorer le fonctionnement d'ESET Secure Data et peut envoyer des informations générales sur le système liées à son fonctionnement en conformité avec la politique de confidentialité.

i) le Fournisseur ne sera aucunement responsable des pertes, des dommages, des dépenses ou des réclamations découlant de la perte, du vol, d'une mauvaise utilisation, de la corruption, des dommages ou de la destruction des mots de passe, des données de configuration, des clés de chiffrement, des codes d'activation de licence et d'autres données générées ou stockées pendant l'utilisation du logiciel.

Les dispositions complémentaires de ESET Secure Data s'appliquent uniquement aux Utilisateurs finaux de ESET Smart Security Premium.

Password Manager Logiciel. Des dispositions complémentaires s'appliquent au logiciel Password Manager comme suit :

1. Déclaration supplémentaire de l'utilisateur final. Vous reconnaissez et acceptez que Vous ne pouvez pas :

a) utiliser le logiciel Password Manager pour faire fonctionner une application cruciale à la mission dont la vie humaine ou des biens dépendent. Vous comprenez que le logiciel Password Manager n'a pas été conçu à cette fin

et que sa défaillance dans ces cas pourrait entraîner la mort, des préjudices corporels ou de graves dommages aux biens ou à l'environnement dont le Fournisseur n'est pas responsable.

LE LOGICIEL PASSWORD MANAGER N'EST PAS CONÇU, PRÉVU ET AUCUNE LICENCE N'EST ACCORDÉE POUR UNE UTILISATION DANS DES ENVIRONNEMENTS DANGEREUX EXIGEANTS DES SYSTÈMES À SÉCURITÉ INTÉGRÉE, INCLUANT, SANS TOUTEFOIS S'Y LIMITER, LA CONCEPTION, LA CONSTRUCTION, L'ENTRETIEN OU L'EXPLOITATION DES INSTALLATIONS NUCLÉAIRES, DES SYSTÈMES DE NAVIGATION OU DE COMMUNICATION AÉRIENNES, LE CONTRÔLE DU TRAFIC AÉRIEN, LES SYSTÈMES DE MAINTIENT EN VIE OU LES SYSTÈMES D'ARMEMENT. LE FOURNISSEUR DÉCLINE EXPRESSÉMENT TOUTE GARANTIE EXPLICITE OU IMPLICITE D'ADÉQUATION À CES USAGES.

b) utiliser le logiciel Password Manager d'une manière qui contrevient à ce Contrat ou aux lois de la République slovaque ou de votre région administrative. Plus précisément, vous ne pouvez pas utiliser le logiciel Password Manager pour mener ou promouvoir des activités illégales, y compris le téléchargement de données de contenu ou de contenu préjudiciable qui pourraient être utilisés pour des activités illégales ou qui viole la loi ou les droits de tiers (y compris les droits de propriété intellectuelle), y compris, mais sans s'y limiter, toute tentative d'accès aux comptes dans le stockage (aux fins des présentes dispositions complémentaires pour le logiciel Password Manager « Stockage » désigne l'espace de stockage de données géré par le Fournisseur ou un tiers autre que le Fournisseur et l'utilisateur dans le but d'activer la synchronisation et la sauvegarde des données utilisateur) ou aux comptes et aux données d'autres utilisateurs du logiciel Password Manager ou du stockage. Si vous ne respectez pas l'une de ces dispositions, le Fournisseur est en droit de résilier immédiatement ce contrat et de vous répercuter le coût de tout recours nécessaire, ainsi que de prendre toutes les mesures nécessaires pour vous empêcher d'utiliser le Logiciel Password Manager sans possibilité de remboursement.

