ESET NOD32 Antivirus

Guide de l'utilisateur

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

Digital Security
Progress. Protected.

ESET NOD32 Antivirus a été développé par ESET, spol. s r.o.

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

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

RÉV. 12/04/2024

ESET NOD32 Antivirus

ESET NOD32 Antivirus représente une nouvelle approche de sécurité informatique véritablement intégrée. La dernière version du moteur d'analyse ESET LiveGrid® garantit la sécurité de votre ordinateur avec grande précision et rapidité. Le résultat est un système intelligent et constamment en alerte, qui protège votre ordinateur des attaques et des programmes malveillants.

ESET NOD32 Antivirus est une solution de sécurité complète qui associe protection maximale et encombrement minimal. Nos technologies avancées se servent de l'intelligence artificielle pour empêcher l'infiltration de virus, de logiciels espions, de chevaux de Troie, de vers, de logiciels publicitaires, de rootkits et d'autres menaces, sans réduire les performances ni perturber votre ordinateur.

Fonctionnalités et avantages

Nouvelle interface utilisateur	L'interface utilisateur de cette version a été redéfinie et simplifiée en fonction des résultats des tests d'ergonomie. Tous les messages et notifications de l'interface graphique ont été examinés avec soin, et l'interface prend désormais en charge les langues telles que l'arabe et l'hébreu qui s'écrivent de droite à gauche. L'aide en ligne est désormais intégrée dans ESET NOD32 Antivirus et propose automatiquement des contenus de support mis à jour.
Mode sombre	Extension qui permet de passer rapidement l'écran dans un thème sombre. Vous pouvez choisir votre modèle de couleurs préféré dans les 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, connus et inconnus. La technologie d'heuristique avancée reconnaît même les logiciels malveillants jamais rencontrés auparavant ; elle vous protège des menaces inconnues et les neutralise avant qu'elles ne puissent causer le moindre dommage à votre ordinateur. La protection de l'accès web et l'anti-hameçonnage surveillent les communications entre les navigateurs internet et les serveurs distants (y compris SSL). La protection du client de messagerie contrôle les communications par courrier électronique reçues via les protocoles POP3(S) et IMAP(S).
Mises à jour régulières	La mise à jour régulière du moteur de détection (précédemment appelé « base des signatures de virus ») et des modules de programme est la meilleure méthode pour bénéficier d'un niveau maximum de sécurité sur votre ordinateur.
ESET LiveGrid® (Évaluation de la réputation effectuée par le service de Cloud)	Vous pouvez vous informer de la réputation des processus et des fichiers en cours d'exécution à partir de ESET NOD32 Antivirus.
Contrôle de périphérique	Analyse automatiquement toutes les clés USB, cartes mémoire et CD/DVD. Bloque les supports amovibles selon le type de support, le fabricant, la taille et d'autres attributs.
Fonctionnalité HIPS (Host Intrusion Prevention System)	Vous pouvez personnaliser le comportement du système de manière plus poussée : spécifier des règles pour le registre système, activer les processus et les programmes et optimiser votre niveau de sécurité.
Mode joueur	Diffère toutes les fenêtres contextuelle, les mises à jour ou les autres activités intensives du système pour économiser les ressources système au bénéfice du jeu et d'autres activités en plein écran.

Un abonnement doit être actif pour que les fonctionnalités d'ESET NOD32 Antivirus soient opérationnelles. Nous vous recommandons de renouveler votre abonnement ESET NOD32 Antivirus plusieurs semaines avant son expiration.

Nouveautés

Nouveautés d'ESET NOD32 Antivirus 17.1

- Petites améliorations apportées à l'Inspecteur de réseau
- Autres corrections de bogues et améliorations mineures

> Pour désactiver les **notifications de nouveautés** :
> 1. Ouvrez Configurations avancées > **Notifications** > **Notifications du Bureau**.
> 2. Cliquez sur **Modifier** en regard de **Notifications du Bureau**.
> 3. Décochez la case **Afficher les notifications de 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 NOD32 Antivirus, consultez les journaux des modifications ESET NOD32 Antivirus.

Quel produit est installé sur mon ordinateur ?

ESET offre plusieurs couches de sécurité à l'aide de nouveaux produits qui vont d'une solution antivirus puissante et rapide à une solution 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 quel produit est installé sur votre ordinateur, ouvrez la fenêtre principale du programme. Le nom du produit apparaît en haut de la fenêtre (voir l'article de la base de connaissances).

Le tableau ci-dessous présente les fonctionnalités disponibles dans chaque produit.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Moteur de détection	✔	✔	✔	✔
Apprentissage machine avancé	✔	✔	✔	✔
Bloqueur d'exploit	✔	✔	✔	✔
Protection contre les attaques basées sur des scripts	✔	✔	✔	✔
Antihameçonnage	✔	✔	✔	✔
Protection de l'accès Web	✔	✔	✔	✔
HIPS (incluant le Bouclier anti-ransomwares)	✔	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Antispam		✔	✔	✔
Pare-feu		✔	✔	✔
Inspecteur de réseau		✔	✔	✔
Protection de la Webcam		✔	✔	✔
Protection contre les attaques réseau		✔	✔	✔
Protection anti-botnet		✔	✔	✔
Transactions bancaires et navigation sécurisées		✔	✔	✔
Confidentialité et sécurité du navigateur		✔	✔	✔
Contrôle parental		✔	✔	✔
Antivol		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Certains produits indiqués ci-dessus peuvent ne pas être disponibles dans votre langue/zone géographique.

Configuration système requise

Pour un fonctionnement optimal de ESET NOD32 Antivirus, votre système doit répondre à la configuration matérielle et logicielle requise suivante :

Processeurs pris en charge

Processeur Intel ou AMD 32 bits (x86) avec un jeu d’instructions SSE2 ou 64 bits (x64), 1 GHz ou vitesse supérieure processeur ARM64, 1 GHz ou vitesse supérieure

Système d'exploitation pris en charge

Microsoft® Windows® 11

Microsoft® Windows® 10

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

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

Configuration requise pour les fonctionnalités ESET NOD32 Antivirus

Consultez la configuration requise pour des fonctionnalités ESET NOD32 Antivirus spécifiques dans le tableau suivant :

Fonctionnalité	Configuration requise
Intel® Threat Detection Technology	Consultez les processeurs pris en charge.
Arrière-plan transparent	Windows 10 version RS4 et version ultérieure.
Outil de nettoyage spécialisé	Processeur autre que ARM64.
Outil de nettoyage système	Processeur autre que ARM64.
Bloqueur d'exploit	Processeur autre que ARM64.
Inspection comportementale approfondie	Processeur autre que ARM64.

Autre

Une connexion Internet est nécessaire pour que l'activation et les mises à jour d'ESET NOD32 Antivirus fonctionnent correctement.

Deux programmes antivirus qui s’exécutent simultanément sur un seul appareil entraînent des conflits de ressources système inévitables, tels que le ralentissement du système pour le rendre inexploitable.

Version obsolète de Microsoft Windows

Problème

- Vous souhaitez installer la dernière version d'ESET NOD32 Antivirus sur un ordinateur sous Windows 7, Windows 8 (8.1) ou Windows Home Server 2011.
- ESET NOD32 Antivirus affiche l'erreur **Système d'exploitation obsolète** pendant l’installation.

Détails

La dernière version d'ESET NOD32 Antivirus requiert les systèmes d’exploitation Windows 10 ou Windows 11.

Solution

Les solutions disponibles sont les suivantes :

Mise à niveau vers Windows 10 ou Windows 11

La mise à niveau est relativement simple. De plus, dans la plupart des cas, vous pouvez l'effectuer sans perdre de fichiers. Avant d'effectuer une mise à niveau vers Windows 10 :

1. Sauvegarder les données importantes.

2. Lisez le FAQ sur la mise à niveau vers Windows 10 ou le FAQ sur la mise à niveau vers Windows 11 de Microsoft et mettez à jour votre système d'exploitation Windows.

Installation d'ESET NOD32 Antivirus version 16.0

Si vous ne pouvez pas mettre à niveau Windows, installez ESET NOD32 Antivirus version 16.0. Pour plus d'informations, reportez-vous à l'aide en ligne d'ESET NOD32 Antivirus version 16.0.

Prévention

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

Mise à jour régulièrement

Selon les statistiques d'ESET 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 ESET analysent ces menaces chaque jour et conçoivent des mises à jour pour améliorer continuellement le niveau de protection des utilisateurs. Pour assurer l'efficacité maximale de ces mises à jour, il est important que les mises à jour soient configurées correctement dans votre système. Pour plus d'informations sur la procédure de configuration des mises à jour, reportez-vous au chapitre Configuration des mises à jour.

Télécharger les patchs de sécurité

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

Sauvegarder les données importantes

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

Rechercher régulièrement les virus sur votre ordinateur

La détection de virus, de vers, de chevaux de Troie et de rootkits, connus et inconnus, est gérée par le module de protection du système de fichiers en temps réel. Cela signifie qu'à chaque fois que vous accédez à un fichier ou que vous l'ouvrez, il est analysé afin de détecter toute trace de logiciels malveillants. Nous vous recommandons de lancer une analyse complète de l'ordinateur au moins une fois par mois, car les logiciels malveillants peuvent varier et le moteur de détection est quotidiennement mis à jour.

Suivre les règles de sécurité de base

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

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

Pages d'aide

Bienvenue dans le guide de l'utilisateur ESET NOD32 Antivirus. Les informations fournies ici permettent de vous présenter le produit et vous aident à sécuriser votre ordinateur.

Mise en route

Avant d'utiliser ESET NOD32 Antivirus, vous pouvez lire des informations sur les différents types de détections et les attaques distantes auxquels vous êtes exposé lorsque vous utilisez votre ordinateur. Nous avons également créé une liste des nouvelles fonctionnalités introduites dans ESET NOD32 Antivirus.

Commencez par installer ESET NOD32 Antivirus. Si ESET NOD32 Antivirus est déjà installé, consultez Utilisation d'ESET NOD32 Antivirus.

Utilisation des pages d'aide ESET NOD32 Antivirus

L'aide en ligne est divisée en plusieurs chapitres et sous-chapitres. Appuyez sur **F1** dans ESET NOD32 Antivirus pour afficher des informations sur la fenêtre actuellement ouverte.

Le programme permet de rechercher une rubrique d'aide au moyen de mots-clés ou en tapant des mots ou des expressions. 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 expressions examine le contenu de toutes les pages et affiche uniquement les pages contenant effectivement le mot ou l'expression en question.

Pour des questions de cohérence et afin d'éviter toute confusion, la terminologie employée dans ce guide est basée sur l'interface utilisateur d'ESET NOD32 Antivirus. Un ensemble uniforme de symboles est également utilisé pour souligner des informations importantes.

> Une remarque est une simple observation succincte. Bien que vous puissiez l'ignorer, elle peut fournir des informations précieuses (fonctionnalités spécifiques ou lien vers une rubrique connexe, par exemple).

Votre attention est requise. Il s'agit généralement d'informations importantes mais qui ne sont pas critiques.

Il s'agit d'informations qui demandent une attention particulière. Les avertissements ont pour but de vous empêcher de commettre des erreurs préjudiciables. Lisez attentivement le texte car il fait référence à des paramètres système très sensibles ou à des actions présentant des risques.

Il s'agit d'un cas pratique qui vise à vous aider à comprendre l'utilisation d'une fonctionnalité spécifique.

Convention	Signification
Gras	Noms des éléments de l'interface (boutons d'option ou boîtes de dialogue, par exemple).
Italique	Espaces réservés pour les informations que vous fournissez. Par exemple, nom du fichier ou chemin d'accès indique que vous devez saisir un chemin d'accès ou un nom de fichier.
`Courier New`	Exemples de code ou commandes.
Lien hypertexte	Permet d'accéder facilement et rapidement à des références croisées ou à une adresse Internet externe. Les liens hypertexte sont mis en surbrillance en bleu et peuvent être soulignés.
%ProgramFiles%	Répertoire du système Windows dans lequel sont stockés les programmes installés sous Windows.

L'**aide en ligne** est la principale source de contenu d'aide. La dernière version de l'aide en ligne s'affiche automatiquement lorsque vous disposez d'une connexion Internet.

Installation

Il existe différentes méthodes pour installer ESET NOD32 Antivirus sur votre ordinateur. Les méthodes d'installation peuvent varier en fonction du pays et du mode de distribution :

- Programme d'installation Live Installer : téléchargé à partir du site web d'ESET ou du CD/DVD. Le package d'installation est universel pour toutes les langues (choisissez la langue appropriée). Le programme d'installation Live Installer est un fichier de petite taille ; les fichiers supplémentaires nécessaires à l'installation d'ESET NOD32 Antivirus sont téléchargés automatiquement.

- Installation hors connexion : utilise un fichier .exe qui est plus volumineux que le fichier Live installer et qui ne nécessite pas de connexion à Internet ou de fichiers supplémentaires pour réaliser l'installation.

Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur avant d'installer ESET NOD32 Antivirus. Si plusieurs solutions antivirus sont installées sur un même ordinateur, elles risquent de provoquer des conflits. Nous recommandons de désinstaller tout autre antivirus de votre système. Reportez-vous à notre article de la base de connaissances pour obtenir une liste des outils de désinstallation des logiciels antivirus courants (disponible en anglais et dans plusieurs autres langues).

Live installer

Lorsque vous avez téléchargé le package d'installation Live installer, double-cliquez sur le fichier d'installation et suivez les instructions indiquées dans l'assistant d'installation.

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

1. Sélectionnez la langue adéquate dans le menu déroulant, puis cliquez sur **Continuer**.

> Si vous installez une version plus récente par rapport à la précédente dont les paramètres sont protégés par mot de passe, saisissez le mot de passe. Vous pouvez configurer le mot de passe de paramètres dans la configuration de l'accès.

2. Sélectionnez vos préférences pour les fonctionnalités suivantes, lisez le Contrat de licence de l'utilisateur final et la Politique de confidentialité. Cliquez ensuite sur **Continuer** ou sur **Tout autoriser et continuer** pour activer toutes les fonctionnalités :

- Système de commentaire ESET LiveGrid®
- Applications potentiellement indésirables
- Programme d\'amélioration du produit

> En cliquant sur **Continuer** ou **Tout autoriser et continuer**, vous acceptez les termes du 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 de l'appareil à l'aide du ESET HOME, connectez votre appareil au compte ESET HOME. Cliquez sur **Ignorer la connexion** pour continuer sans vous connecter à ESET HOME. Vous pouvez connecter votre appareil à votre compte ESET HOME ultérieurement.

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

5. L'Assistant d'installation détermine le produit ESET installé en fonction de votre abonnement. La version avec le plus de fonctionnalités de sécurité est toujours présélectionnée. Cliquez sur **Changer de produit** si vous souhaitez installer une autre version du produit ESET. Cliquez sur **Continuer** pour lancer le processus d'installation. Cette opération peut prendre quelques minutes.

S'il reste des fichiers ou des dossiers de produits ESET désinstallés auparavant, vous êtes invité à autoriser leur suppression. Cliquez sur **Installer** pour continuer.

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

Dépanneur d'installation.

Une fois le produit installé et activé, le téléchargement des modules commence. La protection est initialisée et certaines fonctionnalités peuvent ne pas être entièrement fonctionnelles jusqu'à la fin du téléchargement.

Installation hors connexion

Téléchargez et installez votre produit ESET Windows pour les particuliers à l'aide du programme d'installation hors ligne (.exe) ci-dessous. Choisissez la version du produit ESET pour les particuliers 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 à l'aide d'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 de configuration.

1. Sélectionnez la langue adéquate dans le menu déroulant, puis cliquez sur **Continuer**.

Si vous installez une version plus récente par rapport à la précédente dont les paramètres sont protégés par mot de passe, saisissez le mot de passe. Vous pouvez configurer le mot de passe de paramètres dans la configuration de l'accès.

2. Sélectionnez vos préférences pour les fonctionnalités suivantes, lisez le Contrat de licence de l'utilisateur final et la Politique de confidentialité. Cliquez ensuite sur **Continuer** ou sur **Tout autoriser et continuer** pour activer toutes les fonctionnalités :

- Système de commentaire ESET LiveGrid®
- Applications potentiellement indésirables
- Programme d\'amélioration du produit

En cliquant sur **Continuer** ou **Tout autoriser et continuer**, vous acceptez les termes du 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 appareil à votre compte ESET HOME.

4. Cliquez sur **Ignorer l'activation**. ESET NOD32 Antivirus doit être activé après l'installation pour être entièrement fonctionnel. L'activation du produit nécessite une connexion Internet active.

5. L'Assistant d'installation indique quel produit ESET sera installé selon le programme d'installation hors ligne téléchargé. Cliquez sur **Continuer** pour lancer le processus d'installation. Cette opération peut prendre quelques minutes.

S'il reste des fichiers ou des dossiers de produits ESET désinstallés auparavant, vous êtes invité à autoriser leur suppression. Cliquez sur **Installer** pour continuer.

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

Dépanneur d'installation.

L'abonnement mise à niveau

Cette notification apparaît lorsque l'abonnement utilisé pour activer votre produit ESET a été modifié. L'abonnement modifié vous permet d'activer un produit comportant des fonctionnalités de sécurité supplémentaires. Si aucune modification n'a été effectuée, ESET NOD32 Antivirus affiche une fenêtre d'alerte une fois, appelée **Passez à un produit avec des fonctionnalités supplémentaires**.

Oui (recommandé) : permet d'installer automatiquement le produit avec des fonctionnalités de sécurité supplémentaires.

Non merci : aucune modification n'est apportée et la notification disparaît de manière permanente.

Pour modifier ultérieurement le produit, reportez-vous à cet article de la base de connaissances ESET. Pour plus d'informations sur les abonnements ESET, consultez FAQ sur les abonnements.

Le tableau ci-dessous présente les fonctionnalités disponibles dans chaque produit.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Moteur de détection	✔	✔	✔	✔
Apprentissage machine avancé	✔	✔	✔	✔
Bloqueur d'exploit	✔	✔	✔	✔
Protection contre les attaques basées sur des scripts	✔	✔	✔	✔
Antihameçonnage	✔	✔	✔	✔
Protection de l’accès Web	✔	✔	✔	✔
HIPS (incluant le Bouclier anti-ransomwares)	✔	✔	✔	✔
Antispam		✔	✔	✔
Pare-feu		✔	✔	✔
Inspecteur de réseau		✔	✔	✔
Protection de la Webcam		✔	✔	✔
Protection contre les attaques réseau		✔	✔	✔
Protection anti-botnet		✔	✔	✔
Transactions bancaires et navigation sécurisées		✔	✔	✔
Confidentialité et sécurité du navigateur		✔	✔	✔
Contrôle parental		✔	✔	✔
Antivol		✔	✔	✔
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 avez décidé de changer le produit à activer ou vous souhaitez remplacer le produit installé par un produit avec des fonctionnalités de sécurité supplémentaires.

Changer de produit pendant l’installation.

Le tableau ci-dessous présente les fonctionnalités disponibles dans chaque produit.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Moteur de détection	✔	✔	✔	✔
Apprentissage machine avancé	✔	✔	✔	✔
Bloqueur d'exploit	✔	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Protection contre les attaques basées sur des scripts	✔	✔	✔	✔
Antihameçonnage	✔	✔	✔	✔
Protection de l’accès Web	✔	✔	✔	✔
HIPS (incluant le Bouclier anti-ransomwares)	✔	✔	✔	✔
Antispam		✔	✔	✔
Pare-feu		✔	✔	✔
Inspecteur de réseau		✔	✔	✔
Protection de la Webcam		✔	✔	✔
Protection contre les attaques réseau		✔	✔	✔
Protection anti-botnet		✔	✔	✔
Transactions bancaires et navigation sécurisées		✔	✔	✔
Confidentialité et sécurité du navigateur		✔	✔	✔
Contrôle parental		✔	✔	✔
Antivol		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Abonnement passer à une version antérieure

Cette boîte de dialogue apparaît lorsque l'abonnement utilisé pour activer votre produit ESET a été modifié. L'abonnement modifié ne peut être utilisé qu'avec un autre produit ESET comportant moins de fonctionnalités de sécurité. Le produit a été modifié automatiquement pour éviter toute perte de protection.

Pour plus d'informations sur les abonnements ESET, consultez FAQ sur les abonnements.

Le tableau ci-dessous présente les fonctionnalités disponibles dans chaque produit.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Moteur de détection	✔	✔	✔	✔
Apprentissage machine avancé	✔	✔	✔	✔
Bloqueur d'exploit	✔	✔	✔	✔
Protection contre les attaques basées sur des scripts	✔	✔	✔	✔
Antihameçonnage	✔	✔	✔	✔
Protection de l’accès Web	✔	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
HIPS (incluant le Bouclier anti-ransomwares)	✔	✔	✔	✔
Antispam		✔	✔	✔
Pare-feu		✔	✔	✔
Inspecteur de réseau		✔	✔	✔
Protection de la Webcam		✔	✔	✔
Protection contre les attaques réseau		✔	✔	✔
Protection anti-botnet		✔	✔	✔
Transactions bancaires et navigation sécurisées		✔	✔	✔
Confidentialité et sécurité du navigateur		✔	✔	✔
Contrôle parental		✔	✔	✔
Antivol		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Version antérieure du produit

Le produit actuellement installé possède d’autres fonctionnalités de sécurité que celles que vous allez activer.

Le tableau ci-dessous présente les fonctionnalités disponibles dans chaque produit.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Moteur de détection	✔	✔	✔	✔
Apprentissage machine avancé	✔	✔	✔	✔
Bloqueur d'exploit	✔	✔	✔	✔
Protection contre les attaques basées sur des scripts	✔	✔	✔	✔
Antihameçonnage	✔	✔	✔	✔
Protection de l’accès Web	✔	✔	✔	✔
HIPS (incluant le Bouclier anti-ransomwares)	✔	✔	✔	✔
Antispam		✔	✔	✔
Pare-feu		✔	✔	✔
Inspecteur de réseau		✔	✔	✔
Protection de la Webcam		✔	✔	✔
Protection contre les attaques réseau		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Protection anti-botnet		✔	✔	✔
Transactions bancaires et navigation sécurisées		✔	✔	✔
Confidentialité et sécurité du navigateur		✔	✔	✔
Contrôle parental		✔	✔	✔
Antivol		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Dépanneur d'installation

Si des problèmes se produisent pendant l'installation, l'Assistant d'installation propose un dépanneur qui les résout, si cela est possible.

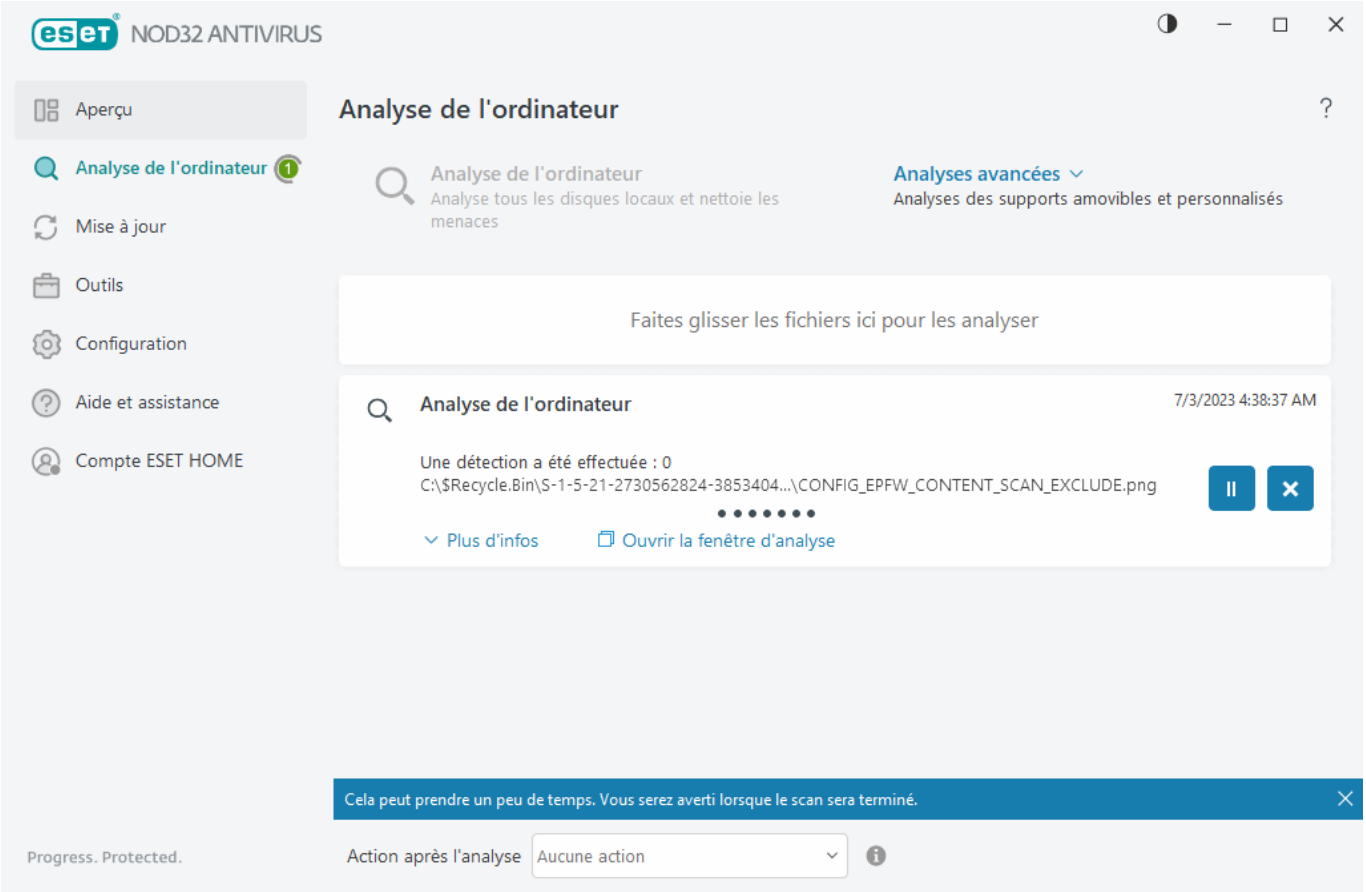
Cliquez sur **Exécuter le dépanneur** pour lancer le dépanneur. Une fois que le dépanneur a terminé, suivez la solution recommandée.

Si le problème persiste, consultez la liste des erreurs d'installation courantes et des résolutions.

Première analyse après l'installation

Après l'installation d'ESET NOD32 Antivirus, une analyse de l'ordinateur démarrera automatiquement après une première mise à jour, afin de rechercher du code malveillant.

Vous pouvez également lancer manuellement une analyse de l'ordinateur depuis la fenêtre principale du programme, en cliquant sur **Analyse de l'ordinateur** > **Analyse intelligente**. Pour plus d'informations sur l'analyse d'ordinateur, reportez-vous à la section Analyse d'ordinateur.



Mise à niveau vers une nouvelle version

Les nouvelles versions d'ESET NOD32 Antivirus offrent des améliorations ou apportent des solutions aux problèmes que les mises à jour automatiques des modules de programme ne peuvent pas résoudre. La mise à niveau vers une version ultérieure peut s'effectuer de différentes manières :

1. Automatiquement, par l'intermédiaire d'une mise à jour du programme.
Les mises à niveau du programme sont distribuées à tous les utilisateurs et peuvent avoir un impact sur certaines configurations système. Elles sont par conséquent mises à disposition après de longues périodes de test afin que leur fonctionnement soit correct sur toutes les configurations système. Pour effectuer la mise à niveau vers une nouvelle version dès que celle-ci est disponible, utilisez l'une des méthodes ci-dessous. Vérifiez que vous avez activé l'option **Mises à jour des fonctionnalités de l'application** dans Configuration avancée > **Mise à jour** > **Profils** > **Mises à jour**.

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

3. Manuellement, en téléchargeant la nouvelle version et en l'installant sur l'installation précédente.

Pour obtenir des informations supplémentaires et des instructions illustrées, voir :

- Mettre à jour les produits ESET—rechercher les derniers modules des produits
- Quels sont les différents types de versions et de mises à jour des produits ESET ?

Mise à niveau automatique des anciens produits

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

Problèmes d'installation courants

Chaque nouvelle version des produits ESET comporte plusieurs correctifs de bogue et améliorations. Les clients existants disposant d'un abonnement valide pour un produit ESET peuvent procéder gratuitement à une mise à niveau vers la version la plus récente du même produit.

Pour terminer l’installation :

1. Cliquez sur **Accepter et continuer** pour accepter les termes du Contrat de licence de l’utilisateur final et reconnaître avoir pris connaissance de la Politique de confidentialité. Si vous n’êtes pas d’accord avec les termes du Contrat de licence de l’utilisateur final, cliquez sur **Désinstaller**. Vous ne pouvez pas revenir à la version précédente.

2. Cliquez sur **Tout autoriser et continuer** pour autoriser le système de commentaires ESET LiveGrid® et le programme d'amélioration du produit ou cliquez sur **Continuer** si vous ne souhaitez pas participer à ce programme.

3. Une fois le nouveau produit ESET activé avec votre clé d'activation, la page Vue d'ensemble s'affiche. Si les informations de votre abonnement sont introuvables, poursuivez avec une version d'essai gratuite. Si l'abonnement utilisé pour le produit précédent n'est pas valide, activez votre produit ESET.

4. Un redémarrage de l’appareil est nécessaire pour terminer l’installation.

ESET NOD32 Antivirus va être installé

Cette boîte de dialogue peut s’afficher :

- Pendant l’installation – Cliquez sur **Continuer** pour installer ESET NOD32 Antivirus.

- Lors de la modification d'un abonnement dans ESET NOD32 Antivirus – Cliquez sur **Activer** pour modifier l'abonnement et activer ESET NOD32 Antivirus.

L'option **Changer de produit**, permet de basculer entre les produits pour les particuliers ESET Windows selon votre abonnement ESET. Pour plus d'informations, consultez Quel produit est installé sur mon ordinateur ?.

Passage à un autre produit

Selon votre abonnement ESET, vous pouvez basculer entre différents produits pour les particuliers ESET Windows. Pour plus d'informations, consultez Quel produit est installé sur mon ordinateur ?.

Enregistrement

Veuillez enregistrer votre abonnement en renseignant les champs contenus dans le formulaire d'enregistrement, puis en cliquant sur **Activer**. Les champs signalés comme obligatoires sont requis. Ces informations seront utilisées uniquement pour les questions liées à votre abonnement ESET.

Progression de l'activation

Patientez quelques secondes jusqu'à la fin du processus d'activation (le temps nécessaire peut varier en fonction de la vitesse de votre connexion Internet ou de votre ordinateur).

Activation réussie

Le processus d'activation est terminé.

Une mise à jour de module commencera dans quelques secondes. Les mises à jour régulières d'ESET NOD32 Antivirus commenceront immédiatement.

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

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

Guide du débutant

Ce chapitre donne un premier aperçu d'ESET NOD32 Antivirus et de ses paramètres de base.

Icône dans la partie système de la barre des tâches

Pour accéder à certaines des fonctionnalités et options de configuration les plus importantes, cliquez avec le bouton droit sur l'icône dans la partie système de la barre des tâches.

Désactiver la protection – Affiche la boîte de dialogue de confirmation qui désactive le moteur de détection ; ce dernier protège le système des attaques malveillantes en contrôlant les fichiers et les communications par messagerie et Internet. Le menu déroulant **Intervalle** permet d'indiquer la durée pendant laquelle la protection est désactivée.

Configurations avancées – Ouvrez les configurations avancées d'ESET NOD32 Antivirus. Pour ouvrir les configurations avancées depuis la fenêtre principale du produit, appuyez sur F5 sur votre clavier ou cliquez sur **Configuration** > **Configurations avancées**.

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

Ouvrir ESET NOD32 Antivirus – Ouvre la fenêtre principale du programme ESET NOD32 Antivirus.

Réinitialiser la disposition des fenêtres – Réinitialise la fenêtre ESET NOD32 Antivirus sur sa taille et sa position par défaut.

Mode couleur – Ouvre les paramètres de l'interface utilisateur dans lesquels vous pouvez changer la couleur de l'interface utilisateur graphique.

Rechercher des mises à jour – Démarre une mise à jour de module ou du produit pour assurer votre protection. ESET NOD32 Antivirus recherche des mises à jour automatiquement plusieurs fois par jour.

À propos – Les informations système fournissent des détails sur la version installée d'ESET NOD32 Antivirus, les modules installés ainsi que des informations sur le système d'exploitation et les ressources du système.

Raccourcis clavier

Pour simplifier la navigation dans ESET NOD32 Antivirus, vous pouvez utiliser les raccourcis clavier suivants :

Raccourcis clavier	Action
F1	ouvre les pages d'aide
F5	ouvre la boîte de dialogue Configuration avancée
Flèche haut/Flèche bas	permet de naviguer parmi les éléments d'un menu déroulant
TAB	permet de passer à l'élément d'interface utilisateur suivant dans une fenêtre
Shift+TAB	permet de passer à l'élément d'interface utilisateur précédent dans une fenêtre
ESC	ferme la boîte de dialogue active
Ctrl+U	affiche des informations sur l'abonnement ESET et votre ordinateur (détails pour l'assistance technique)
Ctrl+R	réinitialise la taille et la position par défaut de la fenêtre du produit à l'écran
ALT + Flèche gauche	permet de naviguer vers l'arrière
ALT + Flèche droite	permet de naviguer vers l'avant
ALT+Home	permet de naviguer dans la page d'accueil

Vous pouvez également utiliser les boutons de la souris vers l'avant ou vers l'arrière pour naviguer.

Profils

Le gestionnaire de profil est utilisé à deux endroits dans ESET NOD32 Antivirus – Dans les sections **Analyse à la demande** et **Mise à jour**.

Analyse de l'ordinateur

Il existe quatre profils d'analyse prédéfinis dans ESET NOD32 Antivirus :

- **Analyse intelligente** : il s'agit du profil d'analyse avancée par défaut. Le profil d'analyse intelligente utilise la technologie d'optimisation intelligente qui exclut les fichiers qui ont été détectés comme étant non infectés lors d'une analyse précédente et qui n'ont pas été modifiés depuis. La durée d'analyse est ainsi réduite avec un impact minimal sur la sécurité du système.

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

- **Analyse approfondie** : Le profil d'analyse approfondie n'utilise pas l'optimisation intelligente par défaut. Par conséquent, aucun fichier n'est exclu de l'analyse à l'aide de ce profil.

- **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 les prochaines analyses. Il est recommandé de créer autant de profils (avec différentes cibles et méthodes, et d'autres paramètres d'analyse) que d'analyses utilisées régulièrement.

Pour créer un profil, ouvrez Configurations avancées > **Moteur de détection** > **Analyses des logiciels malveillants** > **Analyse à la demande** > **Liste des profils** > **Modifier**. La fenêtre **Gestionnaire de profils** dispose du menu déroulant **Profil sélectionné** contenant les profils d'analyse existants, ainsi qu'une option permettant de créer un profil. Pour plus d'informations sur la création d'un profil d'analyse correspondant à vos besoins, reportez-vous à ThreatSense ; vous y trouverez une description de chaque paramètre de configuration de l'analyse.

> Supposons la situation suivante : vous souhaitez créer votre propre profil d'analyse et la configuration **Analyse intelligente** est partiellement adéquate. En revanche, vous ne souhaitez analyser ni les fichiers exécutables compressés par un compresseur d'exécutables, ni les applications potentiellement dangereuses. Vous souhaitez effectuer un **Toujours corriger la détection**. Entrez le nom du nouveau profil dans la fenêtre **Gestionnaire de profils**, puis cliquez sur **Ajouter**. Sélectionnez le nouveau profil dans le menu déroulant **Profil sélectionné** et réglez les paramètres restants selon vos besoin. Cliquez sur **OK** pour enregistrer le nouveau profil.

Mettre à jour

L'éditeur de profils dans Configuration des mises à jour permet de créer de nouveaux profils de mise à jour. Il est conseillé de créer et d'utiliser des profils personnalisés (autre que l'option par défaut **Mon profil**) si votre ordinateur utilise plusieurs voies de connexion aux serveurs de mise à jour.

C'est le cas par exemple d'un ordinateur portable qui se connecte normalement à un serveur local (miroir) sur le réseau local, mais qui télécharge les mises à jour directement à partir des serveurs de mise à jour d'ESET lorsqu'il est déconnecté du réseau local (voyage d'affaires). le premier se connectant au serveur local, le second aux serveurs d'ESET. Une fois ces profils configurés, allez dans **Outils** > **Planificateur** puis modifiez les paramètres de mise à jour de la tâche. Désignez un profil comme principal et l'autre comme secondaire.

Profil de mise à jour – Le profil de mise à jour utilisé actuellement. Pour le changer, choisissez un profil dans le menu déroulant.

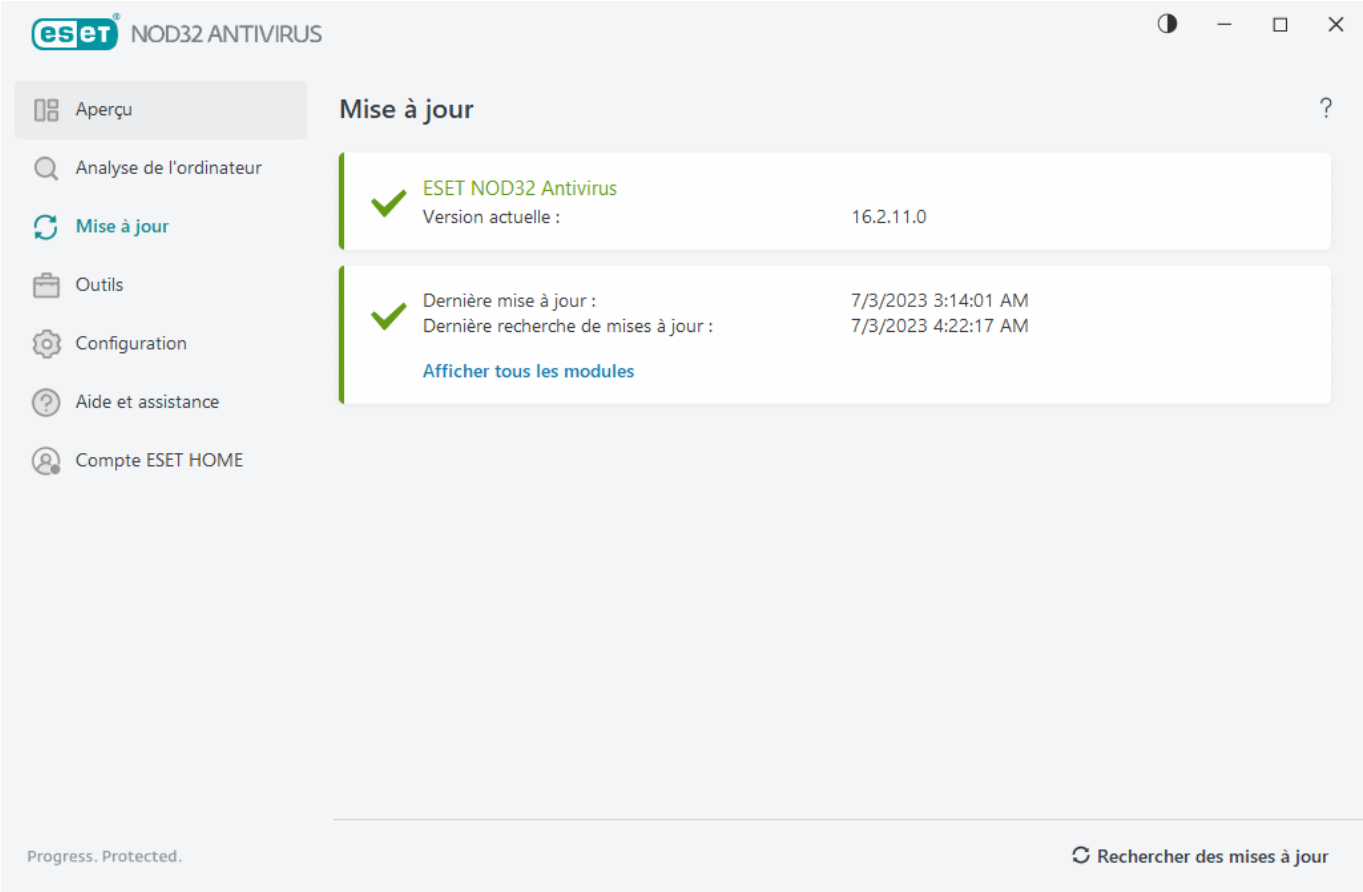
Liste des profils – Permet de créer des profils de mise à jour ou de supprimer ceux existants.

Mises à jour

La mise à jour régulière d'ESET NOD32 Antivirus est la meilleure méthode pour assurer le niveau maximum de sécurité à votre ordinateur. Le module de mise à jour veille à ce que les modules du programme et les composants système soient toujours à jour.

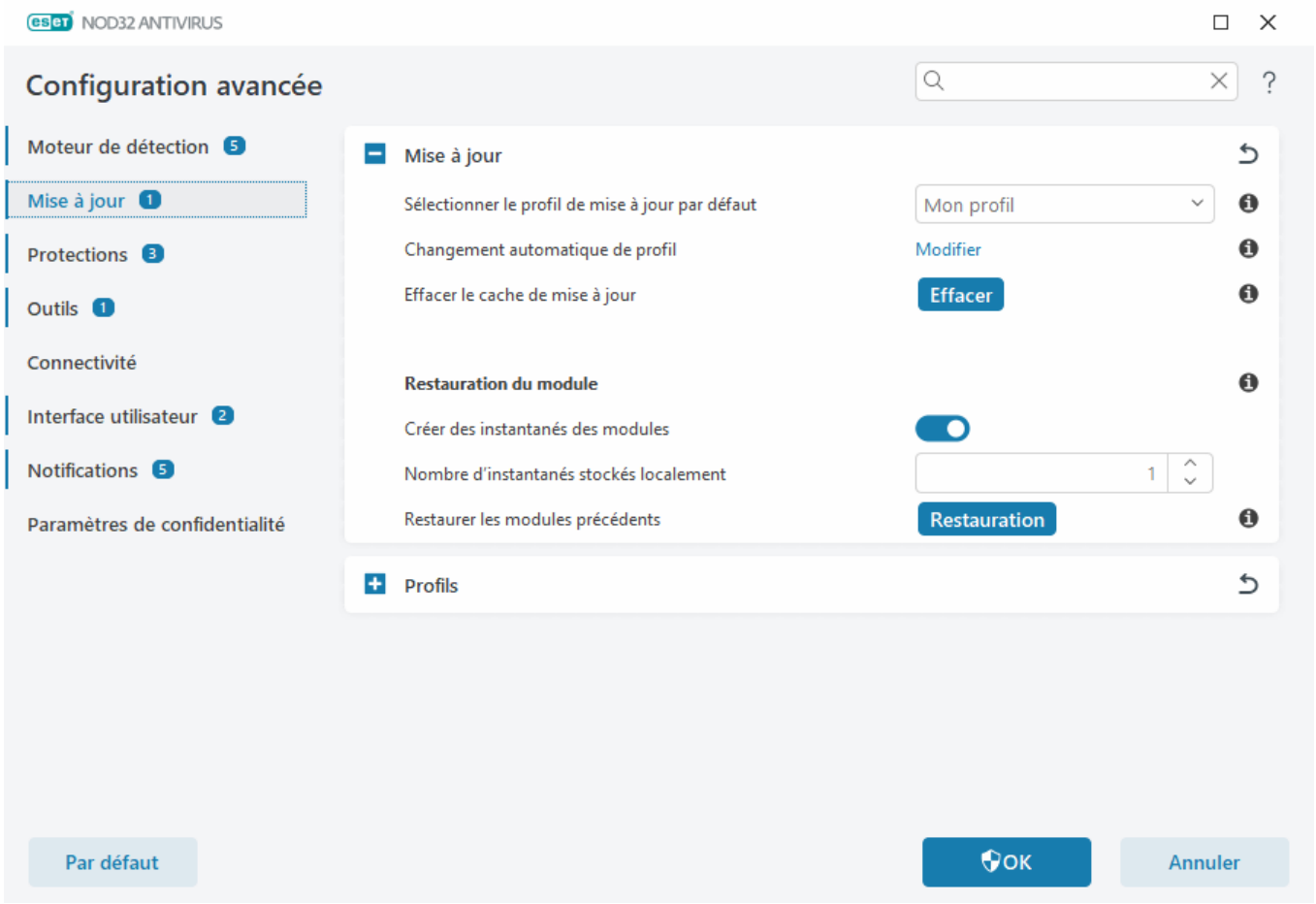
En cliquant sur **Mettre à jour** dans la fenêtre principale du programme, vous pouvez connaître l'état actuel de la mise à jour, notamment la date et l'heure de la dernière mise à jour. Vous pouvez également savoir si une mise à jour est nécessaire.

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



La sectionConfigurations avancées > **Mise à jour** contient des options de mise à jour supplémentaires comme le mode de mise à jour, l'accès au serveur proxy et les connexions LAN.

Si vous rencontrez des problèmes liés à une mise à jour, cliquez sur **Effacer** pour effacer le cache de mise à jour. Si vous ne parvenez toujours pas à mettre à jour les modules du programme, consultez la section Résolution du message « Échec de la mise à jour des modules ».



Activation du produit

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

- Si vous disposez d'une version du produit vendue dans une boîte ou si vous avez reçu un e-mail avec les détails de l'abonnement, activez votre produit en cliquant sur **Utiliser une clé d'activation achetée**. Vous devez entrer la clé d'activation exactement comme elle est indiquée. Clé d'activation : chaîne unique au format XXXX-XXXX-XXXX-XXXX-XXXX ou XXXX-XXXXXXXX qui sert à identifier le titulaire de l'abonnement et à activer la licence. Cette clé d'activation se trouve généralement à l'intérieur ou au dos de l'emballage du produit.

- Après avoir sélectionné Utiliser le compte ESET HOME, vous serez invité à vous connecter à votre compte ESET HOME.

- Si vous souhaitez évaluer ESET NOD32 Antivirus avant d'en faire l'acquisition, sélectionnez Essai gratuit. Indiquez votre adresse électronique et le pays dans lequel vous résidez pour activer ESET NOD32 Antivirus pendant une période limitée. Votre version d'essai gratuite vous sera envoyée par e-mail. Une version d'essai gratuite ne peut être activée qu'une seule fois par client.

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

Vous pouvez modifier l'abonnement de votre produit à tout moment. Pour ce faire, cliquez sur **Aide et assistance** > **Modifier l'abonnement** dans la fenêtre principale du programme. L'ID public s'affiche ; il sert à

identifier votre abonnement auprès de l'assistance ESET.

⚠ En cas d'échec de l'activation du produit

Saisie de votre clé d'activation lors de l'activation

Les mises à jour automatiques sont importantes pour votre sécurité. ESET NOD32 Antivirus ne recevra des mises à jour que lorsque le programme aura été activé.

Lors de la saisie de votre **clé de licence**, il est important de respecter scrupuleusement leur forme. Votre clé d'activation est une chaîne unique au format XXXX-XXXX-XXXX-XXXX-XXXX qui sert à identifier le titulaire de l'abonnement et à activer l'abonnement.

Il est recommandé de copier et de coller la clé d'activation à partir du message d'enregistrement.

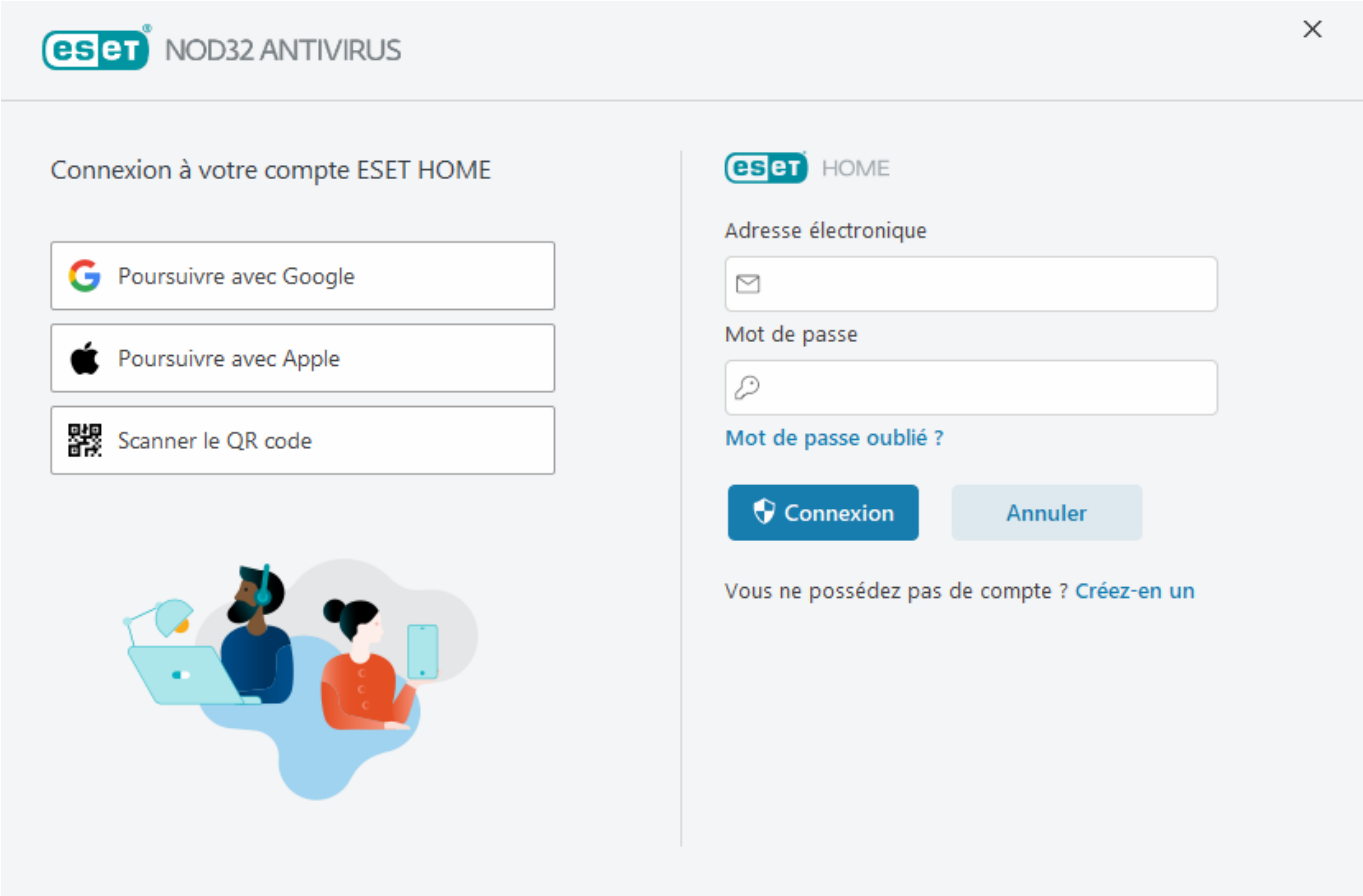
Si vous n'avez pas saisi votre clé d'activation après l'installation, votre produit n'est pas activé. Vous pouvez activer ESET NOD32 Antivirus dans la fenêtre principale du programme > **Aide et assistance** > **Activer l'abonnement**.

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

Utiliser le ESET HOME compte

Connectez votre appareil à ESET HOME pour afficher et gérer tous les abonnements ESET et les appareils activés. Vous pouvez renouveler, mettre à niveau ou prolonger votre abonnement et afficher des informations importantes sur celui-ci. Sur le portail de gestion ESET HOME ou dans l'application mobile, vous pouvez ajouter

différents abonnements, télécharger des produits sur vos appareils, vérifier l'état de la sécurité du produit ou partager des abonnements par e-mail. Pour plus d'informations, consultez l''aide en ligne d'ESET HOME.



Après avoir sélectionné **Utiliser le compte ESET HOME** en tant que 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 ne possédez pas de compte ESET HOME, cliquez sur **Créer un compte** pour vous enregistrer ou consultez les instructions de l'aide en ligne ESET HOME.
> Si vous avez oublié votre mot de passe, cliquez sur **J'ai oublié mon mot de passe** et suivez la procédure à l'écran ou consultez les instructions de l'aide en ligne ESET HOME.

2. Définissez le **nom de l'appareil** qui sera utilisé dans tous les services ESET HOME, puis cliquez sur **Continuer**.

3. Choisissez un abonnement pour l'activation ou ajoutez un nouvel abonnement. Cliquez sur **Continuer** pour activer ESET NOD32 Antivirus.

Activer la version d\'essai gratuite

Pour activer la version d'essai d'ESET NOD32 Antivirus, saisissez une adresse valide dans les champs **Adresse e-mail** et **Confirmer l'adresse e-mail**. Après activation, votre abonnement ESET est généré et envoyé à cette adresse. Celle-ci sera également utilisée pour les notifications d'expiration du produit et les autres communications avec ESET. La version d'essai gratuite ne peut être activée qu'une seule fois.

Sélectionnez votre **pays** dans le menu déroulant des pays pour enregistrer ESET NOD32 Antivirus auprès votre distributeur local qui assurera le support technique.

Clé d'activation ESET gratuite

L'abonnement ESET NOD32 Antivirus n'est pas gratuit.

La clé d'activation ESET est une séquence unique de lettres et de chiffres séparés par un tiret, fournis par ESET afin de permettre l'utilisation légale d'ESET NOD32 Antivirus conformément au contrat de licence de l'utilisateur final. Chaque utilisateur final n'a le droit d'utiliser la clé d'activation que dans la mesure où il dispose du droit d'utiliser ESET NOD32 Antivirus en fonction du nombre de licences accordées par ESET. La clé d'activation est considérée comme confidentielle et ne peut pas être partagée. Vous pouvez toutefois partager un abonnement à l'aide d'ESET HOME.

Des sources sur Internet peuvent vous fournir une clé d'activation ESET « gratuite », mais souvenez-vous des points suivants :

- Cliquer sur une annonce « Abonnement ESET gratuite » peut compromettre votre ordinateur ou votre appareil qui peut être infecté par des logiciels malveillants. Les logiciels malveillants peuvent être cachés dans du contenu web (par exemple des vidéos) non officiel, des sites web qui affichent des publicités pour gagner de l'argent en fonction de vos visites, etc. Il s'agit généralement d'un piège.
- ESET peut désactiver un abonnement piraté et le fait.
- L'utilisation d'une clé d'activation piratée ne respecte pas les termes du contrat de licence de l'utilisateur final que vous devez accepter pour installer ESET NOD32 Antivirus.
- Achetez un abonnement ESET uniquement via des canaux officiels comme www.eset.com, des distributeurs ou des revendeurs ESET (n'achetez pas d'abonnement de sites web tiers non officiels comme eBay ou d'abonnement partagé d'un tiers).
- Le téléchargement d'ESET NOD32 Antivirus est gratuit, mais son activation lors de l'installation nécessite une clé d'activation ESET valide (vous pouvez télécharger et installer le produit, mais il ne fonctionnera pas sans activation).
- Ne partagez pas votre abonnement sur Internet ou les réseaux sociaux (il pourrait être diffusé à grande échelle).

Pour identifier et signalé un abonnement ESET piraté, consultez cet article de la base de connaissances afin d'obtenir des instructions.

Si vous avez des doutes sur l'achat d'un produit de sécurité ESET, vous pouvez utiliser une version d'essai pendant que vous décidez les points suivants :

1. Activer ESET NOD32 Antivirus à l'aide d'une version d'essai gratuite
2. Participer au programme Bêta ESET
3. Installer ESET Mobile Security si vous utilisez un appareil mobile Android. Ce produit est gratuit.

Pour bénéficier d'une remise/prolonger votre licence, renouvelez votre licence ESET.

Échec de l'activation – scénarios courants

En cas d'échec de l'activation d'ESET NOD32 Antivirus, les scénarios les plus courants sont les suivants :

- La clé d'activation est déjà utilisée.
- Vous avez saisi une clé d\'activation non valide.
- Des informations du formulaire d'activation sont absentes ou non valides.
- La communication avec le serveur d'activation a échoué.
- Aucune connexion ou connexion aux serveurs d'activation ESET désactivée.

Vérifiez que vous avez saisi la clé d'activation correcte et que votre connexion Internet est active. Réessayez d'activer ESET NOD32 Antivirus. Si vous utilisez le compte ESET HOME pour l'activation, consultez Abonnement et gestion des abonnements ESET HOME - Aide en ligne.

> Si une erreur spécifique s'affiche (abonnement suspendu ou abonnement surutilisé, par exemple), suivez les instructions dans l'état d'abonnement.

Si vous n'êtes toujours pas en mesure d'activer votre ESET NOD32 Antivirus, le dépanneur d'activation ESET vous présentera les questions courantes, les erreurs et les problèmes liés à l'activation et aux licences (disponible en anglais et dans plusieurs autres langues).

État d'abonnement

Votre abonnement peut avoir différents états. Vous pouvez consulter l'état de votre abonnement dans ESET HOME. Pour ajouter votre abonnement à votre compte ESET HOME, consultez Ajouter un abonnement.

> Si vous ne possédez pas de ESET HOME, vous pouvez créer un compte ESET HOME.

Si l'état de l'abonnement est autre que **Actif**, une erreur s'affichera pendant l'activation ou une notification apparaîtra dans la fenêtre principale du programme.

Pour désactiver les notifications d'état des abonnements, ouvrez Configurations avancées > **Notifications** > **États d'application**. Cliquez sur **Modifier** en regard de l'option **États d'application**, développez **Licences**, puis décochez la case en regard de la notification à désactiver. La désactivation de la notification ne permet pas de résoudre le problème.

Dans le tableau suivant, consultez les descriptions et les solutions recommandées pour différents états d'abonnement :

État d'abonnement	Description	Solution
Actif	L'abonnement est valide et aucune interaction n'est nécessaire. ESET NOD32 Antivirus peut être activé. Les détails de l'abonnement figurent dans la fenêtre principale du programme > **Aide et assistance**.	

État d'abonnement	Description	Solution
Surutilisée	Le nombre d'appareils utilisant cet abonnement est supérieur à celui autorisé. Une erreur d'activation s'affichera.	Pour plus d'informations, voir Échec de l'activation en raison d'un abonnement surutilisé.
Suspendu	Votre abonnement a été suspendu en raison de problèmes de paiement. Pour utiliser l'abonnement, vérifiez que les informations de paiement sont à jour dans ESET HOME ou contactez le revendeur de votre abonnement. Cette erreur peut s'afficher pendant l'activation ou dans la fenêtre principale du programme.	Produit installé : si vous avez un compte ESET HOME, dans la notification affichée dans la fenêtre principale du programme, cliquez sur **Gérer votre abonnement dans ESET HOME** et passez en revue vos informations de paiement. Dans le cas contraire, contactez votre revendeur d'abonnements. Erreur d'activation : si vous avez un compte ESET HOME, dans la fenêtre de l'erreur d'activation, cliquez sur **Ouvrir ESET HOME** et passez en revue vos informations de paiement. Dans le cas contraire, contactez votre revendeur d'abonnements.
Arrivé à expiration	Votre abonnement est arrivé à expiration. Vous ne pouvez donc pas l'utiliser pour activer ESET NOD32 Antivirus. Cette erreur peut s'afficher pendant l'activation ou dans la fenêtre principale du programme. Si ESET NOD32 Antivirus est déjà installé sur votre ordinateur, ce dernier n'est ni protégé ni mis à jour.	Produit installé : dans la notification affichée dans la fenêtre principale du programme, cliquez sur **Renouveler l'abonnement** et suivez les instructions de Comment renouveler mon abonnement ? ou cliquez sur **Activer le produit** et sélectionnez la méthode d'activation. Erreur d'activation : dans la fenêtre de l'erreur d'activation, cliquez sur **Renouveler votre abonnement** et suivez les instructions de Comment renouveler mon abonnement ? ou saisissez une clé d'activation nouvelle ou renouvelée et cliquez sur **Renouveler l'abonnement**.
Annulée	Votre abonnement a été annulé par ESET ou par votre revendeur d'abonnements.	Si le message d'erreur suivant s'affiche : Si votre abonnement est annulé dans la fenêtre principale du programme ou lors de l'activation et qu'il devrait fonctionner correctement, contactez votre revendeur d'abonnements.