2. LIMITATION DE GARANTIE. LE LOGICIEL PASSWORD MANAGER EST FOURNI « TEL QUEL ». AUCUNE GARANTIE D'AUCUNE SORTE, EXPLICITE OU IMPLICITE N'EST OFFERTE. VOUS UTILISEZ LE LOGICIEL À VOS PROPRES RISQUES. LE PRODUCTEUR N'EST PAS RESPONSABLE DE LA PERTE, DES DOMMAGES, DE LA LIMITATION DE DISPONIBILITÉ DE SERVICE SURVENANT AUX DONNÉES, Y COMPRIS DES DONNÉES ENVOYÉES PAR LE LOGICIEL PASSWORD MANAGER À UN DISPOSITIF DE STOCKAGE EXTERNE AUX FINS DE SYNCHRONISATION ET DE SAUVEGARDE DE DONNÉES. LE CHIFFREMENT DES DONNÉES À L'AIDE DU LOGICIEL PASSWORD MANAGER N'ENGAGE AUCUNEMENT LA RESPONSABILITÉ DU FOURNISSEUR QUANT À LA SÉCURITÉ DE CES DONNÉES. VOUS MARQUEZ EXPRESSÉMENT VOTRE ACCORD POUR QUE LES DONNÉES ACQUISES, UTILISÉES, CHIFFRÉES, STOCKÉES, SYNCHRONISÉES OU ENVOYÉES À L'AIDE DU LOGICIEL PASSWORD MANAGER SOIENT ÉGALEMENT STOCKÉES SUR DES SERVEURS TIERS (APPLICABLE UNIQUEMENT À L'UTILISATION DU LOGICIEL PASSWORD MANAGER DANS LES CAS OÙ LES SERVICES DE SYNCHRONISATION ET DE SAUVEGARDE ONT ÉTÉ ACTIVÉS). SI LE FOURNISSEUR À SA DISCRÉTION CHOISIT D'UTILISER UN TEL DISPOSITIF DE STOCKAGE, UN SITE WEB, UN PORTAIL WEB, UN SERVEUR OU UN SERVICE TIERS, IL N'EST PAS RESPONSABLE DE LA QUALITÉ, DE LA SÉCURITÉ OU DE LA DISPONIBILITÉ D'UN TEL SERVICE FOURNI PAR UN TIERS ET EN AUCUN CAS LE FOURNISSEUR N'EST RESPONSABLE ENVERS VOUS DE LA VIOLATION DES OBLIGATIONS CONTRACTUELLES OU JURIDIQUES PAR LE TIERS, NI DES DOMMAGES, DES PERTES DE PROFITS, DES DOMMAGES FINANCIERS OU NON FINANCIERS OU DES PERTES DE TOUTE AUTRE NATURE CAUSÉES PAR L'UTILISATION DU LOGICIEL. LE FOURNISSEUR N'EST PAS RESPONSABLE DU CONTENU DE DONNÉES ACQUISES, UTILISÉES, CHIFFRÉES, STOCKÉES, SYNCHRONISÉES OU ENVOYÉES À L'AIDE DU LOGICIEL PASSWORD MANAGER OU SE TROUVANT DANS LA MÉMOIRE. VOUS RECONNAISSEZ QUE LE FOURNISSEUR N'A PAS ACCÈS AU CONTENU DES DONNÉES STOCKÉES ET N'EST PAS EN MESURE DE LES SURVEILLER OU DE SUPPRIMER DU CONTENU LÉGALEMENT NUISIBLE.

Le Fournisseur détient tous les droits sur les améliorations, les mises à jour et les correctifs du logiciel Password Manager (« Améliorations »), même dans le cas où de telles améliorations ont été créées sur la base des commentaires, des idées ou des suggestions soumises par vous sous une forme quelconque. Vous n'avez droit à aucune compensation, y compris des redevances liées à ces améliorations.

LES ENTITÉS ET LES CONCÉDANTS DE LICENCE DU FOURNISSEUR NE POURRONT ÊTRE TENUS RESPONSABLES DES

RÉCLAMATIONS ET DES OBLIGATIONS DE QUELQUE NATURE QUE CE SOIT PROVENANT OU LIÉ À L'UTILISATION DU LOGICIEL PASSWORD MANAGER PAR VOUS OU PAR DES TIERS, À L'UTILISATION OU À LA NON-UTILISATION D'UN CABINET DE COURTAGE OU D'UN MARCHAND OU À LA VENTE OU L'ACHAT D'UNE VALEUR MOBILIÈRE, QUE CES RÉCLAMATIONS ET CES OBLIGATIONS SOIENT FONDÉES SUR UN PRINCIPE DE DROIT OU D'ÉQUITÉ.

LES ENTITÉS ET LES CONCÉDANTS DE LICENCE DU FOURNISSEUR NE POURRONT ÊTRE TENUS POUR RESPONSABLES DES DOMMAGES DIRECTS, INDIRECTS, SPÉCIAUX, CONSÉCUTIFS OU ACCESSOIRES DÉCOULANT OU LIÉS À UN LOGICIEL TIERS, À DES DONNÉES ACCESSIBLES PAR LE LOGICIEL PASSWORD MANAGER, À L'UTILISATION OU L'INCAPACITÉ D'UTILISER OU D'ACCÉDER AU LOGICIEL PASSWORD MANAGER OU À DES DONNÉES FOURNIES PAR L'INTERMÉDIAIRE DU LOGICIEL PASSWORD MANAGER, QUE LES RÉCLAMATIONS CONCERNANT CES DOMMAGES SOIENT FONDÉES SUR UN PRINCIPE DE DROIT OU D'ÉQUITÉ. PARMI LES DOMMAGES EXCLUS PAR CETTE CLAUSE, ON PEUT CITER, SANS S'Y LIMITER, LA PERTE DE PROFITS, LES DOMMAGES CORPORELS OU MATÉRIELS, LES INTERRUPTIONS D'ACTIVITÉS ET LA PERTE DE RENSEIGNEMENTS COMMERCIAUX OU PERSONNELS. CERTAINS PAYS N'AUTORISENT PAS LA LIMITATION DES DOMMAGES DIRECTS OU INDIRECTS; CETTE RESTRICTION PEUT DONC NE PAS S'APPLIQUER À VOUS. DANS CE CAS LA RESPONSABILITÉ DU FOURNISSEUR SERA LA RESPONSABILITÉ MINIMALE AUTORISÉE PAR LA LOI APPLICABLE.

LES INFORMATIONS FOURNIES PAR LE LOGICIEL PASSWORD MANAGER, Y COMPRIS LES COTATIONS BOURSIÈRES, L'ANALYSE, LES INFORMATIONS SUR LE MARCHÉ BOURSIER, LES NOUVELLES ET LES DONNÉES FINANCIÈRES, PEUVENT ÊTRE RETARDÉES, INEXACTES OU CONTENIR DES ERREURS OU DES OMISSIONS; LES ENTITÉS ET LES CONCÉDANTS DE LICENCE DU FOURNISSEUR DÉCLINENT TOUTE RESPONSABILITÉ À CE SUJET. LE FOURNISSEUR PEUT MODIFIER OU SUPPRIMER N'IMPORTE QUEL ASPECT OU FONCTIONNALITÉ DU LOGICIEL PASSWORD MANAGER OU L'UTILISATION D'UNE OU DE TOUTES LES FONCTIONNALITÉS OU DE LA TECHNOLOGIE DU LOGICIEL PASSWORD MANAGER À N'IMPORTE QUEL MOMENT SANS PRÉAVIS.

SI LES DISPOSITIONS DE CET ARTICLE SONT NULLES POUR UNE RAISON QUELCONQUE OU SI LE FOURNISSEUR EST RÉPUTÉ RESPONSABLE DES PERTES, DES DOMMAGES, ETC... EN VERTU DES LOIS APPLICABLES, LES PARTIES CONVIENNENT QUE LA RESPONSABILITÉ DU FOURNISSEUR SE LIMITERA AU MONTANT TOTAL DES FRAIS DE LICENCE PAYÉS PAR VOUS.

VOUS ACCEPTEZ DE GARANTIR, DE DÉFENDRE ET DE PROTÉGER LE FOURNISSEUR AINSI QUE SES EMPLOYÉS, SES FILIALES, SES SOCIÉTÉS AFFILIÉES, SES PARTENAIRES DE MARQUE MODIFIÉE ET SES AUTRES PARTENAIRES CONTRE LES RÉCLAMATIONS, LES OBLIGATIONS, LES DOMMAGES, LES PERTES, LES COÛTS, LES DÉPENSES, LES FRAIS DE TOUTE PARTIE TIERCE (Y COMPRIS LES PROPRIÉTAIRES DU DISPOSITIF OU DES PARTIES DONT LES DROITS ONT ÉTÉ AFFECTÉS PAR LES DONNÉES UTILISÉES DANS LE LOGICIEL PASSWORD MANAGER OU DANS LA MÉMOIRE).