Échec de l'activation en raison d'un abonnement surutilisé

Problème

- Votre abonnement peut être surutilisé ou utilisé d'une manière abusive
- Échec de l'activation en raison d'un abonnement surutilisé

Solution

Le nombre d'appareils utilisant cet abonnement est supérieur à celui autorisé. Vous êtes peut-être victime d'un piratage ou d'une contrefaçon du logiciel. 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 titulaire d'un abonnement et que vous n'avez pas été invité à saisir votre adresse e-mail :

1. Pour gérer votre abonnement ESET, ouvrez un navigateur web et accédez à https://my.eset.com.. Accédez à ESET License Manager et supprimez ou désactivez des appareils. Pour plus d'informations, consultez la section Que faire en cas d'abonnement surutilisé ?

2. Pour identifier et signaler un abonnement ESET piraté, consultez l'article sur l'identification et le signalement des abonnements ESET piratés afin d'obtenir des instructions.

3. En cas de doute, cliquez sur **Précédent** et envoyez un e-mail au support technique ESET.

Si vous n'êtes pas un détenteur d'abonnement, veuillez contacter le détenteur de cet abonnement pour lui signaler que vous ne parvenez pas à activer le produit ESET en raison d'une surutilisation de l'abonnement. Le détenteur peut résoudre le problème dans le portail ESET HOME.

Si vous êtes invité à confirmer votre adresse e-mail (plusieurs cas uniquement), saisissez l'adresse e-mail que vous avez utilisée pour acheter ou activer ESET NOD32 Antivirus.

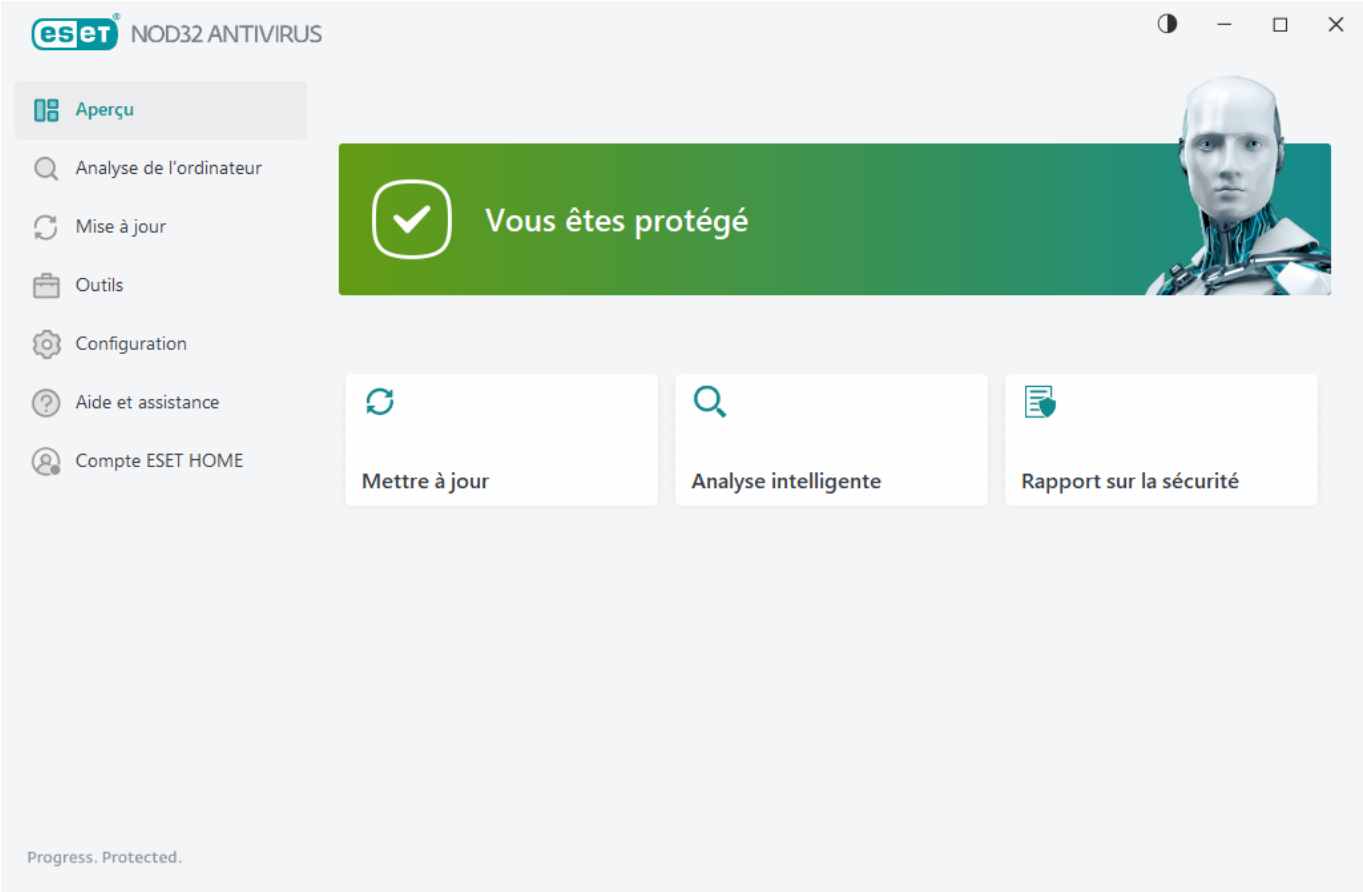
Utilisation d'ESET NOD32 Antivirus

La fenêtre principale du programme ESET NOD32 Antivirus est divisée en deux sections principales. La fenêtre principale de droite affiche les informations correspondant à l'option sélectionnée dans le menu principal à gauche.

> **Instructions illustrées**
> Pour obtenir des instructions illustrées disponibles en anglais et dans plusieurs autres langues, consultez Ouvrir la fenêtre principale du programme des produits ESET pour Windows.

Vous pouvez sélectionner le modèle de couleurs de l'interface utilisateur graphique d'ESET NOD32 Antivirus dans le coin supérieur droit de la fenêtre principale du programme. Cliquez sur l'icône **Modèle de couleurs** (l'icône change en fonction du modèle de couleurs actuellement sélectionné) en regard de l'icône **Réduire**, puis sélectionnez le modèle de couleurs dans le menu déroulant :

- **Identique à la couleur système** – Définit le modèle de couleurs d'ESET NOD32 Antivirus selon les paramètres du système d'exploitation.
- **Sombre** – ESET NOD32 Antivirus aura un modèle de couleurs foncées (mode sombre).
- **Clair** – ESET NOD32 Antivirus aura un modèle de couleurs clairs standard.



Options du menu principal :

Vue d'ensemble – Fournit des informations sur l'état de protection d'ESET NOD32 Antivirus.

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 – Permet d'accéder à l' fonctionnalités qui contribuent à simplifier l'administration du programme et offrent des options supplémentaires aux utilisateurs expérimentés.

Configuration – Fournit des options de configuration pour les fonctionnalités de protection d'ESET NOD32 Antivirus (protection de l'ordinateur et protection Internetet donne accès à Configurations avancées.

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 appareil à ESET HOME ou examinez l'état de la connexion du compte ESET HOME. UtilisezESET HOME pour afficher et gérer vos les abonnements et appareils ESET activés.

Vue d'ensemble

La fenêtre **Vue d'ensemble** affiche des informations sur la protection actuelle de votre ordinateur ainsi que des liens rapides vers les fonctionnalités de sécurité d'ESET NOD32 Antivirus.

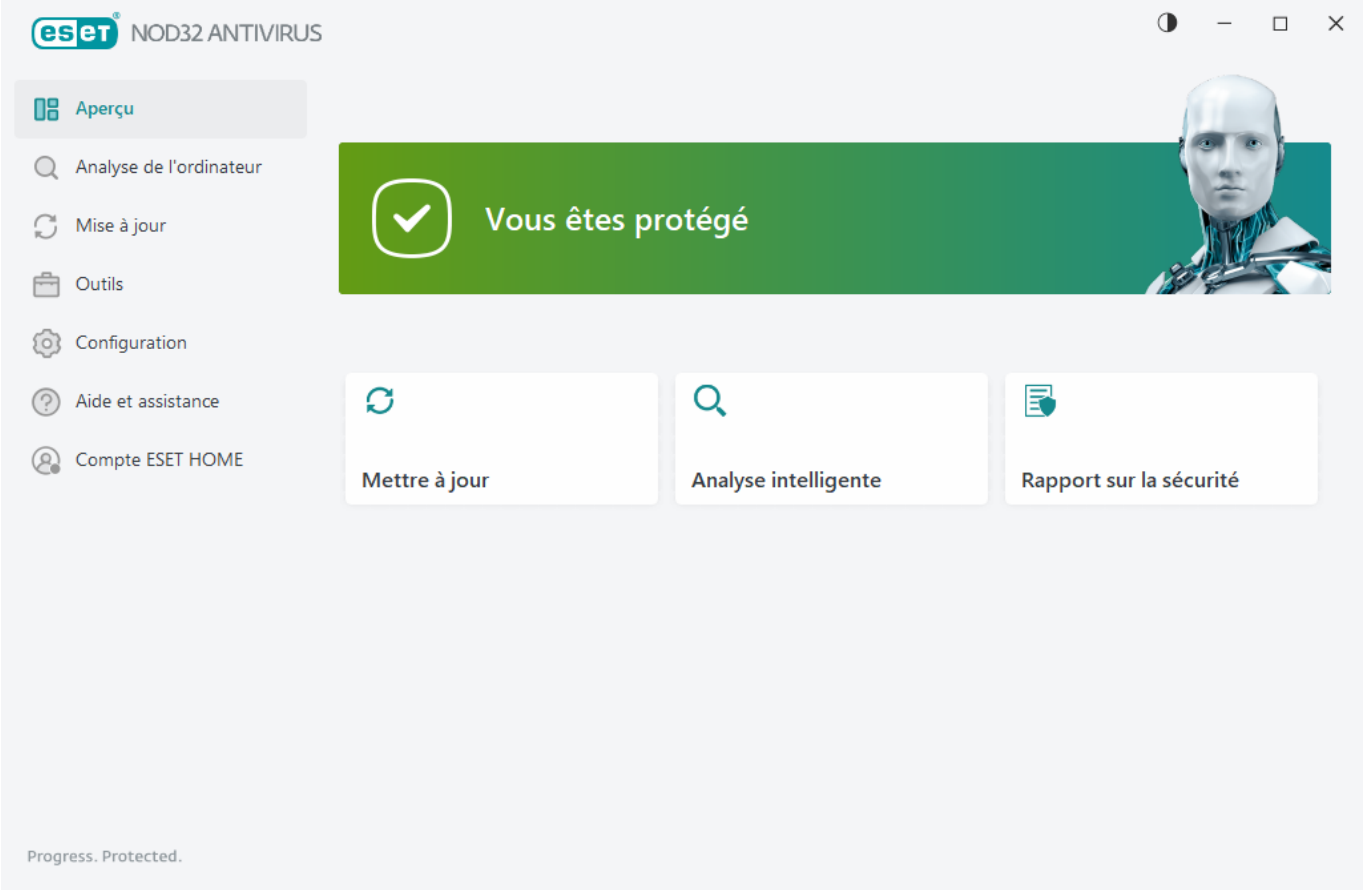
La fenêtre **Vue d'ensemble** affiche des notifications avec des informations détaillées et des solutions recommandées pour renforcer la sécurité d'ESET NOD32 Antivirus, activer d'autres fonctionnalités ou assurer une

protection maximale. S'il y a plusieurs notifications, cliquez sur **X autres notifications** pour développer tout.

Mise à jour : ouvre la page Mise à jour et recherche des mises à jour.

Analyser votre ordinateur : ouvre la page Analyse de l'ordinateur et lance une analyse standard de l'ordinateur.

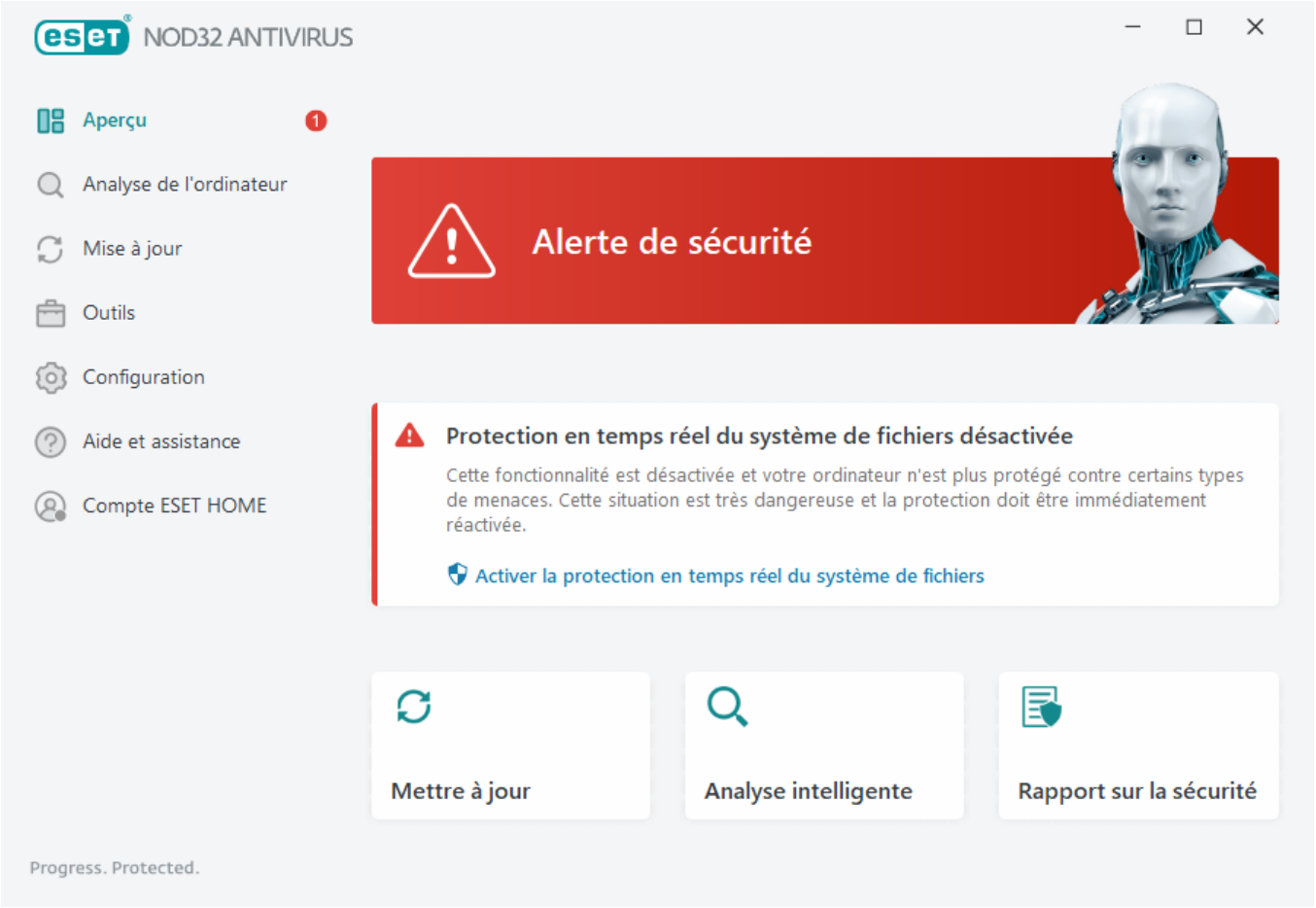
Rapport sur la sécurité : ouvre le rapport sur la sécurité.



L'icône verte et l'état vert **Vous êtes protégé** indiquent 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 d'état de la protection est verte. Une icône représentant un point d'exclamation rouge ou orange indique que la protection maximale n'est pas garantie. Des informations supplémentaires sur l'état de la protection de chaque module, ainsi que des suggestions de solution permettant de restaurer la protection complète, sont affichées sous forme de notification dans la fenêtre **Vue d'ensemble**. Pour changer l'état des différents modules, cliquez sur **Configuration**, puis sur le module souhaité.



L'icône rouge et l'état rouge des **alertes de sécurité** signalent des problèmes critiques.
Cet état peut être affiché pour différentes raisons, par exemple :

- **Le produit n'est pas activé** ou **Abonnement arrivé à expiration** – Cette information est indiquée par l'icône d'état de protection qui devient rouge. Le programme ne peut plus effectuer de mise à jour après expiration de l'abonnement. Suivez les instructions de la fenêtre d'alerte pour renouveler l'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 vous conseillons de vérifier les paramètres de mise à jour. Cette erreur provient généralement de l'entrée incorrecte de données d'authentification ou de la configuration incorrecte des paramètres de connexion.
- **La protection en temps réel du système de fichiers est désactivée** – La protection en temps réel a été désactivée par l'utilisateur. Votre ordinateur n'est plus protégé contre certains types de menace. Cliquez sur **Activer la protection en temps réel du système de fichiers** pour réactiver cette fonctionnalité.
- **Protection antivirus et antispyware désactivée** : vous pouvez réactiver la protection antivirus et antispyware en cliquant sur **Activer la protection antivirus et antispyware**.

L'icône orange indique une protection limitée. Par exemple, il peut s'agir d'un problème de mise à jour ou de l'imminence de l'expiration de votre abonnement.
Cet état peut être affiché pour différentes raisons, par exemple :

- **Mode joueur activé** : l'activation du mode joueur représente un risque potentiel pour la sécurité. L'activation de cette fonctionnalité désactive toutes les fenêtres de notification/d'alerte et arrête

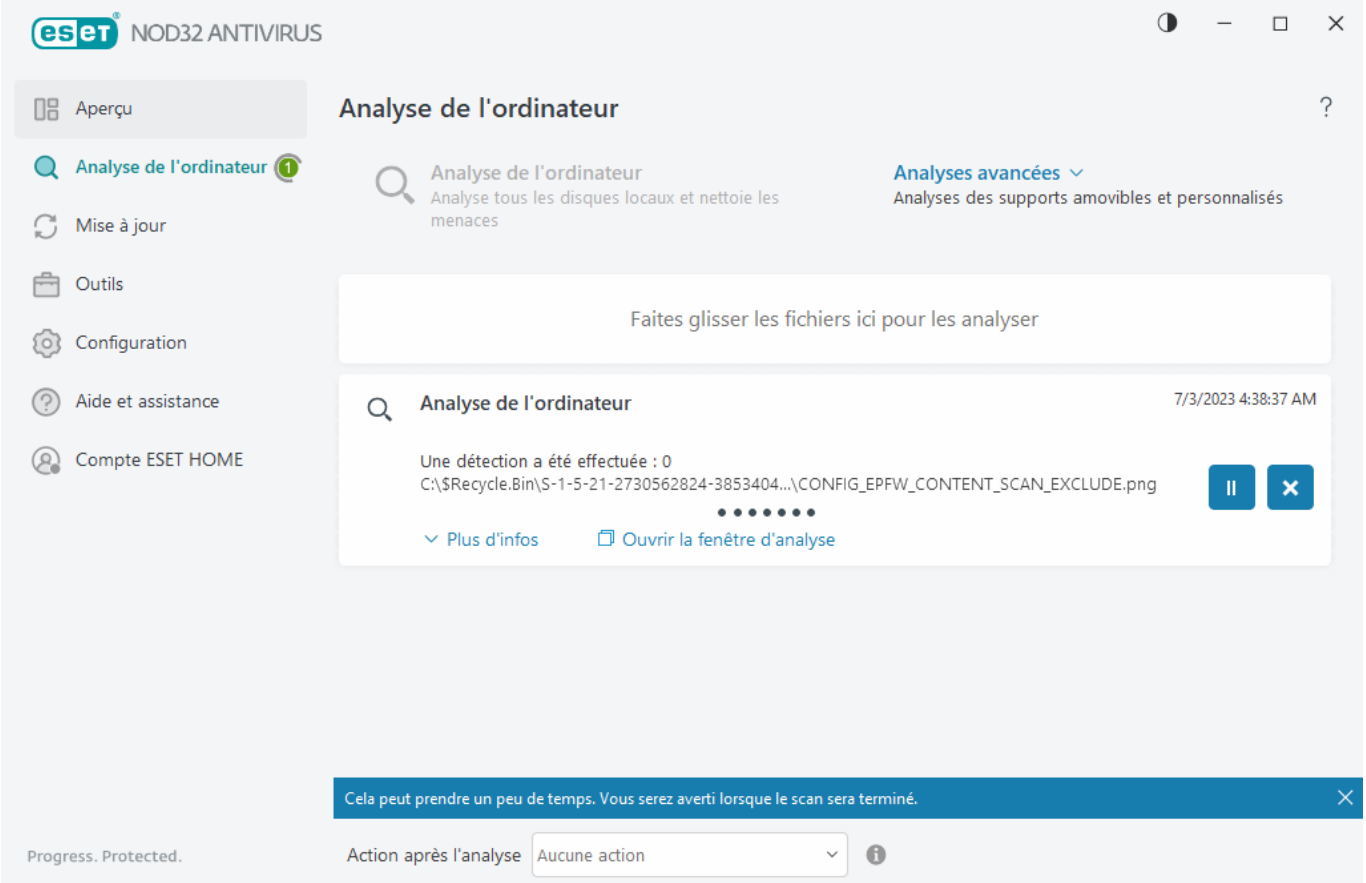
toutes les tâches planifiées.

- **Votre abonnement arrive bientôt à expiration./Votre abonnement arrive à expiration aujourd'hui** – cette information est donnée par l'icône d'état de protection qui affiche un point d'exclamation à côté de l'horloge du système. Après l'expiration de votre abonnement, le programme ne peut plus se mise à jour et l'icône d'état de la protection devient rouge.

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

Analyse de l'ordinateur

L'analyseur à la demande est une partie importante de votre solution antivirus. Il permet d'analyser des fichiers et des répertoires de votre ordinateur. Pour votre sécurité, il est essentiel que l'ordinateur soit analysé régulièrement dans le cadre de mesures de sécurité routinières, pas seulement en cas de suspicion d'une infection. Nous vous recommandons d'effectuer des analyses en profondeur de votre système de façon régulière afin de détecter les virus éventuels qui n'auraient pas été bloqués par la protection en temps réel du système de fichiers lors de leur écriture sur le disque. Cela peut se produire si la protection en temps réel du système de fichiers était désactivée au moment de l'infection, si le moteur de détection n'était plus à jour ou si le fichier n'a pas été détecté comme virus lors de son enregistrement sur le disque.



Deux types d'**analyses de l'ordinateur** sont disponibles. L'option **Analyse intelligente** analyse rapidement le système sans indiquer des paramètres d'analyse. L'**analyse personnalisée** (sous Analyse avancée) permet de sélectionner l'un des profils d'analyse prédéfinis pour cibler des emplacements donnés, ainsi que de choisir des cibles spécifiques à analyser.

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

> Par défaut, ESET NOD32 Antivirus tente de nettoyer ou de supprimer automatiquement les détections effectuées pendant l'analyse de l'ordinateur. Dans certains cas, si aucune action ne peut être exécutée, vous recevez une alerte interactive. Vous devez alors sélectionner une action de nettoyage (supprimer ou ignorer, par exemple). Pour changer le niveau de nettoyage et obtenir des informations plus détaillées, voir Nettoyage. Pour consulter les analyses précédentes, consultez les fichiers journaux.

Analyse intelligente

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

Vous pouvez également utiliser la fonctionnalité d'**analyse par glisser-déposer** pour analyser manuellement un fichier ou un dossier en cliquant dessus, en déplaçant le pointeur de la souris vers la zone marquée tout en maintenant le bouton de la souris enfoncée, puis en le relâchant. L'application est ensuite placée au premier plan.

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

Analyse personnalisée

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

Analyse de supports amovibles

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

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

Répéter la dernière analyse

Vous permet de lancer rapidement l'analyse exécutée précédemment, avec les mêmes paramètres.

Le menu déroulant **Action après l'analyse** permet de définir l'exécution automatique d'une action au terme d'une analyse :

- **Aucune action** – Aucune action n'est exécutée à la fin d'une analyse.
- **Arrêter** – L'ordinateur est mis hors tension à la fin d'une analyse.

• **Redémarrage si nécessaire** – L'ordinateur redémarre uniquement si cela est nécessaire pour terminer le nettoyage des menaces détectées.

• **Redémarrer** – Ferme tous les programmes ouverts et redémarre l'ordinateur à la fin d'une 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 l'interaction de l'utilisateur et redémarre l'ordinateur à la fin d'une analyse.

• **Veille** – Enregistre votre session et met l'ordinateur dans un état à faible consommation d'énergie pour que vous puissiez rapidement reprendre le travail.

• **Veille prolongée** – Déplace tous les éléments en cours d'exécution sur la RAM vers un fichier spécial sur le disque dur. Votre ordinateur est arrêté, mais reprend son état précédent lorsque vous le démarrez.

Les actions **Veille** et **Veille prolongée** sont disponibles selon les paramètres d'alimentation et de mise en veille du système d'exploitation de votre ordinateur ou les capacités du PC/ordinateur portable. N'oubliez pas qu'un ordinateur en veille est un ordinateur en fonctionnement. Il exécute toujours des fonctions de base et consomme de l'électricité lorsqu'il est alimenté par batterie. Pour conserver l'autonomie de la batterie, lors d'un déplacement par exemple, il est recommandé d'utiliser l'option de mise en veille prolongée.

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

Nous recommandons d'exécuter une analyse de l'ordinateur au moins une fois par mois. L'analyse peut être configurée comme tche planifiée dans **Outils** > **Planificateur**. Comment programmer une analyse hebdomadaire de l'ordinateur ?

Lanceur d'analyses personnalisées

Vous pouvez utiliser une analyse personnalisée pour analyser la mémoire, le réseau ou des parties spécifiques d'un disque plutôt que le disque entier. Pour ce faire, cliquez sur **Analyses avancées** > **Analyse personnalisée** ou sélectionnez des cibles spécifiques dans la structure (arborescence) des dossiers.

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

La structure (arborescence) des dossiers contient également des cibles à analyser spécifiques.

• **Mémoire vive** – Analyse l'ensemble des processus et des données actuellement utilisés par la mémoire vive.

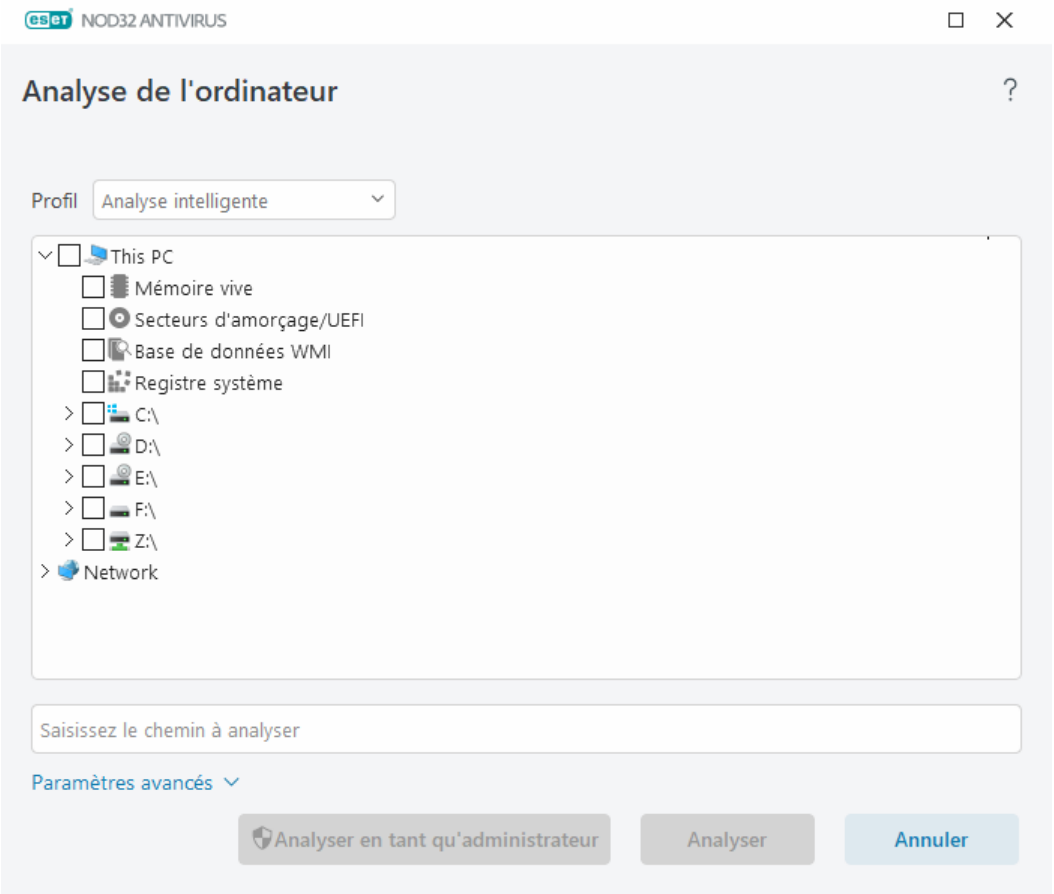
• **Secteurs d'amorçage/UEFI** – Analyse les secteurs d'amorçage et UEFI afin de détecter la présence éventuelle de logiciels malveillants. Pour plus d'informations sur le Scanner UEFI, consultez le glossaire.

• **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 des références à des fichiers infectés ou des logiciels malveillants intégrés en tant que données.

• **Registre système** – Analyse l'ensemble du Registre système, toutes les clés et les sous-clés. Recherche des références à des fichiers infectés ou des logiciels malveillants intégrés en tant que données. Lors du nettoyage des détections, la référence reste dans le Registre pour s'assurer que les données importantes ne sont pas perdues.

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

> **Comment programmer une analyse hebdomadaire de l'ordinateur**
> Pour planifier une tâche régulière, consultez Comment programmer une analyse hebdomadaire de l'ordinateur.



Vous pouvez configurer les paramètres de nettoyage de l'analyse dans Configurations avancées > **Moteur de détection** > **Analyses des logiciels malveillants** > **Analyse à la demande** > **ThreatSense** > **Nettoyage**. Pour effectuer une analyse sans action de nettoyage, cliquez sur **Paramètres avancés** et sélectionnez **Analyse sans nettoyage**. L'historique de l'analyse est enregistré dans le journal de l'analyse.

Lorsque l'option **Ignorer les exclusions** est sélectionnée, les fichiers portant une extension auparavant exclue sont analysés sans exception.

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

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

> Une fois une analyse terminée, vous pouvez consulter le journal d'analyse de l'ordinateur en cliquant sur Afficher le journal.

Progression de l'analyse

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

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

> ### Comment programmer une analyse hebdomadaire de l'ordinateur
> Pour planifier une tâche régulière, consultez Comment programmer une analyse hebdomadaire de l'ordinateur.

Progression de l'analyse – La barre de progression indique l'état de l'analyse en cours d'exécution.

Cible – Nom de l'élément analysé et emplacement.

Détections effectuées – Indique le nombre total de fichiers analysés, de menaces détectées et de menaces nettoyées pendant une analyse.

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

- **Utilisateur** – Nom du compte d'utilisateur qui a lancé l'analyse.
- **Objets analysés** – Nombre d'objets déjà analysés.
- **Durée** – Temps écoulé.

Icône Pause – Suspend une analyse.

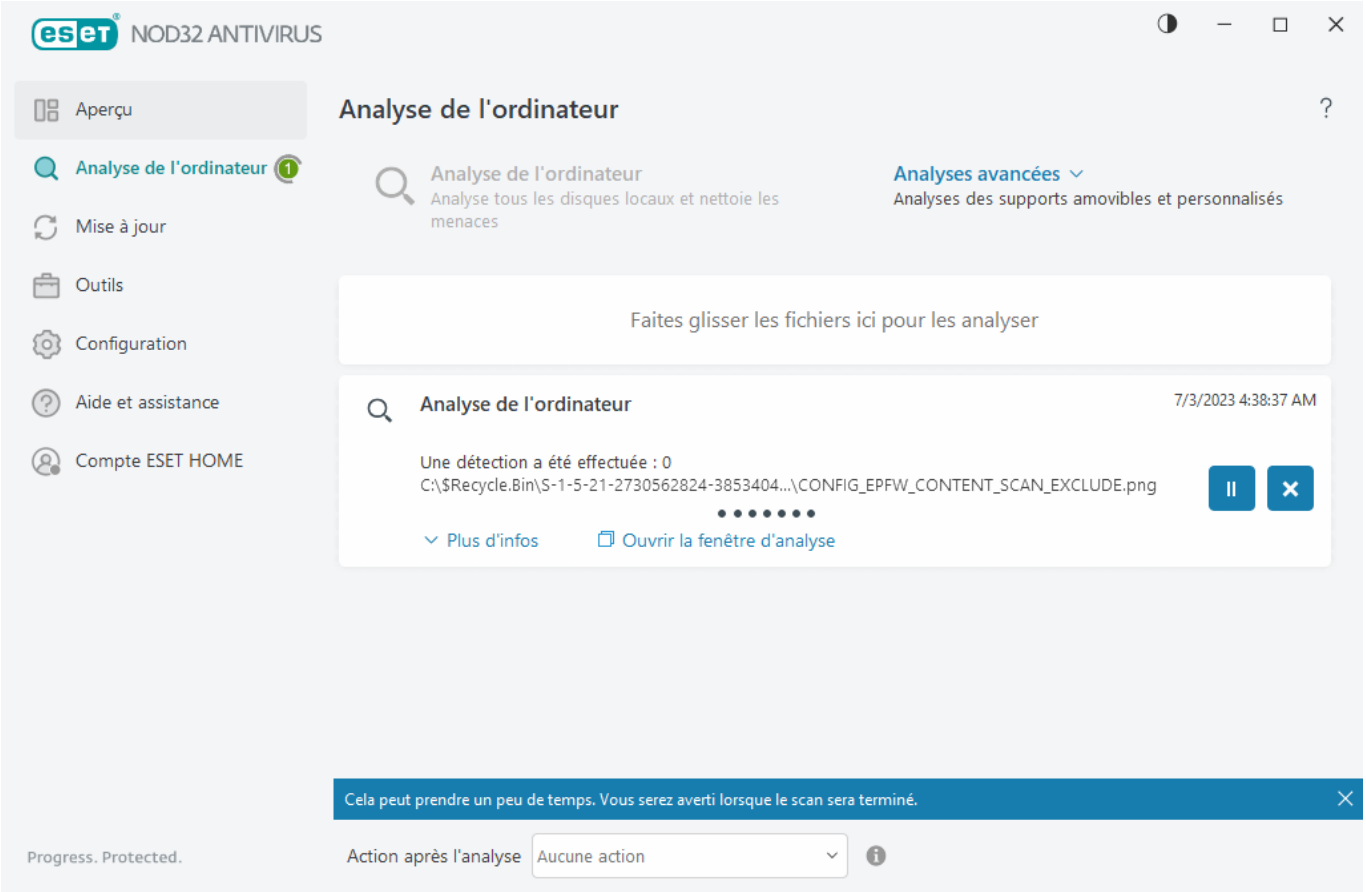
Icône Reprendre – Cette option est visible lorsque l'analyse est suspendue. Cliquez sur l'icône pour poursuivre l'analyse.

Icône Arrêter – Met fin à l'analyse.

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

Faire défiler le journal de l'analyse – Si cette option est activée, le journal de l'analyse défile automatiquement au fur et à mesure de l'ajout des entrées les plus récentes.

> Cliquez sur la loupe ou sur la flèche pour afficher les détails sur l'analyse en cours d'exécution. Vous pouvez exécuter une autre analyse parallèle en cliquant sur **Analyse de votre ordinateur** ou sur **Analyses avancées** > **Analyse personnalisée**.



Le menu déroulant **Action après l'analyse** permet de définir l'exécution automatique d'une action au terme d'une analyse :

- **Aucune action** – Aucune action n'est exécutée à la fin d'une analyse.
- **Arrêter** – L'ordinateur est mis hors tension à la fin d'une analyse.
- **Redémarrage si nécessaire** – L'ordinateur redémarre uniquement si cela est nécessaire pour terminer le nettoyage des menaces détectées.
- **Redémarrer** – Ferme tous les programmes ouverts et redémarre l'ordinateur à la fin d'une 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 l'interaction de l'utilisateur et redémarre l'ordinateur à la fin d'une analyse.
- **Veille** – Enregistre votre session et met l'ordinateur dans un état à faible consommation d'énergie pour que vous puissiez rapidement reprendre le travail.
- **Veille prolongée** – Déplace tous les éléments en cours d'exécution sur la RAM vers un fichier spécial sur le disque dur. Votre ordinateur est arrêté, mais reprend son état précédent lorsque vous le démarrez.

Les actions **Veille** et **Veille prolongée** sont disponibles selon les paramètres d'alimentation et de mise en veille du système d'exploitation de votre ordinateur ou les capacités du PC/ordinateur portable. N'oubliez pas qu'un ordinateur en veille est un ordinateur en fonctionnement. Il exécute toujours des fonctions de base et consomme de l'électricité lorsqu'il est alimenté par batterie. Pour conserver l'autonomie de la batterie, lors d'un déplacement par exemple, il est recommandé d'utiliser l'option de mise en veille prolongée.

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

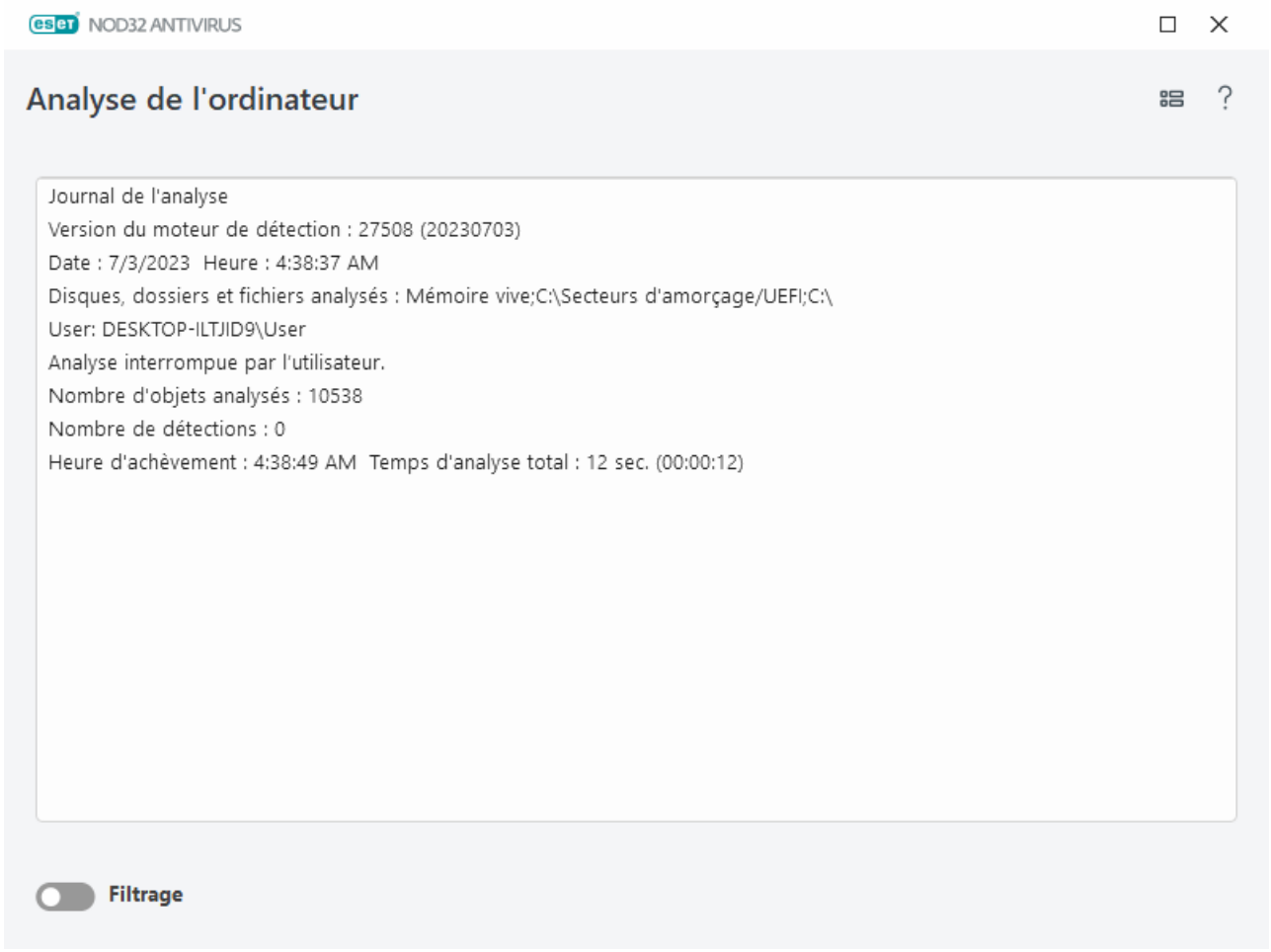
Journal d'analyse de l'ordinateur

Vous pouvez consulter des informations détaillées relatives à une analyse spécifique dans Fichiers journaux. Le journal de l'analyse contient les informations suivantes :

- Version du moteur de détection
- Date and heure de début
- Liste des disques, dossiers et fichiers analysés
- Nom de l'analyse planifiée (analyse planifiée uniquement)
- Utilisateur qui a lancé l'analyse.
- État de l'analyse
- Nombre d'objets analysés
- Nombre de détections effectuées
- Heure d'achèvement
- Durée totale de l'analyse

Le nouveau démarrage d'une tâche planifiée d'analyse de l'ordinateur est ignoré si la même tâche planifiée qui a été exécutée précédemment est toujours en cours d'exécution. La tâche d'analyse planifiée ignorée crée un journal d'analyse de l'ordinateur avec zéro objet analysé et l'état **L'analyse n'a pas commencé, car l'analyse précédente était toujours en cours d'exécution**.

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



Pour plus d'informations sur les entrées « ouverture impossible », « erreur d'ouverture » et/ou « archive endommagée », consultez cet article de la base de connaissances ESET.

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

Action	Utilisation
Filtrer les enregistrements identiques	Active le filtrage des journaux. Le journal n'affichera que les enregistrements du même type que celui sélectionné.
Filtrer	Cette option permet d'ouvrir la fenêtre Filtrage des journaux dans laquelle vous pouvez définir des critères pour des entrées de journal spécifiques. Raccourci clavier : `Ctrl+Shift+F`
Activer le filtre	Active les paramètres du filtre. Si vous activez le filtre pour la première fois, vous devez définir les paramètres. La fenêtre Filtrage des journaux s'ouvre.
Désactiver le filtre	Désactive le filtre (équivaut à cliquer sur le bouton bascule dans la partie inférieure).
Copier	Copie les enregistrements en surbrillance dans le Presse-papiers. Raccourci clavier : `Ctrl+C`
Copier tout	Copie tous les enregistrements dans la fenêtre.
Exporter	Exporte les enregistrements en surbrillance dans le Presse-papiers vers un fichier XML.
Exporter tout	Cette option exporte tous les enregistrements dans la fenêtre vers un fichier XML.

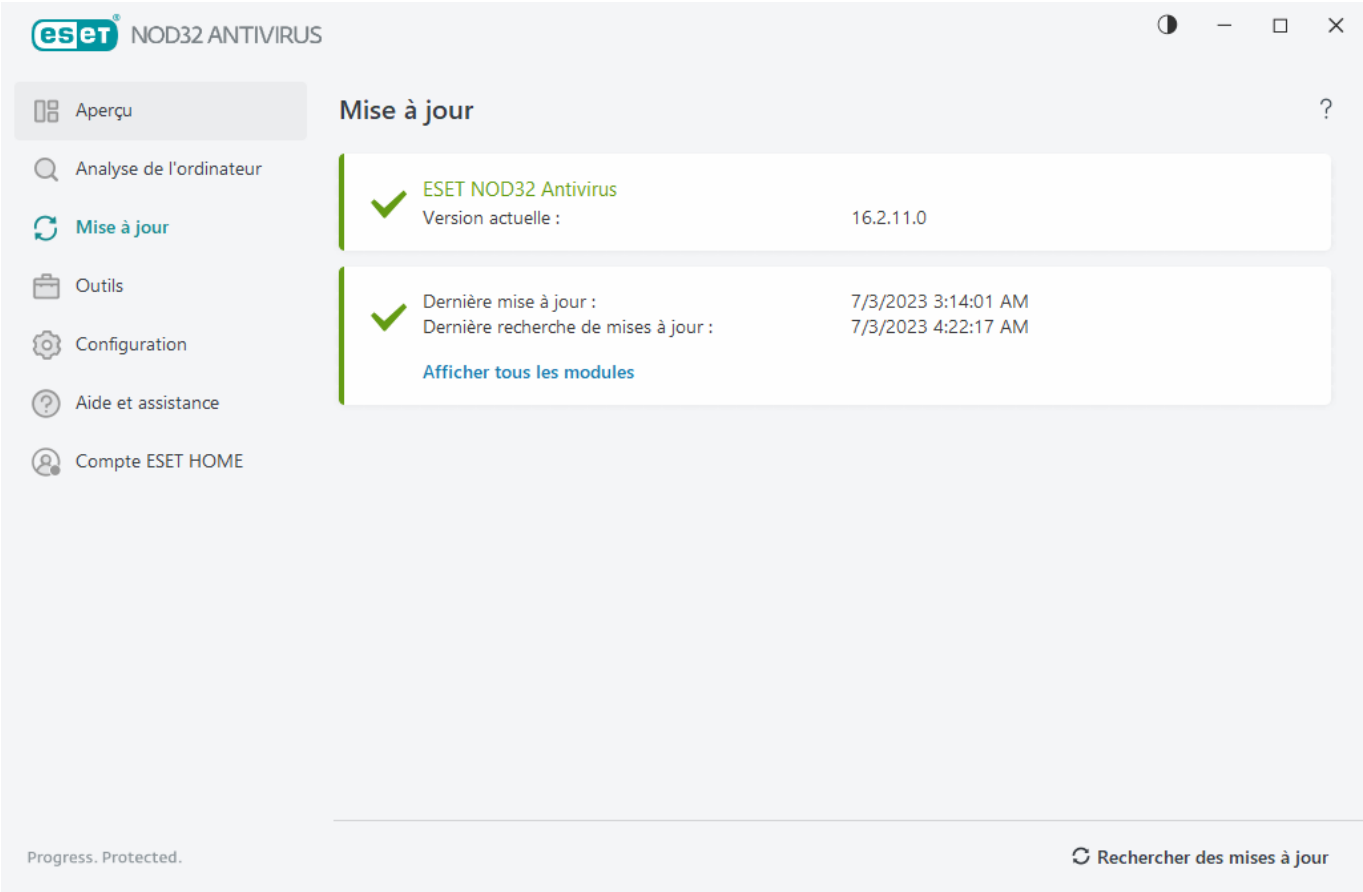
Action	Utilisation
Description de la détection	Ouvre l'encyclopédie des menaces ESET, qui contient des informations détaillées sur les dangers et les symptômes de l'infiltration sélectionnée.

Mettre à jour

La mise à jour régulière d'ESET NOD32 Antivirus est la meilleure méthode pour assurer le niveau maximum de sécurité à votre ordinateur. Le module de mise à jour veille à ce que les modules du programme et les composants système soient toujours à jour.

En cliquant sur **Mettre à jour** dans la fenêtre principale du programme, vous pouvez connaître l'état actuel de la mise à jour, notamment la date et l'heure de la dernière mise à jour. Vous pouvez également savoir si une mise à jour est nécessaire.

Outre les mises à jour automatiques, vous pouvez cliquer sur **Rechercher des mises à jour** pour déclencher une mise à jour manuelle. La mise à jour régulière des composants et des modules du programme est une opération importante qui assure la protection totale contre les attaques des codes malveillants. Il convient donc d'apporter une grande attention à la configuration des modules du produit et à leur fonctionnement. Vous devez activer votre produit à l'aide de votre clé d'activation pour recevoir les mises à jour. Si vous ne l'avez pas fait pendant l'installation, vous devez activer ESET NOD32 Antivirus pour accéder aux serveurs de mise à jour ESET. La clé d'activation vous a été envoyée dans un e-mail par ESET après l'achat d'ESET NOD32 Antivirus.



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

Dernière mise à jour réussie – Affiche la date de la dernière mise à jour réussie. Si vous ne voyez pas de date récente, il se peut que les modules du produit ne soient pas à jour.

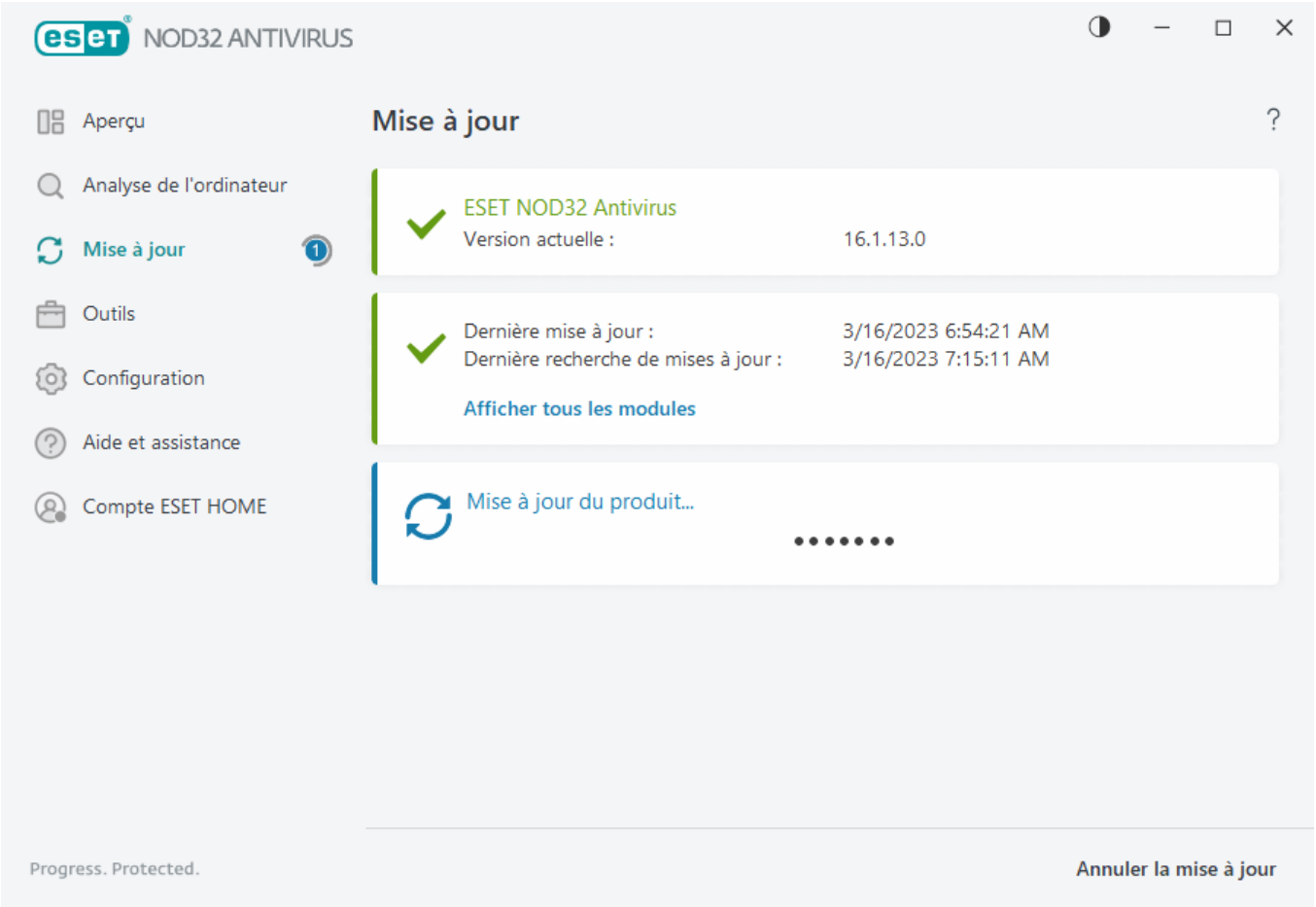
Dernière recherche réussie de mises à jour – Indique la date de la dernière recherche réussie de mises à jour.

Afficher tous les modules – Affiche des informations sur la liste des modules du programme installés.

Cliquez sur **Rechercher des mises à jour** pour rechercher la version la plus récente disponible d'ESET NOD32 Antivirus.

Processus de mise à jour

Après avoir cliqué sur **Rechercher des mises à jour**, le téléchargement commence. La barre de progression qui s'affiche indique le temps de téléchargement restant. Pour interrompre la mise à jour, cliquez sur **Annuler la mise à jour**.



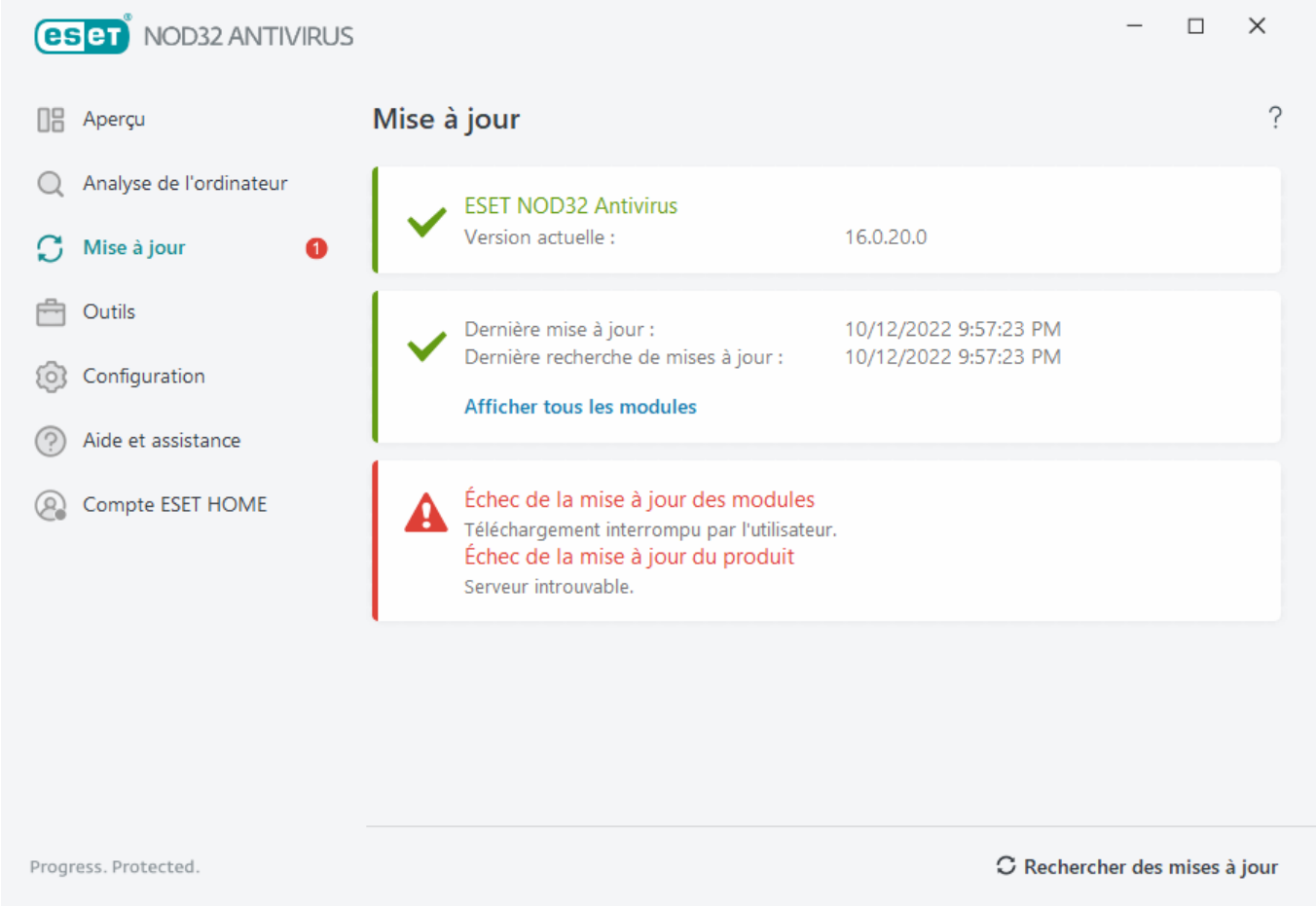
Dans des circonstances normales, une coche verte s'affiche dans la fenêtre **Mise à jour** pour indiquer que le programme est à jour. Si ce n'est pas le cas, le programme n'est pas à jour et le risque d'infection est accru. Veuillez mettre à jour les modules du programme dès que possible.

Échec de la mise à jour

Si un message indiquant l'échec d'une mise à jour des modules s'affiche, les problèmes suivants peuvent en être la cause :

1. **Abonnement non valide** – L'abonnement utilisé pour l'activation n'est pas valide ou est arrivé à expiration. Dans la fenêtre principale du programme, cliquez sur **Aide et assistance** > **Modifier l'abonnement**, puis activez votre produit.

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



Vous devez redémarrer l'ordinateur après une mise à jour réussie d'ESET NOD32 Antivirus vers une nouvelle version afin de vérifier que tous les modules du programme ont bien été mis à jour. Il n'est pas nécessaire de redémarrer l'ordinateur après les mises à jour régulières des modules.

Pour plus d'informations, consultez Résolution du message « Échec de la mise à jour des modules ».

Boîte de dialogue - Redémarrage requis

Un redémarrage de l'ordinateur est nécessaire après la mise à jour d'ESET NOD32 Antivirus vers une nouvelle version. Les nouvelles versions d'ESET NOD32 Antivirus offrent des améliorations ou apportent des solutions aux problèmes que les mises à jour automatiques des modules de programme ne peuvent pas résoudre.

La nouvelle version d'ESET NOD32 Antivirus peut être installée automatiquement, en fonction des paramètres de mise à jour du programme, ou manuellement en téléchargeant et en installant une version plus récente par

rapport à la version précédente.

Cliquez sur **Redémarrer maintenant** pour redémarrer votre ordinateur. Si vous envisagez de redémarrer votre ordinateur ultérieurement, cliquez sur **Me le rappeler ultérieurement**. Vous pourrez redémarrer manuellement votre ordinateur dans la section **Vue d'ensemble** de la fenêtre principale du programme.