3. Données contenus dans le logiciel Password Manager. Sauf indication contraire et par choix explicite de votre part, toutes les données que vous saisissez et qui sont enregistrées dans une base de données du logiciel Password Manager sont stockées dans un format chiffré sur votre ordinateur ou sur tout autre périphérique de stockage tel que défini par vous. Vous comprenez que si l'une des bases de données du logiciel Password manager ou l'un des fichiers étaient supprimés ou endommagés, toutes les données qui y sont contenues seraient irréversiblement perdues et vous comprenez et acceptez le risque d'une telle perte. Le fait que vos données personnelles soient stockées dans un format chiffré sur l'ordinateur ne signifie pas que ces données ne peuvent pas être volées ou détournées par une personne qui découvre le mot de passe principal ou obtient l'accès au dispositif d'activation défini par le client permettant l'ouverture de la base de données. Vous êtes responsable de la sécurité de toutes les méthodes d'accès.

4. Transmission des données personnelles au Fournisseur ou à la Mémoire. Si vous sélectionnez cette option et uniquement dans le but d'assurer la synchronisation et la sauvegarde des données en temps opportun, le logiciel Password Manager transmet ou envoie des données personnelles de la base de données du logiciel Password Manager (c'est-à-dire, les mots de passe, les renseignements, les comptes et les identités de connexion) à la Mémoire par Internet. Les données sont transmises exclusivement sous la forme chiffrée. L'utilisation du logiciel Password Manager pour remplir des formulaires en ligne avec des mots de passe, des renseignements de

connexion ou d'autres données peut exiger que les informations soient transmises par Internet au site identifié par vous. Cette transmission de données n'est pas entreprise par le logiciel Password Manager; le Fournisseur ne peut donc pas être tenu pour responsable de la sécurité de ces interactions avec des sites Web gérés par divers fournisseurs. Toutes les transactions sur Internet en conjonction ou non avec le logiciel Password Manager se font à vos propres risques et périls, et vous serez seul responsable de tout dommage survenant à votre système informatique ou de toute perte de données résultant du téléchargement et/ou de l'utilisation de ce document ou service. Pour réduire le risque de perdre des données précieuses, le Fournisseur recommande aux clients d'effectuer une sauvegarde périodique de la base de données et d'autres fichiers délicats sur des unités de stockage externes. Le Fournisseur n'est pas en mesure de vous fournir une aide quelconque pour la récupération des données perdues ou endommagées. Si le Fournisseur offre des services de sauvegarde pour les fichiers de base de données de l'utilisateur en cas de dommage ou de suppression des fichiers sur les PC des utilisateurs, ce service de sauvegarde est sans aucune garantie et n'implique aucune responsabilité du Fournisseur envers vous.

En utilisant le logiciel Password Manager, vous acceptez que le logiciel puisse communiquer avec les serveurs du Fournisseur de temps en temps afin de vérifier les informations de licence, les correctifs disponibles, les ensembles de modifications provisoires et d'autres mises à jour qui peuvent améliorer, réparer, modifier ou améliorer le fonctionnement du logiciel Password Manager. Le logiciel peut envoyer des informations système générales relatives au fonctionnement du logiciel Password Manager.

5. Renseignements et instructions de désinstallation. Toute information que vous souhaitez conserver se trouvant dans la base de données doit être exportée avant la désinstallation du logiciel Password Manager.

Les dispositions complémentaires pour le logiciel Password Manager s'appliquent uniquement aux utilisateurs finaux de ESET Smart Security Premium.

ESET LiveGuard. Des dispositions complémentaires s'appliquent à ESET LiveGuard comme suit :

Le logiciel contient une fonction d’analyse supplémentaire des fichiers soumis par l’Utilisateur final. Le Fournisseur n'utilisera les fichiers soumis par l'Utilisateur final et les résultats de l'analyse que dans le respect de la Politique de confidentialité et conformément aux dispositions légales applicables.

Les dispositions complémentaires de ESET LiveGuard s'appliquent uniquement aux Utilisateurs finaux de ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Politique de confidentialité

La protection des données personnelles est d’une importance particulière pour ESET, spol. s r. o., ayant son siège social à Einsteinova 24, 851 01 Bratislava, Slovak Republic, enregistré au registre du commerce administré par le tribunal de district de Bratislava I, section Sro, insertion numéro 3586/B, numéro d’enregistrement de l’entreprise : 31333532 en tant que responsable du traitement des données (« ESET » ou « nous »). Nous voulons nous conformer à l’exigence de transparence telle qu'elle est légalement normalisée par le Règlement général sur la protection des données (« RGPD ») de l’UE. À cette fin, nous publions cette politique de confidentialité dans le seul but d'informer notre client (« utilisateur final » ou « vous ») en tant que personne concernée sur les sujets suivants relatifs à la protection des données personnelles :

- Base juridique du traitement des données personnelles,
- Partage des données et confidentialité
- Sécurité des données,

- Vos droits en tant que personne concernée,
- Traitement des données personnelles
- Information de contact.

Base juridique du traitement des données personnelles

Il n'existe que peu de bases juridiques pour le traitement des données que nous utilisons conformément au cadre législatif applicable en matière de protection des données à caractère personnel. Le traitement des données personnelles par ESET est principalement nécessaire pour l'exécution du Contrat de licence de l'utilisateur final (« CLUF ») avec l'utilisateur final (art. 6 (1) (b) RGPD), qui est applicable pour la fourniture de produits ou de services ESET, sauf indication contraire explicite, par exemple :

- La base juridique de l'intérêt légitime (art. 6 (1) (f) RGPD), qui nous permet de traiter les données sur la façon dont nos clients utilisent nos services et leur satisfaction afin de fournir à nos utilisateurs la meilleure protection, le meilleur soutien et la meilleure expérience que nous pouvons offrir. Même le marketing est reconnu par la législation en vigueur comme un intérêt légitime, c'est pourquoi nous nous en servons généralement pour la communication marketing avec nos clients.
- Le consentement (art. 6 (1) (a) RGPD), que nous pouvons vous demander dans des situations spécifiques lorsque nous estimons que cette base juridique est la plus appropriée ou si la loi l'exige.
- Le respect d'une obligation légale (art. 6 (1) (c) RGPD), par exemple la stipulation d'exigences en matière de communication électronique, la conservation des documents de facturation ou des factures.

Partage des données et confidentialité

Nous ne partageons pas vos données avec des tiers. Cependant, ESET est une société qui opère à l'échelle mondiale par l'intermédiaire de sociétés affiliées ou de partenaires dans le cadre de notre réseau de vente, de service et de soutien. Les informations de licence, de facturation et d'assistance technique traitées par ESET peuvent être transférées vers et depuis des sociétés affiliées ou des partenaires aux fins de l'exécution du CLUF, par exemple en fournissant des services ou une assistance.

ESET préfère traiter ses données dans l'Union européenne (UE). Cependant, en fonction de votre emplacement (utilisation de nos produits et/ou services en dehors de l'UE) et/ou du service que vous choisissez, il peut être nécessaire de transférer vos données vers un pays en dehors de l'UE. Par exemple, nous utilisons des services tiers pour l'informatique en nuage. Dans ces cas, nous sélectionnons soigneusement nos fournisseurs de services et garantissons un niveau approprié de protection des données par des mesures contractuelles, techniques et organisationnelles. En règle générale, nous adoptons les clauses contractuelles types de l'UE et, si nécessaire, des dispositions contractuelles complémentaires.

Pour certains pays hors de l'UE, comme le Royaume-Uni et la Suisse, l'UE a déjà déterminé un niveau comparable de protection des données. En raison du niveau comparable de protection des données, le transfert de données vers ces pays ne nécessite aucune autorisation ni accord spécial.