Comment créer des tâches de mise à jour

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

Les mises à jour peuvent également être exécutées sous forme de tâches planifiées. Pour configurer une tâche planifiée, cliquez sur **Outils** > **Planificateur**. Par défaut, les tâches de mise à jour suivantes sont activées dans ESET NOD32 Antivirus :

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

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

Outils

Le menu **Outils** comprend des fonctionnalités qui offrent une sécurité supplémentaire et contribuent à simplifier l'administration d'ESET NOD32 Antivirus. Les outils disponibles sont les suivants :

 Fichiers journaux

 Processus en cours (si ESET LiveGrid® est activé dans ESET NOD32 Antivirus)

 Rapport sur la sécurité

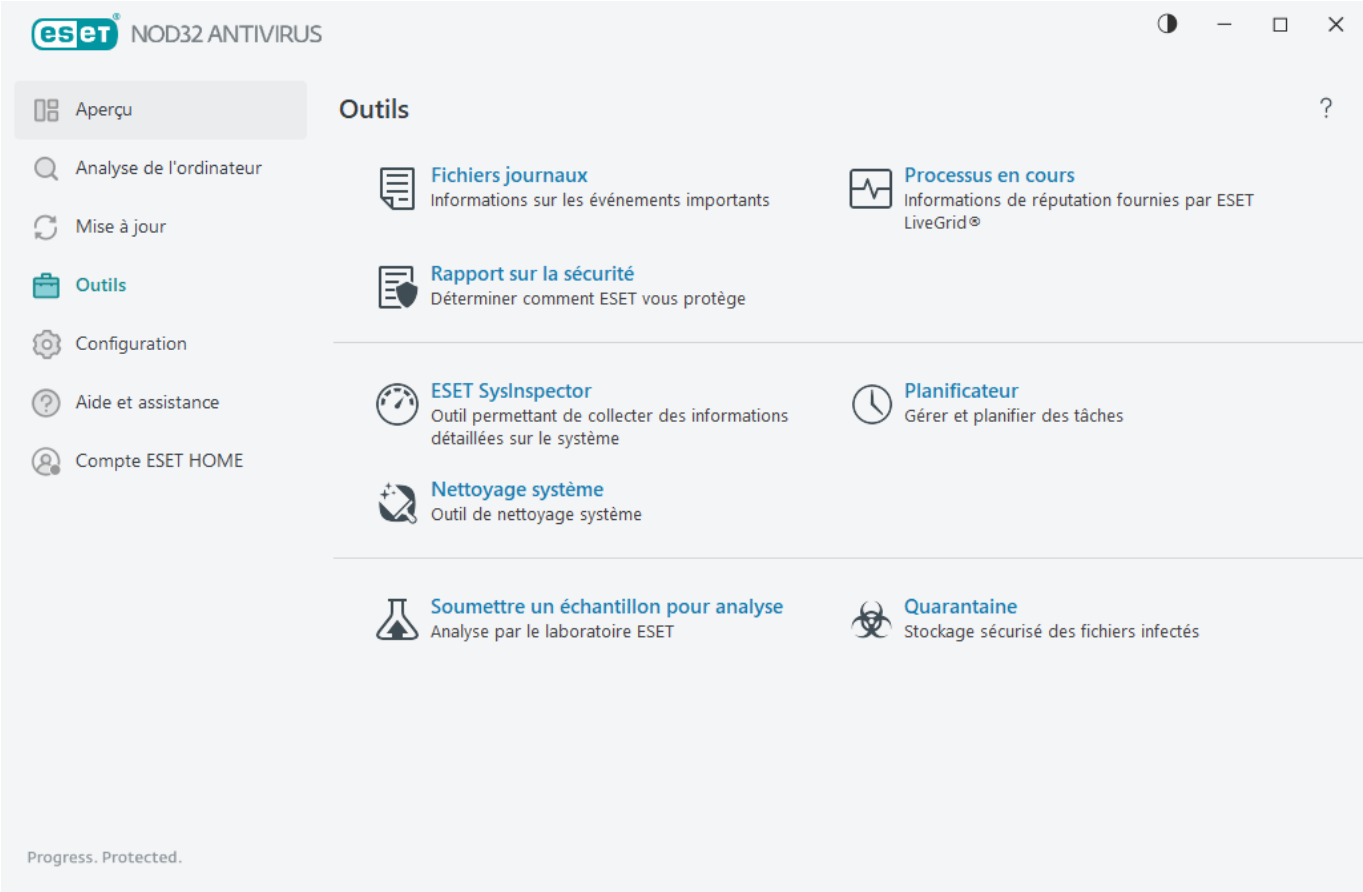
 ESET SysInspector

 Planificateur

 Outil de nettoyage système

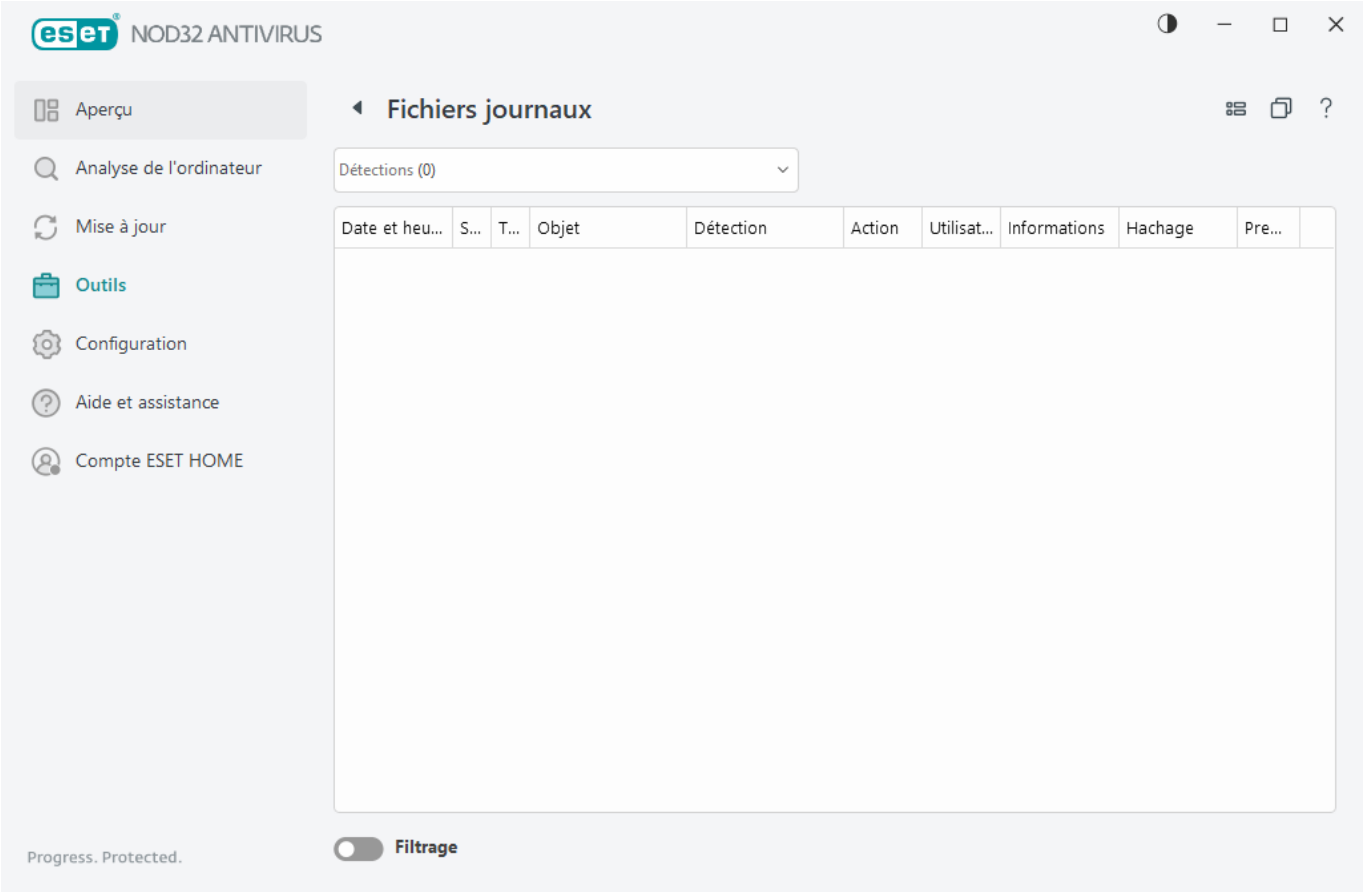
 Soumettre un échantillon pour analyse (peut ne pas être disponible selon votre configuration d'ESET LiveGrid®).

 Quarantaine



Fichiers journaux

Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées. La consignation représente un élément essentiel de l'analyse système, de la détection de menaces et du dépannage. La consignation est toujours active en arrière-plan sans interaction de l'utilisateur. Les informations sont enregistrées en fonction des paramètres de détail actifs. Il est possible de consulter les messages texte et les journaux directement à partir de l'environnement ESET NOD32 Antivirus, ainsi que d'archiver les journaux.



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

- **Détections** – Ce journal contient des informations sur les détections et infiltrations détectées par ESET NOD32 Antivirus. Les informations du journal comprennent l'heure de détection, le type d'analyseur, le type et l'emplacement de l'objet, le nom de la détection, l'action exécutée, le nom de l'utilisateur connecté au moment où l'infiltration a été détectée, le hachage et la première occurrence. Les infiltrations non nettoyées sont toujours signalées par un texte rouge sur fond rouge clair. Les infiltrations nettoyées sont signalées par un texte jaune sur fond blanc. Les applications potentiellement dangereuses ou indésirables non nettoyées sont quant à elles signalées par un texte jaune sur fond blanc.

- **Événements** – Toutes les actions importantes exécutées par ESET NOD32 Antivirus sont enregistrées dans le journal des événements. Le journal des événements contient des informations sur les événements qui se sont produits dans le programme. Il permet aux administrateurs système et aux utilisateurs de résoudre des problèmes. Les informations qu'il contient peuvent aider à trouver une solution à un problème qui s'est produit dans le programme.

- **Analyse de l'ordinateur** : cette fenêtre affiche toutes les analyses effectuées. Chaque ligne correspond à un seul analyse de l'ordinateur. Double-cliquez sur une entrée pour afficher les détails de l'analyse sélectionné.

- **HIPS** – Contient des entrées de règles HIPS spécifiques qui ont été marquées pour enregistrement. Le protocole affiche l'application qui a déclenché l'opération, le résultat (si la règle a été autorisée ou bloquée), ainsi que le nom de la règle.

- **Sites Web filtrés** – Cette liste est utile si vous souhaitez afficher la liste des sites web bloqués par la protection de l'accès web. Chaque journal comprend l'heure, l'adresse URL, l'utilisateur et l'application ayant créé une connexion à un site Web en particulier.

- **Contrôle de périphérique** : contient des enregistrements des supports amovibles ou périphériques qui ont été connectés à l'ordinateur. Seuls les périphériques auxquels correspond une règle de contrôle seront enregistrés dans le fichier journal. Si la règle ne correspond pas à un périphérique connecté, aucune entrée de journal ne sera créée pour un périphérique connecté. Des détails figurent également tels que le type de périphérique, le numéro de série, le nom du fournisseur et la taille du support (le cas échéant).

Sélectionnez le contenu d'un journal, puis appuyez sur **CTRL + C** pour le copier dans le Presse-papiers. Maintenez les touches **CTRL** ou **SHIFT** enfoncées pour sélectionner plusieurs entrées.

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

Cliquez avec le bouton droit sur une entrée pour afficher le menu contextuel. Le menu contextuel permet d'accéder aux options suivantes :

- **Afficher** – Affiche des détails supplémentaires sur le journal sélectionné dans une nouvelle fenêtre.

- **Filtrer les enregistrements identiques** – Si vous activez ce filtre, vous voyez uniquement les enregistrements du même type (diagnostics, avertissement, etc.).

- **Filtrer** – Après avoir cliqué sur cette option, la fenêtre Filtrage des journaux permet de définir des critères de filtrage pour des entrées de journal spécifiques.

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

- **Désactiver le filtre** – Supprime tous les paramètres du filtre (comme décrit ci-dessus).

- **Copier/Copier tout** – Copie les informations sur les entrées sélectionnées.

- **Copier la cellule** – Copie le contenu de la cellule sur laquelle vous avez cliqué avec le bouton droit.

- **Supprimer/Supprimer tout** – Supprime les entrées sélectionnées ou toutes les entrées affichées. Vous devez disposer des privilèges d'administrateur pour effectuer cette action.

- **Exporter/Exporter tout** – Exporte les informations sur les entrées sélectionnées ou toutes les entrées au format XML.

- **Rechercher/Suivant/Précédent** – Après avoir cliqué sur cette option, vous pouvez définir des critères de filtrage pour sélectionner l'entrée spécifique à l'aide de la fenêtre Filtrage des journaux.

- **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 (non disponible pour les détections de logiciel malveillant).

- **Ajouter à la liste autorisée de la protection du navigateur** : ouvre la fenêtreListe autorisée de la protection du navigateur et ajoute l'élément à la liste.

Filtrage des journaux

Cliquez sur **Filtrage** dans **Outils** > **Fichiers journaux** pour définir les critères de filtrage.

La fonctionnalité de filtrage des journaux vous permet de trouver les informations que vous recherchez, en particulier lorsqu'il existe de nombreuses entrées. Elle permet de limiter les entrées de journal, par exemple, si vous recherchez un type spécifique d'événement, d'état ou de période. 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.

Saisissez le mot-clé que vous recherchez dans le champ **Rechercher le texte**. Utilisez le menu déroulant **Rechercher dans les colonnes** pour affiner votre recherche. Choisissez une ou plusieurs entrées dans le menu déroulant **Types d'entrée de journal**. Définissez la **Période** à partir de laquelle vous souhaitez afficher les résultats. Vous pouvez également utiliser d'autres options de recherche, telles que **Mot entier** ou **Respecter la casse**.

Rechercher le texte

Saisissez une chaîne (mot ou partie d'un 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'enregistrements

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

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

Période

Définissez la période pour laquelle vous souhaitez afficher les résultats :

- **Non spécifié** (option par défaut) – N'effectue aucune recherche dans la période ; effectue une recherche dans l'intégralité du journal.
- **Dernier jour**

- **La semaine dernière**
- **Le mois dernier**
- **Période** – Vous pouvez indiquer la période exacte (De : et À :) afin de filtrer les enregistrements correspondant à la période indiquée.

Mot entier

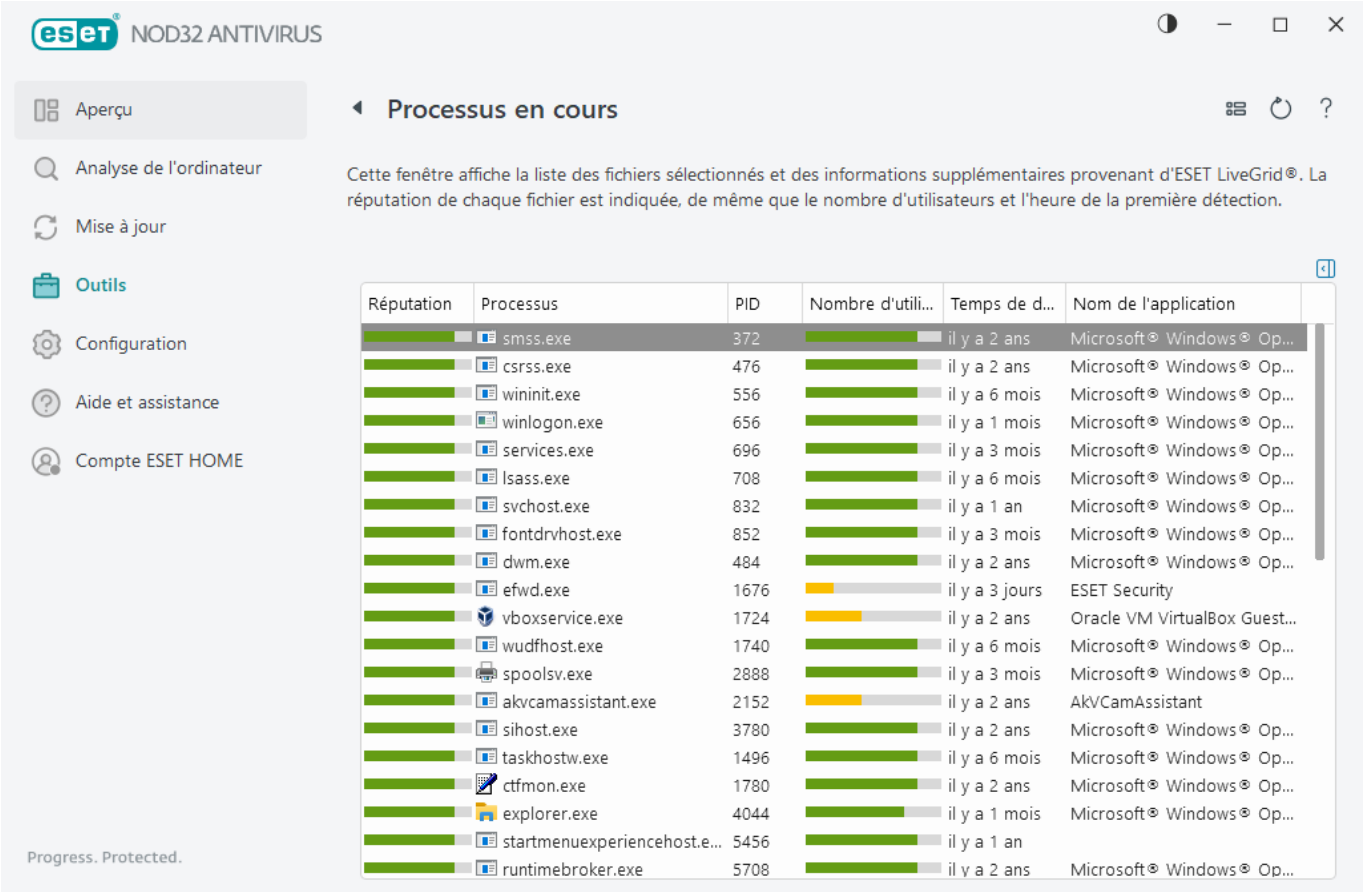
Utilisez cette case à cocher si vous souhaitez rechercher des mots complets afin d'obtenir des résultats plus précis.

Respecter la casse

Activez cette option s'il est important que vous utilisiez des majuscules ou des minuscules pendant le filtrage. Une fois que vous avez configuré vos options de filtrage/recherche, cliquez sur **OK** pour afficher les entrées de journal filtrées ou sur **Rechercher** pour lancer la recherche. La recherche dans les fichiers journaux s'effectue de haut en bas, à partir de la position actuelle (de l'enregistrement sélectionné). La recherche s'arrête lorsqu'elle trouve le premier enregistrement correspondant. Appuyez sur **F3** pour rechercher l'enregistrement suivant ou cliquez avec le bouton droit et sélectionnez **Rechercher** pour affiner vos options de recherche.

Processus en cours

Les processus en cours affichent les programmes ou processus en cours d'exécution sur votre ordinateur et informe ESET immédiatement et en permanence de l'existence de nouvelles infiltrations. ESET NOD32 Antivirus fournit des informations détaillées sur l'exécution des processus afin de protéger les utilisateurs à l'aide de la technologie ESET LiveGrid®.



Réputation – Dans la majorité des cas, ESET NOD32 Antivirus et la technologie ESET LiveGrid® attribuent des niveaux de risque aux objets (fichiers, processus, clés de registre, etc.) sur la base d'une série de règles heuristiques qui examinent les caractéristiques de chaque objet, puis qui évaluent le potentiel d'activité malveillante. Cette analyse heuristique attribue aux objets un niveau de risque allant de 1 – OK (vert) à 9 – Risqué (rouge).

Processus – Nom de l'image du programme ou du processus en cours d'exécution sur l'ordinateur. Vous pouvez également utiliser le Gestionnaire de tâches pour afficher tous les processus en cours d'exécution sur votre ordinateur. Pour ouvrir le Gestionnaire de tâches, cliquez avec le bouton droit sur une zone vide de la barre des tâches, puis cliquez sur **Gestionnaire de tâches** ou appuyez sur les touches **Ctrl**+**Maj**+**Échap** du clavier.

Les applications connues marquées OK (vert) sont saines (répertoriées dans la liste blanche) et sont exclues de l'analyse pour améliorer les performances.

PID– Le numéro d'identifiant du processus peut être utilisé comme paramètre dans divers appels de fonction (comme régler la priorité du processus, par exemple).

Nombre d'utilisateurs – Nombre d'utilisateurs utilisant une application donnée. Ces informations sont collectées par la technologie ESET LiveGrid®.

Temps de découverte – Durée écoulée depuis la détection de l'application par la technologie ESET LiveGrid®.

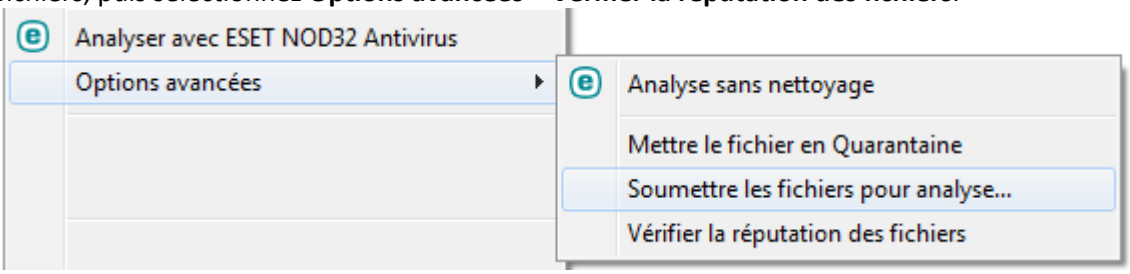
Une application marquée Inconnu (orange) n'est pas nécessairement un logiciel malveillant. Il s'agit généralement d'une nouvelle application. Si ce fichier vous semble toutefois suspect, vous pouvez le soumettre pour analyse au laboratoire de recherche ESET. S'il s'avère être une application malveillante, sa détection sera intégrée à une prochaine mise à jour.

Nom de l'application – Nom d'un programme ou d'un processus.

Cliquez sur une application pour afficher les détails suivants à propos de celle-ci :

- **Chemin** – Emplacement de l'application sur l'ordinateur.
- **Taille** – Taille du fichier en Ko (kilo-octets) ou Mo (méga-octets).
- **Description** – Caractéristiques du fichier basées sur sa description du système d'exploitation.
- **Société** – Nom du fournisseur ou du processus de l'application.
- **Version** – Informations fournies par l'éditeur de l'application.
- **Produit** – Nom de l'application et/ou nom de l'entreprise.
- **Date de création/Date de modification** – Date et heure de création (modification).

Vous pouvez également vérifier la réputation des fichiers qui n'agissent pas en tant que programmes/processus en cours. Pour ce faire, cliquez avec le bouton droit dessus dans un explorateur de fichiers, puis sélectionnez **Options avancées** > **Vérifier la réputation des fichiers**.



Rapport sur la sécurité

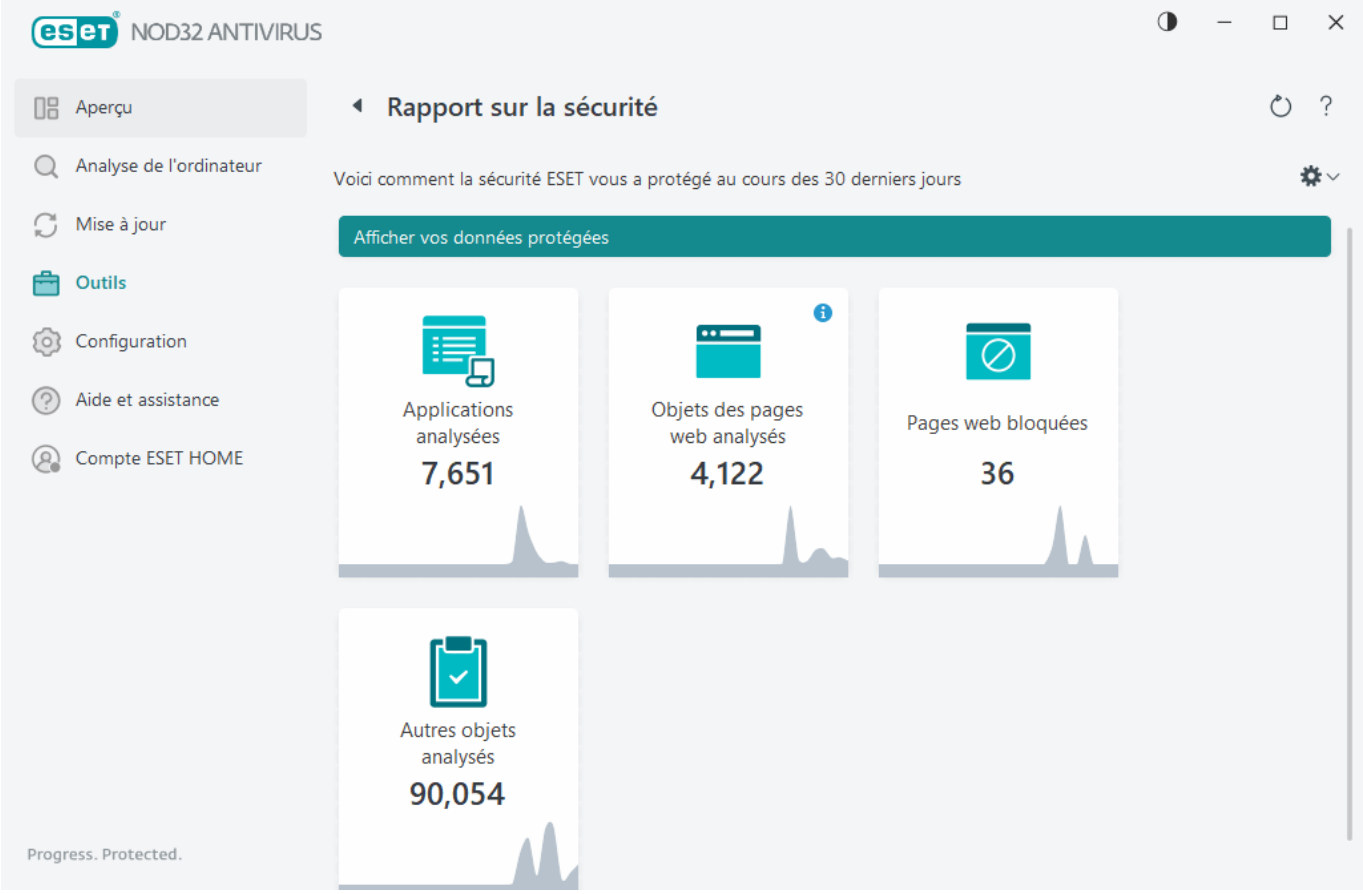
Cette fonctionnalité donne une vue d'ensemble des statistiques pour les catégories suivantes :

- **Pages Web bloquées** – Indique le nombre de pages web bloquées (URL en liste noire pour les applications potentiellement indésirables, l'hameçonnage, une box Internet piratée, une adresse IP ou un certificat).
- **Objets d'e-mail infectés détectés** – Indique le nombre d'objets d'e-mail infectés ayant été détectés.
- **Application potentiellement indésirable détectée** – Indique le nombre d'applications potentiellement indésirables.
- **Documents analysés** – Indique le nombre d'objets de document analysés.
- **Applications analysées** – Indique le nombre d'objets exécutables analysés.
- **Autres objets analysés** – Indique le nombre d'autres objets analysés.
- **Objets des pages Web analysés** – Indique le nombre d'objets de pages Web analysés.
- **Objets des e-mails analysés** – Indique le nombre d'objets d'e-mail analysés.

L'ordre de ces catégories repose sur la valeur numérique (de la plus élevée à la plus basse). Les catégories avec des valeurs nulles ne sont pas affichées. **Cliquez sur Afficher** plus pour développer et afficher les catégories masquées.

Lorsque la fonctionnalité est activée, elle n'est plus affichée comme étant non fonctionnelle dans le rapport sur la sécurité.

Cliquez sur l'engrenage dans le coin supérieur droit pour **activer/désactiver les notifications des rapports** ou sélectionner si les données des 30 derniers jours ou depuis l'activation du produit doivent être affichées. Si ESET NOD32 Antivirus est installé depuis moins de 30 jours, seul le nombre de jours depuis l'installation peut être sélectionné. La période de 30 jours est définie par défaut.



L'option **Réinitialiser les données** permet d'effacer toutes les statistiques et de supprimer les données existantes pour le rapport sur la sécurité. Cette action doit être confirmée, sauf si vous désélectionnez l'option **Demander avant de réinitialiser les statistiques** dans Configuration avancée > **Notifications** > **Alertes interactives** > **Messages de confirmation** > **Messages de confirmation**.

ESET SysInspector

ESET SysInspector est une application qui inspecte méticuleusement votre ordinateur, réunit des informations détaillées sur les composants système, tels que pilotes et applications, connexions réseau ou entrées de registre importantes, puis évalue le niveau de risque de chaque composant. Ces informations peuvent aider à déterminer la cause d'un comportement suspect du système pouvant être dû à une incompatibilité logicielle ou matérielle, ou à une infection par un logiciel malveillant. Pour découvrir comment utiliser ESET SysInspector, consultez l'aide en ligne ESET SysInspector.

La fenêtre ESET SysInspectoraffiche les informations suivantes sur les journaux :

- **Heure** – Heure de création du journal.
- **Commentaire** – Bref commentaire.

- **Utilisateur** – Nom de l'utilisateur qui a créé le journal.
- **État** – État de création du journal.

Les actions disponibles sont les suivantes :

- **Afficher** – Ouvre le journal sélectionné dans ESET SysInspector. Vous pouvez également cliquer avec le bouton droit sur un fichier journal, puis sélectionner **Afficher** dans le menu contextuel.
- **Créer** – Crée un journal. Patientez jusqu'à ce qu'ESET SysInspector soit généré (état **Créé**) avant d'accéder au journal. Le journal est enregistré dans C:\ProgramData\ESET\ESET Security\SysInspector.
- **Supprimer** – Supprime les journaux sélectionnés de la liste.

Les options suivantes sont disponibles dans le menu contextuel lorsqu'un fichier journal ou plusieurs fichiers journaux sont sélectionnés :

- **Afficher** – Ouvre le journal sélectionné dans ESET SysInspector (équivaut à double-cliquer sur un journal).
- **Créer** – Crée un journal. Patientez jusqu'à ce qu'ESET SysInspector soit généré (état **Créé**) avant d'accéder au journal.
- **Supprimer** – Supprime les journaux sélectionnés de la liste.
- **Supprimer tout** – Supprime tous les journaux.
- **Exporter** – Exporte le journal dans un fichier .xml ou un fichier .xml compressé.

Planificateur

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

Le planificateur est accessible depuis la fenêtre principale de ESET NOD32 Antivirus en cliquant sur **Outils** > **Planificateur**. Le **planificateur** contient la liste de toutes les tâches planifiées, des propriétés de configuration telles que la date et l'heure prédéfinies, ainsi que le profil d'analyse utilisé.

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

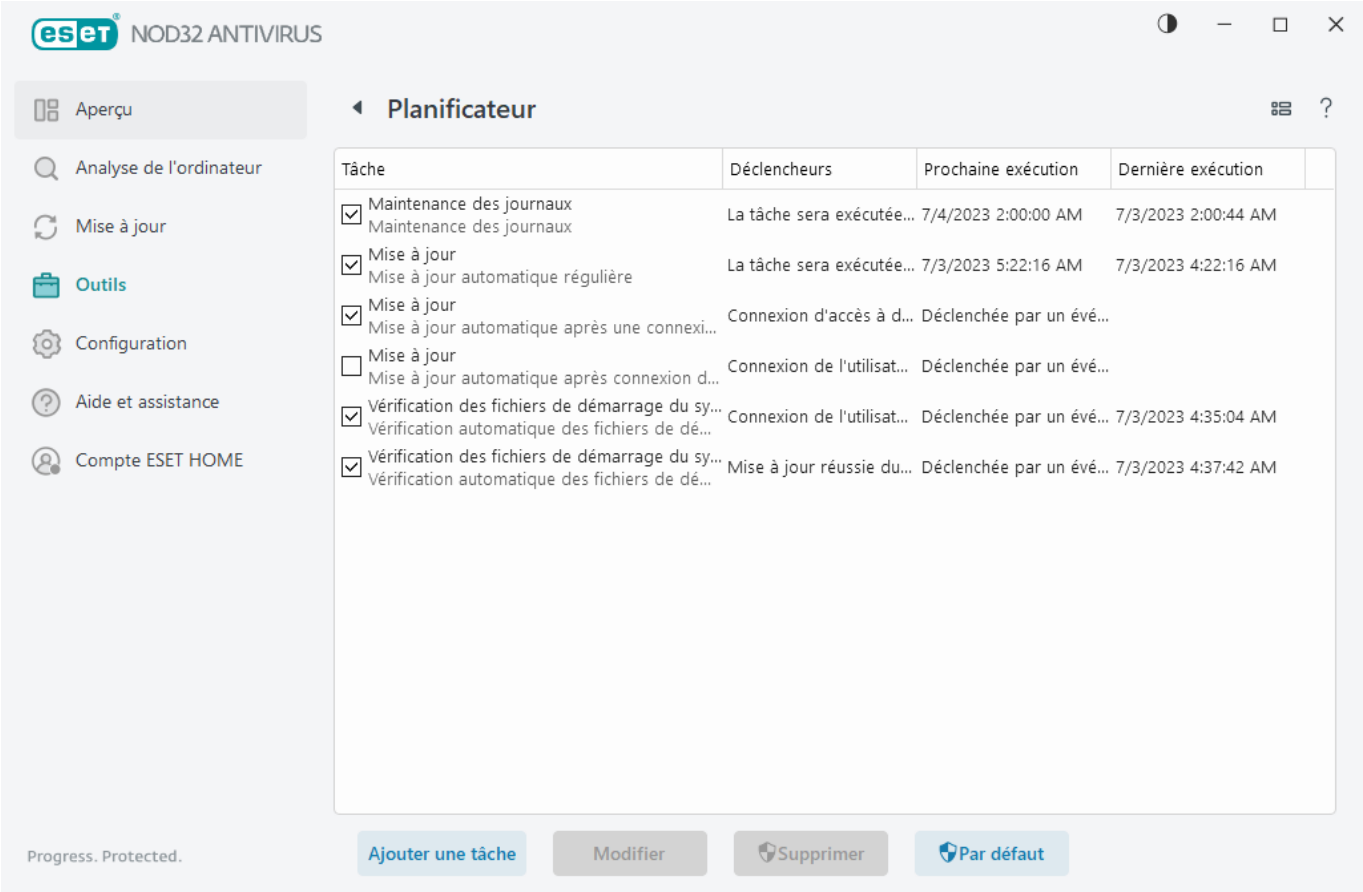
Par défaut, les tâches planifiées suivantes sont affichées dans le **planificateur** :

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

- **Vérification des fichiers de démarrage** (après l'ouverture de session de l'utilisateur)

- **Vérification des fichiers de démarrage** (après la mise à jour réussie du moteur de détection)

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



Ajout d'une nouvelle tâche

1. Cliquez sur **Ajouter une tâche** dans la partie inférieure de la fenêtre.

2. Entrez le nom de la tâche.

3. Sélectionnez la tâche souhaitée dans le menu déroulant :

   - **Exécuter une application externe** – Permet de programmer l'exécution d'une application externe.

   - **Maintenance des journaux** - Les fichiers journaux contiennent également des éléments provenant d'enregistrements supprimés. Cette tâche optimise régulièrement les entrées des fichiers journaux pour garantir leur efficacité.

   - **Contrôle des fichiers de démarrage du système** – Vérifie les fichiers autorisés à s'exécuter au démarrage du système ou lors de l'ouverture de session de l'utilisateur.

   - **Créer un rapport de l'état de l'ordinateur** – Crée un instantané ESET SysInspector de l'ordinateur et collecte des informations détaillées sur les composants système (pilotes, applications) et évalue le niveau de risque de chacun de ces composants.

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

- **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 activant/désactivant la case à cocher correspondante dans la liste des tâches planifiées). Cliquez ensuite sur **Suivant** et sélectionnez l'une des options de planification :

- **Une fois** – La tâche est exécutée à la date et à l'heure prédéfinies.

- **Plusieurs fois** – La tâche est exécutée aux intervalles indiqués.

- **Quotidiennement** – La tâche est exécutée tous les jours à l'heure définie.

- **Chaque semaine** – La tâche est exécutée à l'heure et au jour prédéfinis.

- **Déclenchée par un événement** – La tâche est exécutée après un événement particulier.

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

- **À la prochaine heure planifiée**

- **Dès que possible**

- **Immédiatement, si la durée écoulée depuis la dernière exécution dépasse (heures)** – Représente le délai écoulé depuis la première exécution ignorée de la tâche. Si ce délai est dépassé, la tâche s'exécutera immédiatement. Définissez l'heure à l'aide du compteur ci-dessous.

Pour examiner une tâche planifiée, cliquez avec le bouton droit dessus, puis cliquez sur **Afficher les détails des tâches**.

Options d'analyse planifiée

Cette fenêtre permet de définir des options avancées pour une opération d'analyse de l'ordinateur planifiée.

Pour effectuer une analyse sans action de nettoyage, cliquez sur **Paramètres avancés** et sélectionnez **Analyse sans nettoyage**. L'historique de l'analyse est enregistré dans le journal de l'analyse.

Lorsque l'option **Ignorer les exclusions** est sélectionnée, les fichiers portant une extension exclue de l'analyse sont analysés sans exception.

Le menu déroulant **Action après l'analyse** permet de définir l'exécution automatique d'une action au terme d'une analyse :

- **Aucune action** – Aucune action n'est exécutée à la fin d'une analyse.

- **Arrêter** – L'ordinateur est mis hors tension à la fin d'une analyse.

• **Redémarrage si nécessaire** – L'ordinateur redémarre uniquement si cela est nécessaire pour terminer le nettoyage des menaces détectées.

• **Redémarrer** – Ferme tous les programmes ouverts et redémarre l'ordinateur à la fin d'une 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 l'interaction de l'utilisateur et redémarre l'ordinateur à la fin d'une analyse.

• **Veille** – Enregistre votre session et met l'ordinateur dans un état à faible consommation d'énergie pour que vous puissiez rapidement reprendre le travail.

• **Veille prolongée** – Déplace tous les éléments en cours d'exécution sur la RAM vers un fichier spécial sur le disque dur. Votre ordinateur est arrêté, mais reprend son état précédent lorsque vous le démarrez.

> Les actions **Veille** et **Veille prolongée** sont disponibles selon les paramètres d'alimentation et de mise en veille du système d'exploitation de votre ordinateur ou les capacités du PC/ordinateur portable. N'oubliez pas qu'un ordinateur en veille est un ordinateur en fonctionnement. Il exécute toujours des fonctions de base et consomme de l'électricité lorsqu'il est alimenté par batterie. Pour conserver l'autonomie de la batterie, lors d'un déplacement par exemple, il est recommandé d'utiliser l'option de mise en veille prolongée.

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

Sélectionnez **Impossible d'annuler l'analyse** pour ne pas autoriser les utilisateurs sans privilège à interrompre les actions exécutées après l'analyse.

Sélectionnez l'option **L'analyse peut être interrompue par l'utilisateur pendant (min)** si vous souhaitez autoriser les utilisateurs avec des privilèges limités à interrompre l'analyse de l'ordinateur pendant une période spécifiée.

Consultez également la 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 que vous cliquez avec le bouton droit sur une tâche personnalisée du planificateur et cliquez sur **Afficher les détails des tâches**.

Détails de la tâche

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

• **Exécuter une application externe** – Permet de programmer l'exécution d'une application externe.

• **Maintenance des journaux** - Les fichiers journaux contiennent également des éléments provenant d'enregistrements supprimés. Cette tâche optimise régulièrement les entrées des fichiers journaux pour

garantir leur efficacité.

• **Contrôle des fichiers de démarrage du système** – Vérifie les fichiers autorisés à s'exécuter au démarrage du système ou lors de l'ouverture de session de l'utilisateur.

• **Créer un rapport de l'état de l'ordinateur** – Crée un instantané ESET SysInspector de l'ordinateur et collecte des informations détaillées sur les composants système (pilotes, applications) et évalue le niveau de risque de chacun de ces composants.

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

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

Planification de la tâche

La tâche est exécutée de manière répétée aux intervalles indiqués. Sélectionnez l'une des options de planification suivantes :

• **Une fois** – La tâche est exécutée une fois, à la date et à l'heure prédéfinies.

• **Plusieurs fois** – La tâche est exécutée aux intervalles indiqués (en heures).

• **Quotidiennement** – La tâche est exécutée tous les jours à l'heure définie.

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

• **Déclenchée par un événement** – La tâche est exécutée après un événement particulier.

Ignorer la tâche en cas d'alimentation par batterie – Une tâche ne démarre pas si l'ordinateur est alimenté par batterie au moment de l'exécution prévue. Ceci s'applique également aux ordinateurs alimentés par un onduleur.

Planification de la tâche - Une fois

Exécution de tâche – La tâche spécifiée est exécutée une fois, à la date et à l'heure indiquées.

Planification de la tâche - Quotidienne

La tâche est exécutée tous les jours à l'heure définie.

Planification de la tâche - Hebdomadaire

La tâche sera exécutée de manière répétée chaque semaine aux jour(s) et heure(s) sélectionnés.

Planification de la tâche - Déclenchée par un événement

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

- **Chaque fois que l'ordinateur démarre**
- **Au premier démarrage de l'ordinateur chaque jour**
- **Connexion d'accès à distance à Internet/au réseau VPN**
- **Mise à jour du module réussie**
- **Mise à jour du produit réussie**
- **Ouverture de session de l'utilisateur**
- **Détection de menace**

Lors de la planification d'une tâche déclenchée par un événement, vous pouvez indiquer l'intervalle minimum entre deux exécutions de la tâche. Par exemple, si vous ouvrez une session sur l'ordinateur plusieurs fois par jour, choisissez un intervalle de 24 heures afin de réaliser la tâche uniquement à la première ouverture de session de la journée, puis le lendemain.

Tâche ignorée

Une tâche peut être ignorée si l'ordinateur est éteint ou alimenté par batterie. Sélectionnez à quel moment la tâche ignorée doit être exécutée parmi ces options, puis cliquez sur **Suivant** :

- **À la prochaine heure planifiée** – La tâche est exécutée si l'ordinateur est mis sous tension à la prochaine heure planifiée.
- **Dès que possible** – La tâche s'exécute lorsque l'ordinateur est mis sous tension.
- **Immédiatement, si la durée écoulée depuis la dernière exécution dépasse (heures)** – Représente le délai écoulé depuis la première exécution ignorée de la tâche. Si ce délai est dépassé, la tâche s'exécutera immédiatement.

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

Un exemple de tâche est défini pour s'exécuter de manière répétée toutes les heures. L'option **Immédiatement, si le temps écoulé depuis la dernière exécution planifiée est supérieur à (heures)** est sélectionnée et le délai dépassé est défini sur deux heures. La tâche s'exécute à 13 heures, et une fois terminée, l'ordinateur se met en veille :

- L'ordinateur sort du mode veille à 15 h 30. La première exécution ignorée de la tâche a eu lieu à 14 h 00. Il ne s'est écoulé qu'une heure et demie depuis 14 heures ; la tâche sera donc exécutée à 16 heures.
- L'ordinateur sort du mode veille à 16 h 30. La première exécution ignorée de la tâche a eu lieu à 14 h 00. Deux heures et demie se sont écoulées depuis 14 h 00 ; la tâche sera donc exécutée immédiatement.

Détails de la tâche - Mise à jour

Pour mise 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. Ce procédé est notamment adapté aux portables dont la mise à jour s'effectue normalement depuis un serveur de mise à jour du réseau local, mais dont les propriétaires se connectent souvent à Internet à partir d'autres réseaux. Par conséquent, 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

Cet tâche permet de planifier l'exécution d'une application externe.

Fichier exécutable – Choisissez un fichier exécutable dans l'arborescence, cliquez sur l'option **...** ou saisissez le chemin manuellement.

Dossier de travail – Définissez le répertoire de travail de l'application externe. Tous les fichiers temporaires du **fichier exécutable** sélectionné sont créés dans ce répertoire.

Paramètres – Paramètres de ligne de commande de l'application (facultatif).

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

Outil de nettoyage système

L'outil de nettoyage système est un outil qui permet de restaurer un état utilisable de l'ordinateur après le nettoyage de la menace. Les logiciels malveillants peuvent désactiver les utilitaires système tels que l'éditeur de registre, le gestionnaire des tâches ou Windows Updates. L'outil de nettoyage système restaure en un seul clic les valeurs et paramètres par défaut d'un système donné.

Il signale les problèmes dans cinq catégories de paramètres :

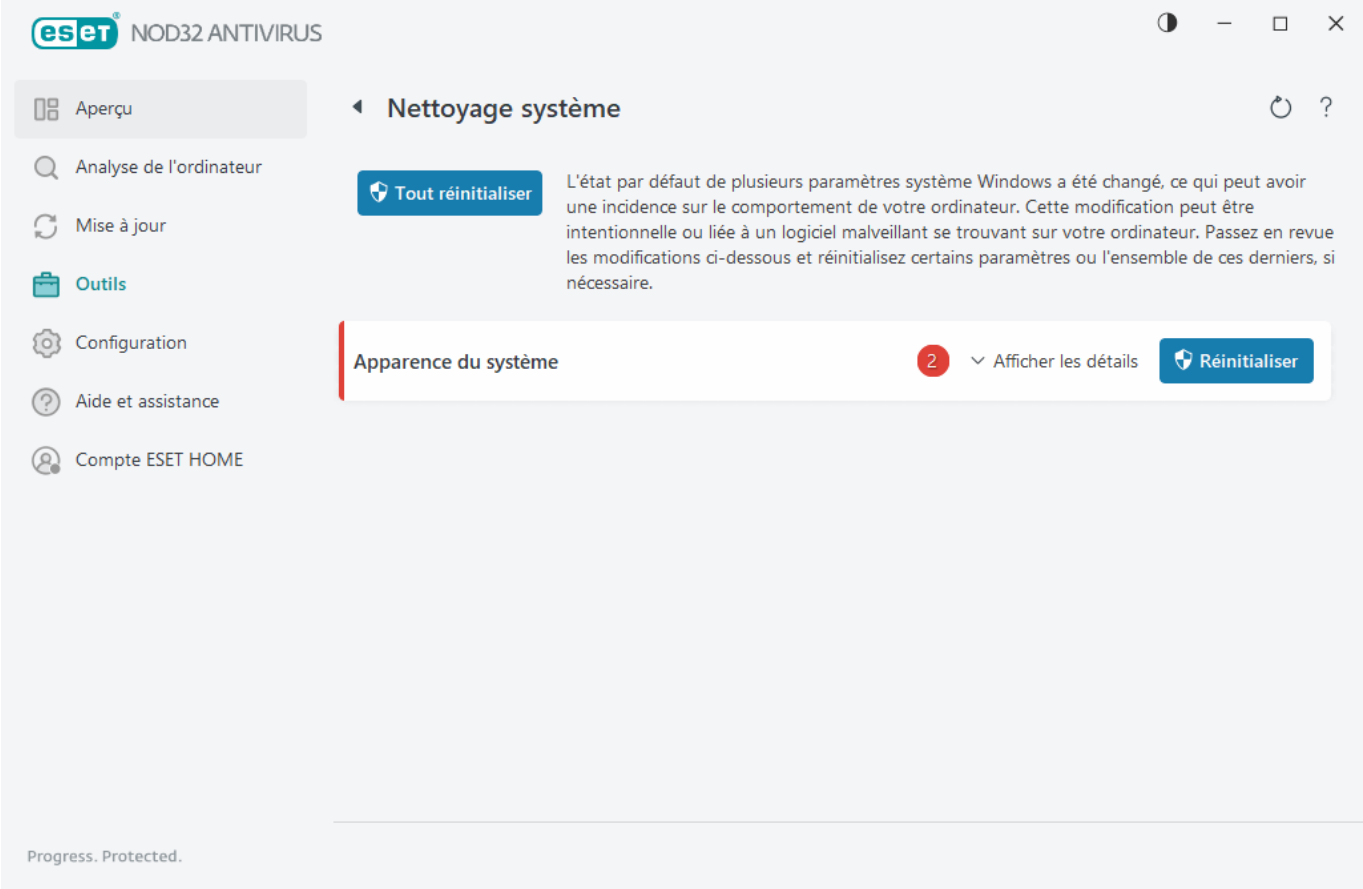
- **Paramètres de sécurité** : modifications des paramètres qui peuvent entraîner une vulnérabilité accrue de votre ordinateur (Windows Update, par exemple).
- **Paramètres système** : modifications des paramètres système qui peuvent modifier le comportement de l'ordinateur (associations de fichiers, par exemple).
- **Apparence du système** : paramètres qui modifient l'aspect du système (papier peint du Bureau, par exemple).
- **Fonctionnalités désactivées** : fonctionnalités et applications importantes qui peuvent être désactivées.
- **Restauration du système Windows** : paramètres de la fonctionnalité Restauration du système Windows, qui permet de rétablir un état précédent du système.

Un nettoyage du système peut être demandé dans les cas suivants :

- lorsqu'une menace est détectée ;

- lorsqu'un utilisateur clique sur **Réinitialiser**

Vous pouvez passer en revue les modifications et réinitialiser les paramètres si nécessaire.



Seul un utilisateur disposant des droits d'administrateur peut effectuer des actions dans l'outil de nettoyage système.

Quarantaine

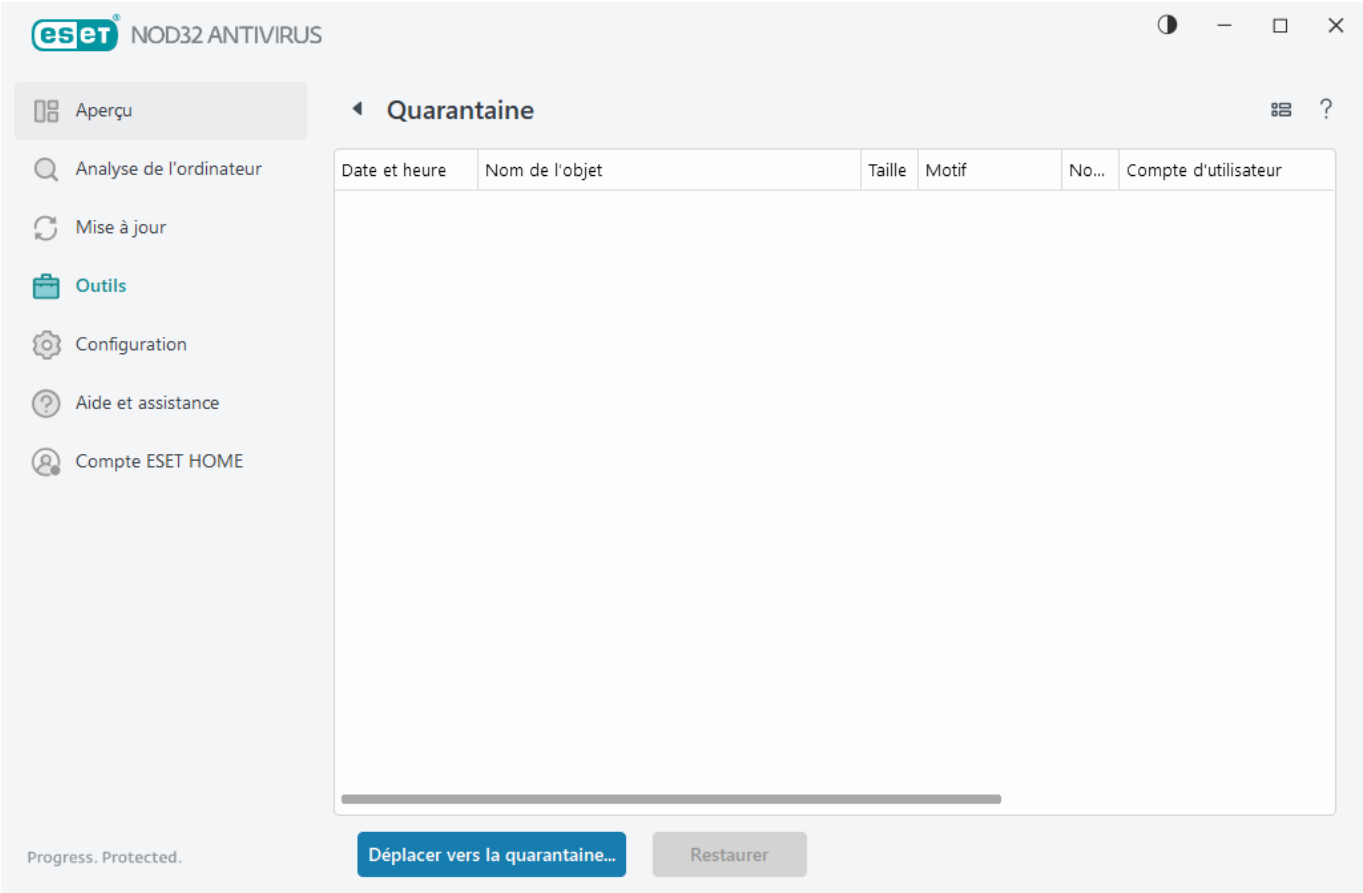
La fonction principale de la quarantaine est de stocker en toute sécurité les objets signalés (tels que les logiciels malveillants, les fichiers infectés ou les applications potentiellement indésirables).

La quarantaine est accessible depuis la fenêtre principale d'ESET NOD32 Antivirus en cliquant sur **Outils** > **Quarantaine**.

Les fichiers stockés dans le dossier de quarantaine peuvent être consultés dans un tableau qui affiche les informations suivantes :

- date et l’heure de la mise en quarantaine ;
- chemin d’accès à l’emplacement d’origine du fichier ;
- taille en octets ;
- raison (l’objet a été ajouté par un utilisateur, par exemple) ;
- nombre de détections (par exemple, des détections en double du même fichier ou s’il s’agit d’une archive

contenant plusieurs infiltrations).



Mise en quarantaine de fichiers

ESET NOD32 Antivirus met automatiquement en quarantaine les fichiers supprimés (si vous n'avez pas annulé cette option dans la fenêtre d'alerte).

D'autres fichiers doivent être mis en quarantaine dans les cas suivants :

a.ils ne peut pas être nettoyés ;

b.s'il n'est pas sûr ou conseillé de les supprimer ;

c.s'ils sont détectés à tort par ESET NOD32 Antivirus ;

d.si un fichier se comporte de manière suspecte, mais n'est pas détecté par les protections.

Pour mettre un fichier en quarantaine, vous avez plusieurs possibilités :

a.Utilisez la fonctionnalité glisser-déposer pour mettre manuellement en quarantaine un fichier ou un dossier en cliquant dessus, en déplaçant le pointeur de la souris vers la zone marquée tout en maintenant le bouton de la souris enfoncée, puis en le relâchant. L'application est ensuite placée au premier plan.

b.Cliquez avec le bouton droit sur le fichier, cliquez sur **Options avancées** > **Mettre le fichier en quarantaine**.

c.Cliquez sur **Déplacer vers la quarantaine** dans la fenêtre **Quarantaine**.

d.Le menu contextuel peut également être utilisé à cet effet : cliquez avec le bouton droit dans la fenêtre

de **Quarantaine** et sélectionnez **Mettre en quarantaine**.

Restoring from Quarantine

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

- Utilisez la fonctionnalité de **restauration** à cette fin. Celle-ci est disponible dans le menu contextuel en cliquant avec le bouton droit sur un fichier donné dans la quarantaine.
- Si un fichier est marqué comme étant une application potentiellement indésirable, l'option **Restaurer et exclure de l'analyse** est activée. Voir aussi Exclusions.
- Le menu contextuel propose également l'option **Restaurer vers** qui permet de restaurer des fichiers vers un emplacement autre que celui d'origine dont ils ont été supprimés.
- La fonctionnalité de restauration n'est pas disponible dans certains cas (pour des fichiers situés sur un partage réseau en lecture seule, par exemple).

Suppression des éléments en quarantaine

Cliquez avec le bouton droit sur un élément donné, puis sélectionnez **Supprimer l'élément en quarantaine**. Vous pouvez également sélectionner l'élément à supprimer, puis appuyer sur **Suppr** sur votre clavier. Si vous souhaitez sélectionner tous les éléments en quarantaine et les supprimer, vous pouvez appuyer sur **Ctrl + A** et sur **Delete** sur votre clavier. Les éléments supprimés le seront définitivement de votre appareil et de la quarantaine.

Soumission de fichiers mis en quarantaine

Si vous avez placé en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été considéré par erreur comme étant infecté (par exemple par l'analyse heuristique du code) et placé en quarantaine, soumettez cet échantillon au laboratoire de recherche d'ESET. Pour soumettre un fichier, cliquez avec le bouton droit sur le fichier et sélectionnez l'option **Soumettre un échantillon pour analyse** dans le menu contextuel.

Description de la détection

Cliquez avec le bouton droit sur un élément et cliquez sur **Description de la 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 être disponibles uniquement en anglais :
> - Restaurer un fichier en quarantaine dans ESET NOD32 Antivirus
> - Supprimer un fichier en quarantaine dans ESET NOD32 Antivirus
> - Mon produit ESET m'a signalé une détection. Que dois-je faire ?

Échec de la mise en quarantaine

Les raisons pour lesquelles des fichiers spécifiques ne peuvent pas être mis en quarantaine sont les suivantes :

- **Vous ne disposez pas des autorisations de lecture**. Vous ne pouvez donc pas afficher le contenu d'un fichier.

- **Vous ne disposez pas des autorisations en écriture**. Vous ne pouvez donc pas modifier le contenu du fichier, c'est-à-dire ajouter du 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 le message d'erreur « Échec de la mise en quarantaine » s'affiche, cliquez sur **Informations supplémentaires**. La fenêtre Liste des erreurs de quarantaine s'affiche. Vous pourrez voir le nom du fichier et la raison pour laquelle il ne peut pas être mis en quarantaine.

Sélectionner un échantillon pour analyse

Si vous trouvez un fichier suspect sur votre ordinateur ou un site suspect sur Internet, vous pouvez le soumettre au laboratoire de recherche d'ESET pour analyse (cette option peut ne pas être disponible selon la configuration d'ESET LiveGrid®).

> **Avant de soumettre des échantillons à ESET**
> Ne soumettez pas un échantillon s'il ne répond pas à au moins l'un des critères suivants :
> • L'échantillon n'est pas du tout détecté par votre produit ESET.
> • Le fichier est détecté à tort comme une menace.
> • Nous n'acceptons pas vos fichiers personnels (pour lesquels vous souhaitez qu'ESET recherche des logiciels malveillants) comme échantillons (le laboratoire de recherche d'ESET n'effectue pas d'analyses à la demande pour les utilisateurs).
> • Utilisez un objet descriptif et indiquez le plus d'informations possible sur le fichier (notez par exemple le site Internet à partir duquel vous l'avez téléchargé ou envoyez une capture d'écran).

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

1. Utilisez le modèle de formulaire de soumission de votre produit. Il se trouve dans **Outils** > **Soumettre un échantillon pour analyse**. La taille maximale d'un échantillon soumis est de 256 Mo.

2. Vous pouvez également soumettre le fichier par e-mail. Si vous préférez, compressez le ou les fichiers à l'aide de WinRAR/WinZIP, protégez l'archive à l'aide du mot de passe « infected » et envoyez-la à samples@eset.com.

3. Pour signaler du courrier indésirable ou du courrier indésirable faux positif, consultez cet article de la base de connaissances ESET.

Dans le formulaire **Sélectionner un échantillon pour analyse**, sélectionnez dans le menu déroulant **Motif de soumission de l'échantillon** la description correspondant le mieux à l'objet de votre message :

- Fichier suspect
- Site suspect (site Web infecté par un logiciel malveillant quelconque),
- Site faux positif
- Fichier faux positif (fichier détecté à tort comme infecté),
- Autre

Fichier/Site : le chemin d'accès au fichier ou au site Web que vous souhaitez soumettre.

Adresse de contact : l'adresse de contact est envoyée à ESET avec les fichiers suspects. Elle pourra servir à vous contacter si des informations complémentaires sont nécessaires à l'analyse. Elle pourra servir à vous contacter si des informations complémentaires sont nécessaires à l'analyse. La spécification d'une adresse de contact est facultative. Sélectionnez **Envoyer de manière anonyme** pour laisser l'adresse vide.

> **Il est possible que vous ne receviez pas de réponse d'ESET.**
> Vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires sont nécessaires à l'analyse. Nos serveurs reçoivent, en effet, chaque jour, des dizaines de milliers de fichiers, ce qui ne permet pas de répondre à tous les envois.
> Si l'échantillon s'avère être une application malveillante, sa détection sera intégrée à une prochaine mise à jour.

Sélectionner un échantillon pour analyse - Fichier suspect

Signes et symptômes observés d'infection par logiciel malveillant : saisissez une description du comportement du fichier suspect que vous avez observé sur votre ordinateur.

Origine du fichier (adresse URL ou fournisseur) : indiquez l'origine du fichier (sa source) et comment vous l'avez trouvé.

Notes et autres informations : saisissez éventuellement d'autres informations ou une description qui faciliteront le traitement du fichier suspect.

> Le premier paramètre (**Signes et symptômes observés d'infection par logiciel malveillant**) est obligatoire. Les autres informations faciliteront la tâche de nos laboratoires lors de l'identification et du traitement des échantillons.

Sélectionner un échantillon pour analyse - Site suspect

Dans le menu déroulant **Pourquoi ce site est-il suspect ?**, sélectionnez l'une des options suivantes :

- **Infecté** : un site Web qui contient des virus ou d'autres logiciels malveillants diffusés par diverses méthodes.
- **L'hameçonnage** est souvent utilisé pour accéder à des données sensibles, telles que numéros de comptes bancaires, codes secrets, etc. Pour en savoir plus sur ce type d'attaque, consultez le glossaire.
- **Scam** : un canular ou site web frauduleux, destiné essentiellement à réaliser un profit rapidement.
- Sélectionnez **Autre** si les options ci-dessus ne correspondent pas au site que vous allez soumettre.

Notes et autres informations : vous pouvez saisir d'autres informations ou une description qui faciliteront l'analyse du site web suspect.

Sélectionner un échantillon pour analyse - Fichier faux positif

Nous vous invitons à soumettre les fichiers qui sont signalés comme infectés alors qu'ils ne le sont pas, afin d'améliorer notre moteur antivirus et antispyware et contribuer à la protection des autres utilisateurs. Les faux positifs (FP) peuvent se produire lorsque le motif d'un fichier correspond à celui figurant dans un moteur de détection.

Nom et version de l'application : titre et version du programme (par exemple : numéro, alias et nom de code).