Sécurité des données

ESET met en œuvre des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté aux risques potentiels. Nous faisons de notre mieux pour assurer la confidentialité, l'intégrité, la disponibilité et la résilience permanentes des systèmes et des services de traitement. Toutefois, en cas de violation des données entraînant un risque pour vos droits et libertés, Nous sommes prêts à notifier l'autorité de

surveillance compétente ainsi que les utilisateurs finaux concernés en tant que personnes concernées.

Droits de la personne concernée

Les droits de chaque utilisateur final sont importants et nous aimerions vous informer que tous les utilisateurs finaux (de n'importe quel pays de l'UE ou hors de l'UE) ont les droits suivants garantis par ESET. Pour faire valoir les droits de la personne concernée, vous pouvez nous contacter par le biais du formulaire d'assistance ou par courriel à l'adresse suivante dpo@eset.sk. À des fins d'identification, nous vous demandons les informations suivantes : Nom, adresse de courriel et (si disponible) clé de licence ou numéro de client et entreprise à laquelle vous appartenez. Veuillez vous abstenir de nous envoyer d'autres données personnelles, telles que la date de naissance. Nous tenons à souligner que pour pouvoir traiter votre demande, ainsi qu'à des fins d'identification, nous traiterons vos données personnelles.

Droit de retrait du consentement. Le droit de retirer le consentement est applicable uniquement dans le cas où le traitement est autorisé moyennant le consentement. Si Nous traitons vos données personnelles moyennant votre consentement, vous avez le droit de retirer ce consentement à tout moment, sans donner de raisons. Le retrait de votre consentement n'est effectif que pour l'avenir et n'affecte pas la légalité des données traitées avant le retrait.

Droit d'opposition. Le droit de s'opposer au traitement est applicable en cas de traitement fondé sur l'intérêt légitime d'ESET ou d'un tiers. Si Nous traitons vos données personnelles pour protéger un intérêt légitime, Vous, en tant que personne concernée, avez le droit de vous opposer à l'intérêt légitime tel que nous l'identifions et au traitement de vos données personnelles à tout moment. Votre opposition est effective uniquement pour l'avenir et n'affecte pas la légalité des traitement de données effectués avant l'opposition. Si nous traitons vos données personnelles à des fins de marketing direct, il n'est pas nécessaire de motiver votre objection. Cela s'applique également au profilage, dans la mesure où il est lié à ce marketing direct. Dans tous les autres cas, nous vous demandons de nous informer brièvement de vos plaintes contre l'intérêt légitime d'ESET à traiter vos données personnelles.

Veuillez noter que dans certains cas, malgré le retrait de votre consentement, nous avons le droit de traiter ultérieurement vos données personnelles en nous fondant sur une autre base juridique, par exemple, pour l'exécution d'un contrat.

Droit d'accès. En tant que personne concernée, vous avez le droit d'obtenir gratuitement et à tout moment des informations sur vos données stockées par ESET.

Droit à la rectification. Si nous traitons par inadvertance des données personnelles incorrectes vous concernant, vous avez le droit de les faire corriger.

Droit à la suppression et droit à la restriction du traitement. En tant que personne concernée, vous avez le droit de demander la suppression ou la restriction du traitement de vos données personnelles. Par exemple, si nous traitons vos données personnelles avec votre consentement, que vous retirez ce consentement et qu'il n'existe aucune autre base juridique, par exemple un contrat, nous supprimons immédiatement vos données personnelles. Vos données personnelles seront également supprimées dès qu'elles ne seront plus nécessaires aux fins énoncées à la fin de notre période de conservation.

Si nous utilisons vos données personnelles dans le seul but de marketing direct et que vous avez révoqué votre consentement ou que vous vous êtes opposé à l'intérêt légitime sous-jacent d'ESET, nous limiterons le traitement de vos données personnelles dans la mesure où nous incluons vos coordonnées dans notre liste noire interne afin d'éviter tout contact non sollicité. Dans les autres cas, vos données personnelles seront supprimées.

Veuillez noter que Nous pouvons être tenus de conserver vos données jusqu'à l'expiration des obligations et des

périodes de conservation émises par le législateur ou les autorités de contrôle. Les obligations et les périodes de conservation peuvent également résulter de la législation slovaque. Par la suite, les données correspondantes seront systématiquement supprimées.

Le droit à la portabilité des données. Nous sommes heureux de vous fournir, en tant que personne concernée, les données personnelles traitées par ESET au format xls.

Droit de déposer une plainte. En tant que personne concernée, vous avez le droit de déposer une plainte auprès d'une autorité de surveillance à tout moment. ESET est soumis à la réglementation des lois slovaques et nous sommes liés par la législation sur la protection des données dans le cadre de l'Union européenne. L'autorité de surveillance des données compétente est l'Office for Personal Data Protection of the Slovak Republic (Office pour la protection des données personnelles de la République slovaque), dont l'adresse est Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Traitement des données personnelles

Les services fournis par ESET mis en œuvre dans notre produit sont fournis conformément aux conditions du CLUF, mais certaines d'entre elles peuvent nécessiter une attention particulière. Nous aimerions vous fournir plus de détails sur la collecte de données liées à la fourniture de nos services. Nous fournissons différents services décrits dans le CLUF et la documentation. À cette fin, nous devons recueillir les renseignements suivants :

Données de licence et de facturation. Le nom, l'adresse courriel, la clé de licence et (le cas échéant) l'adresse, la société à laquelle vous appartenez et les données de paiement sont collectées et traitées par ESET afin de faciliter l'activation de la licence, la livraison de la clé de licence, les rappels d'expiration, les demandes d'assistance, la vérification de l'authenticité de la licence, la fourniture de notre service et d'autres notifications, y compris les messages de marketing, conformément à la législation applicable ou à votre consentement. ESET est légalement obligé de conserver les informations de facturation pour une période de 10 ans, mais les informations de licence seront rendues anonymes au plus tard 12 mois après l'expiration de la licence.

Mise à jour et autres statistiques. Les informations traitées comprennent des informations relatives au processus d'installation et à votre ordinateur, y compris la plate-forme sur laquelle notre produit est installé, ainsi que des informations sur le fonctionnement et la fonctionnalité de nos produits, telles que le système d'exploitation, les informations sur le matériel, les identifiants d'installation, les identifiants de licence, l'adresse IP, l'adresse MAC, les paramètres de configuration du produit, qui sont traitées dans le but de fournir des services de mise à jour et de mise à niveau et dans le but d'assurer la maintenance, la sécurité et l'amélioration de notre infrastructure dorsale.

Ces informations sont séparées des informations d'identification requises pour l'octroi de licences et la facturation, car elles ne nécessitent pas l'identification de l'utilisateur final. La durée de conservation est de 4 ans maximum.

Système de réputation ESET LiveGrid®. Des hachages unidirectionnels liés aux infiltrations sont effectués pour le système de réputation de ESET LiveGrid®, ce qui améliore l'efficacité de nos solutions anti-logiciel malveillant en comparant les fichiers analysés à une base de données d'éléments en liste blanche et en liste noire dans le nuage. L'utilisateur final n'est pas identifié au cours de ce processus.

Système de rétroaction ESET LiveGrid®. Des échantillons suspects et des métadonnées existants dans le cadre du système de rétroaction ESET LiveGrid®, qui permettent à ESET de réagir immédiatement aux besoins de nos utilisateurs finaux et de rester réactif face aux dernières menaces. Nous comptons sur Vous pour nous envoyer

- Des infiltrations telles que des échantillons potentiels de virus et d'autres programmes malveillants et suspects; des objets problématiques, potentiellement indésirables ou potentiellement dangereux, tels que des

fichiers exécutables, des messages électroniques signalés par vous comme pourriel ou marqués par notre produit;

- Des renseignements concernant l'utilisation d'Internet telles que l'adresse IP et les informations géographiques, les paquets IP, les URL et les trames ethernet;

- Les fichiers de vidage sur incident et les informations qu'il contient.