Origine du fichier (adresse URL ou fournisseur) : indiquez l'origine du fichier (sa source) et comment vous l'avez trouvé.

Objectif des applications : description générale, type (navigateur, lecteur multimédia...) et fonctionnalité de l'application.

Notes et autres informations : saisissez éventuellement d'autres informations ou une description qui faciliteront le traitement du fichier suspect.

> les trois premiers paramètres sont nécessaires pour identifier les applications légitimes et les distinguer des codes malveillants. En fournissant des informations supplémentaires, vous facilitez l'identification et le traitement des échantillons par nos laboratoires.

Sélectionner un échantillon pour analyse - Site faux positif

Nous vous invitons à soumettre les sites faussement détectés comme infectés ou signalés à tort comme scam ou hameçonnage. Les faux positifs (FP) peuvent se produire lorsque le motif d'un fichier correspond à celui figurant dans un moteur de détection. Veuillez soumettre ce site Web afin d'améliorer notre moteur antivirus et antihameçonnage, et contribuer à la protection des autres utilisateurs.

Notes et autres informations : saisissez éventuellement d'autres informations ou une description qui faciliteront le traitement du site web suspect.

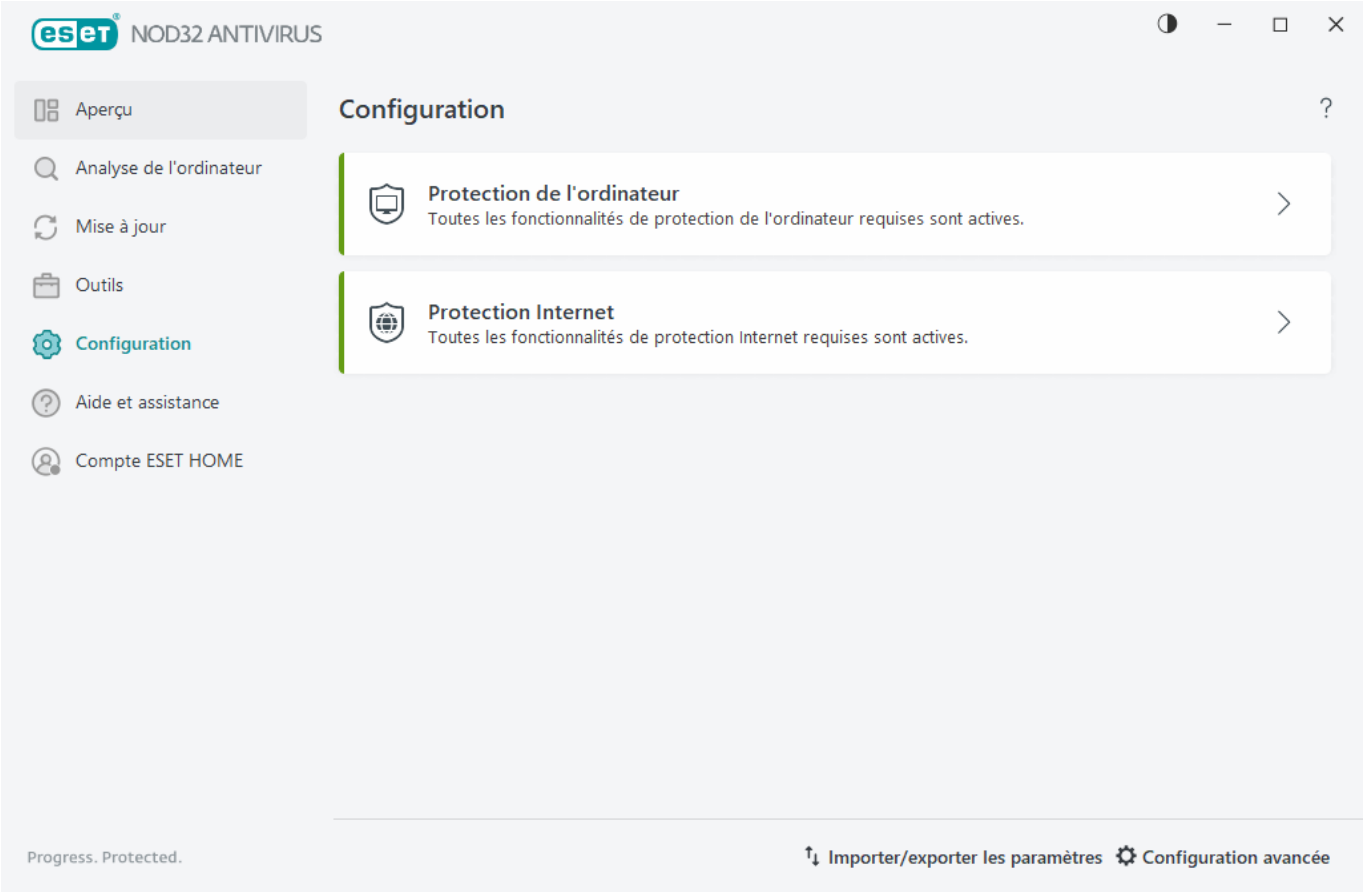
Sélectionner un échantillon pour analyse - Autre

Utilisez ce formulaire si le fichier ne peut pas être classé par catégorie en tant que **fichier suspect** ou **faux positif**.

Motif de soumission du fichier – Décrivez en détail le motif d'envoi du fichier.

Param

Des groupes de fonctionnalités de protection sont disponibles dans la fenêtre principale du programme > **Configuration**.



Le menu **Configuration** se divise en différentes sections :

Protection de l'ordinateur

Protection Internet

D'autres options sont disponibles au bas de la fenêtre de configuration. Cliquez sur Configurations avancées pour configurer d'autres paramètres détaillés pour chaque module. Pour charger les paramètres de configuration à l'aide d'un fichier de configuration .xml ou pour enregistrer les paramètres de configuration actuels dans un fichier de configuration, utilisez l'option Importer/exporter les paramètres.

Protection de l'ordinateur

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

- Protection en temps réel du système de fichiers – Tous les fichiers ouverts, créés ou exécutés sont analysés pour y rechercher la présence éventuelle de code malveillant.

- Contrôle de périphérique – Ce module permet d'analyser, de bloquer ou d'ajuster les filtres étendus/autorisations, et de sélectionner la façon dont l'utilisateur peut accéder à un périphérique (CD/DVD/USB...) et l'utiliser.

- HIPS – Le système HIPS surveille les événements dans le système d'exploitation et réagit en fonction d'un ensemble de règles personnalisées.

• Mode joueur – Active ou désactive le mode joueur. Vous recevez un message d'avertissement (risque potentiel de sécurité) et la fenêtre principale devient orange lorsque le mode joueur est activé.

Pour suspendre ou désactiver un module de protection, cliquez sur l'icône de bouton bascule .

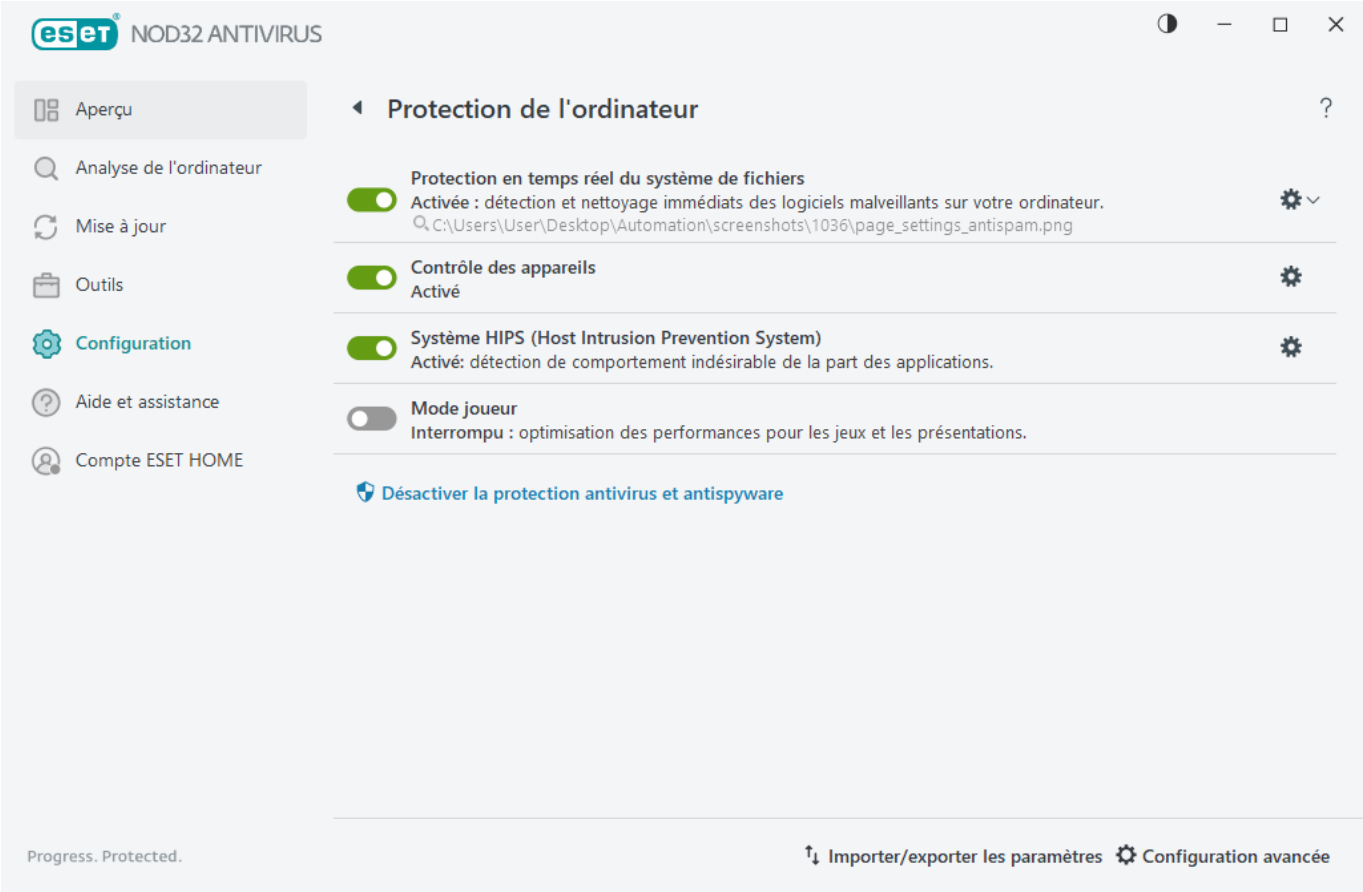
Si vous désactivez les modules de protection, le niveau de protection de votre ordinateur peut diminuer.

Cliquez sur l'icône d'engrenage en regard 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 d'engrenage et sélectionnez l'une des options suivantes :

• **Configurer** – Ouvre la configuration avancée de la protection en temps réel du système de fichiers.

• **Modifier les exclusions** – Ouvre la fenêtre de configuration des exclusions pour exclure des fichiers et des dossiers de l'analyse.



Interrompre la protection antivirus et antispyware jusqu'au redémarrage – Désactive tous les modules de protection antivirus et antispyware. Lorsque vous désactivez la protection, une fenêtre s'ouvre dans laquelle vous pouvez déterminer la durée pendant laquelle la protection est désactivée en sélectionnant une valeur dans le menu déroulant **Intervalle**. N'utilisez cette option que si vous êtes un utilisateur expérimenté ou si vous avez reçu des instructions de l'assistance technique d'ESET.

Une infiltration est détectée

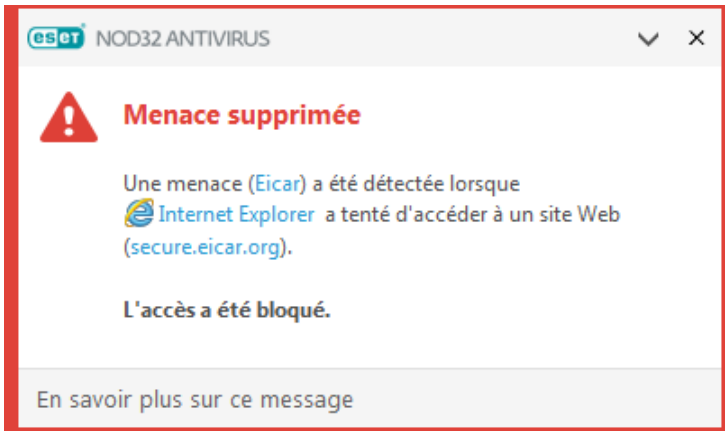
Des infiltrations peuvent atteindre le système à partir de différents points d'entrée : pages Web, dossiers partagés, courrier électronique ou périphériques amovibles (USB, disques externes, CD, DVD, etc.).

Comportement standard

Pour illustrer de manière générale la prise en charge des infiltrations par ESET NOD32 Antivirus, celles-ci peuvent être détectées à l'aide de :

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

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



Recherche de fichiers infectés sur l'ordinateur

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

1.Ouvrez ESET NOD32 Antivirus et cliquez sur **Analyse de l'ordinateur**.

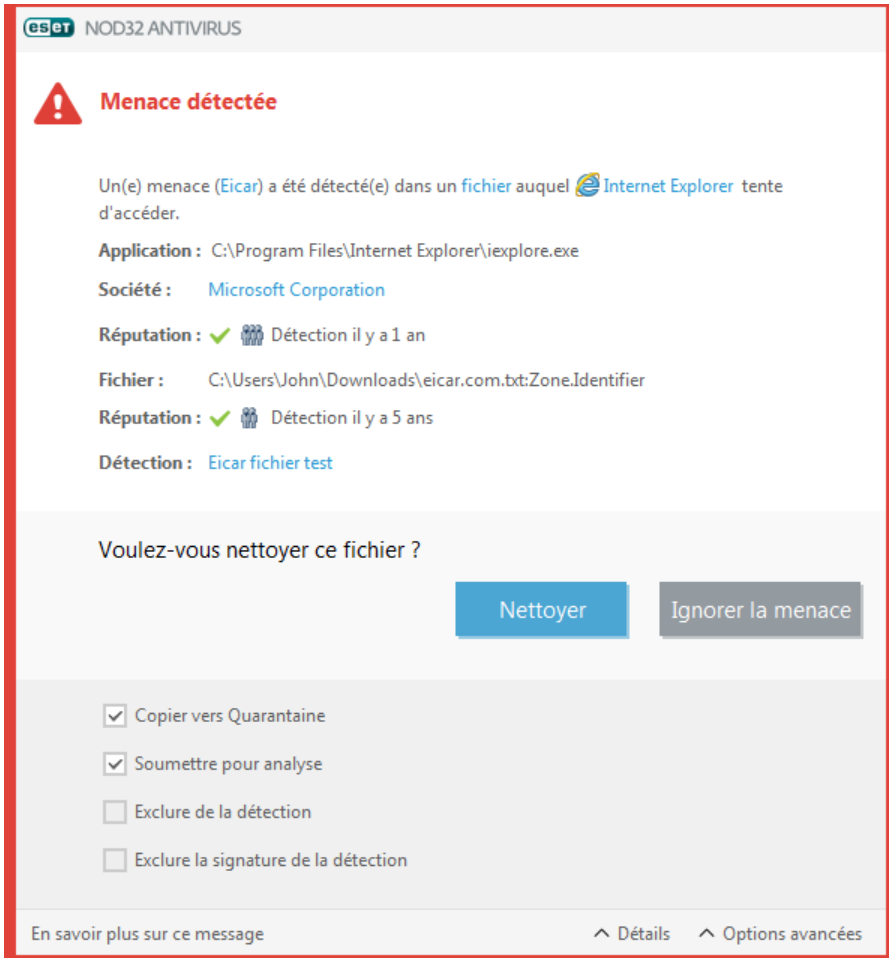
2.Cliquez sur **Analyse intelligente** (pour plus d'informations, reportez-vous à la section Analyse de l'ordinateur).

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

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

Nettoyage et suppression

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



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

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

Restoring from Quarantine

La quarantaine est accessible depuis la fenêtre principale d'ESET NOD32 Antivirus en cliquant sur **Outils** > **Quarantaine**.

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

- Utilisez la fonctionnalité de **restauration** à cette fin. Celle-ci est disponible dans le menu contextuel en cliquant avec le bouton droit sur un fichier donné dans la quarantaine.
- Si un fichier est marqué comme étant une application potentiellement indésirable, l'option **Restaurer et**

exclure de l'analyse est activée. Voir aussi Exclusions.

• Le menu contextuel propose également l'option **Restaurer vers** qui permet de restaurer des fichiers vers un emplacement autre que celui d'origine dont ils ont été supprimés.

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

Menaces multiples

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

Suppression de fichiers dans des archives

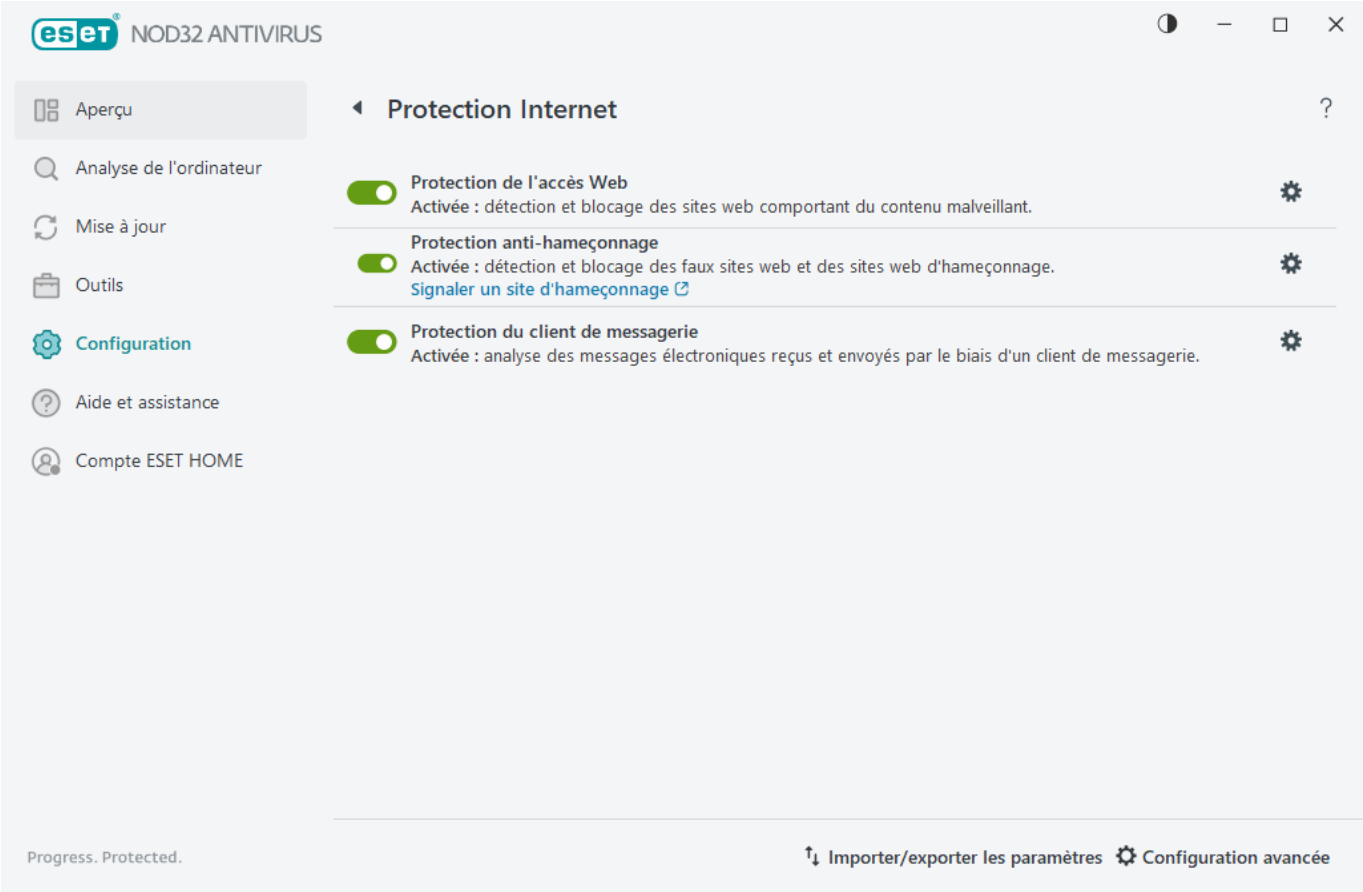
En mode de nettoyage par défaut, l'archive complète n'est supprimée que si elle ne contient que des fichiers infectés et aucun fichier sain. Autrement dit, les archives ne sont pas supprimées si elles contiennent également des fichiers sains. Soyez prudent si vous choisissez un nettoyage strict ; dans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

Protection Internet

La connectivité Internet est une fonctionnalité standard des ordinateurs personnels. Elle est malheureusement devenue le principal mode de transfert des codes malveillants. Ouvrez la fenêtre principale du programme > **Configuration** > **Protection internet** pour configurer les fonctionnalités d'ESET NOD32 Antivirus qui renforcent votre protection internet.

Pour suspendre ou désactiver un module de protection, cliquez sur l'icône de bouton bascule  .

⚠ Si vous désactivez les modules de protection, le niveau de protection de votre ordinateur peut diminuer.



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

La protection de l'accès web analyse les communications HTTP/HTTPS à la recherche de logiciels malveillants et d'hameçonnage. La protection de l'accès web ne doit être désactivée qu'à des fins de résolution de problèmes.

La protection anti-hameçonnage vous permet de bloquer les pages Web connues pour receler du contenu d'hameçonnage. Il est fortement recommandé de laisser l'option d'antihameçonnage activée.

Signaler un site d'hameçonnage : permet de signaler un site web d'hameçonnage/malveillant à ESET pour analyse.

Avant de soumettre un site Web à ESET, assurez-vous qu'il répond à au moins l'un des critères suivants :
- Le site Web n'est pas du tout détecté.
- Le site Web est, à tort, détecté comme une menace. Dans ce cas, vous pouvez signaler une page bloquée incorrectement.

La protection du client de messagerie contrôle les communications par courrier électronique reçues via les protocoles POP3(S) et IMAP(S). ESET NOD32 Antivirus Utilise le plugin de votre client de messagerie pour contrôler toutes les communications concernant le client de messagerie.

Protection antihameçonnage

L'hameçonnage est une activité criminelle qui utilise l'ingénierie sociale (manipulation des utilisateurs pour obtenir des informations confidentielles). Il est utilisé pour accéder à des données sensibles telles que des numéros de compte bancaire, des codes PIN, etc. Pour plus d'informations, reportez-vous au glossaire. ESET NOD32 Antivirus comporte une fonctionnalité anti-hameçonnage qui permet de bloquer les pages web connues

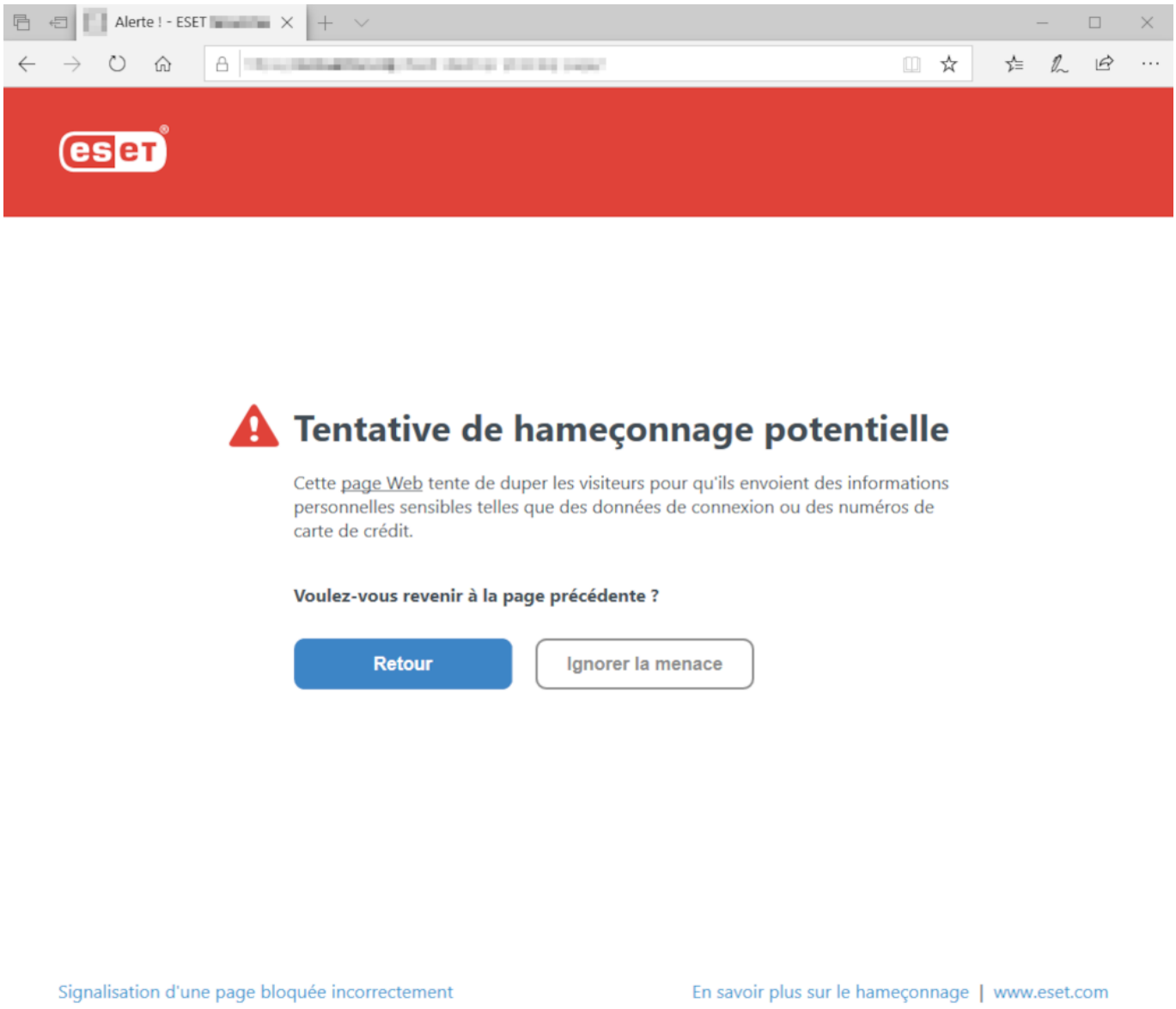
qui présentent ce type de contenu.

L'anti-hameçonnage est activé par défaut. Ce paramètre peut être configuré dans Configurations avancées > **Protections** > **Protection de l'accès web**.

Pour plus d'informations sur la protection antihameçonnage d'ESET NOD32 Antivirus, consultez notre article de la base de connaissances.

Accès à un site Web d'hameçonnage

Lorsque vous accédez à un site web d'hameçonnage reconnu, votre navigateur Web affiche la boîte de dialogue ci-dessous. Si vous souhaitez toujours accéder au site Web, cliquez sur **Ignorer la menace** (non recommandé).



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

Signaler un site d'hameçonnage

Le lien **Signaler une page bloquée de manière incorrecte** vous permet de signaler un site web qui est détecté à tort comme une menace.

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

Importer et exporter les paramètres

Vous pouvez importer ou exporter votre fichier de configuration ESET NOD32 Antivirus.xml personnalisé à partir du menu **Configuration**.

> **Instructions illustrées**
> Pour obtenir des instructions illustrées disponibles en anglais et dans plusieurs autres langues, consultez Importer ou exporter les paramètres de configuration ESET à l'aide d'un fichier .xml.

L'importation et l'exportation des fichiers de configuration s'avèrent utiles si vous devez sauvegarder la configuration actuelle d'ESET NOD32 Antivirus pour l'utiliser ultérieurement. L'option Exporter les paramètres est également pratique lorsque vous souhaitez utiliser votre configuration préférée sur plusieurs systèmes. Vous pouvez importer un fichier .xml pour transférer ces paramètres.

Pour importer une configuration, dans la fenêtre principale du programme, cliquez sur **Configuration** > **Importer/exporter les paramètres**, puis sélectionnez **Importer les paramètres**. Saisissez le nom du fichier de configuration ou cliquez sur le bouton **...** pour accéder au fichier de configuration à importer.

Pour exporter une configuration, dans la fenêtre principale du programme, cliquez sur **Configuration** > **Importer/exporter les paramètres**. Sélectionnez **Exporter les paramètres** et saisissez le chemin d'accès complet au fichier avec le nom. Cliquez sur **...** pour accéder à un emplacement sur votre ordinateur pour enregistrer le fichier de configuration.

> Vous pouvez rencontrer une erreur lors de l'exportation des paramètres si vous ne disposez pas de suffisamment de droits pour écrire le fichier exporté dans le répertoire spécifié.

Aide et assistance

Cliquez sur **Aide et assistance** dans la fenêtre principale du programme pour afficher des informations d'assistance support et des outils de dépannage qui permettant de résoudre les problèmes que vous pouvez rencontrer.

Abonnement

- Résolution des problèmes liés aux abonnements : cliquez sur ce lien pour trouver des solutions aux problèmes liés à l'activation ou au changement d'abonnement.

- Modifier l'abonnement – Cliquez sur cette option pour ouvrir la fenêtre d'activation et activer votre produit. Si votre appareil est connecté à ESET HOME, sélectionnez un abonnement dans votre compte ESET HOME ou ajoutez-en un.

Produit installé

- Nouveautés – Cliquez sur cette option pour ouvrir la fenêtre d'informations sur les fonctionnalités nouvelles et améliorées.

- À propos d'ESET NOD32 Antivirus – Affiche des informations sur votre copie d'ESET NOD32 Antivirus.

- Résolution des problèmes liés aux produits : cliquez sur ce lien pour trouver des solutions aux problèmes les plus fréquents.

- **Changer de produit** – Cliquez sur cette option pour déterminer si ESET NOD32 Antivirus peut être remplacé par une autre gamme de produits avec l'abonnement actuel.

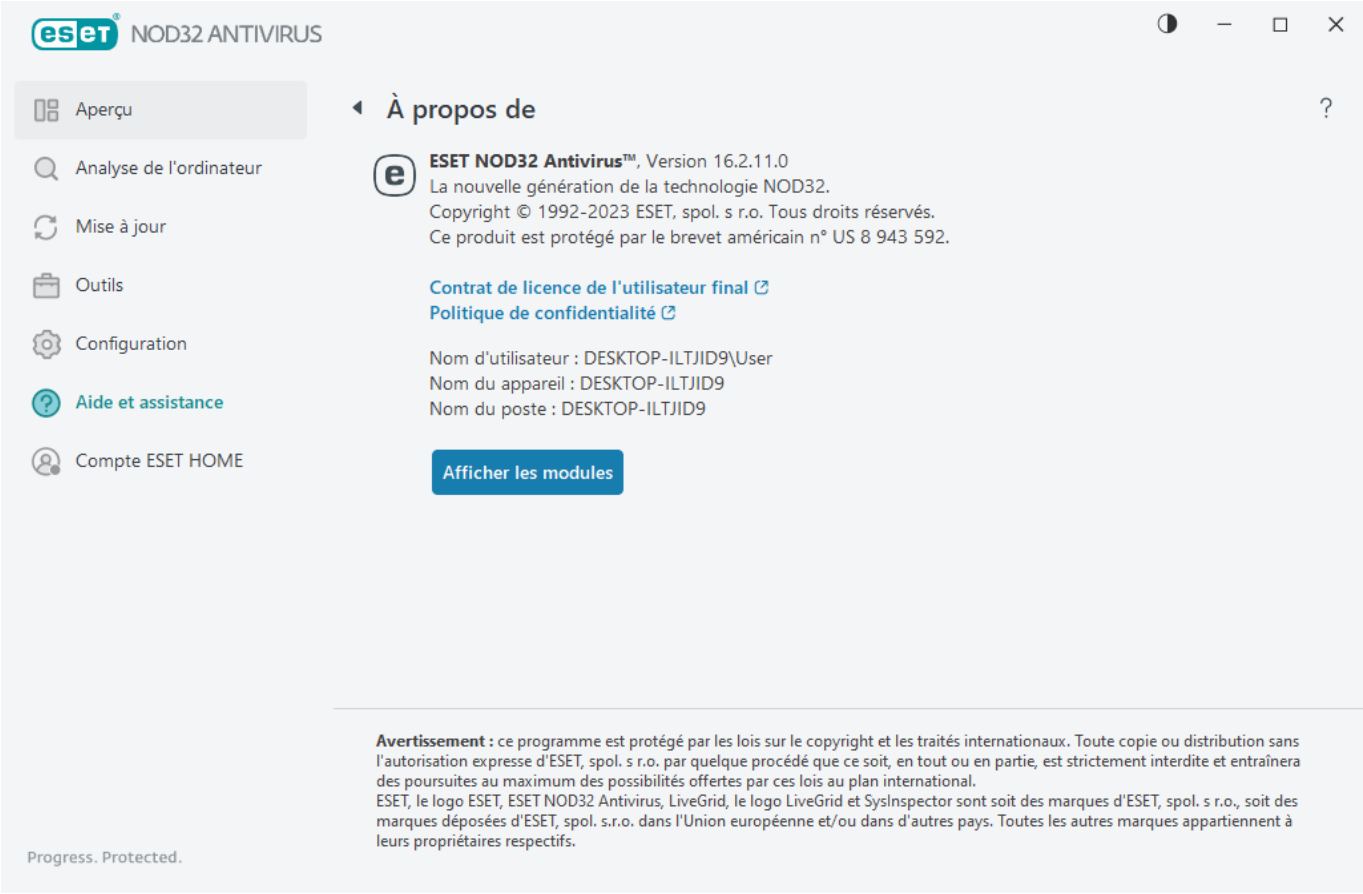
Page d'aide – Cliquez sur ce lien pour lancer les pages d'aide ESET NOD32 Antivirus.

Assistance technique

Base de connaissances – La base de connaissances ESET contient des réponses aux questions les plus fréquentes et les solutions recommandées pour résoudre divers problèmes. Régulièrement mise à jour par les spécialistes techniques d'ESET, la base de connaissances est l'outil le plus puissant pour résoudre différents problèmes.

À propos d'ESET NOD32 Antivirus

Cette fenêtre fournit des informations détaillées sur la version installée d'ESET NOD32 Antivirus et votre ordinateur.



Cliquez sur **Afficher les modules** pour afficher des informations sur la liste des modules du programme chargés.

- Vous pouvez copier les informations sur les modules dans le Presse-papiers en cliquant sur **Copier**. Ce procédé peut être utile pour la résolution des problèmes ou lorsque vous contactez l'assistance technique.

- Cliquez sur **Moteur de détection** dans la fenêtre Modules pour ouvrir ESET Virus radar, qui contient des informations sur chaque version du moteur de détection ESET.

Actualités ESET

Dans cette fenêtre, ESET NOD32 Antivirus vous informe régulièrement des actualités ESET.

Les messages intégrés au produit ont été conçus pour informer les utilisateurs des actualités et autres

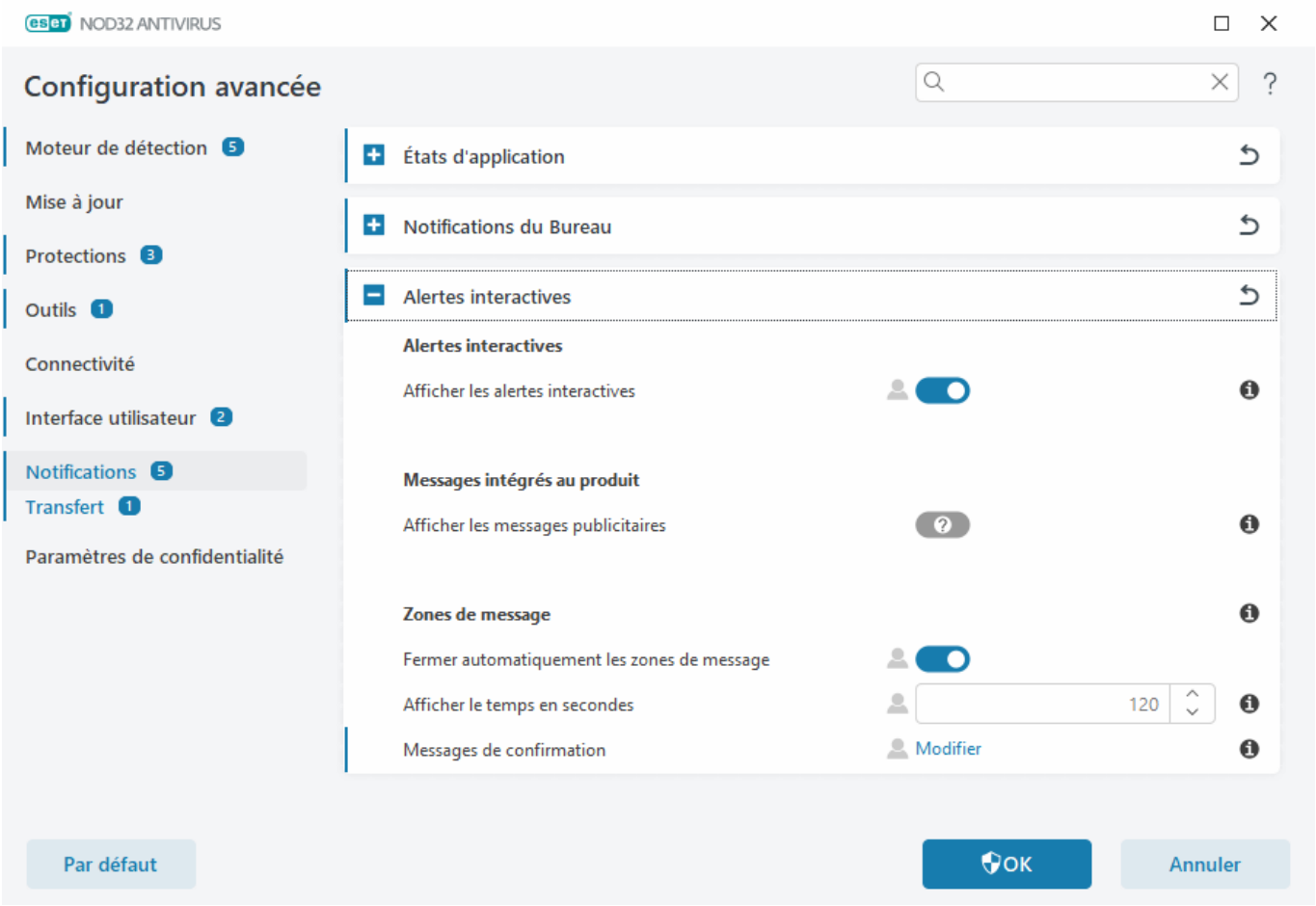
communications d'ESET. L'envoi de messages marketing nécessite le consentement de l'utilisateur. Par conséquent, les messages marketing ne sont pas envoyés à un utilisateur par défaut (affiché sous la forme d'un point d'interrogation). En activant cette option, vous acceptez de recevoir des messages marketing de la part d'ESET. Si vous ne souhaitez pas **recevoir de documents marketing ESET**, désactivez l'option.

Pour activer ou désactiver la réception de messages marketing via une fenêtre de notification, suivez les instructions ci-dessous.

1. Ouvre la boîte de dialogue Configuration avancée.

2. Cliquez sur **Notifications** > **Alertes interactives**.

3. Modifiez l'option **Afficher les messages publicitaires ESET**.



Soumettre les données de configuration système

Pour offrir une assistance adéquate le plus rapidement possible, ESET requiert des informations sur la configuration de ESET NOD32 Antivirus, sur le système et les processus en cours (fichier journal ESET SysInspector), ainsi que les données du Registre. ESET utilise ces données uniquement pour fournir une assistance technique au client.

Après avoir soumis le formulaire web, les données de configuration de votre système sont également envoyées à ESET. Sélectionnez **Toujours envoyer ces informations** si vous souhaitez mémoriser cette action pour ce processus. Pour soumettre le formulaire web sans envoyer de données, cliquez sur **Ne pas envoyer les données** et continuer.

Vous pouvez configurer l'envoi des données de configuration du système dans Configurations avancées > **Outils** > **Diagnostics** > Assistance technique.

> Si vous avez décidé d'envoyer les données de configuration du système, il est nécessaire de remplir et de soumettre le formulaire web. Dans le cas contraire, votre ticket ne sera pas créé et les données de configuration de votre système seront perdues. Si les données de configuration du système ne peuvent pas être envoyées, remplissez le formulaire web et attendez les instructions de l'assistance technique.

Assistance technique

Dans la fenêtre principale du programme, cliquez sur **Aide et assistance** > **Assistance technique**.

Contacter l'assistance technique

Demander une assistance – Si vous ne trouvez pas de réponse à votre problème, vous pouvez utiliser le formulaire situé sur le site Web d'ESET pour prendre rapidement contact avec le service d'assistance technique ESET. Selon vos paramètres, la fenêtre de soumission des données de configuration système s'affiche avant le remplissage du formulaire Web.

Obtenir des informations pour l'assistance technique

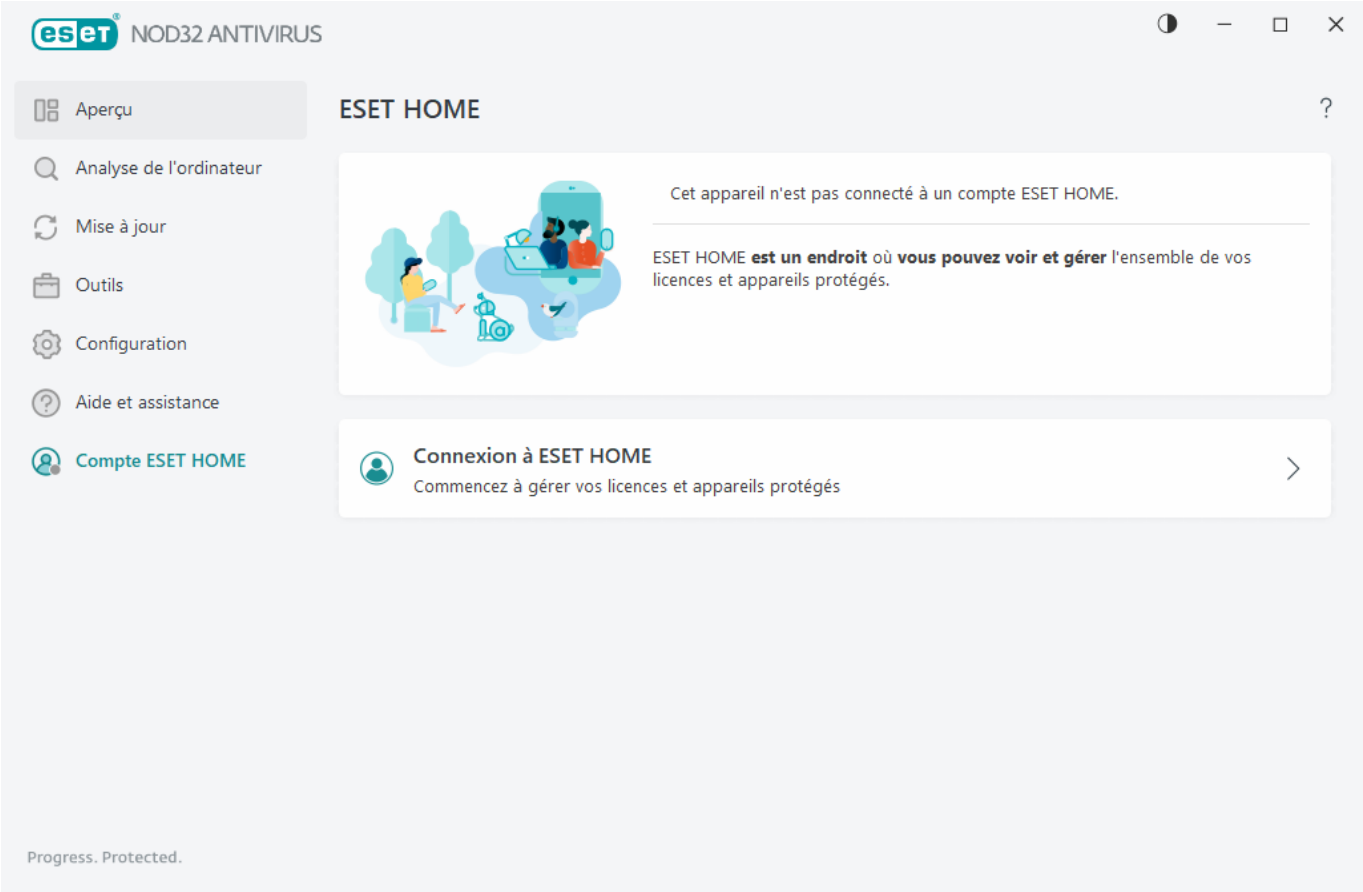
Informations détaillées pour l'assistance technique – Lorsque le système vous y invite, vous pouvez copier et envoyer des informations au support technique ESET (détails des abonnements, nom et version du produit, système d'exploitation et informations sur l'ordinateur).

ESET Log Collector – Mène à l'article de la base de connaissances ESET, à partir duquel vous pouvez télécharger ESET Log Collector. Il s'agit d'une application qui collecte automatiquement les informations et les journaux d'un ordinateur pour résoudre plus rapidement les problèmes. Pour plus d'informations, consultez leguide de l'utilisateur en ligne de ESET Log Collector.

Activez l'option Journalisation avancée pour créer des journaux avancés pour toutes les fonctionnalités disponibles afin d'aider les développeurs à diagnostiquer et résoudre les problèmes. La verbosité minimale des journaux est définie sur le niveau **Diagnostic**. La journalisation avancée est automatiquement désactivée au bout de deux heures, sauf si vous l'avez arrêtée avant en cliquant sur **Arrêter la journalisation avancée**. Lorsque tous les journaux sont créés, la fenêtre de notification s'affiche. Elle offre un accès direct au dossier Diagnostic contenant tous les journaux créés.

Compte ESET HOME

Vous pouvez consulter l'état de la connexion du compte ESET HOME dans la fenêtre principale du programme > **Compte ESET HOME**.



Cet appareil n'est pas connecté à un compte ESET HOME

Cliquez sur Se connecter à ESET HOME pour connecter votre appareil à ESET HOME et gérer vos abonnements et les appareils protégés. Vous pouvez renouveler, mettre à niveau ou prolonger votre abonnement et afficher des informations importantes sur celui-ci. Sur le portail de gestion ESET HOME ou dans l'application mobile, vous pouvez ajouter différents abonnements, télécharger des produits sur vos appareils, vérifier l'état de la sécurité du produit ou partager des abonnements par e-mail. Pour plus d'informations, consultez l''aide en ligne d'ESET HOME.

Cet appareil est connecté à un compte ESET HOME

Vous pouvez gérer à distance la sécurité de votre appareil à l'aide du portail ESET HOME ou de l'application mobile. Cliquez sur **App Store** ou **Google Play** pour afficher un code QR que vous pouvez scanner avec votre téléphone mobile pour télécharger l'application mobile ESET HOME depuis l'App Store ou Google Play.

Compte ESET HOME : nom de votre compte ESET HOME.

Nom de l'appareil : nom de cet appareil affiché dans le compte ESET HOME.

Ouvrir ESET HOME : ouvre le portail de gestion ESET HOME.

Pour déconnecter votre appareil de votre compte ESET HOME, cliquez sur **Déconnexion de ESET HOME** > **Déconnexion**. L'abonnement utilisé pour l'activation restera actif et votre appareil sera protégé.

Connectez-vous à ESET HOME

Connectez votre appareil à ESET HOME pour afficher et gérer tous les abonnements ESET et les appareils activés. Vous pouvez renouveler, mettre à niveau ou prolonger votre abonnement et afficher des informations importantes sur celui-ci. Sur le portail de gestion ESET HOME ou dans l'application mobile, vous pouvez ajouter différents abonnements, télécharger des produits sur vos appareils, vérifier l'état de la sécurité du produit ou partager des abonnements par e-mail. Pour plus d'informations, consultez l''aide en ligne d'ESET HOME.

Connecter votre appareil à ESET HOME :

> Si vous vous connectez à ESET HOME pendant l'installation ou que 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 et activé ESET NOD32 Antivirus avec un abonnement ajouté dans votre compte ESET HOME, vous pouvez connecter votre appareil à ESET HOME à l'aide du portail ESET HOME. Suivez les instructions du guide d'aide en ligne ESET HOME et autorisez la connexion dans ESET NOD32 Antivirus.

1. Dans la fenêtre principale du programme, cliquez sur **un compte ESET HOME** > **Connexion à ESET HOME** ou sur **Connexion à ESET HOME** dans la notification **Connecter cet appareil à un compte ESET HOME**.

2. Connectez-vous à votre compte ESET HOME.

> Si vous ne possédez pas de compte ESET HOME, cliquez sur **Créer un compte** pour vous enregistrer ou consultez les instructions de l'aide en ligne ESET HOME.
> Si vous avez oublié votre mot de passe, cliquez sur **J'ai oublié mon mot de passe** et suivez la procédure à l'écran ou consultez les instructions de l'aide en ligne ESET HOME.

3. Définissez le **Nom de l'appareil**, puis cliquez sur **Continuer**.

4. Une fois la connexion effectuée, une fenêtre de détails s'affiche. Cliquez sur **Terminé**.

Connexion à ESET HOME

Il existe plusieurs méthodes pour se connecter au compte ESET HOME :

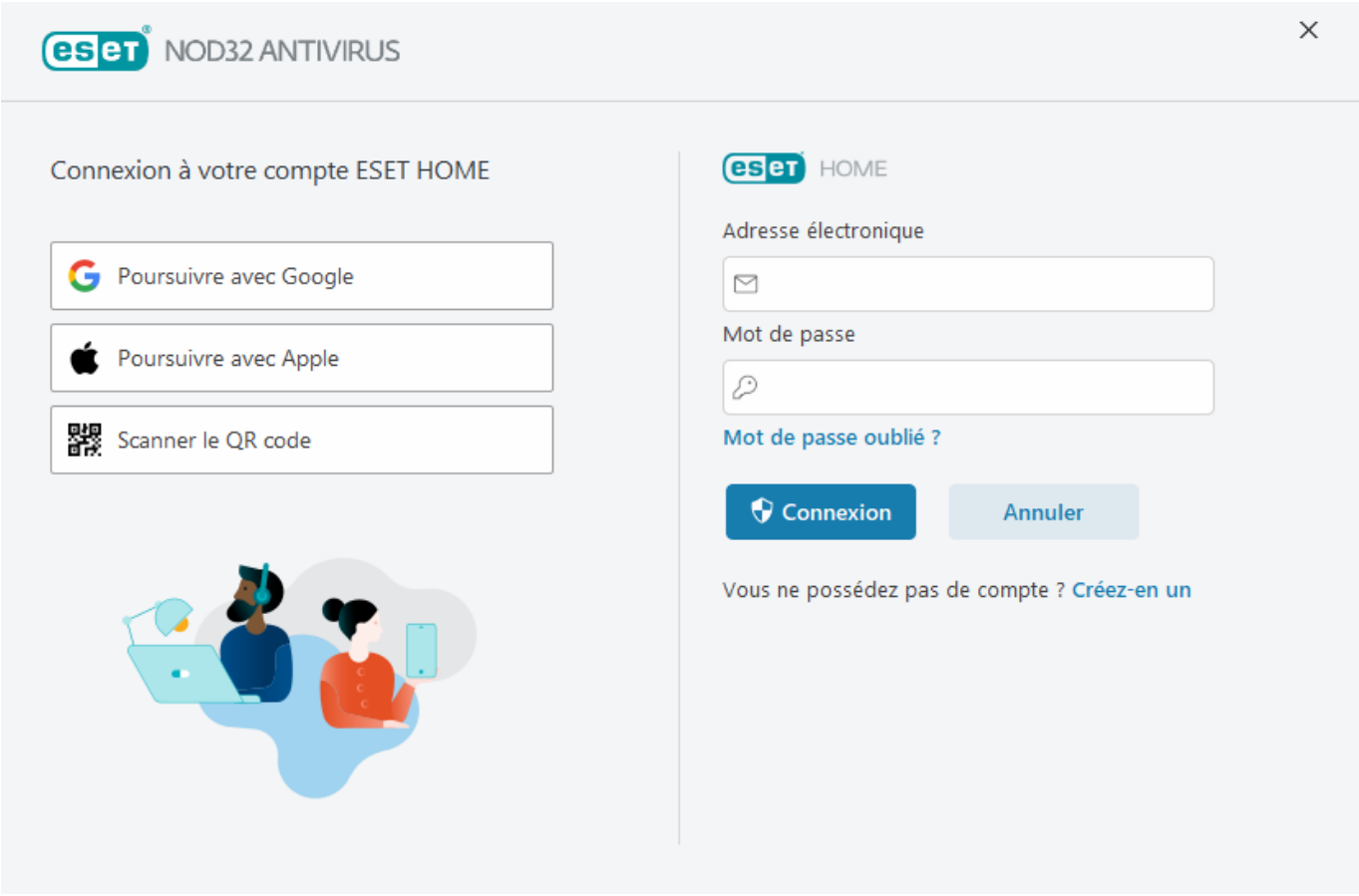
- **Utiliser votre adresse e-mail et votre mot de passe ESET HOME** : saisissez l'**adresse e-mail** et le **mot de passe** que vous avez utilisés pour créer votre compte ESET HOME, puis cliquez sur **Se connecter**.

- **Utiliser votre compte Google/AppleID** : cliquez sur **Continuer avec Google** ou **Continuer avec Apple**, puis connectez-vous au compte adéquat. Une fois connecté, vous serez redirigé vers la page web de confirmation ESET HOME. Pour continuer, retournez dans la fenêtre de votre produit ESET. Pour plus d'informations sur la connexion avec un compte Google/AppleID, consultez les instructions dans l'aide en ligne ESET HOME.

- **Scanner le QR code** : cliquez sur **Scanner le QR code** pour afficher le QR code. Ouvrez votre application mobile ESET HOME et scannez le QR code ou pointez l'appareil photo sur le QR code. Pour plus d'informations, consultez les instructions dans l'aide en ligne ESET HOME.

Si vous ne possédez pas de compte ESET HOME, cliquez sur **Créer un compte** pour vous enregistrer ou consultez les instructions de l'aide en ligne ESET HOME.
Si vous avez oublié votre mot de passe, cliquez sur **J'ai oublié mon mot de passe** et suivez la procédure à l'écran ou consultez les instructions de l'aide en ligne ESET HOME.

Échec de la connexion : erreurs courantes.



Échec de la connexion : erreurs courantes

Impossible de trouver un compte qui correspond à l'adresse e-mail saisie.

L'adresse e-mail saisis ne correspond à aucun compte ESET HOME. Cliquez sur **Précédent**, puis saisissez l'adresse e-mail et le mot de passe corrects.

Pour vous connecter, vous devez créer un compte ESET HOME. Si vous ne possédez pas de compte ESET HOME, cliquez sur **Retour** > **Créer un compte** ou consultez Créer un compte ESET HOME.

Le nom d'utilisateur et le mot de passe ne correspondent pas.

Le mot de passe saisi ne correspond pas à l'adresse e-mail saisie. Cliquez sur **Précédent**, saisissez le bon mot de passe et vérifiez que l'adresse e-mail saisie est correcte. Si vous ne parvenez toujours pas à vous connecter, cliquez sur **Retour** > **J'ai oublié mon mot de passe** pour réinitialiser votre mot de passe et suivez les étapes à l'écran ou consultez J'ai oublié mon mot de passe ESET HOME.

L'option de connexion sélectionnée ne correspond pas à votre compte.

Votre compte est associé à votre compte de réseau social. Pour vous connecter à ESET HOME, cliquez sur **Continuer avec Google** ou **Continuer avec Apple**, puis connectez-vous au compte adéquat. Une fois connecté, vous serez redirigé vers la page web de confirmation ESET HOME. Vous pouvez dissocier votre compte de réseau social de votre compte ESET HOME sur le portail ESET HOME.

Mot de passe incorrect

Cette erreur peut se produire si ESET NOD32 Antivirus est déjà connecté à ESET HOME, que vous apportez des modifications qui nécessitent de vous connecter (désactiver la fonctionnalité Antivol, par exemple) et que le mot de passe saisi ne correspond pas à votre compte. Cliquez sur **Précédent**, puis saisissez le mot de passe correct. Si vous ne parvenez toujours pas à vous connecter, cliquez sur **Retour** > **J'ai oublié mon mot de passe** pour réinitialiser votre mot de passe et suivez les étapes à l'écran ou consultez J'ai oublié mon mot de passe ESET HOME.

Ajout d'un appareil dans ESET HOME

Si vous avez déjà installé et activé ESET NOD32 Antivirus avec un abonnement ajouté dans votre compte ESET HOME, vous pouvez connecter votre appareil à ESET HOME à l'aide du portail ESET HOME :

1. Envoyez une demande de connexion à votre appareil.

2. ESET NOD32 Antivirus affiche la boîte de dialogue **Connecter cet appareil à un compte ESET HOME** avec le nom de votre compte ESET HOME. Cliquez sur **Autoriser** pour connecter l'appareil au compte ESET HOME mentionné.

> En l'absence d'interaction, la demande de connexion sera annulée automatiquement après environ 30 minutes.

Configuration avancée

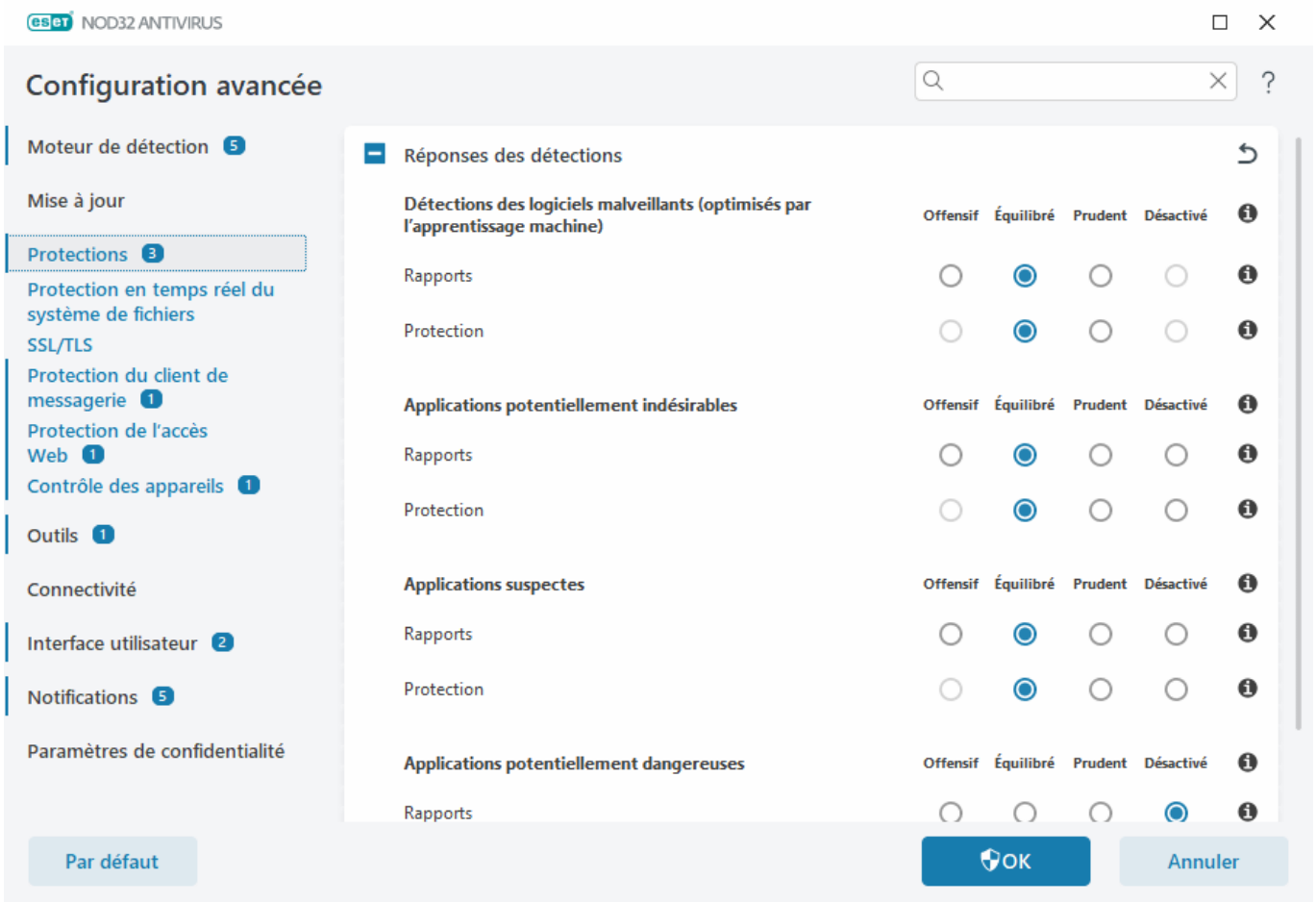
Les configurations avancées vous permettent de configurer des paramètres détaillés d'ESET NOD32 Antivirus en fonction de vos besoins.

Pour ouvrir Configurations avancées, ouvrez la fenêtre principale du programme et appuyez sur la touche **F5** de votre clavier ou cliquez sur **Configuration** > **Configurations avancées**.

> En fonction de la configuration d'accès, vous pouvez être invité à saisir un mot de passe pour ouvrir Configurations avancées.

Dans les configurations avancées, vous pouvez configurer les paramètres suivants :

- Moteur de détection
- Mettre à jour
- Protections
- Outils
- Connectivité
- Interface utilisateur
- Notifications
- Paramètres de confidentialité



Moteur de détection

La commande Configurations avancées > **Moteur de détection** permet de configurer les options suivantes :

- Exclusions
- Options avancées
- Analyseur du trafic réseau

Exclusions

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

Les exclusions de performances permettent d'exclure des fichiers et dossiers de l'analyse. Elles sont utiles pour exclure de l'analyse au niveau des fichiers des applications de jeu ou en cas de comportement anormal du système ou d'augmentation des performances.

Les exclusions de détection permettent d'exclure des objets du détection à l'aide du nom de la détection, du chemin d'accès ou du hachage. Les exclusions de détection n'excluent pas les fichiers et les dossiers de l'analyse

comme le font les exclusions de performances. Elles excluent les objets uniquement lorsqu'ils sont détectés par le moteur de détection et que la liste des exclusions contient une règle appropriée.

Ne pas confondre avec d'autres types d'exclusions :

- Exclusions de processus – Toutes les opérations sur les fichiers attribuées aux processus d'application exclus sont exclues de l'analyse (elles peuvent être nécessaires pour améliorer la vitesse de sauvegarde et la disponibilité du service),
- Extensions de fichier exclues,
- Exclusions HIPS,
- Filtre d'exclusion pour la protection dans le cloud.

Exclusions des performances

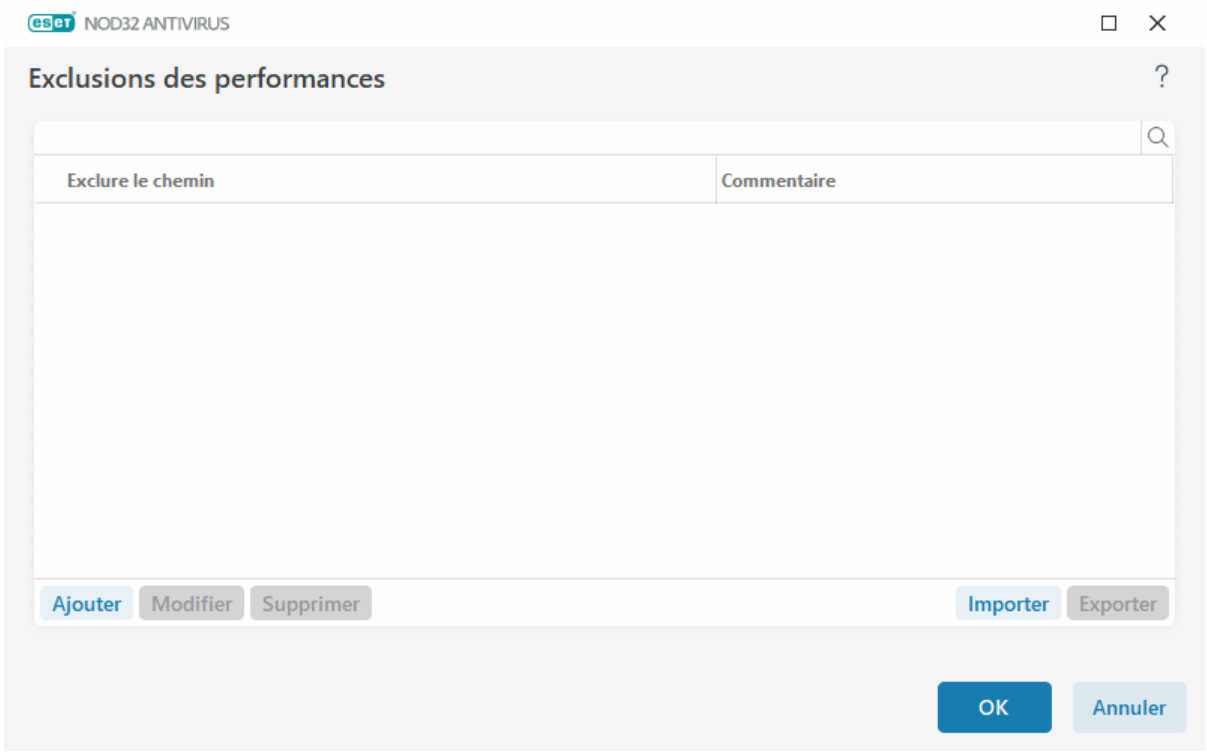
Les exclusions de performances permettent d'exclure des fichiers et dossiers de l'analyse.

Pour que la détection des menaces s'appliquent bien à tous les objets, il est recommandé de ne créer des exclusions 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 dans la liste des exclusions des fichiers et des dossiers à exclure de l'analyse via Configuration avancée > **Moteur de détection** > **Exclusions** > **Exclusions des performances** > **Modifier**.

> Ne confondez pas cette option avec Exclusions de détection, Extensions de fichiers exclues, Exclusions HIPS ou Exclusions des processus.

Pour exclure un objet (chemin d'accès : fichier ou dossier) de l'analyse, cliquez sur **Ajouter** et entrez le chemin 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 commande

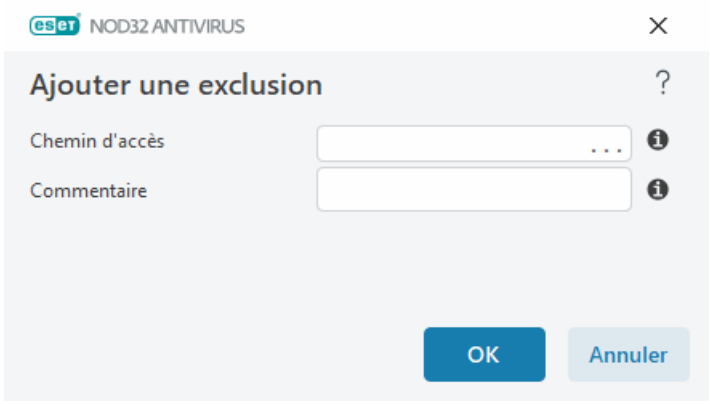
- **Ajouter** – Exclut les objets de la détection.
- **Modifier** – Permet de modifier des entrées sélectionnées.
- **Retirer** – Retire les entrées sélectionnées (CTRL + clic pour sélectionner plusieurs entrées.

Ajout ou modification d'une exclusion de performances

Cette boîte de dialogue exclut un chemin spécifique (fichier ou répertoire) pour cet ordinateur.

Choix d'un chemin ou saisie manuelle

Pour sélectionner un chemin approprié, cliquez sur **...** dans le champ **Chemin**.
En cas de saisie manuelle, consultez d'autres exemples de format d'exclusion ci-dessous.



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 sous-dossiers d'un dossier, saisissez le chemin d'accès au 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 variés dont vous ne connaissez que le premier (par exemple, « D »), utilisez le format suivant :
D????.exe (Les points d'interrogation remplacent les caractères manquants/inconnus.)

Exemples :

• *C:\Tools** – Le chemin doit se terminer par une barre oblique inverse (\) et un astérisque (*) pour indiquer qu'un dossier et que tout son contenu (fichiers et sous-dossiers) seront exclus.

• *C:\Tools*.** – Même comportement que *C:\Tools**

• *C:\Tools* – Le dossier *Tools* ne sera pas exécuté. Du point de vue du scanner, *Tools* peut aussi être un nom de fichier.

• *C:\Tools*.dat* – Cette exclusion exclut les fichiers .dat du dossier *Tools*.

• *C:\Tools\sg.dat* exclut ce fichier se trouvant exactement dans ce chemin.

Variables système dans les exclusions

Vous pouvez utiliser des variables système comme %PROGRAMFILES% pour définir des exclusions d'analyse.

• Pour exclure le dossier Program Files à l'aide de cette variable système, utilisez le chemin d'accès *%PROGRAMFILES%** (songez à 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 dossiers d'un sous-dossier *%PROGRAMFILES%*, utilisez le chemin d'accès *%PROGRAMFILES%\Répertoire_Exclu**

Développer 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 (comme *%TEMP%* ou *%USERPROFILE%*) et les variables d'environnement (comme *%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 (*C:\Tools*\Data\file.dat*, par exemple) peut fonctionner mais n'est pas officiellement prise en charge pour les exclusions de performances.
Lorsque vous utilisez les exclusions de détection, l'emploi de caractères génériques au milieu d'un chemin n'est soumis à aucune restriction.

Ordre des exclusions

- Aucune option ne permet d'ajuster le niveau de priorité des exclusions à l'aide des boutons haut/bas.
- Lorsque la première règle applicable correspond à l'analyseur, la seconde règle applicable n'est pas évaluée.
- Moins il y a de règles, plus les performances d'analyse sont meilleures.
- Évitez de créer des règles simultanées.

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 sous-dossiers d'un dossier, saisissez le chemin d'accès au 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 variés dont vous ne connaissez que le premier (par exemple, « D »), utilisez le format suivant : *D????.exe* (Les points d'interrogation remplacent les caractères manquants/inconnus.)

Exemples :

- *C:\Tools** – Le chemin doit se terminer par une barre oblique inverse (\) et un astérisque (*) pour indiquer qu'un dossier et que tout son contenu (fichiers et sous-dossiers) seront exclus.
- *C:\Tools*.** – Même comportement que *C:\Tools**
- *C:\Tools* – Le dossier *Tools* ne sera pas exécuté. Du point de vue du scanner, *Tools* peut aussi être un nom de fichier.
- *C:\Tools*.dat* – Cette exclusion exclut les fichiers .dat du dossier *Tools*.
- *C:\Tools\sg.dat* exclut ce fichier se trouvant exactement dans ce chemin.

Variables système dans les exclusions

Vous pouvez utiliser des variables système comme %PROGRAMFILES% pour définir des exclusions d'analyse.

- Pour exclure le dossier Program Files à l'aide de cette variable système, utilisez le chemin d'accès *%PROGRAMFILES%** (songez à 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 dossiers d'un sous-dossier *%PROGRAMFILES%*, utilisez le chemin d'accès *%PROGRAMFILES%\Répertoire_Exclu**

Développer 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%*

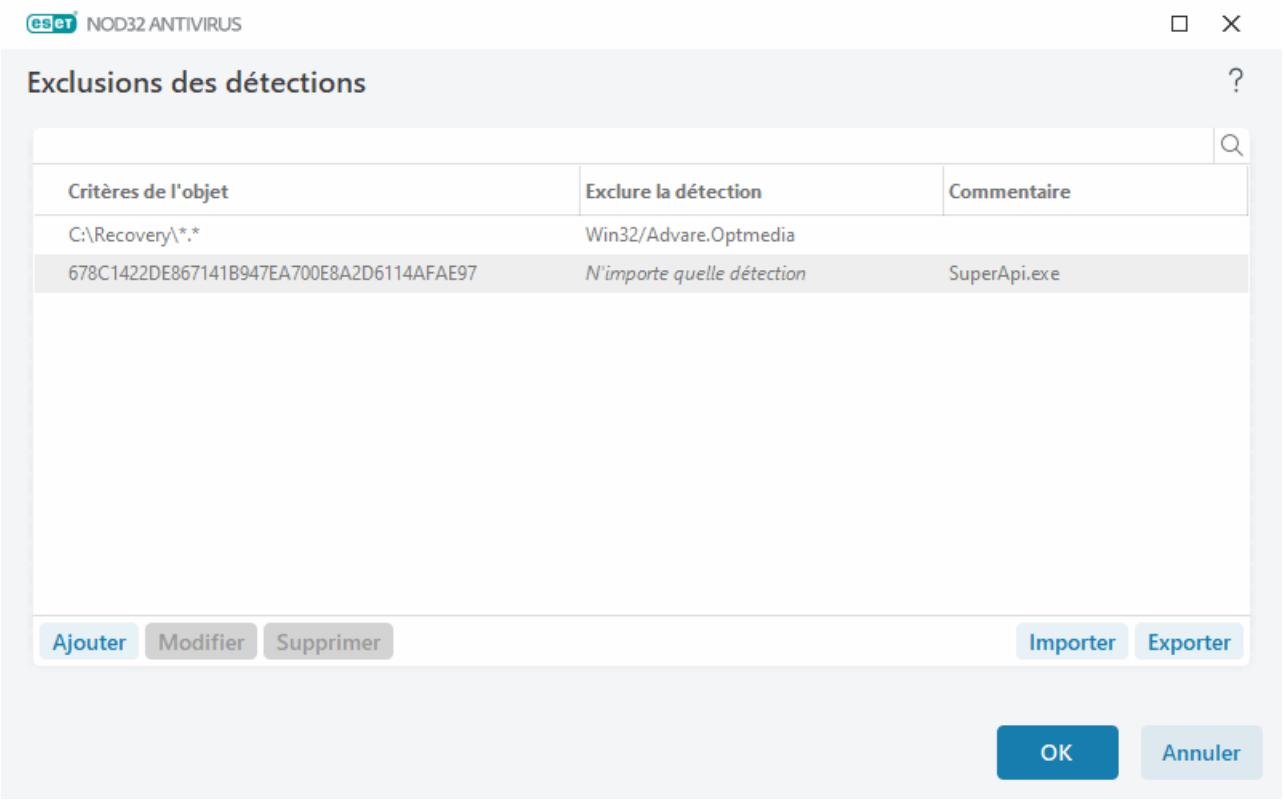
Les variables système spécifiques à l'utilisateur (comme *%TEMP%* ou *%USERPROFILE%*) et les variables d'environnement (comme *%PATH%*) ne sont pas prises en charge.

Exclusions des détections

Les exclusions de détection permettent d'exclure des objets du détection en filtrant le nom de la détection, le chemin de l'objet ou son hachage.

Fonctionnement des exclusions de détection

Les exclusions de détection n'excluent pas les fichiers et les dossiers de l'analyse comme le font les exclusions de performances. Elles excluent les objets uniquement lorsqu'ils sont détectés par le moteur de détection et que la liste des exclusions contient une règle appropriée.
Par exemple (voir la première ligne de l'image ci-dessous), lorsqu'un objet est détecté en tant que Win32/Adware.Optmedia et que le fichier détecté est *C:\Recovery\file.exe*. Sur la deuxième ligne, chaque fichier contenant le hachage SHA-1 approprié sera toujours exclu malgré le nom de la détection.



Pour veiller à ce que toutes les menaces soient détectées, il est recommandé de créer des exclusions de détection uniquement lorsque cela est absolument nécessaire.

Pour ajouter des fichiers et des dossiers à la liste des exclusions, accédez à Configuration avancée > **Moteur de détection** > **Exclusions** > **Exclusions des détections** > **Modifier**.

Ne confondez pas cette option avec Exclusions des performances, Extensions de fichiers exclues, Exclusions HIPS ou Exclusions des processus.

Pour exclure un objet (par son nom de détection ou par 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 être également créée :

- Dans la fenêtre d'alerte signalant la détection (cliquez sur **Afficher les options avancées**, puis sélectionnez

Exclure de la détection).

- Dans le menu contextuel Fichiers journaux, à l'aide de l'Assistant de création d'exclusion de détection.
- En cliquant sur **Outils** > **Quarantaine** et **Restaurer et exclure de l'analyse** dans le menu contextuel.

Critères d'objet des exclusions de détection

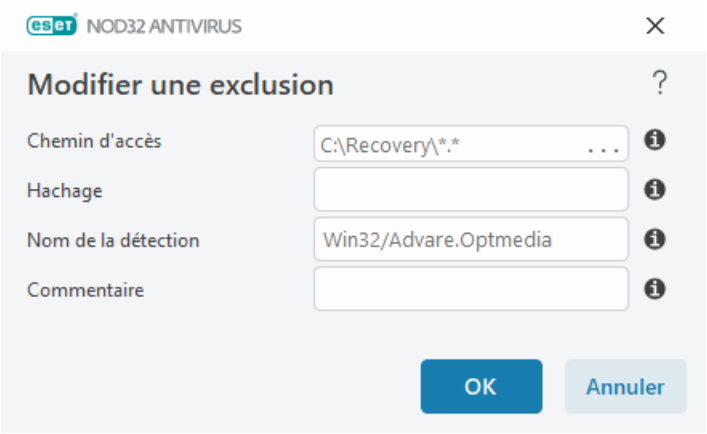
- **Chemin** – Permet de limiter une exclusion de détection pour un chemin spécifié (ou n'importe lequel).
- **Nom de la détection** – Si le nom d'une détection figure en regard d'un fichier exclu, cela signifie que ce fichier n'est exclu que pour cette détection spécifique : il n'est pas exclu complètement. Si le fichier est infecté ultérieurement par un autre logiciel malveillant, il est détecté.
- **Hachage** – Permet d'exclure un fichier selon le hachage spécifié SHA-1, indépendamment du type de fichier, de l'emplacement ou de l'extension de celui-ci.

Ajout ou modification d'une exclusion de détection

Exclure la détection

Un nom de détection ESET valide doit être fourni. Pour un nom de détection valide, consultez les fichiers journaux, puis sélectionnez **Détections** dans le menu déroulant Fichiers journaux. Cela s'avère utilise lorsqu'un échantillon faux positif est détecté dans ESET NOD32 Antivirus. Les exclusions pour les infiltrations réelles sont très dangereuses ; envisagez d'exclure uniquement les fichiers/répertoires concernés en cliquant sur **...** dans le champ **Masque** et/ou seulement pendant une période temporaire. Les exclusions s'appliquent également aux applications potentiellement indésirables, aux applications potentiellement dangereuses et aux applications suspectes.

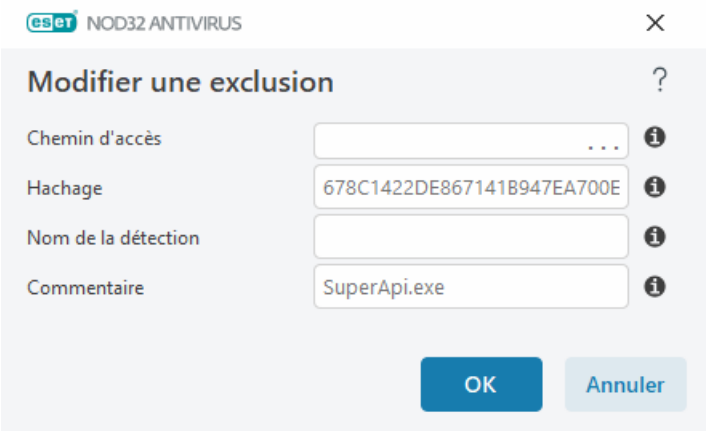
Consultez également Format d'exclusion de chemin.



Reportez-vous à l'exemple d'exclusions de détection ci-dessous.

Exclure le hachage

Permet d'exclure un fichier selon le hachage spécifié SHA-1, indépendamment du type de fichier, de l'emplacement ou de l'extension de celui-ci.



Exclusions par nom de détection

Pour exclure une détection spécifique par son nom, entrez le nom valide de la détection : Win32/Adware.Optmedia

Vous pouvez également utiliser le format suivant lorsque vous excluez une détection de la fenêtre d'alerte ESET NOD32 Antivirus :

@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt

@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan

@NAME=Win32/Bagle.D@TYPE=worm

Éléments de commande

- **Ajouter** – Exclut les objets de la détection.
- **Modifier** – Permet de modifier des entrées sélectionnées.
- **Retirer** – Retire les entrées sélectionnées (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 les détections de logiciels malveillants) :

1. Dans la fenêtre principale du programme, cliquez sur **Outils** > **Fichiers journaux**.
2. Cliquez avec le bouton droit sur une détection dans le **journal des détections**.
3. Cliquez sur **Créer une exclusion**.

Pour exclure une ou plusieurs détections en fonction de **critères d'exclusion**, cliquez sur **Modifier les critères** :

- **Fichiers exacts** – Exclure chaque fichier par son hachage SHA-1.
- **Détection** – Exclure chaque fichier par son nom de détection.
- **Chemin et détection** – Exclure chaque fichier par nom de détection et chemin, notamment le nom de fichier (*file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*, par exemple).

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 via AMSI, l'outil Microsoft Antimalware Scan Interface qui permet l'analyse des scripts PowerShell, des scripts exécutés par l'environnement d'exécution de scripts WSH (Windows Script Host) et des données analysées à l'aide du kit SDK AMSI.

Analyseur du trafic réseau

L'analyseur du trafic réseau fournit une protection contre les logiciels malveillants pour les protocoles d'application, qui intègre plusieurs techniques avancées d'analyse des logiciels malveillants. Il 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 du trafic réseau dans Configurations avancées > **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 d'ESET NOD32 Antivirus suivantes nécessitent l'activation de l'analyseur du trafic réseau :

- Protection de l'accès web
- SSL/TLS
- Protection antihameçonnage
- Protection du client de messagerie

Protection dans le cloud

ESET LiveGrid® (conçu sur le système d'avertissement anticipé ThreatSense.Net) collecte les données soumises par les utilisateurs ESET du monde entier avant de les envoyer au laboratoire de recherche d'ESET. En fournissant des métadonnées et des exemples suspects, ESET LiveGrid® nous permet de réagir immédiatement aux besoins de nos clients et de répondre aux dernières menaces.

Les options disponibles sont les suivantes :

Activation du système de réputation ESET LiveGrid®

Le système de réputation ESET LiveGrid® fournit une liste blanche et une liste noire basées sur le cloud.

Informez-vous de la réputation des fichiers et Processus en cours d'exécution depuis l'interface du programme ou à partir d'un menu contextuel comprenant des informations supplémentaires mises à disposition par ESET LiveGrid®.

Activation du système de commentaires ESET LiveGrid®

En plus du système de réputation ESET LiveGrid®, le système de commentaires ESET LiveGrid® collecte sur votre

ordinateur des informations concernant les nouvelles menaces détectées. Ces informations comprennent :

- Échantillon ou copie du fichier dans lequel la menace est apparue
- Chemin d'accès au fichier
- Nom du 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 NOD32 Antivirus est configuré pour soumettre les fichiers suspects au laboratoire d'ESET pour une analyse détaillée. Les fichiers ayant une extension définie (*.doc* ou *.xls* par exemple) sont toujours exclus. Vous pouvez également ajouter d'autres extensions si vous ou votre entreprise souhaitez éviter d'envoyer certains fichiers.

Pour plus d'informations sur l'envoi des données pertinentes, consultez la politique de confidentialité.

Choix de ne pas activer ESET LiveGrid®

Vous ne perdez rien de la fonctionnalité du logiciel, mais ESET NOD32 Antivirus peut répondre dans certains cas plus rapidement aux nouvelles menaces quand ESET LiveGrid® est activé. Si vous avez déjà utilisé le système ESET LiveGrid® et l'avez désactivé, il est possible qu'il reste des paquets de données à envoyer. Même après la désactivation, ces paquets sont envoyés à ESET. Une fois toutes les informations actuelles envoyées, plus aucun paquet ne sera créé.

Pour en savoir plus sur ESET LiveGrid®, consultez le Glossaire.
Reportez-vous à nos instructions illustrées, disponibles en anglais et dans plusieurs autres langues, pour savoir comment activer ou désactiver ESET LiveGrid® dans ESET NOD32 Antivirus.

Configuration de la protection dans le cloud dans les configurations avancées

Pour accéder aux paramètres d'ESET LiveGrid®, ouvrez Configurations avancées > **Moteur de détection** > **Protection dans le cloud** .

- **Activer le système de réputation ESET LiveGrid® (recommandé)** – Le système de réputation ESET LiveGrid® améliore l'efficacité des solutions de protection contre les logiciels malveillants en comparant les fichiers analysés à une base de données d'éléments mis en liste blanche et noire dans le cloud.
- **Activer le système de réputation ESET LiveGrid®** – Envoie les données pertinentes de soumission (décrites dans la section **Soumission des échantillons ci-dessous**) ainsi que les rapports de défaillance et les statistiques au laboratoire de recherche ESET pour une analyse plus approfondie.
- **Envoyer les rapports de défaillance et les données de diagnostic** – Permet d'envoyer des données de diagnostic associées à ESET LiveGrid® telles que des rapports de défaillance et des fichiers d'image mémoire

des modules. Il est recommandé de conserver cette option activée afin d'aider ESET à diagnostiquer les problèmes, à améliorer les produits et à renforcer la protection des utilisateurs finaux.

• **Soumettre des statistiques anonymes** – Permet à ESET de collecter des informations sur les nouvelles menaces détectées telles que le nom de la menace, la date et l'heure de détection, la méthode de détection et les métadonnées associées, la version du produit et la configuration (informations sur votre système).

• **Adresse de contact (facultative)** – Votre adresse électronique peut être incluse avec les fichiers suspects. Nous pourrons l'utiliser pour vous contacter si des informations complémentaires sont nécessaires pour l'analyse. Notez que vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires s'avèrent nécessaires.

Soumission des échantillons

Soumission manuelle des échantillons : permet de soumettre manuellement des échantillons à ESET à partir du menu contextuel Quarantaine ou Outils.

Soumission automatique des échantillons infectés

Sélectionnez quels échantillons seront soumis à ESET pour analyse afin d'améliorer les prochaines détections (la taille maximale par défaut de l'échantillon est de 64 Mo). Les options disponibles sont les suivantes :

• **Tous les échantillons détectés** – Tous les objets détectés par le moteur de détection (notamment les applications potentiellement indésirables lorsque cette option est activée dans les paramètres du scanner).

• **Tous les échantillons à l'exception des 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.

Soumission automatique des échantillons suspects

Ces échantillons seront également envoyés à ESET si le moteur de détection ne les a pas détectés. Il peut s'agir par exemple d'échantillons ayant failli ne pas être détectés ou qui semblent suspects ou dont le comportement n'est pas clair pour l'un des modules de protection ESET NOD32 Antivirus (la taille maximale par défaut de l'échantillon est de 64 Mo).

• **Exécutables** – Comprend les fichiers exécutables suivants : .exe, .dll, .sys.

• **Archives** – Comprend les fichiers d'archive suivants : .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.

• **Scripts** – Comprend les fichiers de script suivants : .bat, .cmd, .hta, .js, .vbs, .ps1.

• **Autre** – Comprend les fichiers suivants : .jar, .reg, .msi, .sfw, .lnk.

• **Courrier indésirable possible** – Le courrier indésirable possible ou l'ensemble du courrier indésirable possible avec les pièces jointes sera envoyé à ESET pour analyse supplémentaire. L'activation de cette option améliore la détection globale du courrier indésirable et celle pour vous.

• **Documents** – Comprend les documents Microsoft Office ou PDF avec ou sans contenu actif.

Développez la section 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 Exclusion permet d'exclure fichiers/dossiers de la soumission (par exemple, il peut être utile d'exclure des fichiers qui peuvent comporter des informations confidentielles, telles que des documents ou des feuilles de calcul). Les fichiers de la liste ne seront jamais envoyés aux laboratoires d'ESET pour analyse, même s'ils contiennent un code suspect. Les fichiers les plus ordinaires sont exclus par défaut (.doc, etc.). Vous pouvez ajouter des fichiers à la liste des fichiers exclus si vous le souhaitez.

Pour exclure les fichiers téléchargés depuis `download.domain.com`, accédez à Configurations avancées > **Moteur de détection** > **Protection dans le cloud** > **Soumission des échantillons**, puis cliquez sur **Modifier** en regard de l'option **Exclusions**. Ajoutez ensuite l'exclusion `.download.domain.com`.

Taille maximale des échantillons (Mo) – Permet de définir la taille maximale des échantillons soumis automatiquement (1 à 64 Mo).

Filtre d'exclusion pour la protection dans le cloud

Le filtre d'exclusion permet d'exclure certains fichiers ou dossiers de la soumission d'échantillons. Les fichiers de la liste ne seront jamais envoyés aux laboratoires d'ESET pour analyse, même s'ils contiennent un code suspect. Les types de fichiers courants (tels que .doc, etc.) sont exclus par défaut.

cette fonctionnalité s'avère utile pour exclure des fichiers qui peuvent comporter des informations confidentielles (documents ou feuilles de calcul, par exemple).

Pour exclure les fichiers téléchargés depuis download.domain.com, ouvrez Configurations avancées > **Moteur de détection** > **Protection dans le cloud** > **Soumission des échantillons** > **Exclusions** et ajoutez l'exclusion *download.domain.com*.

Analyses des logiciels malveillants

La section **Analyses des logiciels malveillants** est accessible depuis Configurations avancées > **Moteur de détection** > **Analyses des logiciels malveillants**. Elle permet de configurer les paramètres d'analyse des profils d'analyse.

Analyse à la demande

Profil sélectionné – Ensemble spécifique de paramètres utilisés par le scanner à la demande. Pour créer un profil, cliquez sur **Modifier** en regard de **Liste des profils**. Pour plus d'informations, consultez 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 spécifique ou un groupe de cibles, cliquez sur **Modifier** en regard de **Cibles à analyser**, puis sélectionnez une option dans la structure (arborescence) des dossiers. Pour plus d'informations, consultez Cibles à analyser.

Protection à la demande et par apprentissage machine – Vous pouvez configurer les niveaux de rapport et de protection 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 l'option **Utiliser les configurations de protection en temps réel** pour configurer des niveaux de rapport et de protection personnalisés. Consultez Protections pour une explication détaillée des niveaux de rapport et de protection.

ThreatSense : options de configuration avancées, telles que les extensions de fichier que vous souhaitez contrôler et les méthodes de détection utilisées. Pour plus d'informations, consultez ThreatSense.

Profils d'analyse

Il existe quatre profils d'analyse prédéfinis dans ESET NOD32 Antivirus :

- **Analyse intelligente** : il s'agit du profil d'analyse avancée par défaut. Le profil d'analyse intelligente utilise la technologie d'optimisation intelligente qui exclut les fichiers qui ont été détectés comme étant non infectés lors d'une analyse précédente et qui n'ont pas été modifiés depuis. La durée d'analyse est ainsi réduite avec un impact minimal sur la sécurité du système.

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

- **Analyse approfondie** : Le profil d'analyse approfondie n'utilise pas l'optimisation intelligente par défaut. Par conséquent, aucun fichier n'est exclu de l'analyse à l'aide de ce profil.

- **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 les prochaines analyses. Il est recommandé de créer autant de profils (avec différentes cibles et méthodes, et d'autres paramètres d'analyse) que d'analyses utilisées régulièrement.

Pour créer un profil, ouvrez Configurations avancées > **Moteur de détection** > **Analyses des logiciels malveillants** > **Analyse à la demande** > **Liste des profils** > **Modifier**. La fenêtre **Gestionnaire de profils** dispose du menu déroulant **Profil sélectionné** contenant les profils d'analyse existants, ainsi qu'une option permettant de créer un profil. Pour plus d'informations sur la création d'un profil d'analyse correspondant à vos besoins, reportez-vous à ThreatSense ; vous y trouverez une description de chaque paramètre de configuration de l'analyse.

> Supposons la situation suivante : vous souhaitez créer votre propre profil d'analyse et la configuration **Analyse intelligente** est partiellement adéquate. En revanche, vous ne souhaitez analyser ni les fichiers exécutables compressés par un compresseur d'exécutables, ni les applications potentiellement dangereuses. Vous souhaitez effectuer un **Toujours corriger la détection**. Entrez le nom du nouveau profil dans la fenêtre **Gestionnaire de profils**, puis cliquez sur **Ajouter**. Sélectionnez le nouveau profil dans le menu déroulant **Profil sélectionné** et réglez les paramètres restants selon vos besoin. Cliquez sur **OK** pour enregistrer le nouveau profil.

Cibles à analyser

Le menu déroulant **Cibles à analyser** permet de sélectionner des cibles à analyser prédéfinies :

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

La structure (arborescence) des dossiers contient également des cibles à analyser spécifiques.

- **Mémoire vive** – Analyse l'ensemble des processus et des données actuellement utilisés par la mémoire vive.
- **Secteurs d'amorçage/UEFI** – Analyse les secteurs d'amorçage et UEFI afin de détecter la présence éventuelle de logiciels malveillants. Pour plus d'informations 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 des références à des fichiers infectés ou des logiciels malveillants intégrés en tant que données.
- **Registre système** – Analyse l'ensemble du Registre système, toutes les clés et les sous-clés. Recherche des références à des fichiers infectés ou des logiciels malveillants intégrés en tant que données. Lors du nettoyage des détections, la référence reste dans le Registre pour s'assurer que les données importantes ne sont pas perdues.

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

Analyse en cas d'inactivité

Vous pouvez activer l'analyse en cas d'inactivité dans Configuration avancée > **Moteur de détection** > **Analyses des logiciels malveillants** > **Analyse en cas d'inactivité**.

Analyse en cas d'inactivité

Activez le bouton bascule en regard de l'option **Activer l'analyse en cas d'inactivité** pour activer cette fonctionnalité. Lorsque l'ordinateur n'est pas utilisé, une analyse silencieuse de l'ordinateur est effectuée sur tous les disques locaux.

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

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

Détection en cas d’inactivité

Consultez la section Déclencheurs de détection d'inactivité pour une liste complète des conditions qui doivent être satisfaites afin de déclencher l'analyse d'inactivité.

ThreatSense : options de configuration avancées, telles que les extensions de fichier que vous souhaitez contrôler et les méthodes de détection utilisées. Pour plus d'informations, consultez ThreatSense.

Détection en cas d’inactivité

Les paramètres de détection en cas d'inactivité peuvent être configurés dans Configuration avancée > **Moteur de détection** > **Analyses des logiciels malveillants** > **Analyse en cas d'inactivité** > **Détection en cas d'inactivité**. Ces paramètres spécifient un déclencheur pour l'Analyse en cas d'inactivité :

- **Écran ou économiseur d'écran désactivé**
- **Ordinateur verrouillé**
- **Utilisateur déconnecté**

Utilisez le bouton bascule pour chaque état respectif, afin d'activer ou de désactiver les différents déclencheurs de détection d'état inactif.

Analyse au démarrage

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

Les options d'analyse au démarrage font partie d'une tâche planifiée **Contrôle des fichiers de démarrage du système**. Pour modifier ses paramètres, accédez à **Outils** > **Planificateur**, cliquez sur **Vérification automatique des fichiers de démarrage**, puis sur **Modifier**. À la dernière étape, la fenêtre Vérification automatique des fichiers de démarrage s’affichera. Pour des instructions détaillées sur la création et à la gestion de tâches planifiées, voir 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. Pour plus d'informations, consultez ThreatSense.

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 **Cible à analyser** définit la profondeur d'analyse pour les fichiers qui s'exécutent au démarrage du système selon un algorithme sophistiqué secret. Les fichiers sont organisés par ordre décroissant suivant ces critères :

- **Tous les fichiers enregistrés** (la plupart des fichiers sont analysés)

- **Fichiers rarement utilisés**
- **Fichiers couramment utilisés**
- **Fichiers fréquemment utilisés**
- **Seulement les fichiers utilisés fréquemment** (nombre minimum de fichiers analysés)

Il existe en outre deux groupes spécifiques :

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

Les listes des fichiers à analyser sont fixées 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 seront analysés à l'ouverture ou à l'exécution.

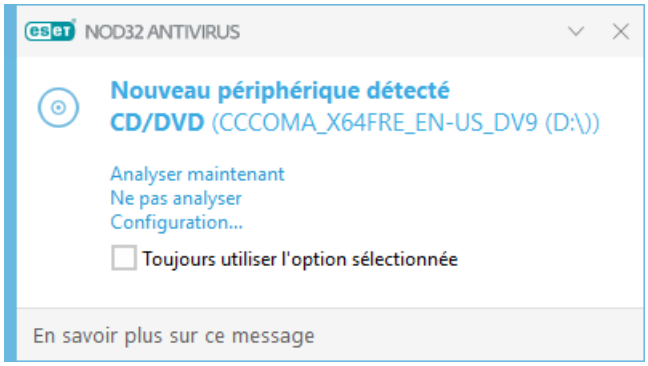
Priorité d'analyse – Niveau de priorité servant à déterminer le démarrage d'une analyse :

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

Supports amovibles

ESET NOD32 Antivirus permet d'analyser automatiquement les supports amovibles (CD/DVD/USB...) lors de leur insertion dans un ordinateur. Cela peut être utile si l'administrateur souhaite empêcher les utilisateurs d'utiliser des appareils amovibles avec du contenu non sollicité.

Lorsqu'un support amovible est inséré et que l'option **Afficher les options d'analyse** est définie dans Configurations avancées > **Moteur de détection** > **Analyses des logiciels malveillants** > **Supports amovibles**, la boîte de dialogue suivante s'affiche :



Options de cette boîte de dialogue :

- **Analyser maintenant** – Cette option déclenche l'analyse du support amovible.
- **Ne pas analyser** – Les appareils amovibles ne sont pas analysés.
- **Configuration** – Ouvre la boîte de dialogue Configuration avancée.
- **Toujours utiliser l'option sélectionnée** – Lorsque cette option est sélectionnée, la même action sera exécutée lorsqu'un support amovible sera inséré plus tard.

En outre, ESET NOD32 Antivirus offre la fonctionnalité de contrôle des périphériques qui permet de définir des règles d'utilisation de périphériques externes sur un ordinateur donné. Pour plus de détails sur le contrôle des périphériques, reportez-vous à la section Contrôle des périphériques.

Pour accéder aux paramètres de l'analyse de supports amovibles, ouvrez Configurations avancées > **Moteur de détection** > **Analyses des logiciels malveillants** > **Appareils amovibles**.

Action effectuée après l'insertion d'un support amovible – Sélectionnez l'action par défaut qui sera exécutée lors de l'insertion d'un appareil amovible (CD/DVD/USB). Choisissez l'action souhaitée lors de l'insertion d'un appareil amovible dans un ordinateur :

- **Ne pas analyser** – Aucune action n'est exécutée et la fenêtre **Nouvel appareil détecté** ne s'ouvre pas.
- **Analyse automatique de périphérique** – Le support amovible inséré fait l'objet d'une analyse à la demande.
- **Afficher les options d'analyse** – Ouvre la section de configuration des **appareils amovibles**.

Protection des documents

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

Pour activer la protection des documents, ouvrez Configurations avancées > **Moteur de détection** > **Analyses des logiciels malveillants** > **Protection des documents**, puis cliquez sur le bouton bascule en regard de l'option

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. Pour plus d'informations, consultez ThreatSense.

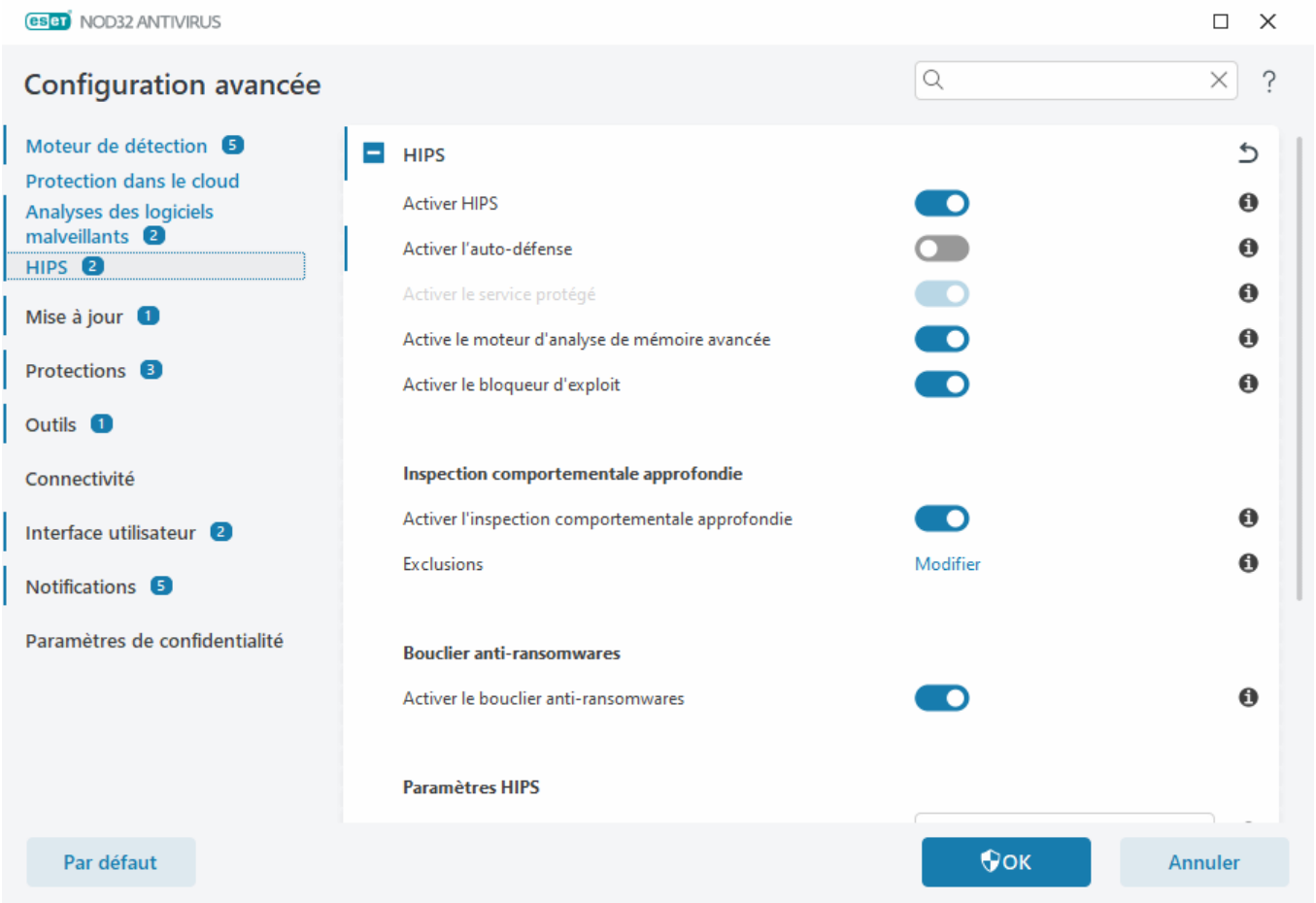
Cette fonctionnalité est activée par des applications utilisant Microsoft Antivirus API (par exemple Microsoft Office 2000 et versions ultérieures, ou Microsoft Internet Explorer 5.0 et versions ultérieures).

HIPS – Host Intrusion Prevention System

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

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

Vous pouvez configurer les paramètres HIPS dans Configurations avancées > **Moteur de détection** > **HIPS** > **HIPS**. L'état du système HIPS (activé/désactivé) est indiqué dans la fenêtre principale du programme ESET NOD32 Antivirus > **Configuration** > **Protection de l'ordinateur**.



HIPS

Activer HIPS – HIPS est activé par défaut dans ESET NOD32 Antivirus. La désactivation de HIPS entraîne celle des autres fonctionnalités HIPS comme le bloqueur d'exploit.

Activer l'auto-défense – ESET NOD32 Antivirus utilise la technologie **Auto-défense** intégrée dans le cadre de la fonctionnalité HIPS pour empêcher les logiciels malveillants d'endommager ou de désactiver la protection antivirus et antispyware. La technologie Auto-défense protège le système, les processus, les clés de registre et les fichiers d'ESET contre toute modification.

Activer le service protégé – Active la protection pour le service ESET (ekrn.exe). Lorsque cette option est activée, le service est démarré en tant que processus Windows protégé pour empêcher toute attaque par des logiciels malveillants.

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

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

Inspection comportementale approfondie

Activer l'inspection comportementale approfondie – autre couche de protection qui fonctionne dans le cadre de la fonctionnalité HIPS. Cette extension de HIPS analyse le comportement de tous les programmes en cours d'exécution sur l'ordinateur et vous averti si le comportement d'un processus est malveillant.

Les exclusions HIPS de l'inspection comportementale approfondie permettent d'exclure des processus de l'analyse. Pour que la détection des menaces éventuelles s'appliquent bien à tous les processus, il est recommandé de ne créer des exclusions que lorsque cela s'avère absolument nécessaire.

Protection contre les rançongiciels

Activer la protection anti-ransomware – Autre couche de protection qui fonctionne dans le cadre de la fonctionnalité HIPS. Pour qu'elle fonctionne, vous devez activer le système de réputation ESET LiveGrid®. Lire des informations supplémentaires sur ce type de protection.

Activer Intel® Threat Detection Technology : permet de détecter les attaques de ransomware 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 les processeurs pris en charge.

Paramètres HIPS

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

Mode de filtrage	Description
Mode automatique	Les opérations sont autorisées, à l'exception de celles bloquées par des règles prédéfinies qui protègent votre système.
Mode intelligent	Mode intelligent – L'utilisateur n'est averti que lors d'événements très suspects.
Mode interactif	L'utilisateur est invité à confirmer les opérations.
Mode basé sur des politiques	Bloque toutes les opérations qui ne sont pas définies par une règle spécifique qui les autorise.
Mode d'apprentissage	Les opérations sont autorisées et une règle est créée après chaque opération. Les règles créées dans ce mode peuvent être affichées dans l'éditeur de **règles HIPS**, mais leur niveau de priorité est inférieur à celui des règles créées manuellement ou en mode automatique. Lorsque vous sélectionnez l'option **Mode d'apprentissage** dans le menu déroulant **Mode de filtrage**, le paramètre **Le mode d'apprentissage prend fin le** devient disponible. Sélectionnez la durée du mode d'apprentissage. La durée maximale est de 14 jours. Lorsque la durée spécifiée est arrivée à son terme, vous êtes invité à modifier les règles créées par HIPS en mode d'apprentissage. Vous pouvez également choisir un autre mode de filtrage ou continuer à utiliser le mode d'apprentissage.

Mode défini après expiration du mode d'apprentissage – Sélectionnez le mode de filtrage qui sera utilisé après expiration du mode d'apprentissage. Après expiration, l'option **Demander à l'utilisateur** requiert des privilèges administratifs pour effectuer un changement au mode de filtrage HIPS.

Le système HIPS surveille les événements dans le système d'exploitation et réagit en fonction de règles qui sont semblables à celles utilisées par le pare-feu. Cliquez sur **Modifier** en regard de **Règles** pour ouvrir l'éditeur de **règles HIPS**. La fenêtre des règles HIPS permet de sélectionner, d'ajouter, de modifier ou de supprimer des règles. Vous trouverez plus de détails sur la création de règles et les opérations HIPS dans Modifier une règle HIPS.

Exclusions HIPS

Les exclusions permettent d'exclure des processus de l'inspection comportementale approfondie HIPS.

Pour modifier les exclusions HIPS, ouvrez Configurations avancées > **Moteur de détection** > **HIPS** > **HIPS** > **Exclusions** > **Modifier**.

> Ne confondez pas cette option avec Extensions de fichiers exclues, Extensions de détection, Exclusions des performances ou Exclusions des processus.

Pour exclure un objet, cliquez sur **Ajouter** et entrez le chemin d'un objet ou sélectionnez-le dans l'arborescence. Vous pouvez aussi modifier ou supprimer des entrées sélectionnées.

Configuration avancée de HIPS

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

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

Consigner toutes les opérations bloquées – Toutes les opérations bloquées sont inscrites dans le journal HIPS. Utilisez cette fonctionnalité uniquement lorsque l'assistance technique ESET vous le demande ou que vous résolvez des problèmes, car elle peut générer un fichier journal très volumineux et ralentir votre ordinateur.

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

Pilotes dont le chargement est toujours autorisé

Le chargement des pilotes répertoriés dans cette liste est toujours autorisé quel que soit le mode de filtrage HIPS, sauf s'il est bloqué explicitement par une règle de l'utilisateur.

Ajouter – Ajoute un nouveau pilote.

Modifier – Modifie un pilote sélectionné.

Supprimer – Supprime un pilote de la liste.

Réinitialiser – Recharge un ensemble de pilotes système.

Cliquez sur **Réinitialiser** si vous ne souhaitez pas que les pilotes que vous avez ajoutés manuellement soient inclus. Cette commande peut s'avérer utile lorsque vous avez ajouté plusieurs pilotes et que vous ne pouvez pas les supprimer manuellement de la liste.

Après l'installation, la liste des pilotes est vide. ESET NOD32 Antivirus complète automatiquement la liste au fil du temps.

Fenêtre interactive HIPS

La fenêtre de notification HIPS permet de créer une règle en fonction des nouvelles actions détectées par le système HIPS, puis de définir les conditions dans lesquelles autoriser ou refuser cette action.

Les règles créées dans la fenêtre de notification sont considérées comme étant équivalentes aux règles créées manuellement. La règle créée à partir d'une fenêtre de notification peut être moins spécifique que celle qui a déclenché l'affichage de la boîte de dialogue. En d'autres termes, après la création d'une règle dans la boîte de dialogue, la même opération peut déclencher la même fenêtre. Pour plus d'informations, voir Priorité des règles HIPS.

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

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

L'option **Créer une règle et l'enregistrer de manière permanente** créera une règle HIPS pouvant être modifiée ultérieurement dans la section Gestion des règles HIPS (requiert des privilèges d'administration).

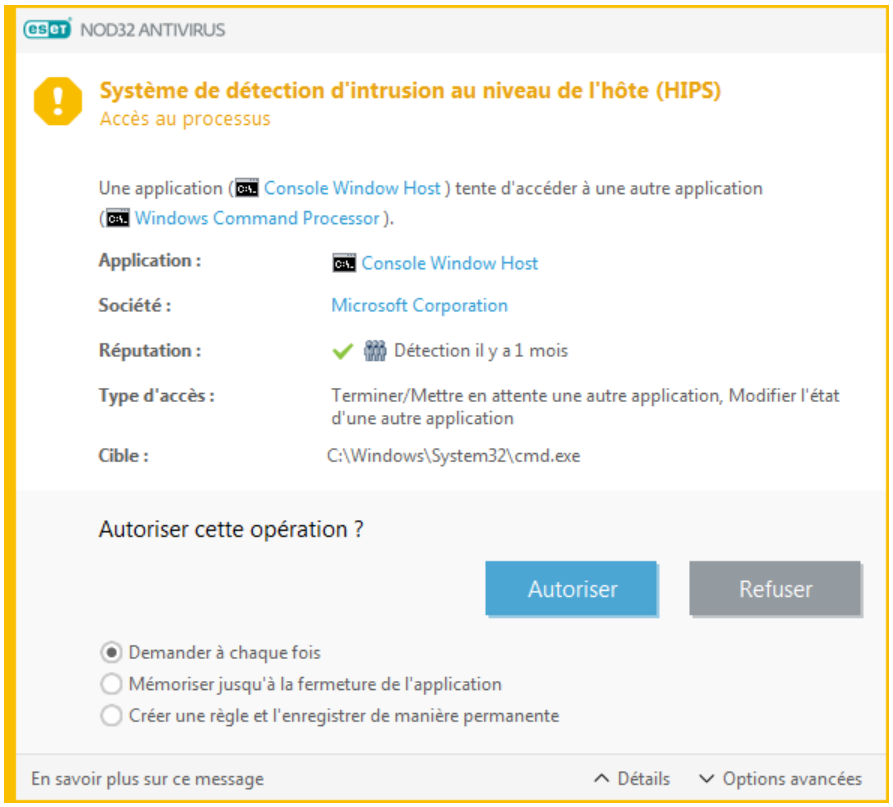
Cliquez sur **Détails** en bas pour déterminer quelle application déclenche l'opération, quelle est la réputation du fichier ou quel type d'opération il vous est demandé d'autoriser ou de refuser.

Vous pouvez accéder aux configurations des paramètres de règle plus détaillés en cliquant sur **Options avancées**. Les options suivantes sont disponibles si vous sélectionnez **Créer une règle et l'enregistrer de manière**

permanente :

- **Créer une règle valide uniquement pour cette application** – Si vous décochez cette case, la règle sera créée pour toutes les applications source.
- **Uniquement pour l'opération** – Choisissez la ou les opérations (fichier/application/registre) de la règle. Voir la description de toutes les opérations HIPS.
- **Uniquement pour la cible** – Choisissez la ou les cibles (fichier/application/registre) de la règle.

> **Notification HIPS sans fin ?**
> Pour arrêter l'affichage des notifications, remplacez le mode de filtrage par **Automatique** dans Configurations avancées > **Moteur de détection** > **HIPS** > **HIPS**.



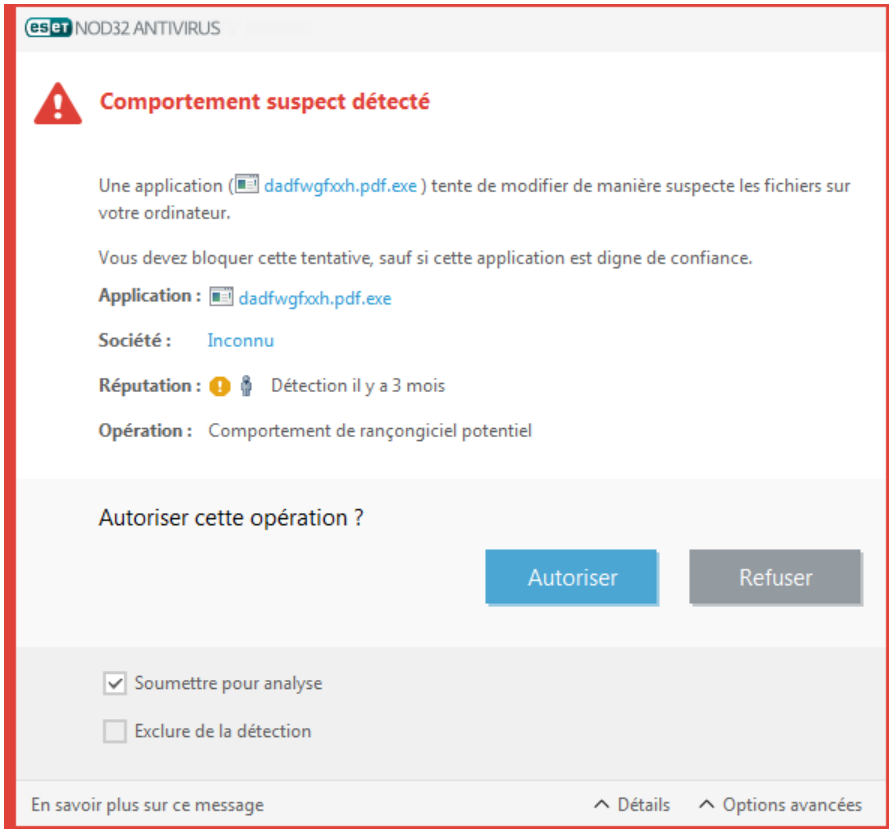
Fin du mode d'apprentissage

Le mode d'apprentissage crée et enregistre automatiquement des règles. Vous pouvez consulter toutes les règles créées dans les Paramètres de règle HIPS. Ce mode est idéal pour la configuration initiale du système HIPS, mais il ne doit être activé que pendant une courte période. Aucune intervention de l'utilisateur n'est requise, car ESET NOD32 Antivirus enregistre les règles conformément aux paramètres prédéfinis. Passez en mode **interactif** ou **basé sur des stratégies** une fois que toutes les règles relatives aux processus requis s'exécutant dans le système d'exploitation ont été créées afin d'éviter les risques de sécurité.

Vous pouvez reporter cette décision si vous ne souhaitez pas modifier les paramètres.

Comportement de rançongiciel potentiel détecté

Cette fenêtre interactive s'affiche lorsqu'un comportement de rançongiciel potentiel est détecté. Vous pouvez choisir de **refuser** ou d'**autoriser** l'opération.



Cliquez sur **Détails** pour afficher des paramètres de détection spécifiques. Cette boîte de dialogue permet de **soumettre le fichier pour analyse** ou de l'**exclure de la détection**.

Pour que la protection contre les rançongiciels fonctionne correctement, ESET LiveGrid® doit être activé.

Gestion des règles HIPS

Liste des règles définies par l'utilisateur et ajoutées automatiquement depuis le système HIPS. Vous trouverez des informations détaillées sur la création de règles et sur les opérations HIPS au chapitre Paramètres de règle HIPS. Consultez également Principe général HIPS.

Colonnes

Règle – Nom de règle défini par l'utilisateur ou sélectionné automatiquement.

Activé – Désactivez le bouton bascule si vous souhaitez conserver la règle dans la liste, mais ne souhaitez pas l'utiliser.

Action – La règle spécifie une action (**Autoriser**, **Bloquer** ou **Demander**) à exécuter, si les conditions sont remplies.

Sources – La règle est utilisée uniquement si l'événement est déclenché par une ou des applications.

Cibles – La règle est utilisée uniquement si l'opération est liée à un fichier, une application ou une entrée de registre spécifique.

Niveau de verbosité – Si vous activez cette option, les informations sur cette règle sont écrites dans le journal HIPS.

Notifier – Une petite fenêtre de notification apparaît dans le coin inférieur droit si un événement est déclenché.

Éléments de commande

Ajouter – Permet de créer une règle.

Modifier – Permet de modifier des entrées sélectionnées.

Supprimer – Supprime les entrées sélectionnées.

Priorité des règles HIPS

Aucune option ne permet d'ajuster le niveau de priorité des règles HIPS à l'aide des boutons haut/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 pour une application spécifique a une priorité supérieure à celle de 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 remplacer les règles définies par l'auto-défense).
- Une règle que vous créez et qui pourrait bloquer votre système d'exploitation ne sera pas appliquée (elle aura la priorité la plus basse).

Modification d'une règle HIPS

Consultez d'abord Gestion des règles HIPS.

Nom de règle – Nom de règle défini par l'utilisateur ou sélectionné automatiquement.

Action – Spécifie une action (**Autoriser**, **Bloquer** ou **Demander**) à exécuter, si les conditions sont remplies.

Opérations affectant – Vous devez sélectionner le type d'opération auquel s'applique la règle. La règle est utilisée uniquement pour ce type d'opération et pour la cible sélectionnée.

Activé – Désactivez le bouton bascule si vous souhaitez conserver la règle dans la liste, mais ne souhaitez pas l'appliquer.

Niveau de verbosité – Si vous activez cette option, les informations sur cette règle sont écrites dans le journal HIPS.

Avertir l'utilisateur – Une petite fenêtre de notification apparaît dans l'angle inférieur droit si un événement est

déclenché.

La règle se compose de parties qui décrivent les conditions de déclenchement de cette règle :

Applications source – La règle est utilisée uniquement si l'événement est déclenché par cette ou ces applications. Dans le menu déroulant, sélectionnez **Applications spécifiques**, puis cliquez sur **Ajouter** 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 est utilisée uniquement si l'opération est liée à cette cible. Dans le menu déroulant, sélectionnez **Fichiers spécifiques**, puis 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 est utilisée uniquement si l'opération est liée à cette cible. Dans le menu déroulant, sélectionnez **Applications spécifiques**, puis 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 Registre – La règle est utilisée uniquement si l'opération est liée à cette cible. Dans le menu déroulant, sélectionnez **Entrées spécifiques**, puis cliquez sur **Ajouter** pour effectuer une saisie manuelle ou sur **Ouvrir l'Éditeur du Registre** pour sélectionner une clé dans le registre. Vous pouvez également sélectionner **Toutes les entrées** dans le menu déroulant pour ajouter toutes les applications.

> Le fonctionnement de certaines règles prédéfinies par HIPS ne peut pas être bloqué et est autorisé par défaut. En outre, les opérations système ne sont pas toutes surveillées par le système HIPS. Ce système HIPS surveille les opérations qui peuvent être considérées comme dangereuses.

Description des opérations importantes :

Opérations sur le fichier

- **Supprimer le fichier** – L'application demande l'autorisation de supprimer le fichier cible.
- **Écrire dans le fichier** – L'application demande l'autorisation d'écrire dans le fichier cible.
- **Accès direct au disque** – L'application essaie de lire des informations du disque ou d'écrire sur le disque d'une manière inhabituelle, non conforme aux procédures Windows classiques. Les fichiers peuvent être modifiés sans que les règles correspondantes soient appliquées. Cette opération peut provenir d'un logiciel malveillant qui essaie de contourner la détection, d'un logiciel de sauvegarde qui tente de faire une copie exacte d'un disque ou encore d'un gestionnaire de partition qui essaie de réorganiser les volumes du disque.
- **Installer l'élément hook global** – Fait référence à l'appel de la fonction SetWindowsHookEx depuis la bibliothèque MSDN.
- **Charger le pilote** – Installation et chargement de pilotes dans le système.

Opérations sur l'application

- **Déboguer une autre application** – Ajout d'un système de débogage au processus. Lors du débogage d'une application, de nombreux détails concernant son comportement peuvent être affichés et modifiés. Vous pouvez également accéder à ses données.

• **Intercepter les événements d'une autre application** – L'application source essaie de récupérer les événements destinés à une application spécifique (il peut s'agir par exemple d'un programme keylogger d'enregistrement des touches qui essaie de capturer les événements d'un navigateur).

• **Arrêter/Mettre en attente une autre application** – Met un processus en attente, le reprend ou l'arrête (accessible directement depuis l'explorateur des processus ou le volet des processus).

• **Démarrer une nouvelle application** – Démarrage de nouvelles applications et de nouveaux processus.

• **Modifier l'état d'une autre application** – L'application source essaie 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 importante : vous la configurez en tant qu'application cible dans une règle qui bloque l'utilisation de cette opération.

Opérations sur le Registre

• **Modifier les paramètres de démarrage** – Toute modification apportée aux paramètres qui définissent les applications à exécuter au démarrage de Windows. Elles peuvent notamment être recherchées à l'aide de la clé Run du registre Windows.

• **Supprimer du registre** – Suppression d'une clé de registre ou de sa valeur.

• **Renommer la clé de registre** – Changement du nom des clés de registre.

• **Modifier le registre** – Création de nouvelles valeurs de clés de registre, modification de valeurs existantes, déplacement de données dans l'arborescence de base de données ou configuration des droits d'utilisateur ou de groupe pour les clés de registre.

Vous pouvez utiliser des caractères génériques qui peuvent présenter des restrictions lors le la saisie d'un dossier. Au lieu d'utiliser une clé particulière, vous pouvez utiliser un astérisque (*) dans les chemins de registre. Par exemple *HKEY_USERS*\software* peut vouloir dire *HKEY_USER\.default\software* mais pas *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** n'est pas un chemin valide de clé de registre. Un chemin de clé de registre contenant le symbole « * » signifie « ce chemin ou tout autre niveau après ce symbole ». C'est le seul moyen d'utiliser des caractères génériques pour les cibles séjour. L'évaluation porte tout d'abord sur la partie spécifique du chemin, puis sur celle figurant après le symbole (*).

Si vous créez une règle très générique, l'avertissement concernant ce type de règle s'affiche.

Dans l'exemple suivant, nous allons montrer comment limiter le comportement indésirable d'une application spécifique :

1. Nommez la règle et sélectionnez **Bloquer** (ou **Demander** si vous préférez effectuer un choix ultérieurement) dans le menu déroulant **Action**.

2. Activez le bouton bascule situé en regard de l'option **Avertir l'utilisateur** pour afficher une notification à chaque fois qu'une règle est appliquée.

3. Dans la section **Opérations affectant**, sélectionnez au moins une opération pour laquelle la règle sera appliquée.

4. Cliquez sur **Suivant**.

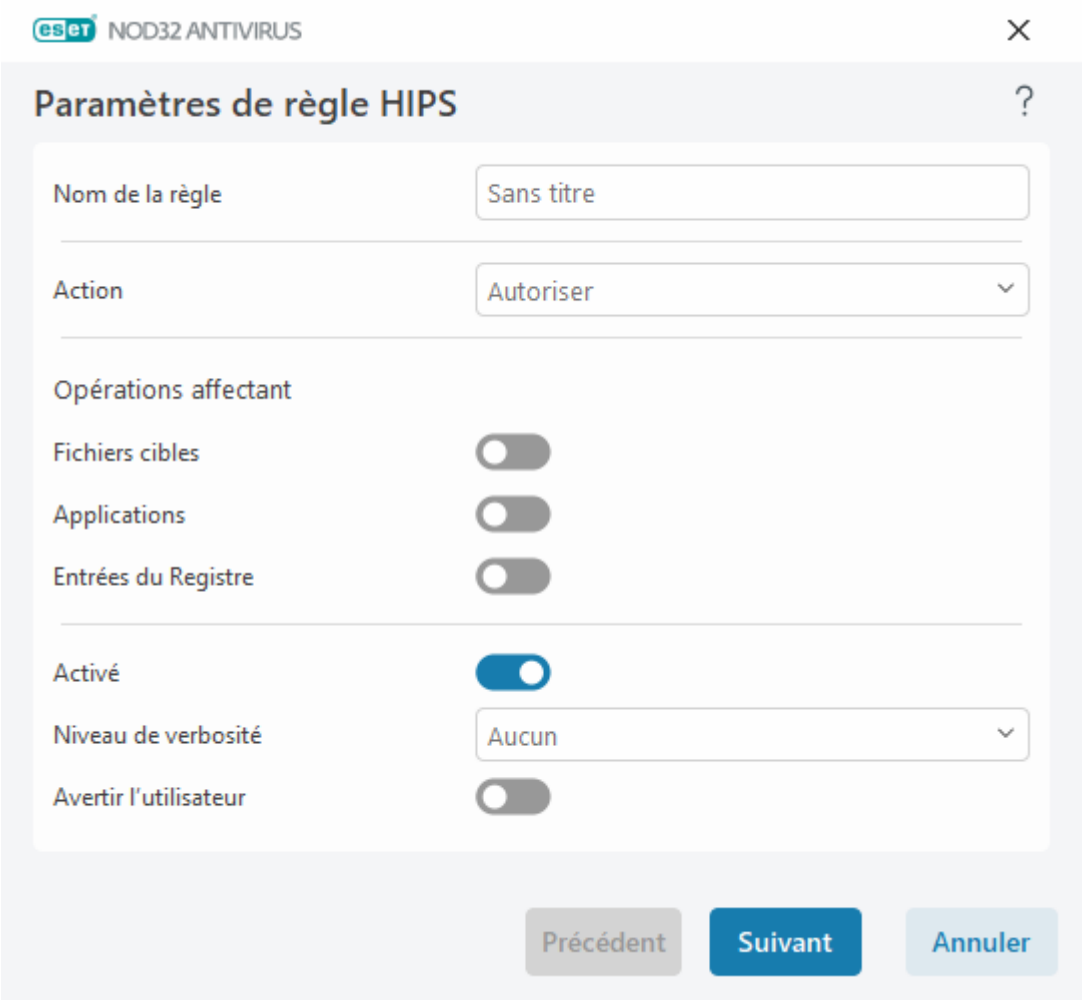
5. Dans la fenêtre **Applications source**, sélectionnez **Toutes les applications** dans le menu déroulant pour appliquer la nouvelle règle à toutes les applications qui tentent d'effectuer les opérations sélectionnées sur les applications spécifiées.

6. Cliquez sur **Ajouter**, sur **...** pour sélectionner un chemin d'accès à une application spécifique, puis appuyez sur **OK**. Ajoutez des applications supplémentaires si vous le souhaitez.
Par exemple : *C:\Program Files (x86)\Untrusted application\application.exe*

7. Sélectionnez l'opération **Écrire dans le fichier**.

8. Dans le menu déroulant, sélectionnez **Tous les fichiers**. Ainsi, les applications sélectionnées à l'étape précédente ne pourront écrire dans aucun fichier.

9. Cliquez sur **Terminer** pour enregistrer la nouvelle règle.



Ajouter le chemin de l'application/du registre pour HIPS

Sélectionnez un chemin d'application de fichier en cliquant sur l'option **...** Lors de la sélection d'un dossier, toutes les applications situées dans cet emplacement sont incluses.

L'option **Ouvrir l'Éditeur du Registre** démarrer l'éditeur du registre Windows (regedit). Lors de l'ajout d'un chemin de registre, saisissez l'emplacement correct dans le champ **Valeur**.

Exemples du chemin de fichier ou de 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 Configurations avancées > **Mise à jour**. Cette section permet de spécifier les informations concernant les sources des mises à jour, telles que les serveurs de mise à jour utilisés et les données d'authentification donnant accès à ces serveurs.

Mettre à jour

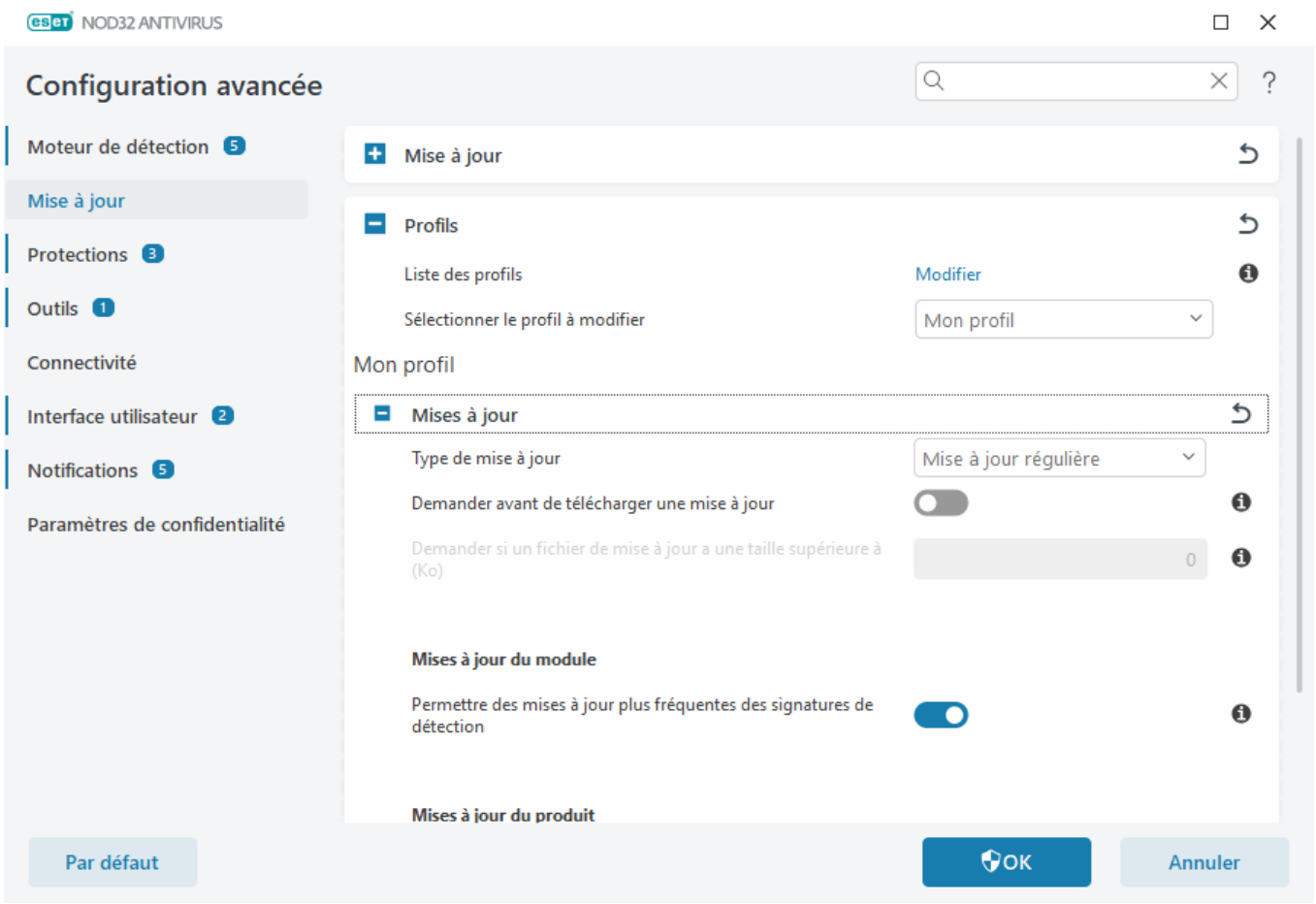
Le profil de mise à jour en cours d'utilisation est affiché dans le menu déroulant **Sélectionner le profil de mise à jour par défaut**.

Pour créer un profil, consultez la section Profils de mise à jour.

Si vous rencontrez des problèmes lors du téléchargement du moteur de détection ou des mises à jour de modules, cliquez sur **Effacer** en regard de l'option **Vider le cache de mise à jour** pour supprimer les fichiers de mise à jour/le cache temporaires.

Restauration des modules

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



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

Profils

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

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

Mises à jour

Par défaut, l'option **Type de mise à jour** est définie sur **Mise à jour régulière** pour que les fichiers de mise à jour soient téléchargés automatiquement du serveur ESET lorsque le trafic réseau est le moins surchargé. Les mises à jour des versions bêta (option **Mise à jour des versions bêta**) ont subi toutes les phases internes de test et seront disponibles très prochainement pour le grand public. Vous pouvez activer ces versions bêta afin d'accéder aux dernières méthodes de détection et aux derniers correctifs. Toutefois, ces versions ne sont peut-être pas suffisamment stables pour être utilisées en permanence et NE DOIVENT PAS être utilisées sur des serveurs de production et des stations de travail qui exigent les plus grandes disponibilité et stabilité.

Demander avant de télécharger une mise à jour – Le programme affiche une notification dans laquelle vous pouvez confirmer ou refuser les téléchargements des fichiers de mise à jour.

Demander si un fichier de mise à jour a une taille supérieure à (Ko) – Le programme affiche une boîte de dialogue de confirmation si la taille du fichier de mise à jour est supérieure à la valeur indiquée. Si la taille du fichier de mise à jour est définie sur 0 Ko, le programme affiche toujours une boîte de dialogue de confirmation.

Mises à jour du module

Activer des mises à jour plus fréquentes des signatures de détection – Les signatures de détection sont mise à jour à 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 d'ESET NOD32 Antivirus.

Options de connexion

Pour utiliser un serveur proxy afin de télécharger les mises à jour, consultez la section Options de connexion.

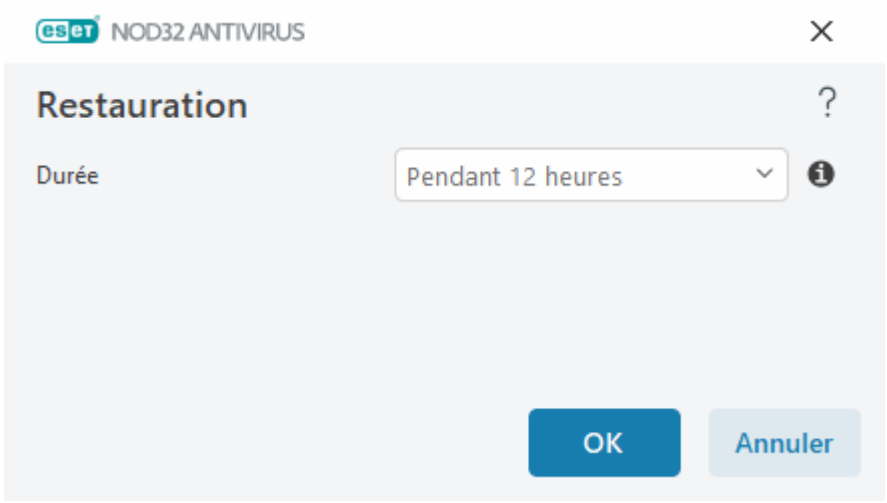
Paramètres avancés de mises à jour

Si vous pensez qu'une mise à jour du moteur de détection ou que des modules du programme sont instables ou corrompus, vous pouvez restaurer la version précédente et désactiver temporairement les mises à jour. D'un autre côté, il est aussi possible d'activer les mises à jour précédemment désactivées si vous les avez reportées pour une durée indéterminée.

ESET NOD32 Antivirus enregistre des instantanés du moteur de détection et de modules du programme à utiliser avec la fonctionnalité de restauration. Pour créer des instantanés de la base de virus, conservez l'option **Créer des instantanés des modules** activée. Lorsque cette option est activée, le premier instantané est créé pendant la première mise à jour. Le deuxième est créé après 48 heures. Le champ **Nombre d'instantanés stockés localement** définit le nombre d'instantanés du moteur de détection stockés.

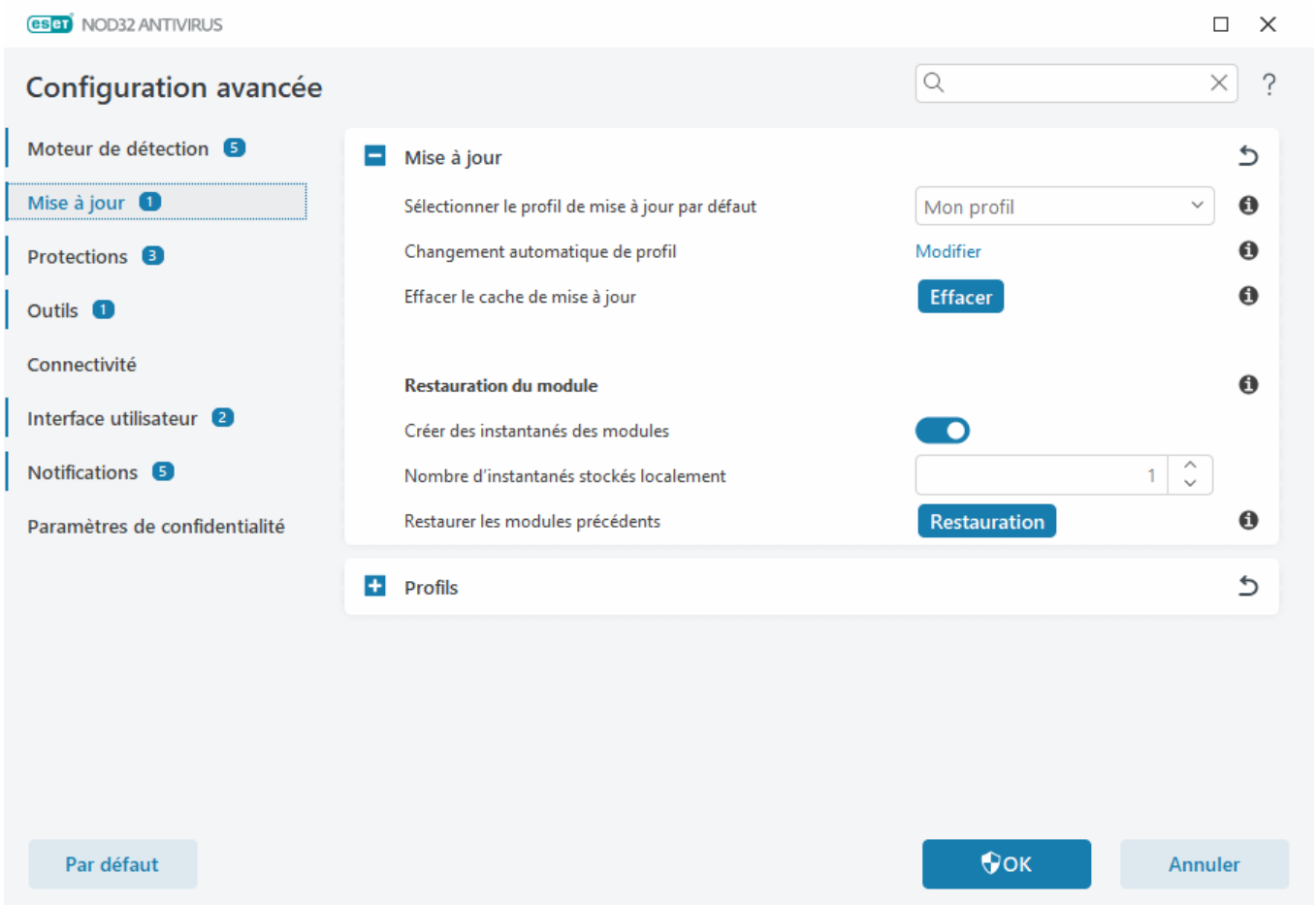
> Lorsque le nombre maximal d'instantanés est atteint (3, par exemple), l'instantané le plus ancien est remplacé par un nouveau toutes les 48 heures. ESET NOD32 Antivirus restaure les versions des mises à jour du moteur de détection et des modules du programme en fonction de l'instantané le plus ancien.

Si vous cliquez sur **Restaurer** dans Configurations avancées > **Mise à jour** > **Mise à jour**, vous devez sélectionner une **durée** dans le menu déroulant qui représente la période durant laquelle les mises à jour du moteur de détection et celles des modules de programme sont suspendues.



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

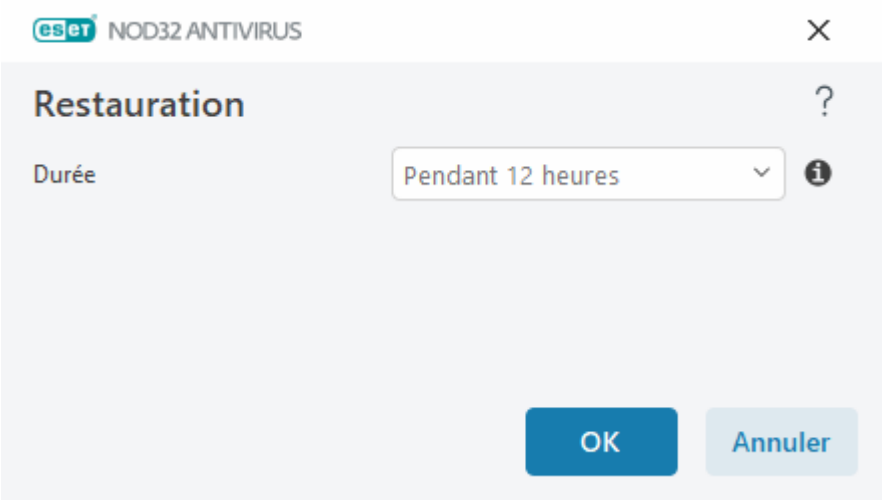
Si une restauration est exécutée, le bouton **Restaurer** devient **Autoriser les mises à jour**. Aucune mise à jour n'est autorisée pendant la durée sélectionnée dans le menu déroulant **Suspendre les mises à jour**. La version du moteur de détection revient à la version la plus ancienne disponible, stockée sous forme d'instantané dans le système de fichiers de l'ordinateur local.



Supposons que le numéro 22700 correspond au numéro de version le plus récent du moteur de détection. Les moteurs de détection 22698 et 22696 sont stockés sous forme d'instantanés. Notez que le numéro 22697 n'est pas disponible. Dans cet exemple, l'ordinateur était éteint pendant la mise à jour 22697 et une mise à jour plus récente a été mise à disposition avant que la version 22697 n'ait été téléchargée. Si le champ **Nombre d'instantanés stockés localement** est défini sur 2 et que vous cliquez sur **Restaurer**, le moteur de détection (y compris les modules du programme) sera restauré à la version numéro 22696. Ce processus peut prendre un certain temps. Vérifiez si le moteur de détection est bien retourné à une version antérieure dans l'écran Mise à jour.

Intervalle de la restauration

Si vous cliquez sur **Restaurer** dans Configurations avancées > **Mise à jour** > **Mise à jour**, vous devez sélectionner une **durée** dans le menu déroulant qui représente la période durant laquelle les mises à jour du moteur de détection et celles des modules de programme sont suspendues.



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

Mises à jour du produit

La section **Mises à jour du produit** permet d'installer automatiquement les nouvelles mises à jour des fonctionnalités lorsqu'elles sont disponibles.

Les mises à jour des fonctionnalités de l'application offrent de nouvelles fonctionnalités ou modifient celles qui existent déjà depuis les versions précédentes. Cette mise à jour peut s'effectuer sans intervention de l'utilisateur ou après sa notification. Le redémarrage de l'ordinateur peut être nécessaire après la mise à jour des fonctionnalités de l'application.

Mises à jour des fonctionnalités de l'application : lorsque cette option est activée, les mises à jour des fonctionnalités de l'application sont effectuées automatiquement.

Options de connexion

Pour accéder aux options de configuration du serveur proxy pour un profil de mise à jour spécifique, ouvrez Configurations avancées > **Mise à jour** > **Profils** > **Mises à jour** > **Options de connexion**. Cliquez sur le menu déroulant **Mode proxy** et sélectionnez l'une des trois options suivantes :

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

Sélectionnez l'option **Utiliser les paramètres globaux de serveur proxy** pour utiliser la configuration de serveur proxy déjà spécifiée dans Configurations avancées > **Connectivité** > **Serveur proxy**.

Sélectionnez **Ne pas utiliser de serveur proxy** pour indiquer qu'aucun serveur proxy ne sera utilisé pour la mise à jour d'ESET NOD32 Antivirus.

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

- Un autre serveur proxy que celui défini dans Configurations avancées > **Connectivité** est utilisé pour mettre à jour ESET NOD32 Antivirus. Dans cette configuration, les informations du nouveau proxy doivent être spécifiées adresse du **serveur proxy**, **port** de communication (3128 par défaut) et **nom d'utilisateur** et **mot de passe** du serveur proxy, si nécessaire).
- Les paramètres de serveur proxy ne sont pas définis globalement, mais ESET NOD32 Antivirus se connecte à un serveur proxy pour les mises à jour.
- Votre ordinateur est connecté à Internet par l'intermédiaire d'un serveur proxy. Les paramètres sont pris dans Internet Explorer pendant l'installation du programme, mais s'ils sont modifiés (par exemple en cas de changement de fournisseur de services Internet), vérifiez que les paramètres du proxy sont corrects dans la fenêtre. Dans le cas contraire, le programme ne pourra pas se connecter aux serveurs de mise à jour.

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

Utiliser une connexion directe si le proxy HTTP n'est pas disponible – Le proxy est ignoré pendant la mise à jour s'il n'est pas joignable.

> Les champs **Nom d'utilisateur** et **Mot de passe** de cette section sont propres au serveur proxy. Ne renseignez ces champs que si un nom d'utilisateur et un mot de passe sont nécessaires pour accéder au serveur proxy. Ces champs ne doivent être renseignés que si vous savez que vous avez besoin d'un mot de passe pour accéder à Internet via un serveur proxy.

Protections

Les protections vous prémunissent des attaques contre le système en contrôlant les échanges de fichiers et d'e-mails, ainsi que les communications internet. Par exemple, si un objet classé comme logiciel malveillant est détecté, la correction commence. Les protections peuvent l'éliminer en le bloquant, puis en le nettoyant, en le supprimant ou en le mettant en quarantaine.

Pour configurer en détail les protections, ouvrez Configurations avancées > **Protections**.

> Les modifications apportées aux protections ne doivent être effectuées que par un utilisateur expérimenté. Une configuration incorrecte des paramètres peut entraîner une diminution du niveau de protection.

Dans cette section :

Réponses des détections

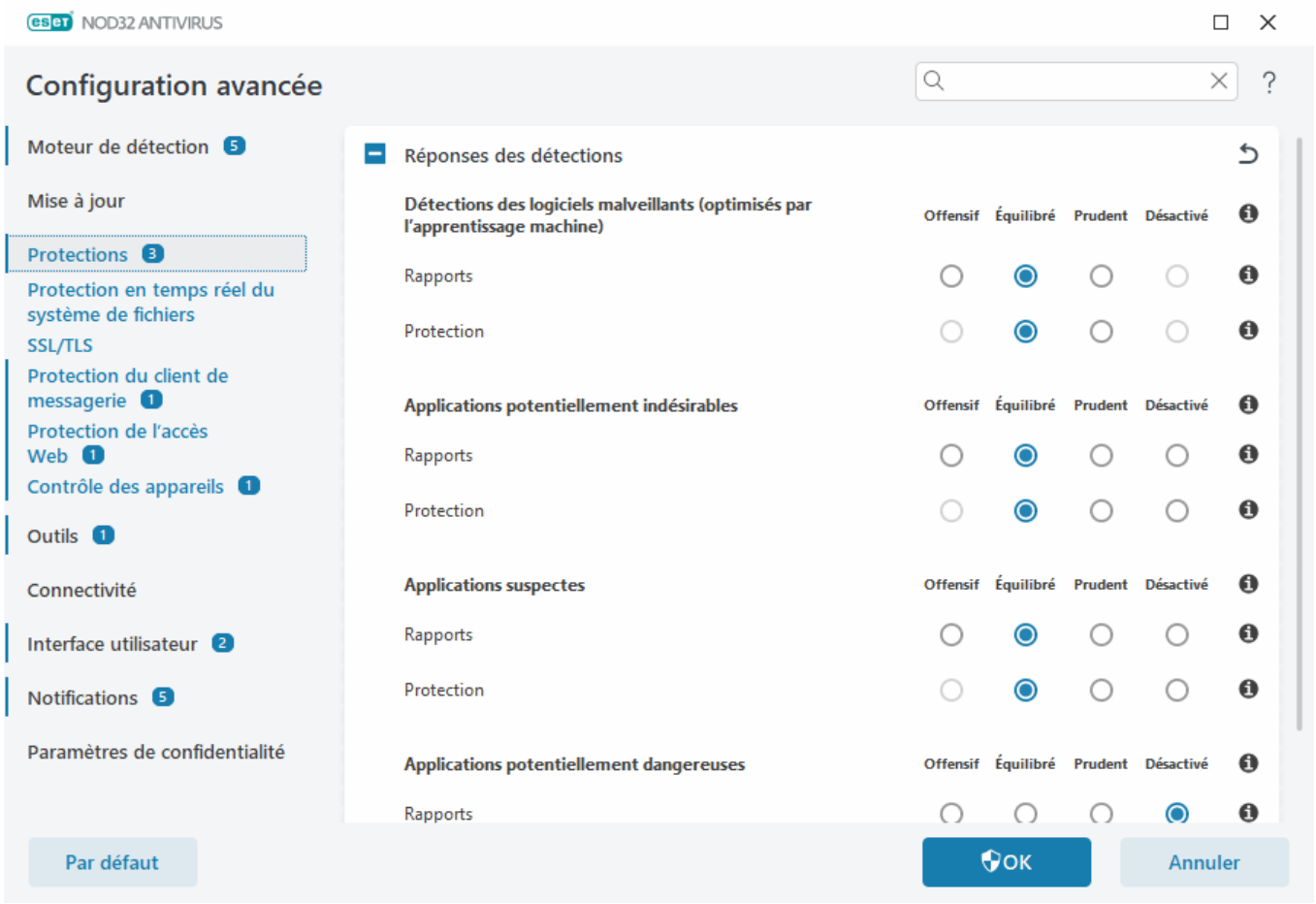
Les réponses des détections vous permettent de configurer les niveaux de rapport et de protection pour les catégories suivantes :

- **Détections des logiciels malveillants (optimisés par l'apprentissage machine)** – Un virus d'ordinateur est un fragment de code malveillant ajouté à des fichiers qui sont sur votre ordinateur. Le terme « virus » est souvent utilisé de manière incorrecte. Le terme « logiciel malveillant »(malware, en anglais) est plus précis. La détection des logiciels malveillants est effectuée par le module du moteur de détection associé au composant d'apprentissage machine. Pour plus d'informations sur ce type de protection, reportez-vous au glossaire.

- **Applications potentiellement indésirables** : un grayware (ou application potentiellement indésirable) est un type de logiciel dont l'objectif n'est pas nécessairement malveillant, contrairement à d'autres types de logiciels malveillants comme les virus et les chevaux de Troie. Il peut toutefois installer d'autres logiciels non souhaités, modifier le comportement de l'appareil numérique, ou effectuer des activités non approuvées ou non attendues par l'utilisateur. Pour plus d'informations sur ce type de protection, reportez-vous au glossaire.

- **Les applications suspectes** comprennent des programmes compressés par des compresseurs ou des programmes de protection. Ces types de protections sont souvent exploités par des créateurs de logiciels malveillants pour contourner les détections.

- **Applications potentiellement dangereuses** : il s'agit de logiciels commerciaux légitimes susceptibles d'être utilisés à des fins malveillantes. Cette catégorie comprend les programmes d'accès à distance, les applications de décodage des mots de passe ou les keyloggers (programmes qui enregistrent chaque frappe au clavier de l'utilisateur). Pour plus d'informations sur ce type de protection, reportez-vous au glossaire.



Amélioration de la protection

L'apprentissage machine avancé fait maintenant partie des protections en tant que couche de protection avancée qui améliore la détection reposant sur l'apprentissage machine. Pour plus d'informations sur ce type de protection, reportez-vous au glossaire.

Configuration du signalement

Lorsqu'une détection est effectuée (une menace est détectée et classée comme étant un logiciel malveillant, par exemple), les informations sont consignées dans le journal Détections. Des notifications de bureau s'affichent aussi si elles sont configurées dans ESET NOD32 Antivirus.

Le seuil de signalement est configuré pour chaque catégorie (appelée « CATÉGORIE ») :

1. Détections de logiciels malveillants
2. Applications potentiellement indésirables
3. Applications potentiellement dangereuses
4. Applications suspectes

Signalement effectué avec le moteur de détection, y compris le composant d'apprentissage machine. Vous pouvez définir un seuil de signalement supérieur à celui de la protection. Ces paramètres de signalement n'ont aucun impact sur le blocage, le nettoyage et la suppression des objets.

Lisez ce qui suit avant de modifier un seuil (ou un niveau) pour les signalements de CATÉGORIE :

Seuil	Explication
Offensif	Rapports sur CATÉGORIE configurés sur une sensibilité maximale. D'autres détections sont signalées. Le paramètre **Offensif** peut identifier à tort des objets comme étant CATÉGORIE.
Équilibré	Rapports sur CATÉGORIE configurés comme étant équilibrés. Cette configuration est optimisée pour équilibrer les performances et la précision des taux de détection et le nombre d'objets signalés à tort.
Prudent	Rapports sur CATÉGORIE configurés pour réduire le nombre d'objets identifiés à tort tout en maintenant un niveau de protection suffisant. Les objets ne sont signalés que lorsque la probabilité est évidente et correspond au comportement CATÉGORIE.
Désactivé	Les rapports sur CATÉGORIE ne sont pas actifs. Les détections de ce type ne sont pas recherchées, signalées ni nettoyées. Par conséquent, cette configuration désactive la protection de ce type de détection. Le paramètre Désactivé n'est pas disponible pour les rapports sur les logiciels malveillants. La valeur par défaut est celle des applications potentiellement dangereuses.

Disponibilité des modules de protection ESET NOD32 Antivirus

La disponibilité (activé ou désactivé) d'un module de protection pour un seuil de CATÉGORIE sélectionné est la suivante :

	Offensif	Équilibré	Prudent	Désactivé*
Module d'apprentissage machine avancé	✔ (mode offensif)	✔ (mode conservateur)	X	X
Module du moteur de détection	✔	✔	✔	X
Autres modules de protection	✔	✔	✔	X

* Non recommandé.

Détermination de la version du produit, des versions des modules du programme et des dates de version

1. Cliquez sur **Aide et assistance** > **À propos d'ESET NOD32 Antivirus**.
2. Dans l'écran **À propos de**, la première ligne de texte contient le numéro de version de votre produit ESET.
3. Cliquez sur **Composants installés** pour accéder à des informations sur des modules spécifiques.

Remarques

Plusieurs remarques à prendre en compte lors de la configuration d'un seuil pour votre environnement :

- Le seuil **Équilibré** est recommandé pour la plupart des configurations.
- Seuil de signalement le plus élevé, taux de détection le plus élevé, mais probabilité plus grande d'objets identifiés à tort.
- Du point de vue du monde réel, rien ne garantit un taux de détection de 100 %, ni une chance de 0% d'éviter une catégorisation incorrecte des objets non infectés en tant que logiciels malveillants.
- Gardez ESET NOD32 Antivirus et ses modules à jour pour optimiser l'équilibre entre performances, précision des taux de détection et nombre d'objets signalés à tort.

Configuration de la protection

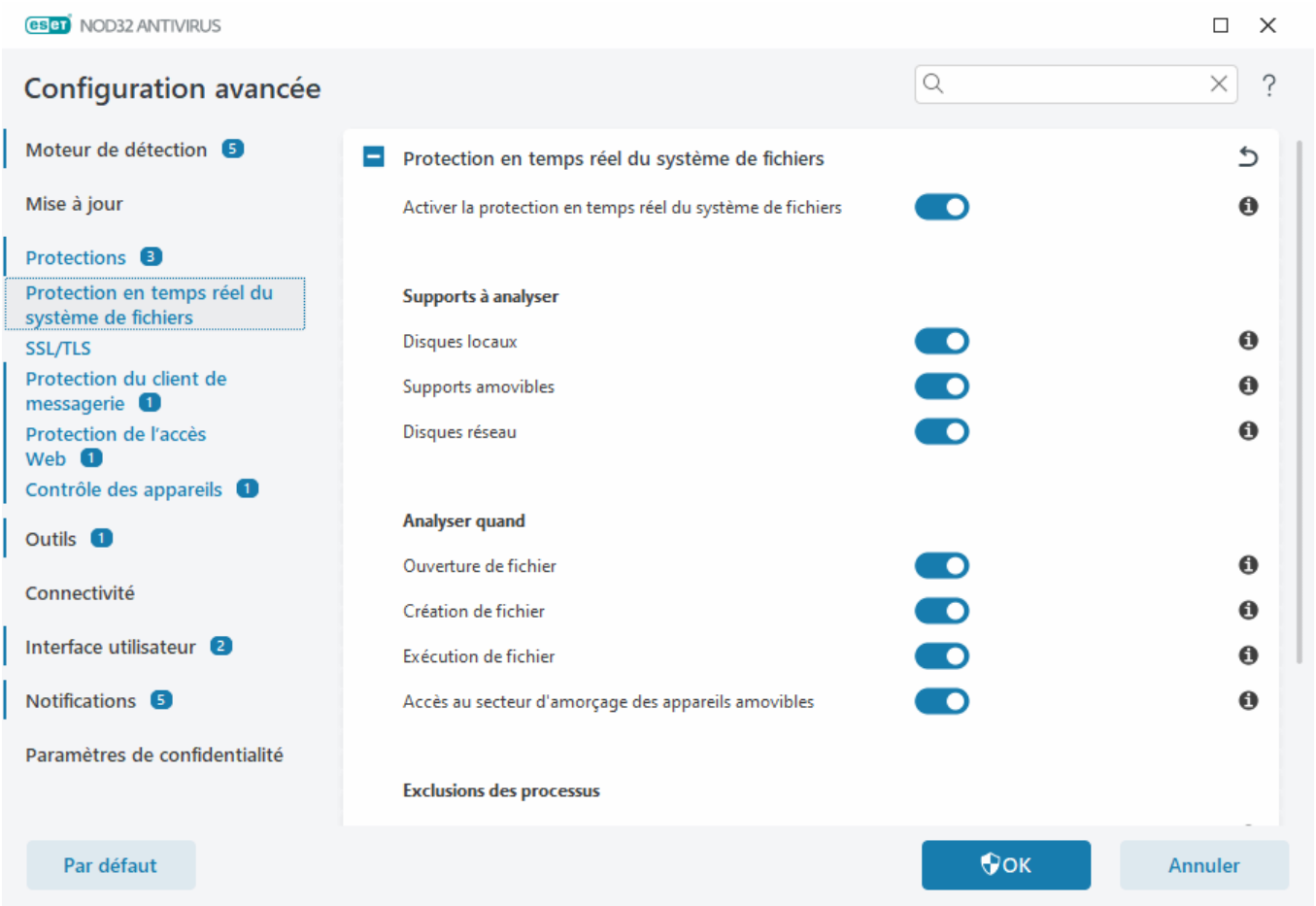
Si un objet classé en tant que CATÉGORIE est signalé, le programme le bloque, puis le nettoie, le supprime ou le met en quarantaine.

Lisez ce qui suit avant de modifier un seuil (ou un niveau) pour une protection de CATÉGORIE :

Seuil	Explication
Offensif	Les détections du niveau Offensif (ou d'un niveau inférieur) signalées sont bloquées et la correction automatique (le nettoyage) est commencée. Cette configuration est recommandée lorsque tous les endpoints ont été analysés avec des paramètres offensifs et que des objets signalés à tort ont été ajoutés aux exclusions de détection.
Équilibré	Les détections du niveau Équilibré (ou d'un niveau inférieur) signalées sont bloquées et la correction automatique (le nettoyage) est commencée.
Prudent	Les détections du niveau Prudent signalées sont bloquées et la correction automatique (le nettoyage) est commencée.
Désactivé	Cette option s'avère utile pour identifier et exclure les objets signalés à tort. Le paramètre Désactivé n'est pas disponible pour la protection contre les logiciels malveillants. La valeur par défaut est celle des 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 rechercher du code malveillant lors de leur ouverture, création ou exécution.



Par défaut, la protection en temps réel du système de fichiers est lancée au démarrage du système et assure une analyse ininterrompue. Il n'est pas recommandé de désactiver l'option **Activer la protection en temps réel du système de fichiers** dans Configurations avancées > **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 font l'objet de recherches de menaces potentielles :

- **Disques locaux** – Analyse tous les disques durs système et fixes (par exemple : *C:*\, *D:*\).
- **Supports amovibles** – Analyse les CD/DVD, clés USB, cartes mémoire, etc.
- **Lecteurs réseau** – Analyse tous les lecteurs réseau mappés (par exemple : *H:*\ comme *store04*) ou les lecteurs réseau à accès direct (par exemple : *store08*).

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

Analyser quand

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

- **Ouverture de fichier** – Lance l'analyse lorsqu'un fichier est ouvert.
- **Création de fichier** – Analyse un fichier créé ou modifié.
- **Exécution de fichier** – Lance l'analyse lorsqu'un fichier est exécuté.
- **Accès au secteur d'amorçage des appareils amovibles** – Lorsqu'un appareil amovible contenant un secteur d'amorçage est inséré dans l'appareil, celui-ci est immédiatement analysé. Cette option n'active pas l'analyse des fichiers d'appareil amovible. Cette analyse se trouve dans **Supports à analyser** > **Appareils amovibles**. Pour que l'**accès au secteur d'amorçage des supports amovibles** fonctionne correctement, gardez l'option **Secteurs d'amorçage/UEFI** activée dans ThreatSense.

Exclusions des processus

Consultez Exclusions des processus.

ThreatSense

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

Pour garantir un impact minimal de la protection en temps réel sur le système, les fichiers déjà analysés ne sont pas analysés plusieurs fois (sauf s'ils ont été modifiés). Les fichiers sont immédiatement réanalysés après chaque

mise à jour du moteur de détection. Ce comportement est contrôlé à l'aide de l'**optimisation intelligente**. Si l'**optimisation intelligente** est désactivée, tous les fichiers sont analysés à chaque accès. Pour modifier ce paramètre, ouvrez Configurations avancées > **Protections** > **Protection en temps réel du système de fichiers**. Cliquez ensuite sur **ThreatSense** > **Autre**, puis sélectionnez ou désélectionnez **Activer l'optimisation intelligente**.

La protection en temps réel du système de fichiers vous permet également de configurer des paramètres ThreatSense supplémentaires.

Exclusions des processus

La fonctionnalité Exclusions des processus 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 des fichiers) sont utilisées pendant la sauvegarde. Le seul moyen efficace d'éviter les deux situations est de désactiver le programme contre les logiciels malveillants. 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. Un outil de sauvegarde exclu peut accéder aux fichiers infectés sans déclencher d'alerte. C'est pourquoi les autorisations étendues ne sont autorisées que dans le module de protection en temps réel.

Ne confondez pas cette option avec Extensions de fichiers exclues, Exclusions HIPS, Exclusions de détection ou Exclusions des performances.

Les exclusions de processus permettent de réduire le risque de conflits potentiels et d'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/d'une application est une exclusion de son fichier exécutable (*.exe*).

Vous pouvez ajouter des fichiers exécutables à la liste des processus exclus dans Configurations avancées > **Protections** > **Protection en temps réel du système de fichiers** > **Protection en temps réel du système de fichiers** > **Exclusions des 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 aussi celles des performances de la sauvegarde, car celle-ci n'est pas ralentie pendant son exécution.

Cliquez sur **Modifier** pour ouvrir la fenêtre de gestion **Exclusions des processus**, dans laquelle vous pouvez ajouter des exclusions et accéder au fichier exécutable (*Backup-tool.exe*, par exemple) qui sera exclu de l'analyse.
Dès que le fichier *.exe* est ajouté aux exclusions, l'activité de ce processus n'est pas surveillée par ESET NOD32 Antivirus et aucune analyse n'est effectuée sur les opérations de fichier effectuées par celui-ci.

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.

Vous pouvez aussi **modifier** des processus existants ou les **supprimer** des exclusions.

La protection de l'accès web ne tient pas compte de cette exclusion. Par conséquent, si vous excluez le fichier exécutable de votre navigateur web, les fichiers téléchargés sont toujours analysés. Ainsi, 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 permet d'**ajouter** des processus exclus du moteur de détection. Les exclusions de processus permettent de réduire le risque de conflits potentiels et d'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/d'une application est une exclusion de son fichier exécutable (*.exe*).

Sélectionnez le chemin d'accès au fichier d'une application visée par l'exception en cliquant sur ... (*C:\Program Files\Firefox\Firefox.exe*, par exemple). 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 surveillée par ESET NOD32 Antivirus et aucune analyse n'est effectuée sur les opérations de fichier effectuées par celui-ci.

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.

Vous pouvez aussi **modifier** des processus existants ou les **supprimer** des exclusions.

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

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

Après l'installation de ESET NOD32 Antivirus, tous les paramètres sont optimisés pour garantir le niveau maximum de système de sécurité aux utilisateurs. Pour restaurer les paramètres par défaut, cliquez sur en regard de Configurations avancées > **Protections** > **Réponses des détections**.

Vérification de la protection en temps réel

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

Le fichier peut être téléchargé à l'adresse suivante : http://www.eicar.org/download/eicar.com
Une fois que vous avez saisi cette URL dans votre navigateur, un message doit s'afficher pour vous indiquer que la menace a été supprimée.

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

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

La protection en temps réel est désactivée

Si un utilisateur désactive par mégarde la protection en temps réel, vous devez réactiver la fonctionnalité. Pour réactiver la protection en temps réel, sélectionnez **Configuration** 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 ne se lance pas au démarrage du système, c'est probablement parce que l'option **Activer la protection en temps réel du système de fichiers** est désactivée. Pour vous assurer que cette option est activée, ouvrez Configurations avancées > **Protections** > **Protection en temps réel du système de fichiers**.

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

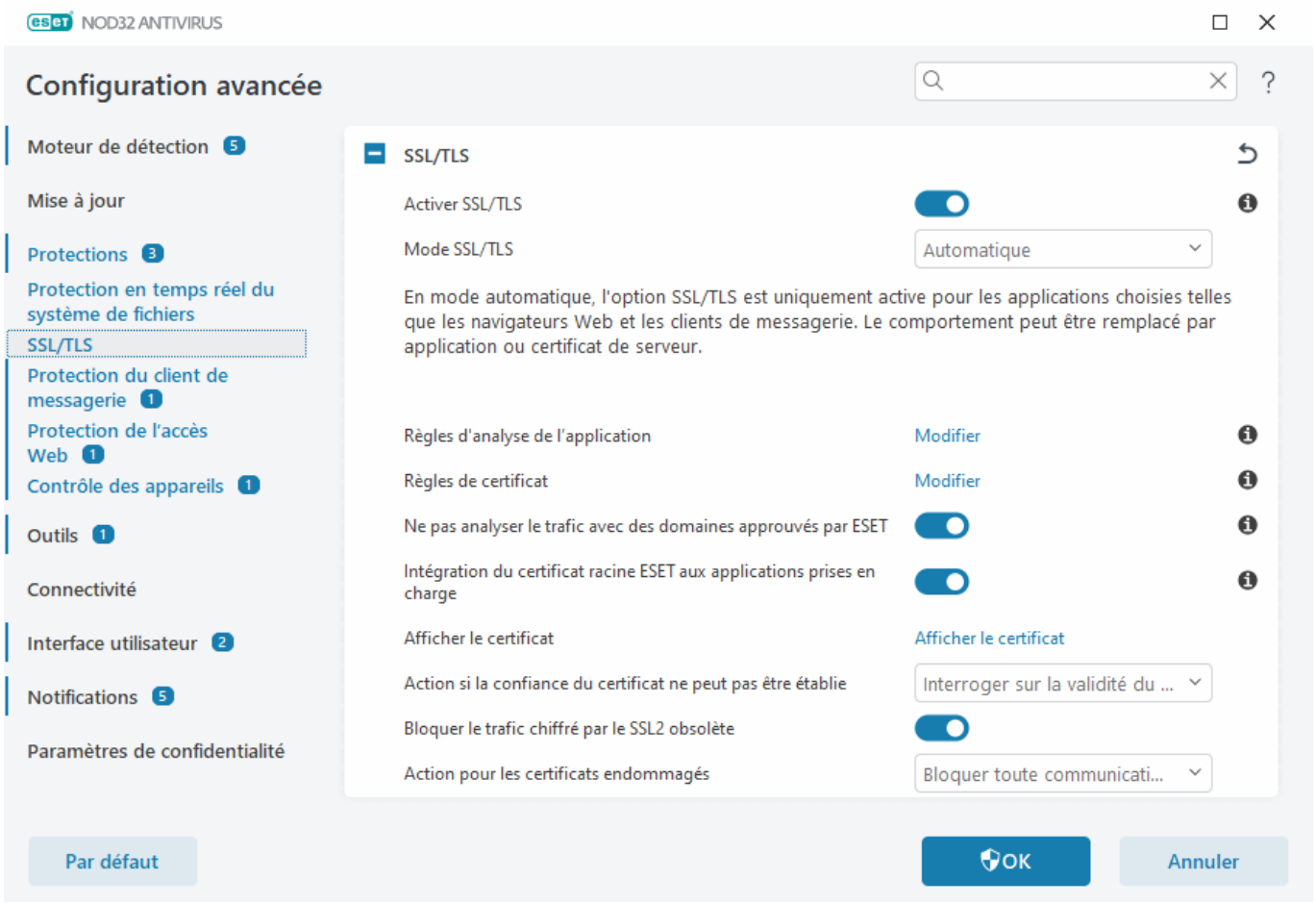
Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si deux programmes antivirus sont installés, ils risquent de provoquer des conflits. Nous recommandons de désinstaller tout autre antivirus de votre système avant d'installer ESET.

La protection en temps réel ne démarre pas

Si la protection en temps réel n'est pas lancée au démarrage du système (et si **Activer la protection en temps réel du système de fichiers** est activé), le problème peut provenir de conflits avec d'autres programmes. Pour résoudre ce problème, créez un journal ESET SysInspector et envoyez-le à l'assistance technique ESET pour analyse.

SSL/TLS

ESET NOD32 Antivirus peut rechercher les menaces de communication qui utilisent le protocole SSL. Vous pouvez utiliser plusieurs modes de filtrage pour examiner les communications SSL protégées à l'aide de certificats approuvés, de certificats inconnus ou de certificats exclus de la vérification des communications SSL protégées. Pour modifier les paramètres SSL/TLS, ouvrez Configurations avancées > **Protections** > **SSL/TLS**.



Activer SSL/TLS : si cette option est désactivée, ESET NOD32 Antivirus n'analyse pas les communications sur SSL/TLS.

Le mode SSL/TLS est disponible dans les options suivantes :

Mode de filtrage	Description
Automatique	Ce mode par défaut n'analyse que les applications appropriées telles que les navigateurs Web et les clients de messagerie. Vous pouvez le remplacer en sélectionnant les applications dans lesquelles les communications sont analysées.
Interactif	Si vous entrez un nouveau site protégé par SSL (avec un certificat inconnu), une boîte de dialogue de sélection d'action s'affiche. Ce mode vous permet de créer la liste des certificats SSL/applications qui seront exclus de l'analyse.
Basé sur des politiques	Sélectionnez cette option pour analyser toutes les communications SSL protégées, à l'exception des communications protégées par des certificats exclus de la vérification. Si une nouvelle communication utilisant un certificat signé inconnu est établie, vous n'êtes pas informé et la communication est automatiquement filtrée. Lorsque vous accédez à un serveur disposant d'un certificat non approuvé indiqué comme approuvé (il figure dans la liste des certificats approuvés), la communication vers le serveur est autorisée et le contenu du canal de communication est filtré.

Règles d'analyse de l'application : permet de personnaliser le comportement d'ESET NOD32 Antivirus pour des applications spécifiques.

Règles de certificat : permet de personnaliser le comportement d'ESET NOD32 Antivirus pour des certificats SSL spécifiques.

Ne pas analyser le trafic avec des domaines approuvés par ESET : lorsque cette option est activée, les communications avec les domaines approuvés sont exclues de l'analyse. Une liste blanche intégrée gérée par ESET détermine la fiabilité d'un domaine.

Intégration du certificat racine ESET aux 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 NOD32 Antivirus ajoute automatiquement le certificat ESET SSL Filter CA aux navigateurs connus (Opera par exemple). Pour les navigateurs utilisant le magasin de certification système, le certificat est ajouté automatiquement. Par exemple, Firefox est automatiquement configuré pour approuver les autorités racines dans le magasin de certification 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 confiance 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 (par exemple, un certificat arrivé à expiration, un certificat non approuvé, un certificat non valide pour le domaine spécifique ou une signature qui peut être analysée mais qui ne signe pas correctement le certificat). Les sites web légitimes utilisent toujours des certificats approuvés. S'ils n'en fournissent pas, cela peut signifier qu'un pirate déchiffre vos communications ou que le site web connaît des difficultés techniques.

Si **Interroger sur la validité du certificat** est activé (sélectionné par défaut), vous êtes invité à sélectionner une action lorsque la communication chiffrée est établie. Une boîte de dialogue de sélection d'action apparaît ; vous pouvez marquer le certificat comme étant fiable ou exclu. Si le certificat ne figure pas dans la liste TRCA, la fenêtre est rouge. S'il y figure, la fenêtre est verte.

Vous pouvez sélectionner **Bloquer toute communication utilisant le certificat** pour toujours mettre fin à la connexion chiffrée au site utilisant le certificat non approuvé.

Bloquer le trafic chiffré par le SSL2 obsolète : les communications utilisant la version antérieure du protocole SSL seront automatiquement bloquées.

Action pour les certificats endommagés : un certificat endommagé est un certificat qui utilise un format non reconnu par ESET NOD32 Antivirus ou qui a été reçu endommagé (par exemple, écrasé par des données aléatoires). Dans ce cas, nous recommandons de conserver l'option **Bloquer toute communication utilisant le certificat** activée. Si l'option **Interroger sur la validité du certificat** est sélectionnée, l'utilisateur est invité à sélectionner une action à exécuter lorsque la communication chiffrée est établie.

> **Exemples illustrés**
>
> Les articles suivants de la base de connaissances ESET peuvent être disponibles uniquement en anglais :
> - Notifications de certificat dans les produits pour les particuliers ESET Windows
> - « Trafic réseau chiffré : certificat non approuvé » s'affiche lors de la consultation de pages web

Règles d'analyse de l'application

Les **Règles d'analyse de l'application** peuvent être utilisées pour personnaliser le comportement d'ESET NOD32 Antivirus pour des applications spécifiques et mémoriser les actions choisies lorsque le **Mode SSL/TLS** est en **Mode interactif**. La liste peut être consultée et modifiée dans Configurations avancées > **Protections** > **SSL/TLS** > **Règles d'analyse de l'application** > **Modifier**.

La fenêtre **Règles d'analyse de l'application** comprend les éléments suivants :

Colonnes

Application – Choisissez un fichier exécutable dans l'arborescence, cliquez sur l'option **...** ou saisissez le chemin manuellement.

Action d'analyse – Sélectionnez **Analyser** ou **Ignorer** pour analyser ou ignorer la communication. Sélectionnez **Automatique** pour effectuer une analyse en mode automatique et demander quelle action entreprendre en mode interactif. Sélectionnez **Demander** pour demander toujours à l'utilisateur quelle action effectuer.

Éléments de commande

Ajouter – Ajoute une application filtrée.

Modifier – Sélectionnez l'application à configurer, puis cliquez sur **Modifier**.

Supprimer – Sélectionnez l'application à supprimer, puis cliquez sur **Supprimer**.

Importer/Exporter – Importez des applications depuis un fichier ou enregistrez votre liste actuelle d'applications dans un fichier.

OK/Annuler – Cliquez sur **OK** si vous souhaitez enregistrer les modifications. Sinon, cliquez sur **Annuler** pour quitter sans enregistrer.

Règles de certificat

Les **Règles de certificat** peuvent être utilisées pour personnaliser le comportement d'ESET NOD32 Antivirus pour des certificats SSL spécifiques et mémoriser les actions choisies lorsque le **Mode SSL/TLS** est en **Mode interactif**. La liste peut être consultée et modifiée dans Configurations avancées > **Protections** > **SSL/TLS** > **Règles de certificat** > **Modifier**.

La fenêtre **Règles de certificat** est composée des éléments suivants :

Colonnes

Nom : nom du certificat.

Émetteur du certificat : nom du créateur du certificat.

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

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

Analyser : sélectionnez **Analyser** ou **Ignorer** comme **Action d'analyse** pour analyser ou ignorer les communications sécurisées par ce certificat. Sélectionnez **Automatique** pour effectuer une analyse en mode

automatique et demander quelle action entreprendre en mode interactif. Sélectionnez **Demander** pour demander toujours à l'utilisateur quelle action effectuer.

Éléments de commande

Ajouter : Ajoutez un nouveau certificat et définissez ses paramètres en ce qui concerne l'accès et les options d'analyse.

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

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

OK/Annuler – Cliquez sur **OK** si vous souhaitez enregistrer les modifications. Sinon, cliquez sur **Annuler** pour quitter sans enregistrer.

Trafic réseau chiffré

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

Lorsqu'un site Web utilise un certificat non valide ou ne pouvant pas être vérifié et qu'ESET NOD32 Antivirus est configuré pour demander à l'utilisateur l'action à effectuer dans ce cas (par défaut, oui pour les certificats ne pouvant pas être vérifiés, non pour les certificats non valides), une boîte de dialogue s'affiche pour **autoriser** ou **bloquer** la connexion. Si le certificat ne se trouve pas dans Trusted Root Certification Authorities store (TRCA), il n'est pas considéré comme étant approuvé.

Lorsque l'option **Mode SSL/TLS** est définie sur **Mode interactif**, une boîte de dialogue demande pour chaque site web d'**analyser** ou d'**ignorer** le trafic. Certaines applications vérifient que le trafic SSL n'est ni modifié ni inspecté par quelqu'un. Dans ce cas, ESET NOD32 Antivirus doit **ignorer** ce trafic pour que les applications continuent de fonctionner.

> **Exemples illustrés**
> Les articles suivants de la base de connaissances ESET peuvent être disponibles uniquement en anglais :
> - Notifications de certificat dans les produits pour les particuliers ESET Windows
> - « Trafic réseau chiffré : certificat non approuvé » s'affiche lors de la consultation 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 Configurations avancées > **Protections** > **Protection du client de messagerie** et choisissez une option de configuration parmi les suivantes :

- Protection du transport des messages
- Protection des boîtes aux lettres
- ThreatSense

Protection du transport des messages

Les protocoles IMAP(S) et POP3(S) sont les protocoles les plus répandus qui permettent de recevoir des e-mails dans une application cliente de messagerie. Le protocole IMAP (Internet Message Access Protocol) est un autre protocole Internet pour la récupération des e-mails. IMAP présente certains avantages par rapport à POP3, par exemple, plusieurs clients peuvent se connecter simultanément à la même boîte aux lettres et conserver des informations sur l'état des messages, telles que le type de lecture, de réponse ou de suppression des messages. Le module de protection qui fournit ce contrôle est automatiquement initié au démarrage du système et est alors actif dans la mémoire.

ESET NOD32 Antivirus protège ces protocoles, quel que soit le client de messagerie utilisé, sans avoir à reconfigurer le 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. Toutefois, les communications avec le serveur Microsoft Exchange peuvent être analysées par le module d'intégration dans les clients de messagerie tels que Microsoft Outlook.

ESET NOD32 Antivirus 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 NOD32 Antivirus 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 consulter la configuration de l'analyseur, ouvrez Configurations avancées > **Protections** > SSL/TLS.

Pour configurer la protection du transport des messages, ouvrez Configurations avancées > **Protections** > **Protection du client de messagerie** > **Protection du transport des messages**.

Activer la protection du transport des messages : lorsque cette option est activée, les communications du transport des messages sont analysées par ESET NOD32 Antivirus.

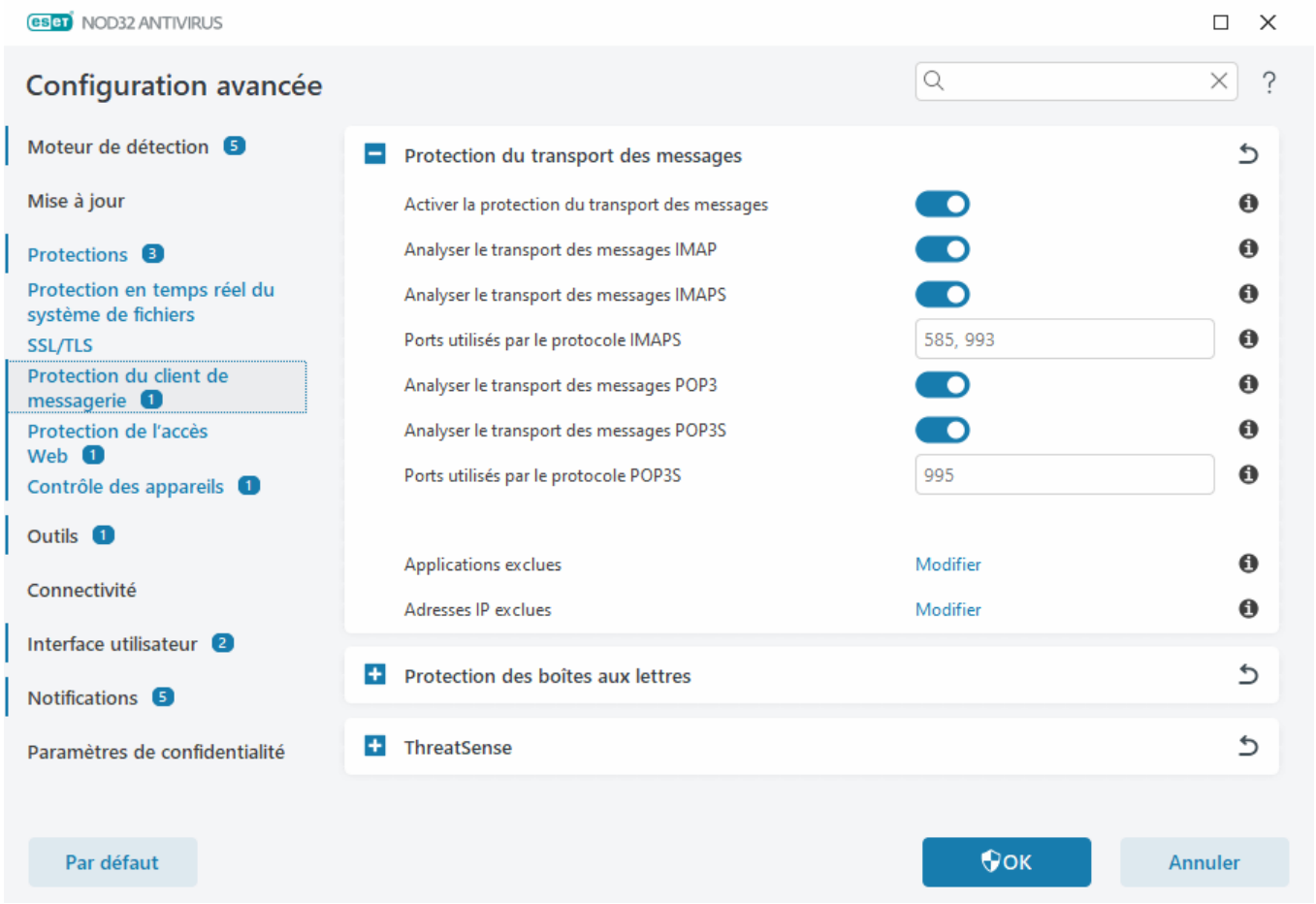
Vous pouvez choisir les protocoles de transport des messages qui seront analysés en cliquant sur le bouton bascule situé en regard des options suivantes (par défaut, l'analyse de tous les protocoles est activée) :

- **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 NOD32 Antivirus analyse 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**. Plusieurs numéros de ports doivent être séparés par une virgule.

Applications exclues : permet d'exclure des applications spécifiques de l'analyse par la protection du transport des messages. Cette option s'avère utile lorsque la protection de l'accès web entraîne des problèmes de compatibilité.

Adresses IP exclues : permet d'exclure des adresses distantes spécifiques de l'analyse par la protection du transport des messages. Cette option s'avère utile lorsque la protection de l'accès web entraîne des problèmes de compatibilité.



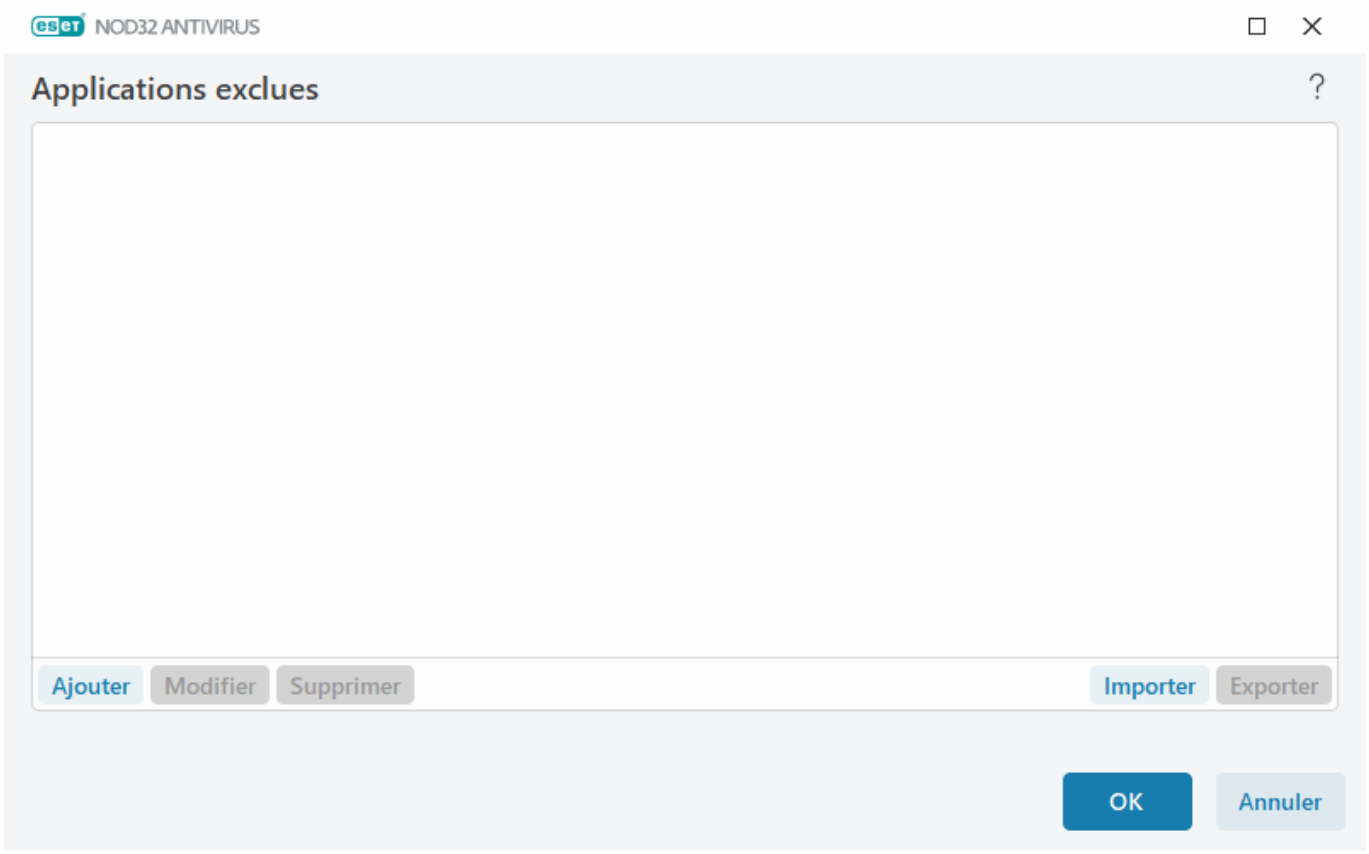
Applications exclues

Pour exclure l'analyse des communications pour des applications spécifiques, ajoutez-les à la liste. Les communications HTTP(S)/POP3(S)/IMAP(S) liées aux adresses sélectionnées ne font pas l'objet d'une détection des menaces. Il est recommandé d'utiliser cette option uniquement pour les applications qui ne fonctionnent pas correctement lorsque leur communication est vérifiée.

L'exécution des applications et des services est disponible automatiquement lorsque vous cliquez sur **Ajouter**. Cliquez sur **...** et accédez à une application pour ajouter manuellement l'exclusion.

Modifier – Modifie les entrées sélectionnées de la liste.

Supprimer – Supprime les entrées sélectionnées de la liste.



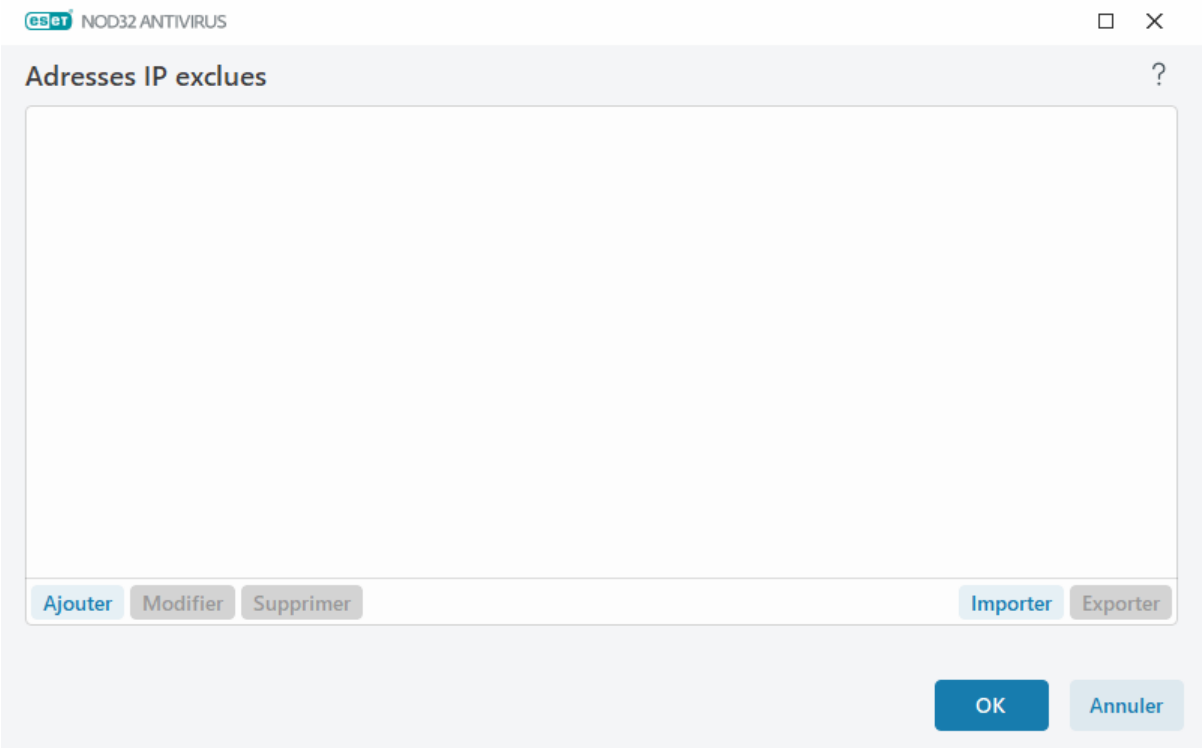
Adresses IP exclues

Les adresses figurant dans cette liste sont exclues de l'analyse. Les communications HTTP(S)/POP3(S)/IMAP(S) liées aux adresses sélectionnées ne font pas l'objet d'une détection des menaces. Il est recommandé d'utiliser cette option uniquement pour les adresses que vous savez être fiables.

Cliquez sur **Ajouter** pour exclure une adresse/une plage d'adresses/un sous-réseau IP d'un point distant.

Cliquez sur **Modifier** pour modifier l'adresse IP sélectionnée.

Cliquez sur **Supprimer** pour supprimer les entrées sélectionnées de la liste.



Exemples d'adresses IP

Ajouter une adresse IPv4:

Adresse unique – Ajoute l'adresse IP d'un ordinateur (par exemple, *192.168.0.10*).

Plage d'adresses – Saisissez l'adresse IP de début et de fin pour définir la plage IP de plusieurs ordinateurs (par exemple *192.168.0.1 à 192.168.0.99*).

Sous-réseau – Le sous-réseau (groupe d'ordinateurs) est 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 tout le type de sous-réseau dans *192.168.1.0/24*.

Ajouter une adresse IPv6:

Adresse unique – Ajoute l'adresse IP d'un ordinateur auquel la règle doit être appliquée, par exemple *2001:718:1c01:16:214:22ff:fec9:ca5*.

Sous-réseau – Le sous-réseau (groupe d'ordinateurs) est défini par une adresse IP et un masque (par exemple : *2002:c0a8:6301:1::1/64*).

Protection des boîtes aux lettres

L'intégration d'ESET NOD32 Antivirus à votre boîte aux lettres augmente le niveau de protection active contre le code malveillant dans les e-mails.

Pour configurer la protection des boîtes aux lettres, ouvrez Configurations avancées > **Protections** > **Protection du client de messagerie** > **Protection des boîtes aux lettres**.

Activer la protection de la messagerie par les modules d'extension clients – Lorsque cette option est désactivée, la protection par les modules d'extension des clients de messagerie est désactivée.

Sélectionnez les e-mails à analyser :

- **Courrier reçu**
- **Courrier envoyé**

- **Courrier lu**
- **E-mail modifié**

> Il est recommandé de conserver l'option **Activer la protection de la messagerie par les modules d'extension clients** activée. Même si l'intégration n'est pas activée ou fonctionnelle, les communications par messagerie demeurent protégées par la protection du transport des messages (IMAP/IMAPS et POP3/POP3S).

Optimisation de la gestion des pièces jointes : si l'optimisation est désactivée, toutes les pièces jointes sont analysées immédiatement. Les performances du client de messagerie peuvent être ralenties.

Intégrations : vous permet d'intégrer la protection des boîtes aux lettres à votre client de messagerie. Pour plus d'informations, consultez Intégrations.

Réponse : permet de personnaliser la gestion du courrier indésirable. Pour plus d'informations, consultez Réponse.

Intégrations

L'intégration d'ESET NOD32 Antivirus au client de messagerie augmente le niveau de protection active contre le code malveillant dans les e-mails. Si votre client de messagerie est pris en charge, vous pouvez activer l'intégration dans ESET NOD32 Antivirus. Une fois le produit intégré à votre client de messagerie, la barre d'outils d'ESET NOD32 Antivirus est insérée directement dans le client de messagerie, ce qui permet une protection plus efficace des messages. Pour modifier les paramètres d'intégration, ouvrez Configurations avancées > **Protections** > **Protection du client de messagerie Protection des boîtes 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 module d'extension. L'avantage principal du plugin réside dans le fait qu'il est indépendant du protocole utilisé. Lorsqu'un client de messagerie reçoit un message chiffré, il le déchiffre et l'envoie au scanner de virus. Pour obtenir la liste complète des versions de Microsoft Outlook prises en charge, consultez cet article de la base de connaissances ESET

Traitement avancé du client de messagerie : traite les événements Outlook Messaging API (MAPI) supplémentaires : Objet modifié (`fnevObjectModified`) and Objet créé (`fnevObjectCreated`). Si vous constatez un ralentissement du système lors de l'utilisation du client de messagerie, désactivez cette option.

Barre d'outils Microsoft Outlook

La protection Microsoft Outlook fonctionne comme un module d'extension. Une fois ESET NOD32 Antivirus installé, cette barre d'outils contenant la protection antivirus options est ajoutée à Microsoft Outlook :

ESET NOD32 Antivirus – Double-cliquez sur l'icône pour ouvrir la fenêtre principale d'ESET NOD32 Antivirus.

Analyser à nouveau les messages – Vous permet de lancer manuellement la vérification des messages. Vous pouvez indiquer les messages à vérifier et activer une nouvelle analyse du message reçu. Pour plus d'informations, consultez Protection des boîtes aux lettres.

Configuration de l'analyseur – Affiche les options de configuration de la protection des boîtes aux lettres.

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 d'ESET NOD32 Antivirus intégrée dans les clients de messagerie permet aux utilisateurs de spécifier plusieurs options pour la vérification du courrier électronique. L'option **Analyser à nouveau les messages** offre deux modes d'analyse :

Tous les messages du dossier en cours – Analyse les messages du dossier affiché.

Messages sélectionnés uniquement – Analyse uniquement les messages marqués par l'utilisateur.

La case à cocher **Réanalyser les messages déjà analysés** permet d'exécuter une autre analyse sur des messages déjà analysés.

Réponse

En fonction des résultats de l'analyse des messages, ESET NOD32 Antivirus peut déplacer les messages analysés ou ajouter du texte personnalisé à l'objet. Vous pouvez configurer ces paramètres dans Configurations avancées > **Protections** > **Protection du client de messagerie** > **Protection des boîtes aux lettres** > **Réponse**.

Si un message contient une détection, ESET NOD32 Antivirus tente de le nettoyer par défaut. Si le message ne peut pas être nettoyé, vous pouvez choisir une **Action à entreprendre si le nettoyage est impossible** :

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

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

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

sont les suivantes :

- **Jamais** – Aucune notification ne sera ajoutée.
- **Lorsqu'une détection se produit** – Seuls les messages contenant un code malveillant sont marqués comme contrôlés (valeur par défaut).
- **À tous les e-mails lors de l'analyse** – Le programme ajoute des messages à tous les e-mails analysés.

Mettre à jour l'objet d'un e-mail reçu et lu/Mettre à jour l'objet d'un e-mail envoyé – Activez cette option pour ajouter le texte personnalisé spécifié ci-dessous au message.

Texte ajouté à l'objet des messages détectés – Modifiez ce texte si vous souhaitez modifier le format du préfixe de l'objet d'un e-mail infecté. Cette fonction remplace l'objet du message "Bonjour" au format suivant : « [détection %DETECTIONNAME%] ». La variable %DETECTIONNAME% représente la détection.

ThreatSense

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

les options de configuration de la technologie ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

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

Pour ouvrir la fenêtre de configuration, cliquez sur **ThreatSense** dans les Configurations avancées de chaque module utilisant la technologie ThreatSense (reportez-vous aux informations ci-dessous). Différents scénarios de sécurité peuvent nécessiter des configurations différentes. Dans cette optique, ThreatSense est configurable individuellement pour les modules de protection suivants :

- Protection en temps réel du système de fichiers
- Analyse en cas d'inactivité
- Analyse au démarrage
- Protection des documents
- Protection du client de messagerie
- Protection de l’accès Web
- Analyse de l'ordinateur

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

Objets à analyser

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

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

Secteurs d'amorçage/UEFI – Analyse les secteurs d'amorçage afin de détecter la présence éventuelle de logiciels malveillants dans l'enregistrement d'amorçage principal. Pour plus d'informations sur UEFI, consultez le glossaire.

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

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

Archives auto-extractibles – Les archives auto-extractibles (SFX) sont des archives qui sont extraites automatiquement.

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

Options d'analyse

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

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

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

Nettoyage

Les paramètres de nettoyage déterminent le comportement d'ESET NOD32 Antivirus lors du nettoyage des objets. Quatre niveaux de nettoyage sont possibles :

ThreatSense comporte les niveaux de correction (nettoyage, par exemple) suivants :

Correction dans ESET NOD32 Antivirus

Niveau de nettoyage	Description
Toujours corriger la détection	Tentative de correction de la détection tout en nettoyant les objets sans aucune intervention de l'utilisateur final. Dans certains cas rares (par exemple, les fichiers système), si la détection ne peut pas être corrigée, l'objet signalé est conservé à son emplacement d'origine.
Corriger la détection si cette opération est sûre. Sinon, conserver	Tentative de correction de la détection lors du nettoyage des objets sans aucune intervention de la part de l'utilisateur final. Dans certains cas (fichiers système ou archives contenant à la fois des fichiers nettoyés et des fichiers infectés), si une détection ne peut pas être corrigée, l'objet signalé est laissé à son emplacement d'origine.
Corriger la détection si cette opération est sûre. Sinon, demander à l'utilisateur	Tentative de correction de la détection lors du nettoyage des objets. Dans certains cas, si aucune action ne peut être exécutée, l'utilisateur final reçoit une alerte interactive. Il doit alors sélectionner une action corrective (supprimer ou ignorer, par exemple). Ce paramètre est recommandé dans la plupart des cas.
Toujours demander à l'utilisateur final	Une fenêtre interactive s'affiche lors du nettoyage des objets et l'utilisateur final doit sélectionner une action corrective (supprimer ou ignorer, par exemple). Ce niveau a été conçu pour les utilisateurs expérimentés qui connaissent les mesures à prendre en cas de détection.

Exclusions

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

Autre

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

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

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

Consigner tous les objets – Le journal d'analyse affiche tous les fichiers analysés dans des archives auto-extractibles, même ceux qui ne sont pas infectés (peut générer beaucoup de données et augmenter la taille du

fichier du journal d'analyse).

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

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

Limites

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

Paramètres d’objet

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

Durée d’analyse maximale pour l’objet (s) – Définit la durée maximale de l’analyse des fichiers dans un objet conteneur (tel qu’une archive RAR/ZIP ou un e-mail avec plusieurs pièces jointes). Ce paramètre ne s’applique pas aux fichiers autonomes. Si une valeur définie par l’utilisateur a été saisie et que le temps s’est écoulé, une analyse s’arrêtera dès que possible, que l’analyse de chaque fichier d’un objet conteneur soit terminée ou non.
Dans le cas d'une archive contenant des fichiers volumineux, l'analyse s'arrêtera dès qu'un fichier de l'archive sera extrait (par exemple, lorsqu'une variable définie par l'utilisateur est de 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 pour les archives plus volumineuses, utilisez les options **Taille d’objet maximale** et **Taille maximale du fichier dans l'archive** (non recommandé en raison d'éventuels risques de sécurité).
Valeur par défaut : illimitée.

Configuration de l’analyse d’archive

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

Taille maximale de fichier dans l'archive – Cette option permet de spécifier la taille maximale des fichiers (après extraction) à analyser contenus dans les archives. 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.

Protection de l’accès Web

La protection de l'accès web vous permet de configurer les paramètres avancés du module Protection internet. Les options suivantes sont disponibles dans Configurations avancées > **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 l'anti-hameçonnage ne sont pas assurés.

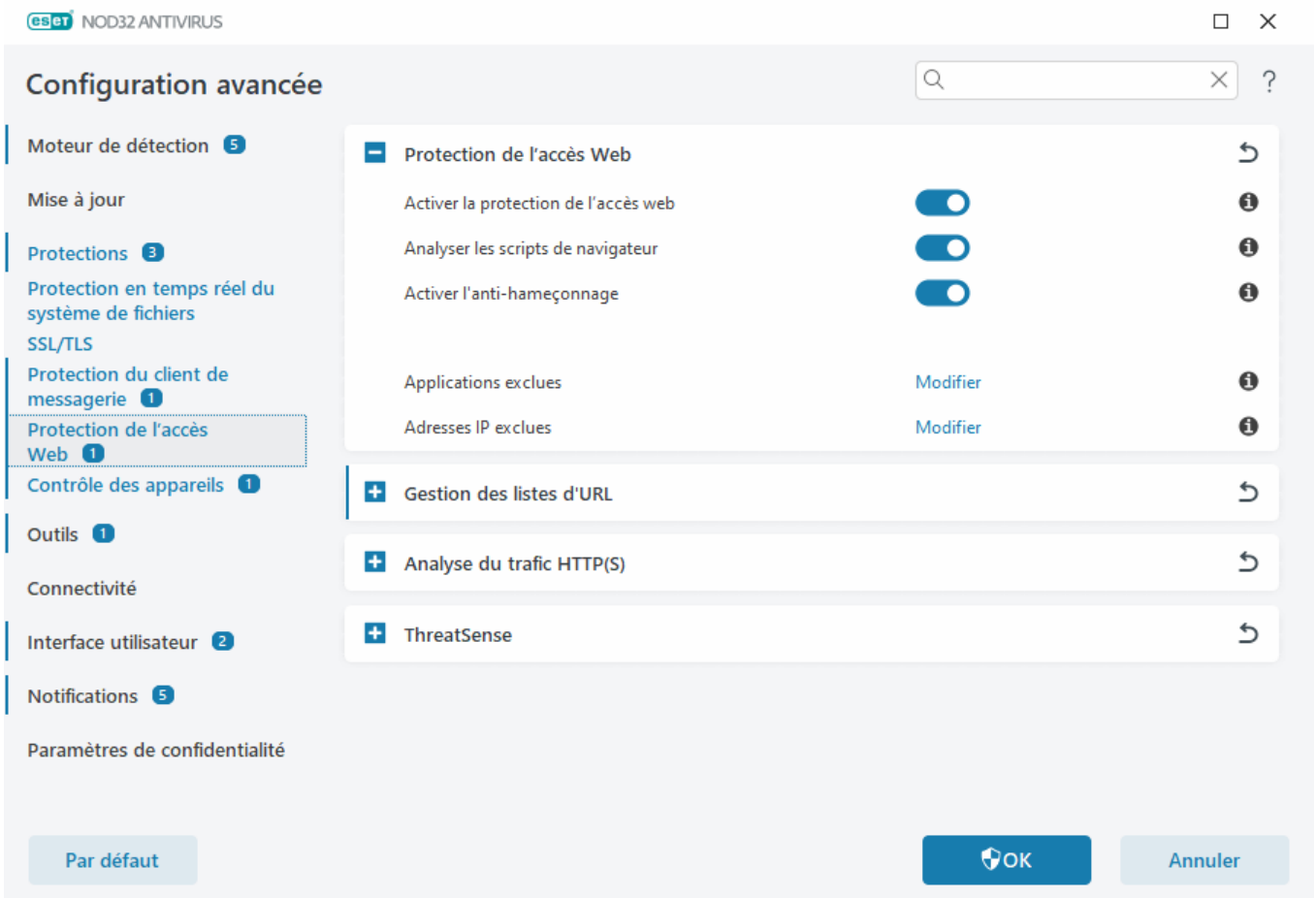
> Nous vous recommandons vivement de laisser la protection de l'accès web activée et de n'exclure aucune application ou adresse IP par défaut.

Analyser les scripts de navigateur : lorsque cette option est activée, le moteur de détection vérifie tous les programmes JavaScript exécutés par des navigateurs web.

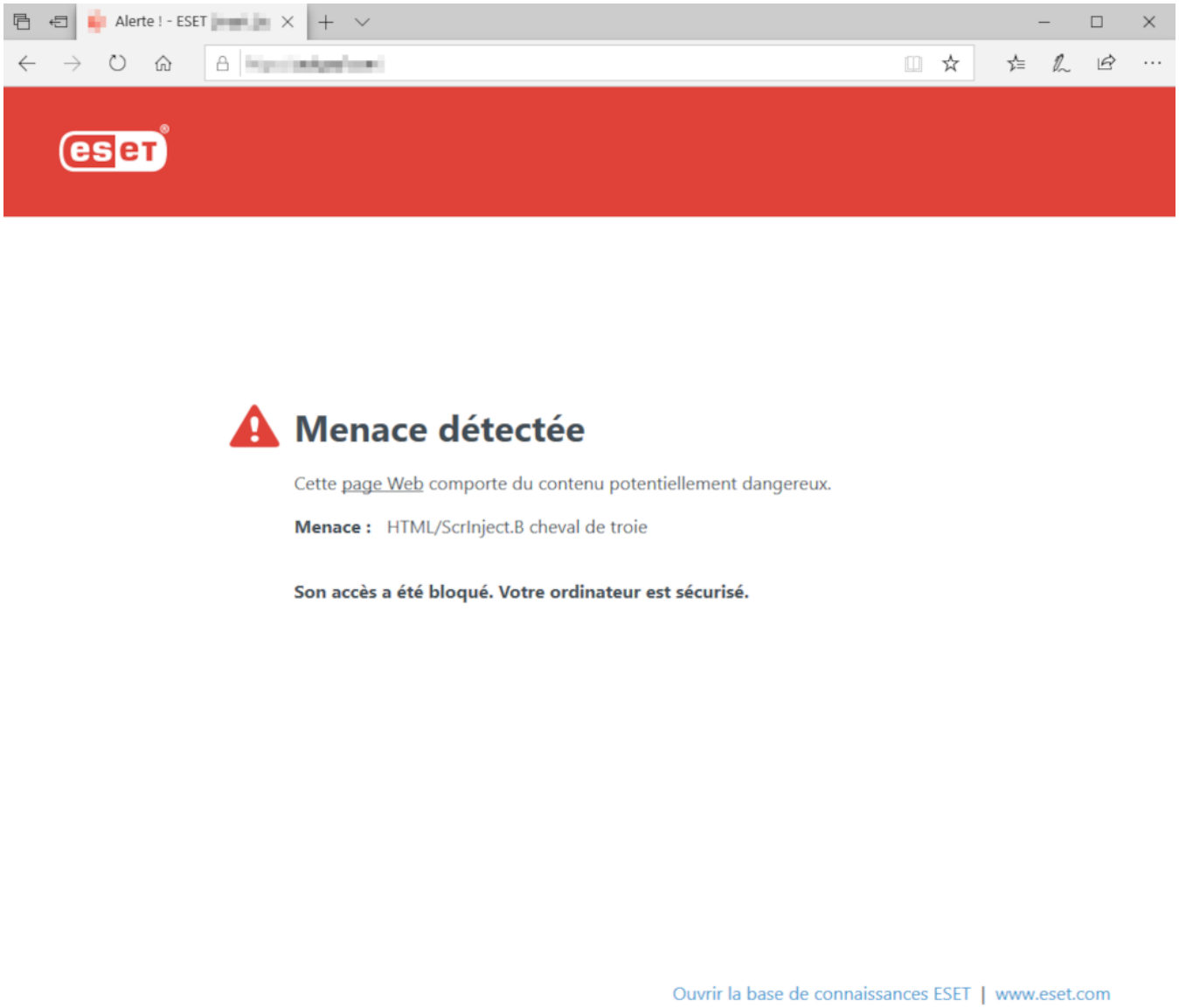
Activer l'anti-hameçonnage : lorsque cette option est activée, les pages web d'hameçonnage sont bloquées. Pour plus d'informations, reportez-vous à la section Protection antihameçonnage.

Applications exclues : permet d'exclure des applications spécifiques de l'analyse par la protection de l'accès web. Cette option s'avère utile lorsque la protection de l'accès web entraîne des problèmes de compatibilité.

Adresses IP exclues : permet d'exclure des adresses distantes spécifiques de l'analyse par la protection de l'accès web. Cette option s'avère utile lorsque la protection de l'accès web entraîne des problèmes de compatibilité.



Lorsque le site web est bloqué, la protection de l'accès web affiche le message suivant dans votre navigateur :



Instructions illustrées

Les articles suivants de la base de connaissances ESET peuvent être disponibles uniquement en anglais :

- Exclure un site web fiable du blocage par la protection de la protection de l'accès web
- Bloquer un site web à l'aide d'ESET NOD32 Antivirus

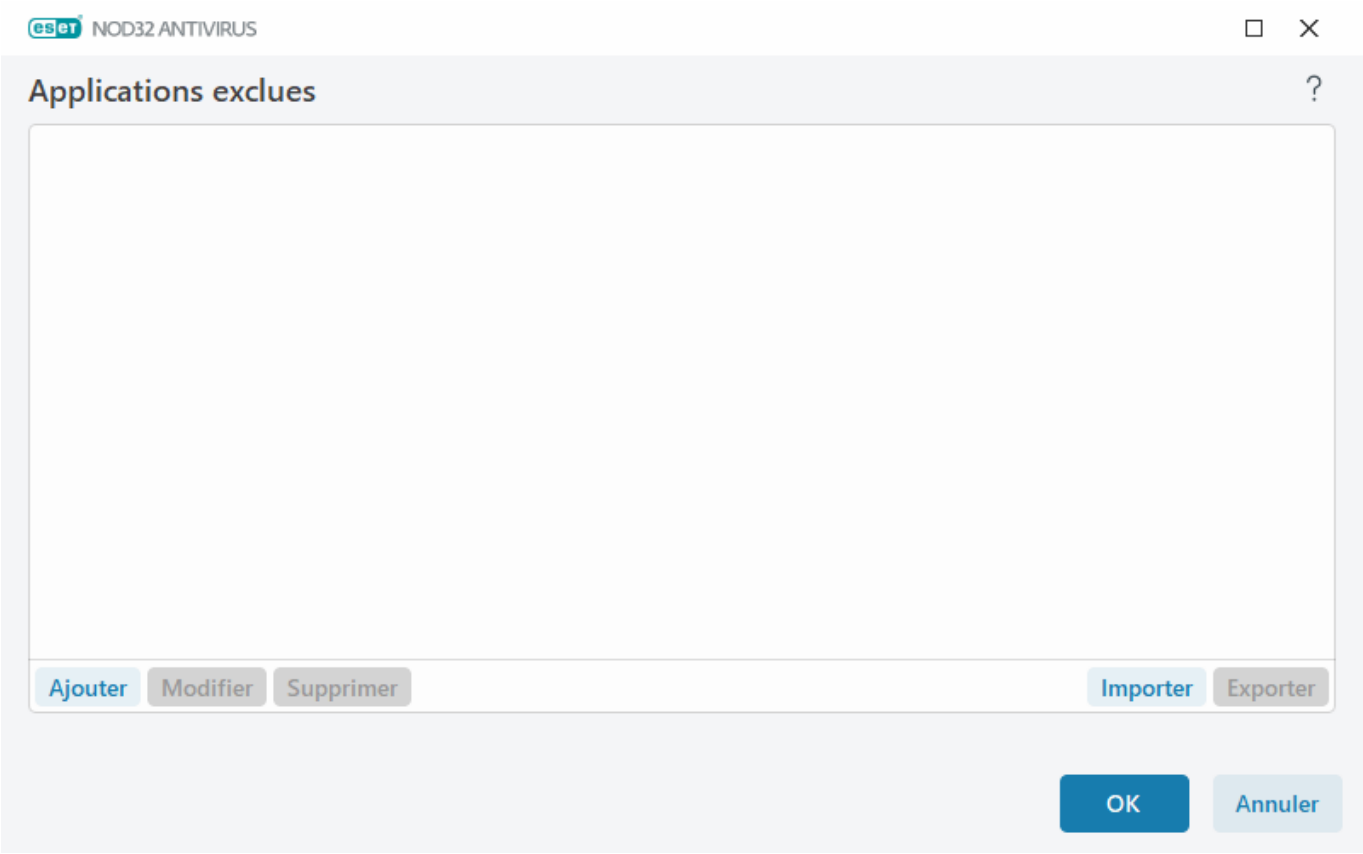
Applications exclues

Pour exclure l'analyse des communications pour des applications spécifiques, ajoutez-les à la liste. Les communications HTTP(S)/POP3(S)/IMAP(S) liées aux adresses sélectionnées ne font pas l'objet d'une détection des menaces. Il est recommandé d'utiliser cette option uniquement pour les applications qui ne fonctionnent pas correctement lorsque leur communication est vérifiée.

L'exécution des applications et des services est disponible automatiquement lorsque vous cliquez sur **Ajouter**. Cliquez sur **...** et accédez à une application pour ajouter manuellement l'exclusion.

Modifier – Modifie les entrées sélectionnées de la liste.

Supprimer – Supprime les entrées sélectionnées de la liste.



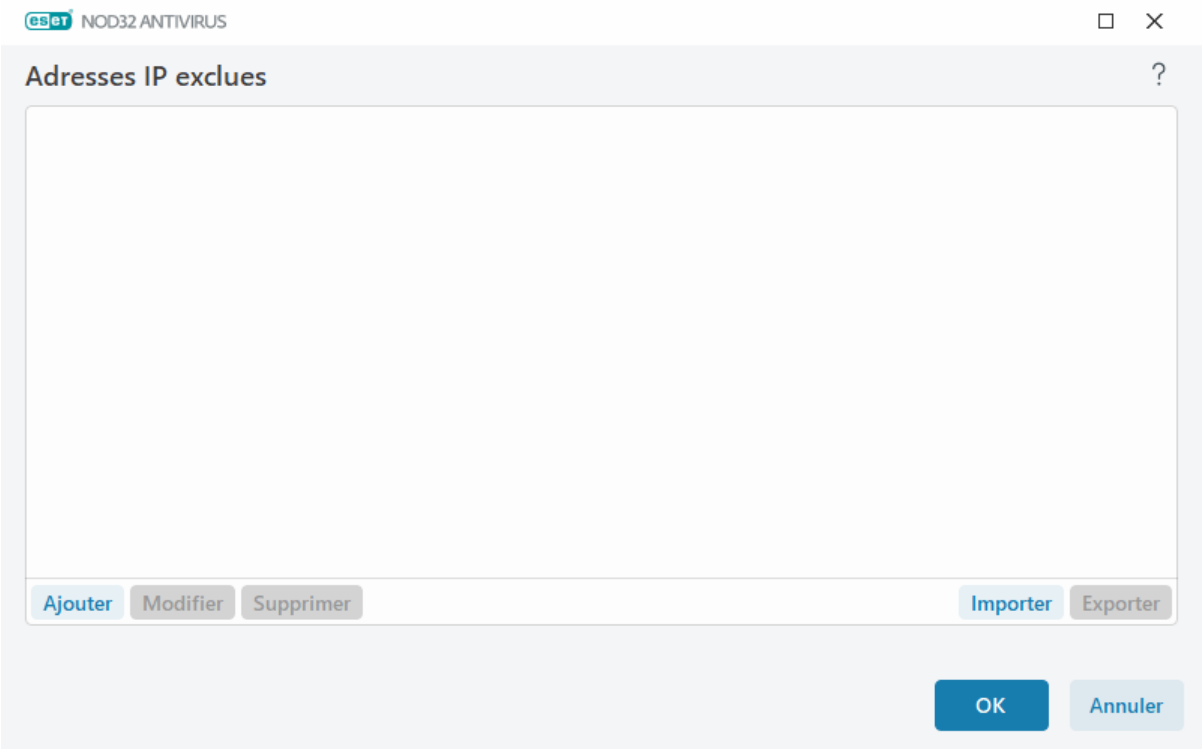
Adresses IP exclues

Les adresses figurant dans cette liste sont exclues de l'analyse. Les communications HTTP(S)/POP3(S)/IMAP(S) liées aux adresses sélectionnées ne font pas l'objet d'une détection des menaces. Il est recommandé d'utiliser cette option uniquement pour les adresses que vous savez être fiables.

Cliquez sur **Ajouter** pour exclure une adresse/une plage d'adresses/un sous-réseau IP d'un point distant.

Cliquez sur **Modifier** pour modifier l'adresse IP sélectionnée.

Cliquez sur **Supprimer** pour supprimer les entrées sélectionnées de la liste.



Exemples d'adresses IP

Ajouter une adresse IPv4:

Adresse unique – Ajoute l'adresse IP d'un ordinateur (par exemple, *192.168.0.10*).

Plage d'adresses – Saisissez l'adresse IP de début et de fin pour définir la plage IP de plusieurs ordinateurs (par exemple *192.168.0.1 à 192.168.0.99*).

Sous-réseau – Le sous-réseau (groupe d'ordinateurs) est 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 tout le type de sous-réseau dans *192.168.1.0/24*.

Ajouter une adresse IPv6:

Adresse unique – Ajoute l'adresse IP d'un ordinateur auquel la règle doit être appliquée, par exemple *2001:718:1c01:16:214:22ff:fec9:ca5*.

Sous-réseau – Le sous-réseau (groupe d'ordinateurs) est défini par une adresse IP et un masque (par exemple : *2002:c0a8:6301:1::1/64*).

Gestion des listes d'URL

La **Gestion des listes d'URL** dans Configurations avancées > **Protections** > **Protection de l'accès web** vous permet de spécifier les adresses HTTP à bloquer, autoriser ou exclure de l'analyse du contenu.

L'option SSL/TLS doit être activée si vous souhaitez filtrer les adresses HTTPS en plus des adresses HTTP. Sinon, seuls les domaines des sites HTTPS que vous avez visités sont ajoutés et non l'URL complète.

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

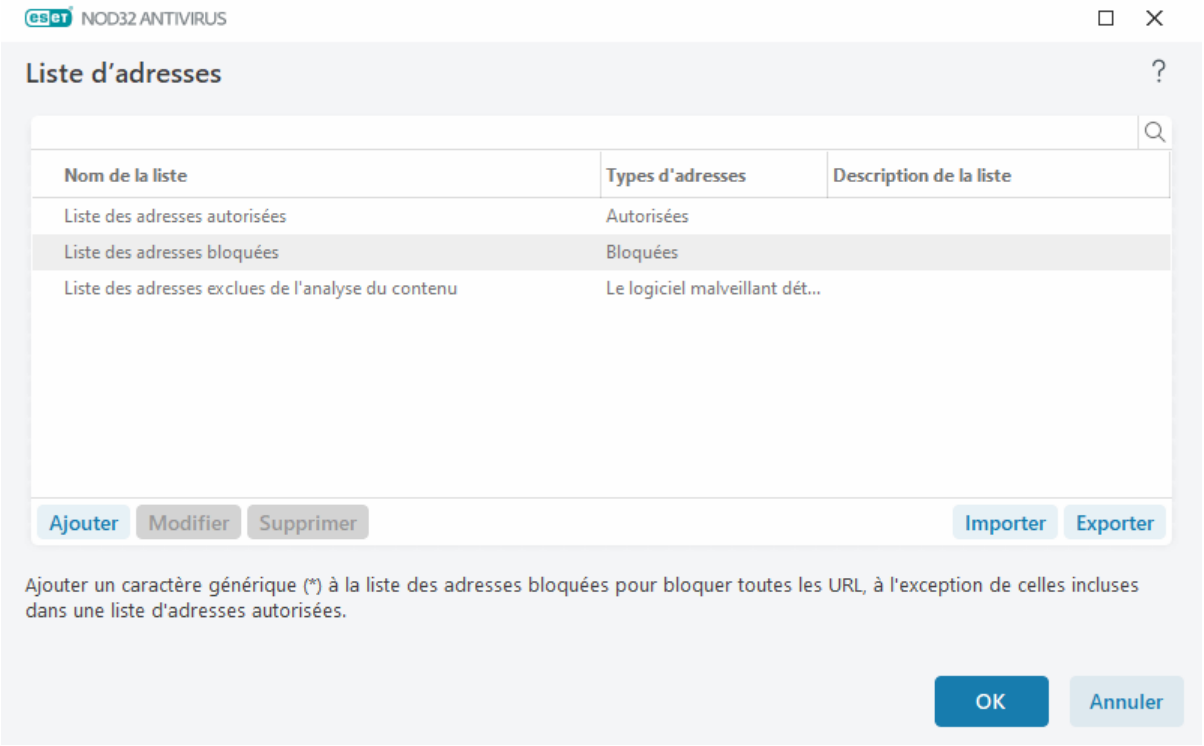
Si vous souhaitez bloquer toutes les adresses HTTP, à l'exception des adresses figurant dans la **liste des adresses autorisées** active, ajoutez un astérisque (*) à la **liste des adresses bloquées** active.

Vous ne pouvez pas utiliser le symbole « * » (astérisque) et le caractère « ? » (point d'interrogation) dans les listes. L'astérisque remplace toute chaîne de caractères, tandis que le point d'interrogation remplace n'importe

quel caractère. Faites attention lors la définition des adresses exclues, car la liste ne doit contenir que des adresses fiables et sûres. De la même manière, veillez à employer correctement les symboles « * » et « ? » dans cette liste. Reportez-vous à Ajout d'un masque de domaine/d'adresse HTTP pour déterminer comment faire correspondre un domaine complet avec tous ses sous-domaines en toute sécurité. Pour activer une liste, sélectionnez l'option **Liste active**. Si vous souhaitez être averti lors de la saisie d'une adresse figurant dans la liste actuelle, sélectionnez l'option **Notifier lors de l'application**.

Adresses approuvées par ESET

Si l'option **Ne pas analyser le trafic avec des domaines approuvés par ESET** est activée, les protocoles SSL/TLS et les domaines sur liste blanche gérés par ESET ne seront pas affectés par la configuration de la gestion des listes d'URL.



Éléments de commande

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

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

Supprimer : permet de supprimer les listes existantes. Cette option n'est disponible que pour les listes créées à l'aide de l'option **Ajouter** et non les listes par défaut.

Liste d'adresses

Dans cette section, vous pouvez spécifier des listes d'adresses HTTP(S) qui seront bloquées, autorisées ou exclues de la vérification.

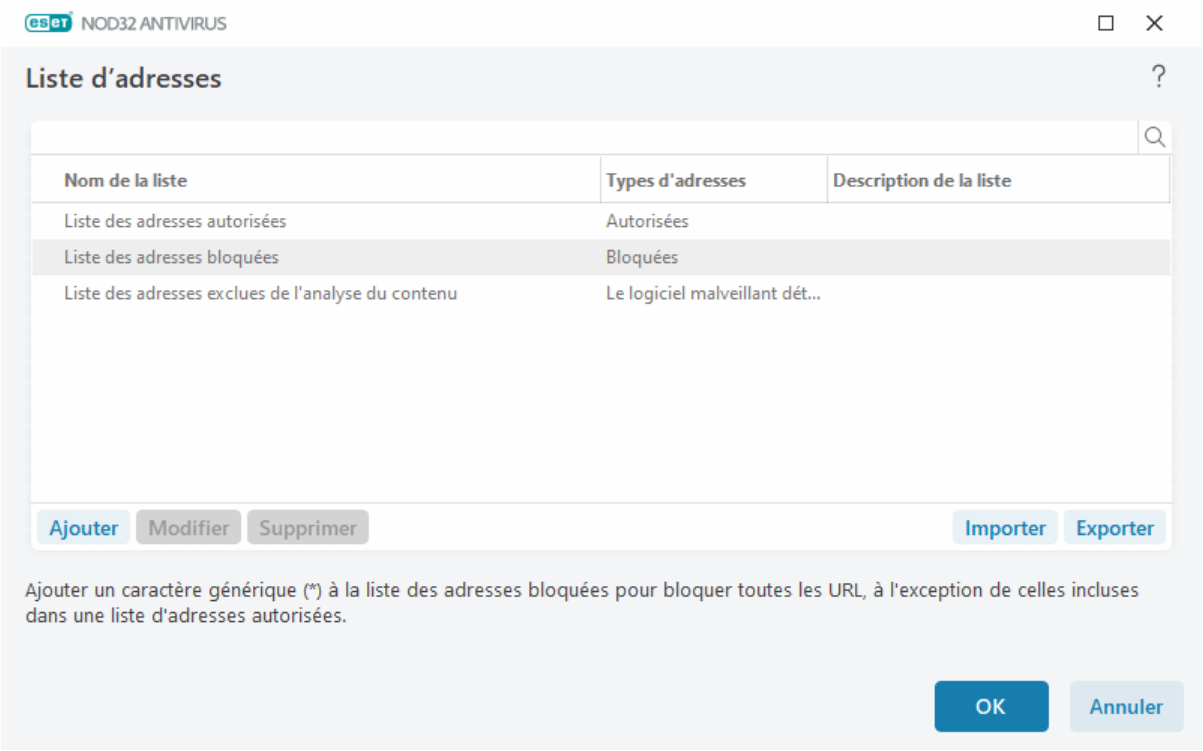
Par défaut, les trois listes suivantes sont disponibles :

• **Liste des adresses exclues de l'analyse du contenu** – Aucune vérification de la présence de code malveillant n'est effectuée pour les adresses répertoriées 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 si la liste des adresses bloquées contient un astérisque (correspond à tout), l'utilisateur n'est autorisé à accéder qu'aux adresses répertoriées dans cette liste. Les adresses de cette liste sont autorisées même si elles sont incluses dans la liste des adresses bloquées.

• **Liste des adresses bloquées** - L'utilisateur n'est pas autorisé à accéder aux adresses répertoriées dans cette liste, à moins qu'elles ne figurent également dans la liste des adresses autorisées.

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 être disponibles uniquement en anglais :

- Exclure un site web fiable du blocage par la protection de la protection de l'accès web
- Bloquer un site Web à l'aide des produits ESET pour les particuliers

Pour plus d'informations, consultez Gestion des listes d'URL.

Création d'une liste d'adresses

Cette boîte de dialogue permet de configurer une nouvelle liste de masques/adresses URL qui seront, bloqués, autorisés ou exclus de la vérification.

Vous pouvez configurer les options suivantes :

Type de liste d'adresses : trois types de liste sont disponibles :

• **Le logiciel malveillant détecté est ignoré** – Aucune vérification de la présence de code malveillant n'est

effectuée pour les adresses répertoriées dans la liste.

- **Bloqué** : l'accès aux adresses spécifiées dans cette liste est bloqué.

- **Autorisé** : l'accès aux adresses répertoriées dans cette liste est autorisé. Les adresses de cette liste sont autorisées même si elles correspondent aux adresses bloquées.

Nom de liste – Spécifiez 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 – Tapez une brève description de la liste (facultatif). Ce champ n'est pas disponible lors de la modification de l'une des listes prédéfinies.

Pour activer une liste, sélectionnez l'option **Liste active** en regard de celle-ci. Si vous souhaitez être averti lorsqu'une liste spécifique est utilisée lors de l'accès à des sites web, sélectionnez l'option **Notifier lors de l'application**. Vous recevrez par exemple une notification lorsqu'un site web sera bloqué ou autorisé en raison de son inclusion dans la liste des adresses bloquées ou autorisées. La notification contient le nom de la liste.

Niveau de verbosité – Les informations sur la liste spécifique utilisée lors de l'accès aux sites web peuvent être écrites dans les fichiers journaux.

Éléments de commande

Ajouter – Ajoutez une nouvelle adresse URL à la liste (entrez plusieurs valeurs avec un séparateur).

Modifier – Permet de modifier une adresse existante dans la liste. Disponible uniquement pour les adresses créées avec l'option **Ajouter**.

Supprimer – Permet de supprimer des adresses existantes de la liste. Disponible uniquement pour les adresses créées avec l'option **Ajouter**.

Importer – Importez un fichier comportant des adresses URL (séparez les valeurs par un saut de ligne, par exemple *.txt utilisant le codage UTF-8).

Ajout d'un masque d'URL

Reportez-vous aux instructions de cette boîte de dialogue pour entrer le masque d'adresse/de domaine souhaité.

ESET NOD32 Antivirus permet de bloquer l'accès à des sites Web spécifiques et d'empêcher le navigateur Internet d'en afficher le contenu. Par ailleurs, il permet à l'utilisateur de spécifier des adresses à exclure de la vérification. Si l'utilisateur ignore le nom complet du serveur distant ou s'il souhaite spécifier un groupe de serveurs distants, il peut employer des « masques ». Ces masques peuvent contenir les symboles « ? » et « * » :

- ? pour représenter un caractère quelconque ;

- * pour représenter une chaîne de caractères.

Par exemple *.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 initiale « *. » est traitée spécialement si elle est utilisée au début du nom de domaine. Pour

commencer, le caractère générique * ne correspond pas au caractère barre oblique (« / ») dans ce cas. Cela a pour but d'éviter de contourner le masque. Par exemple, le masque **.domaine.com* ne correspondra pas à *http://toutdomaine.com/toutchemin#.domaine.com* (un tel suffixe peut être ajouté à toute adresse URL sans affecter le téléchargement). Ensuite, le « *. » correspond également à une chaîne vide dans ce cas spécial. Elle vise à permettre une correspondance avec tout le domaine, y compris tous les éventuels sous-domaines en utilisant un seul et unique masque. Par exemple, le masque **.domaine.com* correspond également à *http://domaine.com*. L'utilisation de **domaine.com* serait incorrecte, car ce masque correspondrait aussi à *http://unautredomaine.com*.

Analyse du trafic HTTP(S)

Par défaut, ESET NOD32 Antivirus est configuré pour analyser le trafic HTTP et HTTPS utilisé par les navigateurs internet et d'autres applications. Vous ne devez désactiver l'analyse du trafic que si vous rencontrez des problèmes liés à des logiciels tiers et que vous souhaitez déterminer si le problème est causé par ESET NOD32 Antivirus.

Activer l'analyse du trafic HTTP – Le trafic HTTP est toujours contrôlé 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 un serveur et un client. ESET NOD32 Antivirus contrôle les communications à l'aide des protocoles SSL (Secure Socket Layer) et TLS (Transport Layer Security). Le programme analyse uniquement le trafic sur les ports définis dans **Ports utilisés par le protocole HTTPS**, quelle que soit la version du système d'exploitation (vous pouvez ajouter des ports aux ports prédéfinis 443 et 0 à 65 535).

ThreatSense

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

les options de configuration de la technologie ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

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

Pour ouvrir la fenêtre de configuration, cliquez sur **ThreatSense** dans les Configurations avancées de chaque module utilisant la technologie ThreatSense (reportez-vous aux informations ci-dessous). Différents scénarios de sécurité peuvent nécessiter des configurations différentes. Dans cette optique, ThreatSense est configurable individuellement pour les modules de protection suivants :

- Protection en temps réel du système de fichiers

- Analyse en cas d'inactivité
- Analyse au démarrage
- Protection des documents
- Protection du client de messagerie
- Protection de l’accès Web
- Analyse de l'ordinateur

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

Objets à analyser

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

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

Secteurs d'amorçage/UEFI – Analyse les secteurs d'amorçage afin de détecter la présence éventuelle de logiciels malveillants dans l'enregistrement d'amorçage principal. Pour plus d'informations sur UEFI, consultez le glossaire.

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

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

Archives auto-extractibles – Les archives auto-extractibles (SFX) sont des archives qui sont extraites automatiquement.

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

Options d’analyse

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

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

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

Nettoyage

Les paramètres de nettoyage déterminent le comportement d'ESET NOD32 Antivirus lors du nettoyage des objets. Quatre niveaux de nettoyage sont possibles :

ThreatSense comporte les niveaux de correction (nettoyage, par exemple) suivants :

Correction dans ESET NOD32 Antivirus

Niveau de nettoyage	Description
Toujours corriger la détection	Tentative de correction de la détection tout en nettoyant les objets sans aucune intervention de l'utilisateur final. Dans certains cas rares (par exemple, les fichiers système), si la détection ne peut pas être corrigée, l'objet signalé est conservé à son emplacement d'origine.
Corriger la détection si cette opération est sûre. Sinon, conserver	Tentative de correction de la détection lors du nettoyage des objets sans aucune intervention de la part de l'utilisateur final. Dans certains cas (fichiers système ou archives contenant à la fois des fichiers nettoyés et des fichiers infectés), si une détection ne peut pas être corrigée, l'objet signalé est laissé à son emplacement d'origine.
Corriger la détection si cette opération est sûre. Sinon, demander à l'utilisateur	Tentative de correction de la détection lors du nettoyage des objets. Dans certains cas, si aucune action ne peut être exécutée, l'utilisateur final reçoit une alerte interactive. Il doit alors sélectionner une action corrective (supprimer ou ignorer, par exemple). Ce paramètre est recommandé dans la plupart des cas.
Toujours demander à l'utilisateur final	Une fenêtre interactive s'affiche lors du nettoyage des objets et l'utilisateur final doit sélectionner une action corrective (supprimer ou ignorer, par exemple). Ce niveau a été conçu pour les utilisateurs expérimentés qui connaissent les mesures à prendre en cas de détection.

Exclusions

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

Autre

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

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

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

Consigner tous les objets – Le journal d'analyse affiche tous les fichiers analysés dans des archives auto-extractibles, même ceux qui ne sont pas infectés (peut générer beaucoup de données et augmenter la taille du fichier du journal d'analyse).

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

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

Limites

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

Paramètres d'objet

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

Durée d'analyse maximale pour l'objet (s) – Définit la durée maximale de l'analyse des fichiers dans un objet conteneur (tel qu'une archive RAR/ZIP ou un e-mail avec plusieurs pièces jointes). Ce paramètre ne s'applique pas aux fichiers autonomes. Si une valeur définie par l'utilisateur a été saisie et que le temps s'est écoulé, une analyse s'arrêtera dès que possible, que l'analyse de chaque fichier d'un objet conteneur soit terminée ou non.
Dans le cas d'une archive contenant des fichiers volumineux, l'analyse s'arrêtera dès qu'un fichier de l'archive sera extrait (par exemple, lorsqu'une variable définie par l'utilisateur est de 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 pour les archives plus volumineuses, utilisez les options **Taille d'objet maximale** et **Taille maximale du fichier dans l'archive** (non recommandé en raison d'éventuels risques de sécurité).
Valeur par défaut : illimitée.

Configuration de l'analyse d'archive

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

Taille maximale de fichier dans l'archive – Cette option permet de spécifier la taille maximale des fichiers (après extraction) à analyser contenus dans les archives. 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 de périphérique

ESET NOD32 Antivirus permet le contrôle automatique des appareils (CD / DVD /USB, etc.). Ce module permet de bloquer ou d'ajuster les filtres étendus/autorisations, et de définir les autorisations des utilisateurs à accéder à un périphérique et à l'utiliser. Ce procédé peut être utile si l'administrateur souhaite empêcher l'utilisation de périphériques avec du contenu non sollicité.

Périphériques externes pris en charge :

- Stockage sur disque (disque dur, disque amovible USB)
- CD/DVD
- Imprimante USB
- FireWireStockage
- Bluetooth Périphérique
- Lecteur de carte à puce
- Périphérique d'image
- Modem
- LPT/COM port
- Appareil portable (appareils alimentés par batterie tels que les lecteurs multimédia, les smartphones, les appareils plug-and-play, etc.)
- Tous les types de périphérique

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

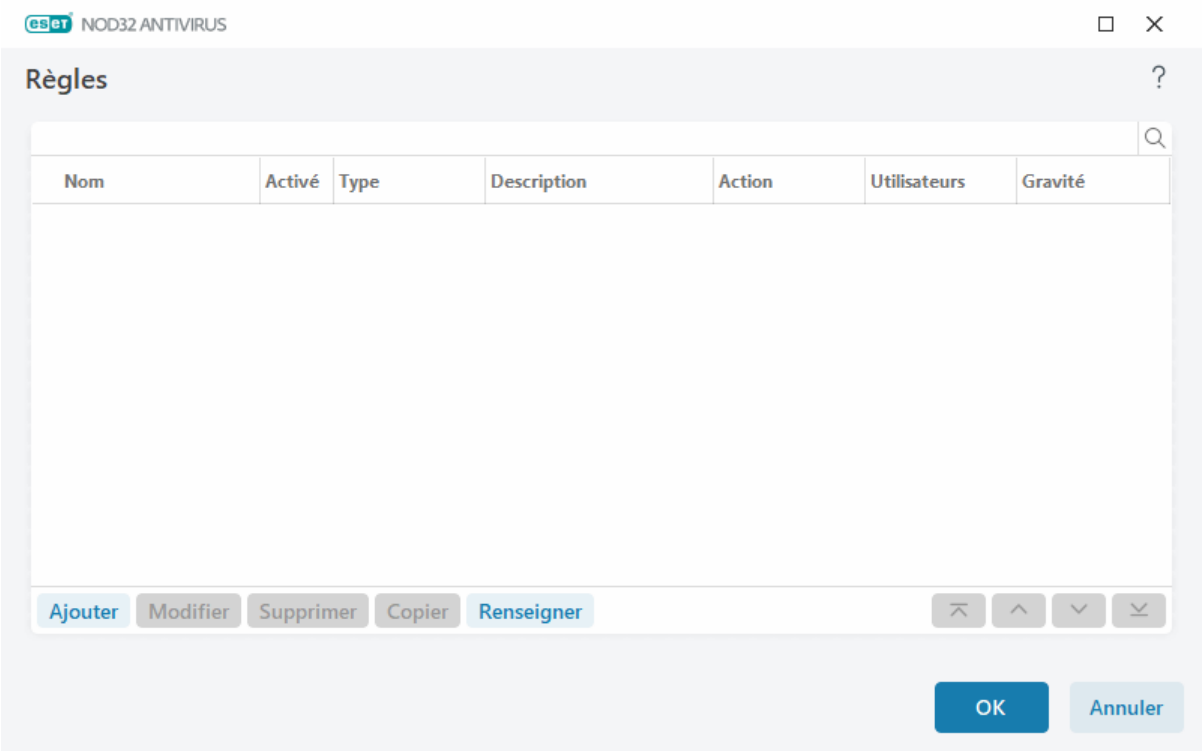
Cliquez sur le bouton bascule **Activer le contrôle des appareils** pour activer la fonctionnalité Contrôle des appareils dans ESET NOD32 Antivirus. Vous devez redémarrer votre ordinateur pour que cette modification prenne effet. Une fois le contrôle des appareils activé, vous pouvez définir des **règles** dans la fenêtre Éditeur de règles.

Vous pouvez créer des groupes de périphériques différents auxquels différentes règles sont appliquées. Vous pouvez également créer un seul groupe d'appareils auquel la règle avec l'action **Autoriser** ou **Blocage d'écriture** est appliquée. Les périphériques non reconnus sont ainsi bloqués par le contrôle de périphérique lorsqu'ils sont connectés à votre ordinateur.

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

Éditeur de règles de contrôle de périphérique

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



Des appareils spécifiques peuvent être autorisés ou bloqués par utilisateur ou groupe d'utilisateurs et basés sur des paramètres d'appareils supplémentaires qui peuvent être spécifiés dans la configuration des règles. La liste des règles contient plusieurs descriptions de la règle, telles que le nom, le type d'appareil externe, l'action à exécuter après la connexion d'un appareil externe à l'ordinateur et le niveau de gravité d'après le journal. Voir aussi Ajout de règles de contrôle des appareils.

Cliquez sur **Ajouter** ou **Modifier** pour gérer une règle. Cliquez sur **Copier** pour créer une règle à l'aide d'options prédéfinies utilisées pour une autre règle sélectionnée. Les chaînes XML qui s'affichent lorsque vous cliquez sur une règle peuvent être copiées dans le Presse-papiers ou aider les administrateurs système à exporter/importer ces données et à les utiliser, par exemple dans .

En appuyant sur **CTRL** et en cliquant, vous pouvez sélectionner plusieurs règles et appliquer des actions à toutes les règles sélectionnées (par exemple les supprimer ou les déplacer dans la liste). La case à cocher **Activé** permet d'activer ou de désactiver une règle ; elle peut s'avérer utile si vous souhaitez conserver la règle.

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

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

Les entrées des journaux peuvent être consultées dans la fenêtre principale du programme > **Outils** > Fichiers journaux.

Le journal du contrôle de périphérique enregistre toutes les occurrences où le contrôle de périphérique est déclenché.

Périphériques détectés

Le bouton **Renseigner** permet de donner une vue d'ensemble de tous les périphériques actuellement connectés avec des informations sur : le type de périphérique, le fournisseur, le modèle et le numéro de série (le cas échéant). Si vous souhaitez afficher tous les appareils masqués, sélectionnez **Afficher les appareils masqués**.

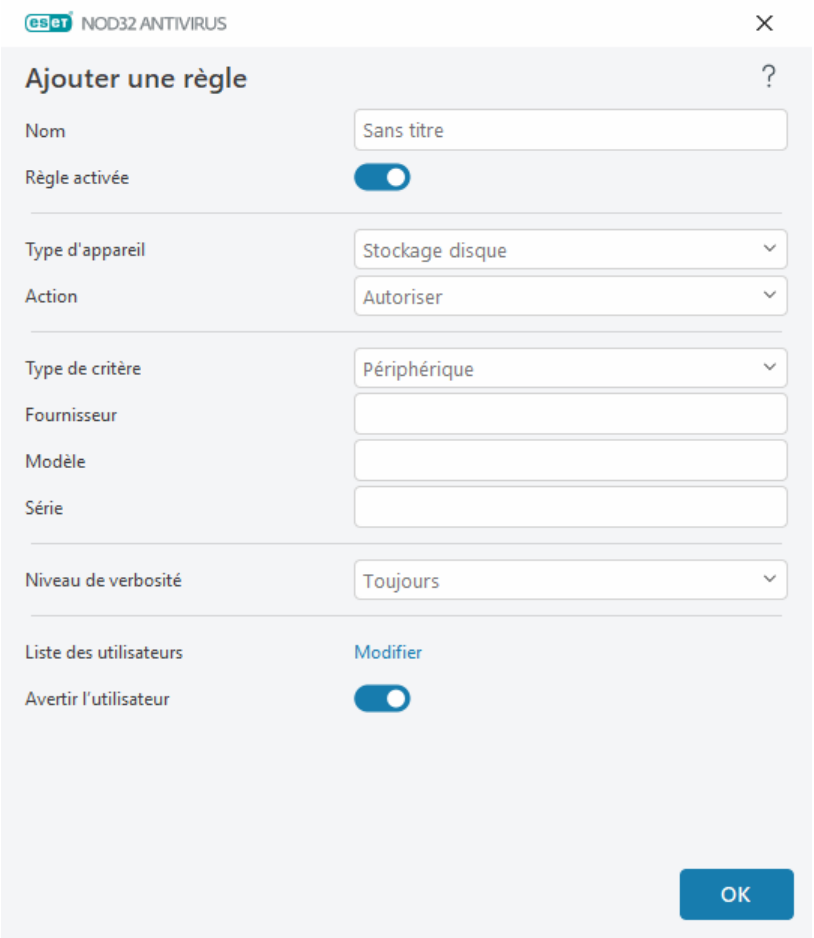
Sélectionnez un appareil dans la liste des appareils détectés, puis cliquez sur **OK** pour ajouter une règle de contrôle des appareils avec des informations prédéfinies (tous les paramètres peuvent être réglés).

Les appareils en mode de faible consommation (veille) sont signalés par une icône d'avertissement . Pour activer le bouton **OK** et ajouter une règle pour cet appareil :

- Reconnectez l'appareil.
- Utilisez l'appareil (par exemple, lancez l'application Caméra dans Windows pour mettre en éveil une webcam).

Ajout de règles de contrôle de périphérique

Une règle de contrôle des appareils définit une action à exécuter lorsqu'un appareil répondant aux critères de la règle est connecté à l'ordinateur.



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

Type de périphérique

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

Action

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

- **Autoriser** – L'accès complet au périphérique est autorisé.
- **Bloquer** – L'accès au périphérique est bloqué.
- **Blocage d'écriture** – L'accès en lecture seule au périphérique est autorisé.
- **Avertir** – À chaque connexion d'un périphérique, l'utilisateur est averti s'il est autorisé/bloqué, et une entrée est enregistrée dans le journal. Comme les appareils ne sont pas mémorisés, une notification continuera de s'afficher en cas de connexions suivantes d'un même appareil.

Il convient de noter que toutes les actions (autorisations) ne sont pas disponibles pour tous les types de périphériques. S'il s'agit d'un périphérique de stockage, les quatre actions sont disponibles. Pour les périphériques autres que les périphériques de stockage, seules trois actions sont disponibles (par exemple, l'action **Blocage d'écriture** n'étant pas disponible pour Bluetooth, un tel périphérique ne peut être qu'autorisé ou sujet à un avertissement).

Type de critère

Sélectionnez **Groupe de périphériques** ou **Périphérique**.

D'autres paramètres présentés ci-dessous peuvent être utilisés afin d'affiner les règles pour différents appareils. Tous les paramètres respectent la casse et prennent en charge les caractères génériques (*, ?) :

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

> Si ces paramètres ne sont pas définis, la règle ignore ces champs lors de la recherche de correspondances. Les paramètres de filtrage de tous les champs de texte respectent 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 caractère ou plus).

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

Journalisation de la gravité

ESET NOD32 Antivirus enregistre tous les événements importants dans un journal, accessible directement à partir du menu du programme. Cliquez sur **Outils** > **Fichiers journaux**, puis sélectionnez **Contrôle de périphérique** dans le menu déroulant **Journaliser**.

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

Liste de l'utilisateur

Les règles peuvent être restreintes à certains utilisateurs ou groupes d'utilisateurs en les ajoutant dans la liste des utilisateurs (cliquez sur **Modifier** en regard de l'option **Liste des utilisateurs**).

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

Limites de la liste des utilisateurs

La liste des utilisateurs ne peut pas être définie pour des règles avec des types d'appareilsspécifiques :

- Imprimante USB
- Périphérique Bluetooth
- Lecteur de carte à puce
- Périphérique d'image
- Modem
- Port LPT/COM

Avertir l'utilisateur – Si un appareil bloqué par une règle existante est inséré, une fenêtre de notification s'affiche.

Groupe de périphériques

Un périphérique connecté à votre ordinateur peut présenter un risque de sécurité.

La fenêtre Groupes de périphériques se divise en deux parties. La partie droite de la fenêtre contient la liste des périphériques appartenant à un groupe donné. La partie gauche comporte les groupes créés. Sélectionnez un groupe pour afficher les appareils dans le volet droit.

Lorsque vous ouvrez la fenêtre Groupes de périphériques et que vous sélectionnez un groupe, vous pouvez ajouter ou supprimer des périphériques de la liste. Une autre méthode pour ajouter des périphériques au groupe consiste à les importer à partir d'un fichier. Vous pouvez aussi cliquer sur le bouton **Renseigner** pour que tous les périphériques connectés à votre ordinateur soient répertoriés dans la fenêtre **Périphériques détectés**. Sélectionnez des appareils dans la liste renseignée, puis cliquez sur **OK** pour les ajouter au groupe.

Éléments de commande

Ajouter : vous pouvez ajouter un groupe en saisissant son nom ou un appareil à un groupe existant selon l'endroit de la fenêtre où vous avez cliqué sur le bouton.

Modifier : permet de modifier le nom du groupe sélectionné ou les paramètres du périphérique (fabricant, modèle, numéro de série, etc.).

Supprimer : permet de supprimer le groupe ou le périphérique sélectionné selon la partie de la fenêtre où vous avez cliqué sur le bouton.

Importer : permet d'importer une liste d'appareils à partir d'un fichier texte. L'importation d'appareils à partir d'un fichier texte demande une mise en forme correcte :

- Chaque appareil doit se trouver au début d'une nouvelle ligne.
- Le **fournisseur**, le **modèle** et la **série** doivent être indiqués pour chaque appareil et séparés par une virgule.

Voici un exemple de contenu de fichier texte :

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Exporter : permet d'exporter une liste d'appareils vers un fichier.

Le bouton **Renseigner** permet de donner une vue d'ensemble de tous les périphériques actuellement connectés avec des informations sur : le type de périphérique, le fournisseur, le modèle et le numéro de série (le cas échéant).

Ajouter un appareil

Pour ajouter un appareil à un groupe existant, cliquez sur **Ajouter** dans la fenêtre à droite. D'autres paramètres présentés ci-dessous peuvent être utilisés afin d'affiner les règles pour différents appareils. Tous les paramètres respectent la casse et prennent en charge les caractères génériques (*, ?) :

- **Fabricant** – Permet de filtrer par nom ou ID de fabricant.
- **Modèle** – Nom du périphérique.
- **N° de série** – Les périphériques externes ont généralement leur propre numéro de série. Dans le cas d'un CD/DVD, il s'agit du numéro de série du support et pas du lecteur CD.
- **Description** – Votre description de l'appareil pour une meilleure organisation.

Si ces paramètres ne sont pas définis, la règle ignore ces champs lors de la recherche de correspondances. Les paramètres de filtrage de tous les champs de texte respectent 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 caractère ou plus).

Cliquez sur **OK** pour enregistrer les modifications. Cliquez sur **Annuler** pour fermer la fenêtre **Groupes d'appareils** sans enregistrer les modifications.

Une fois le groupe d'appareils créé, vous devez ajouter une nouvelle règle de contrôle des appareils pour le groupe d'appareils créé et sélectionner l'action à exécuter.

Il convient de noter que toutes les actions (autorisations) ne sont pas disponibles pour tous les types de périphériques. Les quatre actions sont disponibles s'il s'agit d'un appareil de stockage. Pour les appareils autres que les appareils de stockage, seules trois actions sont disponibles (par exemple, l'action **Blocage d'écriture** n'étant pas disponible pour Bluetooth, un tel appareil ne peut être qu'autorisé, bloqué ou sujet à un avertissement).

ThreatSense

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

les options de configuration de la technologie ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

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

Pour ouvrir la fenêtre de configuration, cliquez sur **ThreatSense** dans les Configurations avancées de chaque module utilisant la technologie ThreatSense (reportez-vous aux informations ci-dessous). Différents scénarios de sécurité peuvent nécessiter des configurations différentes. Dans cette optique, ThreatSense est configurable individuellement pour les modules de protection suivants :

- Protection en temps réel du système de fichiers
- Analyse en cas d'inactivité
- Analyse au démarrage
- Protection des documents
- Protection du client de messagerie
- Protection de l’accès Web

- Analyse de l'ordinateur

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

Objets à analyser

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

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

Secteurs d'amorçage/UEFI – Analyse les secteurs d'amorçage afin de détecter la présence éventuelle de logiciels malveillants dans l'enregistrement d'amorçage principal. Pour plus d'informations sur UEFI, consultez le glossaire.

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

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

Archives auto-extractibles – Les archives auto-extractibles (SFX) sont des archives qui sont extraites automatiquement.

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

Options d'analyse

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

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

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

Nettoyage

Les paramètres de nettoyage déterminent le comportement d'ESET NOD32 Antivirus lors du nettoyage des objets. Quatre niveaux de nettoyage sont possibles :

ThreatSense comporte les niveaux de correction (nettoyage, par exemple) suivants :

Correction dans ESET NOD32 Antivirus

Niveau de nettoyage	Description
Toujours corriger la détection	Tentative de correction de la détection tout en nettoyant les objets sans aucune intervention de l'utilisateur final. Dans certains cas rares (par exemple, les fichiers système), si la détection ne peut pas être corrigée, l'objet signalé est conservé à son emplacement d'origine.
Corriger la détection si cette opération est sûre. Sinon, conserver	Tentative de correction de la détection lors du nettoyage des objets sans aucune intervention de la part de l'utilisateur final. Dans certains cas (fichiers système ou archives contenant à la fois des fichiers nettoyés et des fichiers infectés), si une détection ne peut pas être corrigée, l'objet signalé est laissé à son emplacement d'origine.
Corriger la détection si cette opération est sûre. Sinon, demander à l'utilisateur	Tentative de correction de la détection lors du nettoyage des objets. Dans certains cas, si aucune action ne peut être exécutée, l'utilisateur final reçoit une alerte interactive. Il doit alors sélectionner une action corrective (supprimer ou ignorer, par exemple). Ce paramètre est recommandé dans la plupart des cas.
Toujours demander à l'utilisateur final	Une fenêtre interactive s'affiche lors du nettoyage des objets et l'utilisateur final doit sélectionner une action corrective (supprimer ou ignorer, par exemple). Ce niveau a été conçu pour les utilisateurs expérimentés qui connaissent les mesures à prendre en cas de détection.

Exclusions

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

Autre

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

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

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

Consigner tous les objets – Le journal d'analyse affiche tous les fichiers analysés dans des archives auto-extractibles, même ceux qui ne sont pas infectés (peut générer beaucoup de données et augmenter la taille du

fichier du journal d'analyse).

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

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

Limites

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

Paramètres d'objet

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

Durée d'analyse maximale pour l'objet (s) – Définit la durée maximale de l'analyse des fichiers dans un objet conteneur (tel qu'une archive RAR/ZIP ou un e-mail avec plusieurs pièces jointes). Ce paramètre ne s'applique pas aux fichiers autonomes. Si une valeur définie par l'utilisateur a été saisie et que le temps s'est écoulé, une analyse s'arrêtera dès que possible, que l'analyse de chaque fichier d'un objet conteneur soit terminée ou non.
Dans le cas d'une archive contenant des fichiers volumineux, l'analyse s'arrêtera dès qu'un fichier de l'archive sera extrait (par exemple, lorsqu'une variable définie par l'utilisateur est de 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 pour les archives plus volumineuses, utilisez les options **Taille d'objet maximale** et **Taille maximale du fichier dans l'archive** (non recommandé en raison d'éventuels risques de sécurité).
Valeur par défaut : illimitée.

Configuration de l'analyse d'archive

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

Taille maximale de fichier dans l'archive – Cette option permet de spécifier la taille maximale des fichiers (après extraction) à analyser contenus dans les archives. 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 de niveau de nettoyage d'un module de protection souhaité, développez **ThreatSense** (par exemple, **Protection en temps réel du système de fichiers**), puis choisissez un **niveau de nettoyage** dans le menu déroulant.

ThreatSense comporte les niveaux de correction (nettoyage, par exemple) suivants :

Correction dans ESET NOD32 Antivirus

Niveau de nettoyage	Description
Toujours corriger la détection	Tentative de correction de la détection tout en nettoyant les objets sans aucune intervention de l'utilisateur final. Dans certains cas rares (par exemple, les fichiers système), si la détection ne peut pas être corrigée, l'objet signalé est conservé à son emplacement d'origine.
Corriger la détection si cette opération est sûre. Sinon, conserver	Tentative de correction de la détection lors du nettoyage des objets sans aucune intervention de la part de l'utilisateur final. Dans certains cas (fichiers système ou archives contenant à la fois des fichiers nettoyés et des fichiers infectés), si une détection ne peut pas être corrigée, l'objet signalé est laissé à son emplacement d'origine.
Corriger la détection si cette opération est sûre. Sinon, demander à l'utilisateur	Tentative de correction de la détection lors du nettoyage des objets. Dans certains cas, si aucune action ne peut être exécutée, l'utilisateur final reçoit une alerte interactive. Il doit alors sélectionner une action corrective (supprimer ou ignorer, par exemple). Ce paramètre est recommandé dans la plupart des cas.
Toujours demander à l'utilisateur final	Une fenêtre interactive s'affiche lors du nettoyage des objets et l'utilisateur final doit sélectionner une action corrective (supprimer ou ignorer, par exemple). Ce niveau a été conçu pour les utilisateurs expérimentés qui connaissent les mesures à prendre en cas de détection.

Extensions de fichier exclues de l'analyse

Les extensions de fichier exclues font partie d'ThreatSense. Pour configurer les extensions de fichier exclues, cliquez sur **ThreatSense** dans les Configurations avancées pour n'importe quel module utilisant 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 d'ThreatSense vous permet de définir les types de fichiers à analyser.

> Ne confondez pas cette option avec Exclusions des processus, Exclusions HIPS ou Exclusions de fichier/dossier.

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

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

Pour ajouter une nouvelle extension à la liste, cliquez sur **Ajouter**. Saisissez l'extension dans le champ correspondant (comme tmp) et cliquez sur **OK**. Lorsque vous sélectionnez **Entrer plusieurs valeurs**, vous pouvez ajouter plusieurs extensions de fichier en les séparant par des lignes, des virgules ou des points-virgules (par exemple, choisissez **Point-virgule** comme séparateur dans le menu déroulant et saisissez `edb;eml;tmp`).
Vous pouvez utiliser un symbole spécial ? (point d'interrogation). Qui symbolise n'importe quel caractère (par exemple, `?db`).

Pour voir l'extension exacte (le cas échant) d'un fichier dans un système d'exploitation Windows, vous devez cocher la case **Extensions de noms de fichiers** dans **Explorateur Windows** > **Affichage** (onglet).

Autres paramètres ThreatSense

Pour modifier ces paramètres, ouvrez Configurations avancées > **Protections** > **Protection en temps réel du système de fichiers** > **Paramètres ThreatSense supplémentaires**.

Autres paramètres ThreatSense pour les fichiers nouveaux et les fichiers modifiés

La probabilité d'infection de fichiers nouveaux ou modifiés est comparativement supérieure à celle de fichiers existants. Pour cette raison, le programme vérifie ces fichiers avec d'autres paramètres d'analyse. ESET NOD32 Antivirus utilise l'heuristique avancée qui détecte les nouvelles menaces avant la mise à disposition de la mise à jour du moteur de détection avec les méthodes d'analyse basées sur les signatures.

Outre les nouveaux fichiers, l'analyse porte également sur les **archives auto-extractibles** (.sfx) et les **fichiers exécutables compressés** (en interne). Par défaut, les archives sont analysées jusqu'au dixième niveau d'imbrication et sont contrôlées indépendamment de leur taille réelle. Pour modifier les paramètres d'analyse d'archive, désactivez **Paramètres d'analyse d'archive par défaut**.

Autres paramètres ThreatSense pour les fichiers exécutés

Heuristique avancée à l'exécution du fichier : Par défaut, l'heuristique avancée est utilisée lorsque des fichiers sont exécutés. Lorsque ce paramètre est activé, il est fortement recommandé de conserver les options Optimisation intelligente et ESET LiveGrid® activées pour limiter l'impact sur les performances système.

Heuristique avancée lors de l'exécution de fichiers à partir de périphériques amovibles : L'heuristique avancée émule le code dans un environnement virtuel et évalue son comportement avant qu'il ne soit autorisé à s'exécuter à partir d'un support amovible.

Outils

Vous pouvez configurer des paramètres avancés pour les fonctionnalités qui offrent une sécurité supplémentaire et simplifient l'administration d'ESET NOD32 Antivirus dans Configurations avancées > **Outils**.

- Microsoft Windows® update
- ESET CMD

- Fichiers journaux
- Mode joueur
- Diagnostics

Microsoft Windows® update

La fonctionnalité Windows Update est un élément important de la protection des utilisateurs contre les logiciels malveillants. C'est pourquoi il est essentiel d'installer les mises à jour de Microsoft Windows dès qu'elles sont disponibles. ESET NOD32 Antivirus vous informe des mises à jour manquantes en fonction du niveau que vous spécifiez dans Configurations avancées > **Outils**. Les niveaux suivants sont disponibles :

- **Pas de mise à jour** – Aucune mise à jour système n'est proposée au téléchargement.
- **Mises à jour optionnelles** – Les mises à jour marquées comme étant faiblement prioritaires et au-dessus sont proposées au téléchargement.
- **Mises à jour recommandées** – Les mises à jour marquées comme étant courantes et au-dessus sont proposées au téléchargement.
- **Mises à jour importantes** – Les mises à jour marquées comme étant importantes et au-dessus sont proposées au téléchargement.
- **Mises à jour critiques** – Seules les mises à jour critiques sont proposées pour le téléchargement.

Boîte de dialogue - Mises à jour système

S'il existe des mises à jour pour votre système d'exploitation, ESET NOD32 Antivirus affiche une notification dans la fenêtre principale du programme > **Vue d'ensemble**. Cliquez sur **Plus d'informations** pour ouvrir la fenêtre des mises à jour système.

La fenêtre Mises à jour système affiche la liste des mises à jour disponibles prêtes pour le téléchargement et l'installation. Le type de mise à jour s'affiche à côté du nom de la mise à jour.

Double-cliquez sur une mise à jour pour afficher la fenêtre Informations sur la mise 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.

Mise à jour les informations

La fenêtre Mises à jour système affiche la liste des mises à jour disponibles prêtes pour le téléchargement et l'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 avec le bouton droit sur une ligne de mise à jour et cliquez sur **Afficher les informations** pour afficher une nouvelle fenêtre comportant des informations supplémentaires.

ESET CMD

Il s'agit d'une fonctionnalité qui permet d'utiliser des commandes ecmd avancées. Elle vous offre la possibilité d'exporter et d'importer des paramètres à l'aide d'une ligne de commande (ecmd.exe). Auparavant, Il n'était possible d'exporter et d'importer des paramètres que dans l'interface utilisateur graphique. La configuration de ESET NOD32 Antivirus peut être exportée dans un fichier *.xml*.

Lorsqu'ESET CMD est activé, deux méthodes d'autorisation sont disponibles :

- **Aucune** : aucune autorisation. Il n'est pas recommandé d'utiliser cette méthode car elle permet l'importation de n'importe quelle configuration non signée, ce qui constitue un risque potentiel.

- **Mot de passe de configuration avancée** : un mot de passe est nécessaire pour importer une configuration à partir d'un fichier .xml devant être signé (reportez-vous à la section relative à la signature d'un fichier de configuration .xml plus bas). Le mot de passe spécifié dans la configuration de l'accès doit être fourni avant l'importation d'une nouvelle configuration. Si la configuration de l'accès n'est pas activée, que le mot de passe ne correspond pas ou que le fichier de configuration .xml n'est pas signé, la configuration n'est pas importée.

Une fois qu'ESET CMD est activé, vous pouvez utiliser la ligne de commande pour exporter ou importer des configurations de ESET NOD32 Antivirus. Vous pouvez le faire manuellement ou créer un script pour l'automatisation.

Pour utiliser les commandes ecmd avancées, vous devez les exécuter avec des privilèges d'administrateur ou ouvrir une invite de commandes Windows (cmd) à l'aide de la commande **Exécuter en tant qu'administrateur**. Si vous ne procédez pas ainsi, le message **Error executing command** s'affiche. Le dossier de destination doit aussi exister lors de l'exportation d'une configuration. La commande d'exportation fonctionne toujours 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 ne peuvent être exécutées que localement.

Signature d'un fichier de configuration *.xml* :

1. Téléchargez le fichier exécutable XmlSignTool.

2. Ouvrez une invite de commandes Windows (cmd) en utilisant **Exécuter en tant qu'administrateur**.

3. Accédez à l'emplacement d'enregistrement du fichier `xmlsigntool.exe`

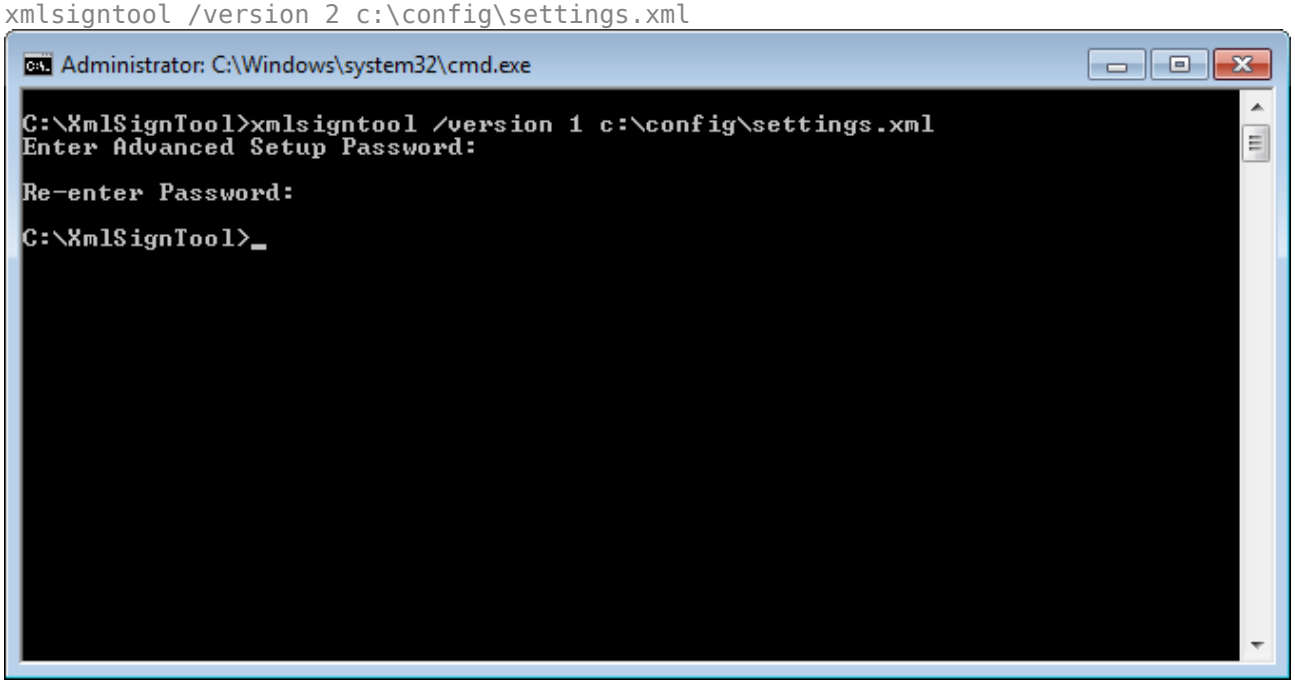
4. Exécutez une commande pour signer le fichier de configuration *.xml* : `xmlsigntool /version 1|2 <xml_file_path>`

La valeur du paramètre `/version` dépend de la version de ESET NOD32 Antivirus. Utilisez `/version 1` pour les versions de ESET NOD32 Antivirus antérieures à la version 11.1. Utilisez `/version 2` pour la version actuelle de ESET NOD32 Antivirus.

5. Lorsque l'utilitaire XmlSignTool vous y invite, saisissez le mot de passe de la configuration avancée et saisissez-le de nouveau. Le fichier de configuration *.xml* est à présent signé. Il peut être utilisé pour importer une autre instance de ESET NOD32 Antivirus avec ESET CMD à l'aide de la méthode d'autorisation du mot de passe.

Commande de signature du fichier de configuration exporté :

```
xmlsigntool /version 2 c:\config\settings.xml
```



Si le mot de passe de la configuration de l'accès change et si vous souhaitez importer une configuration qui a été signée avec un ancien mot de passe, vous devez signer de nouveau le fichier de configuration *.xml* à l'aide du mot de passe actuel. Vous pouvez ainsi utiliser un ancien fichier de configuration sans l'exporter sur un autre ordinateur exécutant ESET NOD32 Antivirus avant l'importation.

Il n'est pas recommandé d'activer ESET CMD sans autorisation, car cela permet l'importation de configuration non signée. Définissez le mot de passe dans Configuration avancée > **Interface utilisateur** > **Configuration de l'accès** pour empêcher toute modification non autorisée par les utilisateurs.

Fichiers journaux

La configuration de la journalisation d'ESET NOD32 Antivirus figure dans Configurations avancées > **Outils** > **Fichiers journaux**. La section des fichiers 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. Les options suivantes peuvent être spécifiées pour les fichiers journaux :

Verbosité minimale des journaux – Spécifie le niveau minimum de verbosité des événements à consigner :

- **Diagnostic** – Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** – Enregistre tous les messages d'information, y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.

- **Avertissements** – Enregistre les erreurs critiques et les messages d'avertissement.
- **Erreurs** – Enregistre les erreurs du type « Erreur de téléchargement du fichier » et les erreurs critiques.
- **Critique** – Répertorie toutes les erreurs critiques (erreur de démarrage de la protection antivirus, etc...).

> Toutes les connexions bloquées sont enregistrées lorsque vous sélectionnez le niveau de verbosité Diagnostic.

Les entrées des journaux plus anciennes que le nombre de jours spécifiés dans le champ **Supprimer automatiquement les entrées plus anciennes que (jours)** seront automatiquement supprimées.

Optimiser automatiquement les fichiers journaux – Si cette option est activée, les fichiers journaux sont automatiquement défragmentés si le pourcentage est supérieur à la valeur spécifiée dans le champ **Si le nombre d'entrées inutilisées dépasse (%)**.

Cliquez sur **Optimiser** pour démarrer la défragmentation des fichiers journaux. Au cours de ce processus, toutes les entrées vides du journal sont supprimées, ce qui améliore les performances et accélère le traitement des journaux. Cette amélioration se constate notamment si les journaux comportent un grand nombre d'entrées.

L'option **Activer le protocole texte** permet d'activer le stockage des journaux dans un autre format de fichier séparé des fichiers journaux :

- **Répertoire cible** – Répertoire dans lequel les fichiers journaux sont stockés (s'applique uniquement aux formats texte/CSV). Chaque section de journal dispose de son propre fichier avec un nom de fichier 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 sont stockés dans un fichier texte dans lequel les données sont séparées par des tabulations. Le même processus s'applique au format de fichier **CSV** (fichier séparé par des virgules). Si vous choisissez **Événement**, les journaux sont stockés dans le journal des événements Windows (qui peut être affiché dans Observateur d'événements accessible à partir du Panneau de configuration) au lieu d'un fichier.
- **Supprimer tous les fichiers journaux** – Efface tous les fichiers journaux sélectionnés dans le menu déroulant **Type**. Une notification indiquant la suppression des journaux s'affiche.

> Pour résoudre les problèmes plus rapidement, ESET peut vous demander de fournir les journaux de votre ordinateur. ESET Log Collector facilite la collecte des informations nécessaires. Pour plus d'informations sur ESET Log Collector, consultez cet article de la base de connaissances ESET.

Mode joueur

Le mode joueur est une fonctionnalité destinée aux utilisateurs qui ne veulent pas être interrompus lors de l'utilisation de leur logiciel. Ils ne souhaitent pas être dérangés par des fenêtres de notification/d'alerte et veulent réduire les contraintes sur l'CPU. Le mode joueur peut également être utilisé au cours de présentations qui ne peuvent pas être interrompues par l'activité antivirus. Lorsque cette fonctionnalité est activée, toutes les fenêtres contextuelles sont désactivées et l'activité du planificateur est complètement arrêtée. La protection du système continue à fonctionner en arrière-plan, mais n'exige aucune interaction de la part de l'utilisateur.

Vous pouvez activer ou désactiver le mode joueur dans la fenêtre principale du programme en cliquant sur

Configuration > **Protection de l'ordinateur**, puis sur  ou  à côté de **Mode joueur**. L'activation du mode joueur constitue un risque potentiel pour la sécurité. C'est la raison pour laquelle l'icône d'état de la protection située dans la barre des tâches devient orange et affiche un symbole d'avertissement. Ce symbole apparaît également dans la fenêtre principale du programme, où **Mode joueur activé** apparaît en orange.

Activez l'option **Activer le mode joueur automatiquement lors de l'exécution d'applications en mode plein écran** dans Configuration avancée > **Outils** > **Mode joueur** pour que le mode joueur démarre dès que vous lancez une application en mode plein écran et s'arrête lorsque vous quittez l'application.

Activez l'option **Désactiver automatiquement le mode joueur après** pour définir une durée après laquelle le mode joueur est automatiquement désactivé.

Diagnostics

L'option Diagnostics fournit un fichier d'image mémoire en cas de défaillance d'une application lors des processus ESET (par exemple ekrn). Dès qu'une application présente une défaillance, un fichier d'image mémoire est généré. Ce fichier permet aux développeurs de déboguer et de résoudre différents ESET NOD32 Antivirus problèmes.

Cliquez sur le menu déroulant en regard de l'option **Type de fichier d'image mémoire**, puis sélectionnez l'une des trois options disponibles :

- Sélectionnez **Désactiver** pour désactiver cette fonctionnalité.
- **Mini** (par défaut) – Enregistre le plus petit ensemble d'informations utiles qui peut permettre d'identifier les raisons de l'arrêt inopiné de l'application. Ce type de fichier d'image mémoire peut être utile lorsque l'espace disponible est limité. Toutefois, en raison des informations limitées qui figurent dans ce fichier, les erreurs qui n'étaient pas directement provoquées par la menace, car cette dernière ne s'exécutait pas au moment du problème, risquent de ne pas être détectées par l'analyse de ce fichier.
- **Complet** – Enregistre tout le contenu de la mémoire système en cas d'arrêt inopiné de l'application. Un fichier d'image mémoire complet peut contenir des données provenant des processus en cours au moment de sa collecte.

Répertoire cible – Répertoire dans lequel est généré le fichier d'image mémoire lors de la défaillance.

Ouvrir le dossier de diagnostics – Cliquez sur **Ouvrir** pour ouvrir ce répertoire dans une nouvelle fenêtre de l'*Explorateur Windows*.

Créer un fichier d'image mémoire de diagnostics – Cliquez sur **Créer** pour créer des fichiers d'image mémoire de diagnostic dans le **répertoire cible**.

Journalisation avancée

Activer la journalisation avancée des messages marketing – Enregistrez tous les événements liés aux messages marketing dans le produit.

Activer la journalisation avancée de l'analyseur de l'ordinateur – Enregistrez tous les événements qui se produisent lors de l'analyse des fichiers et des dossiers par l'analyse de l'ordinateur ou la protection.

Activer la journalisation avancée du contrôle des appareils – Enregistrez tous les événements qui se produisent

dans le contrôle des appareils. Les développeurs peuvent ainsi diagnostiquer et résoudre les problèmes liés au contrôle des appareils.

Activer la journalisation avancée de Direct Cloud – Enregistrez tous les événements qui se produisent dans ESET LiveGrid®. Les développeurs peuvent ainsi diagnostiquer et résoudre les problèmes liés à ESET LiveGrid®.

Activer la journalisation avancée de la protection des documents – Enregistrez tous les événements qui se produisent dans la protection des documents pour permettre un diagnostic et la résolution des problèmes.

Activer la journalisation avancée de la protection du client de messagerie – Enregistrez tous les événements qui se produisent dans la protection du client de messagerie et le module d'extension du client de messagerie pour permettre un diagnostic et la résolution des problèmes.

Activer la journalisation avancée du noyau – Enregistrez tous les événements qui se produisent dans le noyau ESET (ekrn).

Activer la journalisation avancée des licences – Enregistrez toutes les communications du produit avec les serveurs d'activation ESET ou ESET License Manager.

Activer le suivi de la mémoire – Enregistrez tous les événements qui permettent aux développeurs de diagnostiquer les fuites de mémoire.

Activer la journalisation avancée de l'analyseur du trafic réseau : enregistrez toutes les données passant par l'analyseur du trafic réseau au format PCAP pour 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 – Enregistrez des informations supplémentaires sur le système d'exploitation telles que les processus en cours, l'activité de l'UC et les opérations du disque. Celles-ci peuvent aider les développeurs à diagnostiquer et résoudre les problèmes liés au produit ESET s'exécutant sur votre système d'exploitation.

Activer la journalisation avancée des messages Push – Enregistrez tous les événements qui se produisent pendant les messages Push.

Activer la journalisation avancée de la protection en temps réel du système de fichiers – Enregistrez tous les événements qui se produisent lors de l'analyse des fichiers et des dossiers par la protection en temps réel du système de fichiers.

Activer la journalisation avancée du moteur de mise à jour – Enregistrez tous les événements qui se produisent pendant le processus de mise à jour. Les développeurs peuvent ainsi diagnostiquer et résoudre les problèmes liés au moteur de mise à jour.

Les fichiers journaux sont situés dans *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Assistance technique

Lorsque vous contactez l'assistance technique ESET dans ESET NOD32 Antivirus, vous pouvez envoyer les données de configuration système. Sélectionnez **Toujours soumettre** dans le menu déroulant **Soumettre les données de configuration système** pour soumettre automatiquement les données. Vous pouvez également sélectionner **Demander avant soumission** pour que le système vous demande si vous souhaitez soumettre effectivement les données.

Connectivité

Dans des réseaux spécifiques, les communications entre votre ordinateur et Internet peuvent s'effectuer par l'intermédiaire d'un serveur proxy. Si vous utilisez un serveur proxy, vous devez définir les paramètres ci-après. Sinon, ESET NOD32 Antivirus et ses modules ne peuvent pas être mis à jour automatiquement. Dans ESET NOD32 Antivirus, la configuration du serveur proxy est disponible dans deux sections différentes des Configurations avancées.

Les paramètres globaux du serveur proxy peuvent être configurés dans Configurations avancées >**Connectivité** >**Serveur proxy**. La spécification du serveur proxy à ce niveau définit les paramètres de serveur proxy globaux pour l'intégralité d'ESET NOD32 Antivirus. Les paramètres définis ici seront utilisés par tous les modules qui requièrent une connexion à Internet.

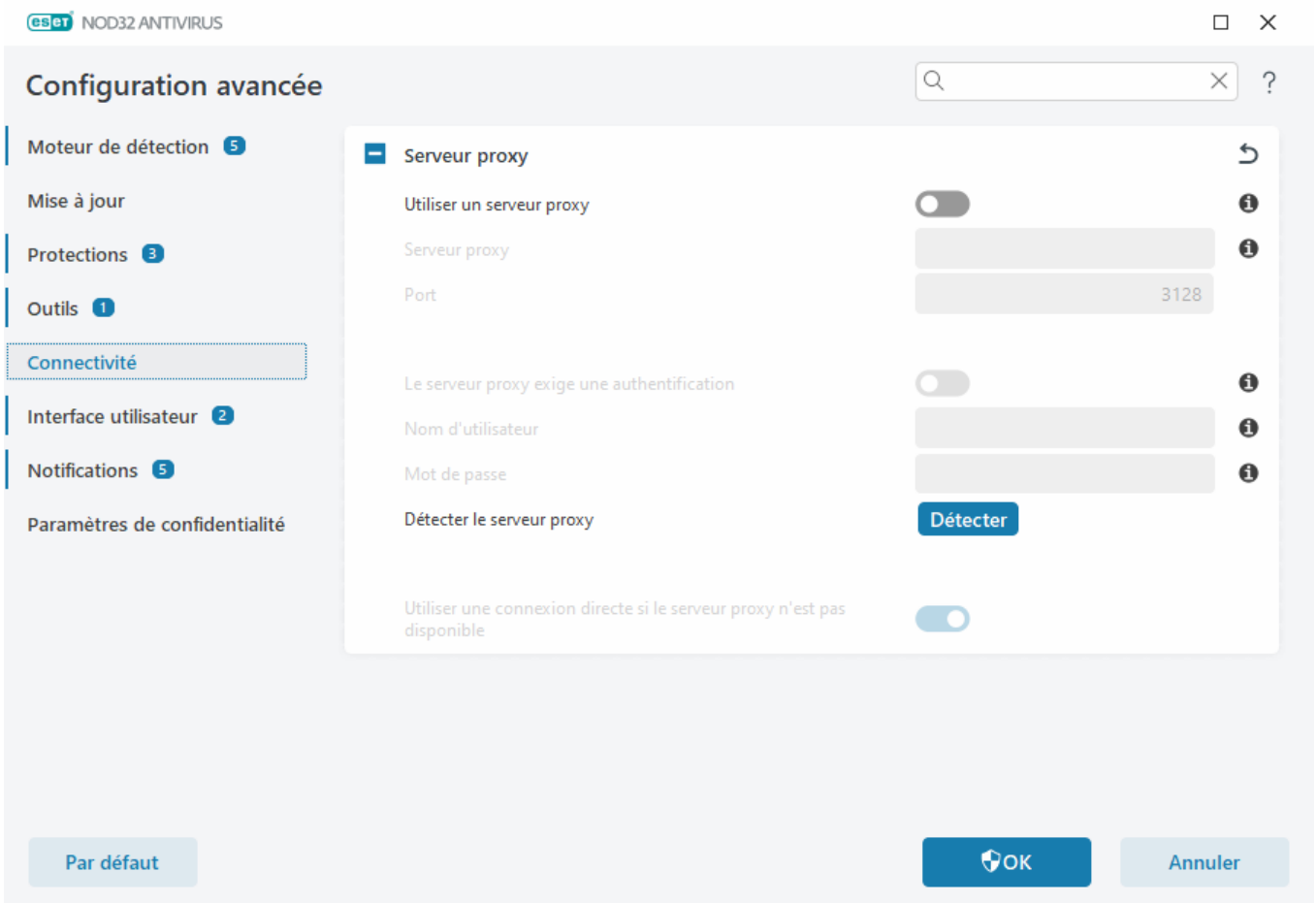
Pour spécifier les paramètres globaux du serveur proxy, activez **Utiliser un serveur proxy** et saisissez l'adresse du **serveur proxy** avec le numéro de **port** du serveur proxy.

Si les communications avec le serveur proxy exigent une authentification, sélectionnez **Le serveur proxy nécessite une authentification** et entrez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants. Cliquez sur **Détecter le serveur proxy** pour détecter et renseigner automatiquement les paramètres du serveur proxy. ESET NOD32 Antivirus copiera les paramètres spécifiés dans les options internet pour Internet Explorer ou Google Chrome.

> Vous devez saisir manuellement votre nom d'utilisateur et votre mot de passe dans les paramètres **Serveur proxy**.

Utiliser une connexion directe si le proxy HTTP n'est pas disponible – Si ESET NOD32 Antivirus est configuré pour se connecter via le proxy et que ce dernier est injoignable, ESET NOD32 Antivirus ignore le proxy et communique directement avec les serveurs ESET.

Les paramètres du serveur proxy peuvent également configurés dans Configurations avancées > **Mise à jour** > **Profils** > **Mises à jour** > **Options de connexion** en sélectionnant **Connexion via un serveur proxy** dans le menu déroulant **Mode proxy**. Cette configuration ne s'applique qu'aux mises à jour et est recommandée pour les ordinateurs portables recevant des mises à jour de modules à partir de sites distants. Pour plus d’informations, consultez Configuration avancée des mises à jour.



Interface utilisateur

Pour configurer le comportement de l'interface utilisateur graphique (GUI) du programme, ouvrez Configurations avancées > **Interface utilisateur**.

Vous pouvez ajuster l'apparence du programme et les effets dans l'écran des configurations avancées Éléments de l'interface utilisateur.

Afin de bénéficier de la sécurité maximum de votre logiciel de sécurité, vous pouvez empêcher toute désinstallation ou 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 adapter l'environnement de travail d'ESET NOD32 Antivirus (GUI) à vos besoins dans Configurations avancées > **Interface utilisateur** > **Éléments de l'interface utilisateur**.

Mode couleur – Sélectionnez le modèle de couleur de l'interface utilisateur graphique ESET NOD32 Antivirus dans le menu déroulant :

- **Identique à la couleur système** – Définit le modèle de couleurs d'ESET NOD32 Antivirus selon les

paramètres du système d'exploitation.

- **Sombre** – ESET NOD32 Antivirus aura un modèle de couleurs foncées (mode sombre).
- **Clair** – ESET NOD32 Antivirus aura un modèle de couleurs clairs standard.

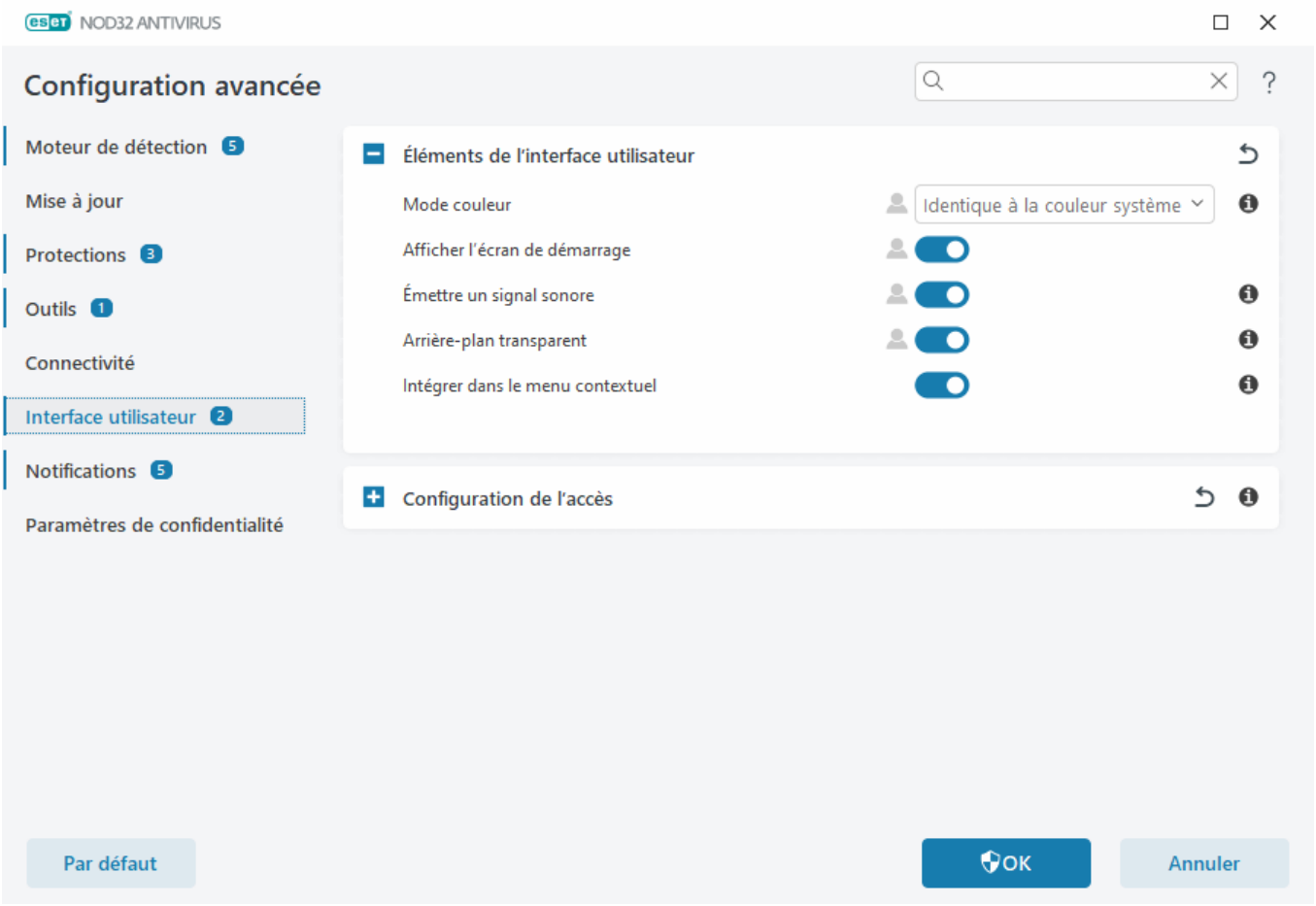
> Vous pouvez également sélectionner le modèle de couleurs de l'interface utilisateur graphique d'ESET NOD32 Antivirus dans le coin supérieur droit de la fenêtre principale du programme.

Afficher l'écran de démarrage – Affiche l'écran de démarrage d'ESET NOD32 Antivirus au démarrage.

Utiliser un signal sonore – émet un signal sonore en cas d'événement important lors d'une analyse, par exemple lorsqu'une menace est découverte ou lorsque l'analyse est terminée.

Arrière-plan transparent – Active un effet d'arrière-plan transparent pour la fenêtre principale du programme. L'arrière-plan transparent n'est disponible que pour les dernières versions de Windows (RS4 et versions ultérieures).

Intégrer dans le menu contextuel – Intègre les options ESET NOD32 Antivirus dans le menu contextuel.



Configuration de l'accès

Les paramètres de ESET NOD32 Antivirus constituent une partie essentielle de votre stratégie de sécurité. Des modifications non autorisées peuvent mettre en danger la stabilité et la protection de votre système. Pour éviter des modifications non autorisées, les paramètres de la configuration d'ESET NOD32 Antivirus peuvent être protégés par mot de passe. La configuration de l'accès peut être définie dans Configurations avancées > **Interface**

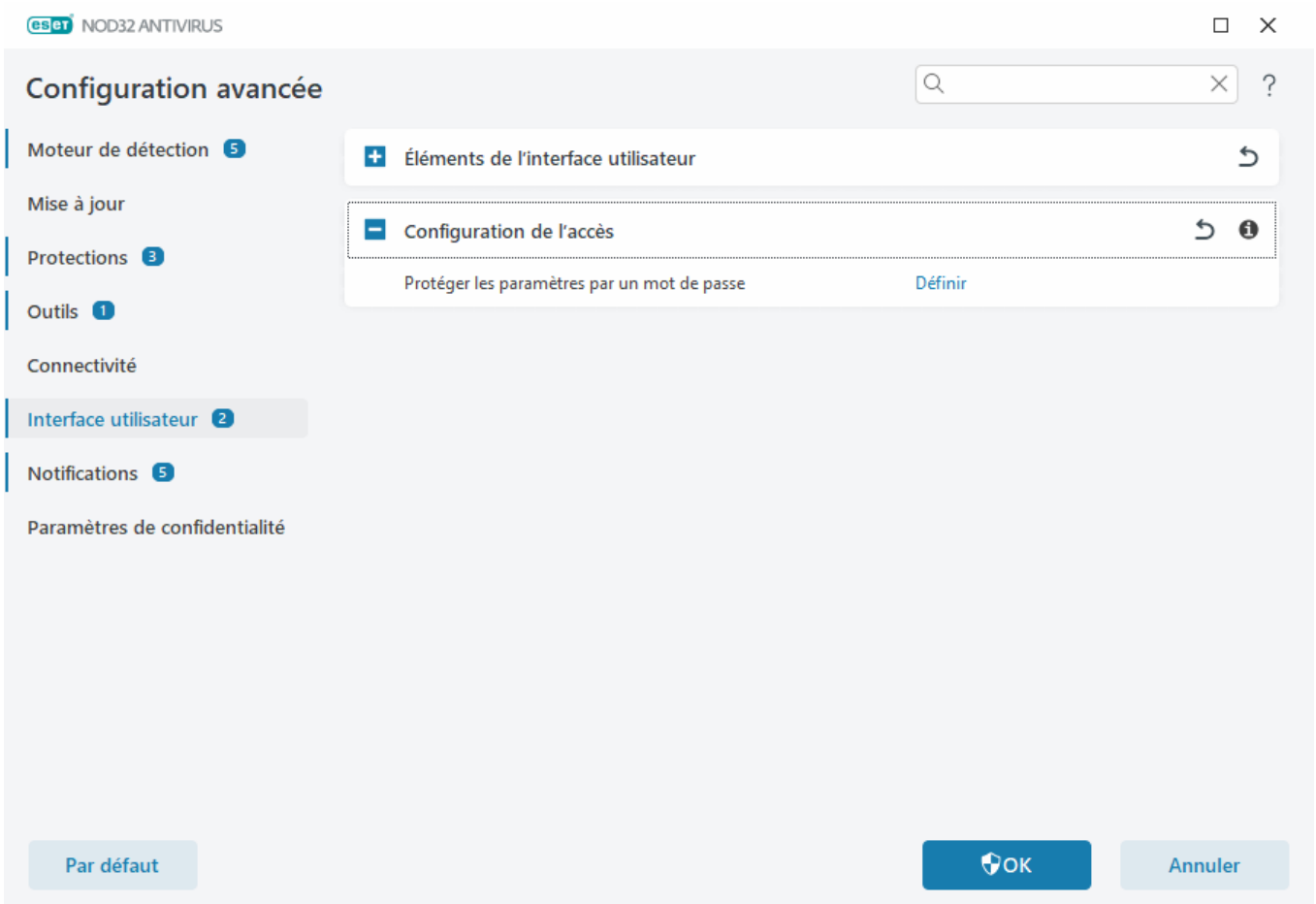
utilisateur > **Configuration de l'accès**.

Pour définir un mot de passe afin de protéger les paramètres de configuration et empêcher la désinstallation d'ESET NOD32 Antivirus, cliquez sur **Définir** en regard de l'option **Protéger les paramètres par un mot de passe**.

> Lorsque vous souhaitez accéder à la configuration avancée protégée, la fenêtre de saisie du mot de passe s'affiche. Si vous avez oublié ou perdu votre mot de passe, cliquez sur l'option **Restaurer le mot de passe** ci-dessous, puis saisissez l'adresse e-mail utilisée pour l'enregistrement de l'abonnement. ESET vous enverra un e-mail contenant le code de vérification et les instructions de réinitialisation de votre mot de passe.
> - Comment déverrouiller la configuration avancée

Pour changer votre mot de passe, cliquez sur **Modifier le mot de passe** en regard de l'option **Protéger les paramètres par mot de passe**.

Pour supprimer votre mot de passe, cliquez sur **Supprimer** en regard de l'option **Protéger les paramètres par mot de passe**.



Mot de passe des configurations avancées

Pour protéger les configurations avancées d'ESET NOD32 Antivirus et éviter toute modification non autorisée, saisissez 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. Saisissez votre ancien mot de passe dans le champ **Ancien mot de passe**.
2. Saisissez le 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 est nécessaire pour accéder aux configurations avancées.

Si vous avez oublié votre mot de passe, consultez l'article Déverrouiller le mot de passe de paramètres dans les produits ESET pour les particuliers.

Pour récupérer votre clé d'activation ESET perdue, la date d'expiration de votre abonnement, ou d'autres informations d'abonnement pour ESET NOD32 Antivirus, consultez J'ai perdu ma clé d'activation.

Prise en charge des lecteurs d’écran

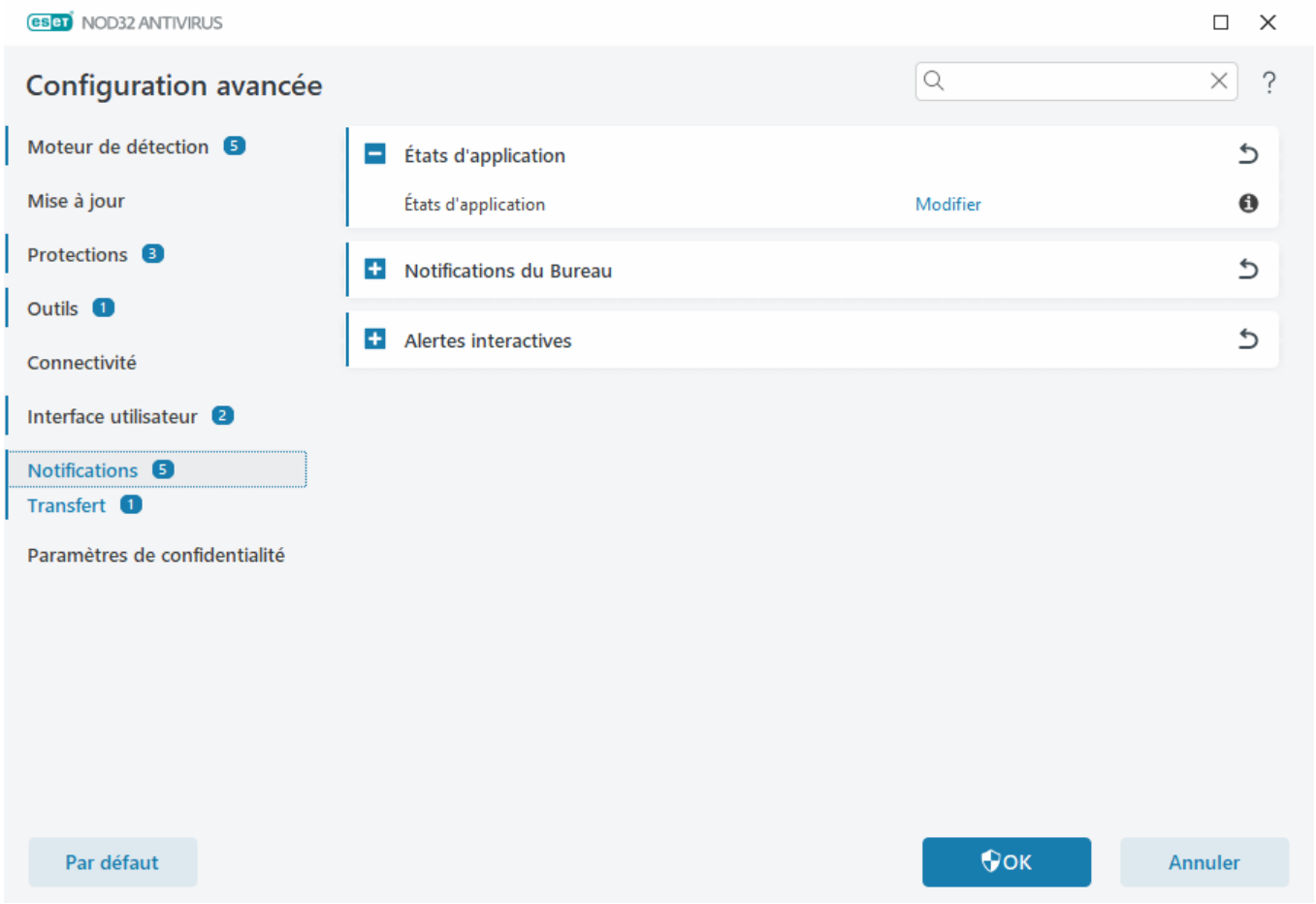
ESET NOD32 Antivirus peut être utilisé avec des lecteurs d’écran pour permettre aux utilisateurs ESET malvoyants de naviguer dans le produit ou de configurer les paramètres. Les lecteurs d’écran suivants sont pris en charge : (JAWS, NVDA, Narrator).

Pour que le logiciel de lecture d’écran puisse accéder correctement à l'interface utilisateur graphique d'ESET NOD32 Antivirus, suivez les instructions de cet article de la base de connaissances.

Notifications

Pour gérer les notifications d'ESET NOD32 Antivirus, ouvrez Configurations avancées > **Notifications**. Vous pouvez configurer les types de notifications suivants :

- États d'application : notifications affichées dans la fenêtre principale du programme > **Vue d'ensemble**.
- Notifications du Bureau : petites notifications en regard 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 e-mail) : sont envoyées à l'adresse e-mail indiquée.



États d'application

États d'application : cliquez sur **Modifier** pour sélectionner les états d'application qui seront affichés dans la section d'accueil de la fenêtre principale du programme > **Vue d'ensemble**.