Nous ne souhaitons pas collecter vos données en dehors de ce cadre, mais il est parfois impossible de l'éviter. Les données collectées accidentellement peuvent être incluses dans les logiciels malveillants eux-mêmes (collectées à votre insu ou sans votre accord) ou dans des noms de fichiers ou des URL. Nous ne souhaitons pas qu'elles fassent partie de nos systèmes; nous ne les traitons pas non plus aux fins déclarées dans la présente politique de confidentialité.

Toutes les informations obtenues et traitées par le système de rétroaction ESET LiveGrid® sont destinées à être utilisées sans identification de l'utilisateur final.

Évaluation de la sécurité des périphériques connectés au réseau. Pour fournir la fonction d'évaluation de la sécurité, nous traitons le nom du réseau local et les informations sur les périphériques de votre réseau local, telles que la présence, le type, le nom, l'adresse IP et l'adresse MAC du périphérique dans votre réseau local en relation avec les informations sur la licence. Les informations incluent également le type de sécurité pour sans fil et le type de chiffrement pour sans fil des périphériques de routeur. Les informations relatives à la licence permettant d'identifier l'utilisateur final seront rendues anonymes au plus tard 12 mois après l'expiration de la licence.

Assistance technique. Les coordonnées et les informations de licence ainsi que les données contenues dans vos demandes d'assistance peuvent être nécessaires au service d'assistance. En fonction du moyen que vous choisissez pour nous contacter, nous pouvons recueillir votre adresse de courriel, votre numéro de téléphone, les renseignements de licence, les détails du produit et la description de votre dossier d'assistance. Vous pouvez être invité à nous fournir d'autres renseignements pour faciliter le service d'assistance. Les données traitées pour l'assistance technique sont stockées pendant 4 ans.

Protection contre l'utilisation abusive des données. Si le compte ESET HOME sur https://home.eset.com est créé et que la fonction est activée par l'utilisateur final à la suite du vol de l'ordinateur, les informations suivantes seront collectées et traitées : les données de localisation, les captures d'écran, les données relatives à la configuration de l'ordinateur et les données enregistrées par la caméra de l'ordinateur. Les données collectées sont stockées sur nos serveurs ou sur les serveurs de nos fournisseurs de services avec une durée de conservation de 3 mois.

Password Manager Si vous choisissez d'activer la fonction Password Manager, les données relatives à vos données de connexion sont stockées sous une forme chiffrée uniquement sur votre ordinateur ou un autre périphérique désigné. Si vous activez le service de synchronisation, les données chiffrées seront entreposées sur nos serveurs ou ceux de nos fournisseurs de service afin d'assurer ledit service. Ni ESET ni le fournisseur de services n'ont accès aux données chiffrées. Vous seul avez la clé pour déchiffrer les données. Les données seront supprimées lors de la désactivation de la fonction.

ESET LiveGuard. Si vous choisissez d'activer la fonction ESET LiveGuard, sachez que des échantillons tels que des fichiers prédéfinis et sélectionnés par l'utilisateur final nous seront envoyés. Les échantillons que vous choisissez pour l'analyse à distance seront téléchargés vers le service ESET, et le résultat de l'analyse sera renvoyé sur votre ordinateur. Tout échantillon suspect est traité conformément aux informations recueillies par le système de rétroaction ESET LiveGrid®.

Programme d'amélioration de l'expérience client. Si vous avez choisi d'activer le Programme d'amélioration de

l'expérience client , les informations de télémétrie anonymes relatives à l'utilisation de nos produits seront collectées et utilisées avec votre consentement.

Veuillez noter que si la personne qui utilise nos produits et services n'est pas l'utilisateur final qui a acheté le produit ou le service et a conclu le CLUF avec nous, (par exemple, un employé de l'utilisateur final, un membre de la famille ou une personne autrement autorisée à utiliser le produit ou le service par l'utilisateur final conformément au CLUF, le traitement des données est effectué dans l'intérêt légitime d'ESET au sens de l'article 6 (1) f) du RGPD pour permettre à l'utilisateur autorisé par l'utilisateur final d'utiliser les produits et services que nous fournissons conformément au CLUF.

Information de contact

Si vous souhaitez exercer votre droit en tant que personne concernée ou si vous avez une question ou une préoccupation, envoyez-nous un message à l'adresse suivante :

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk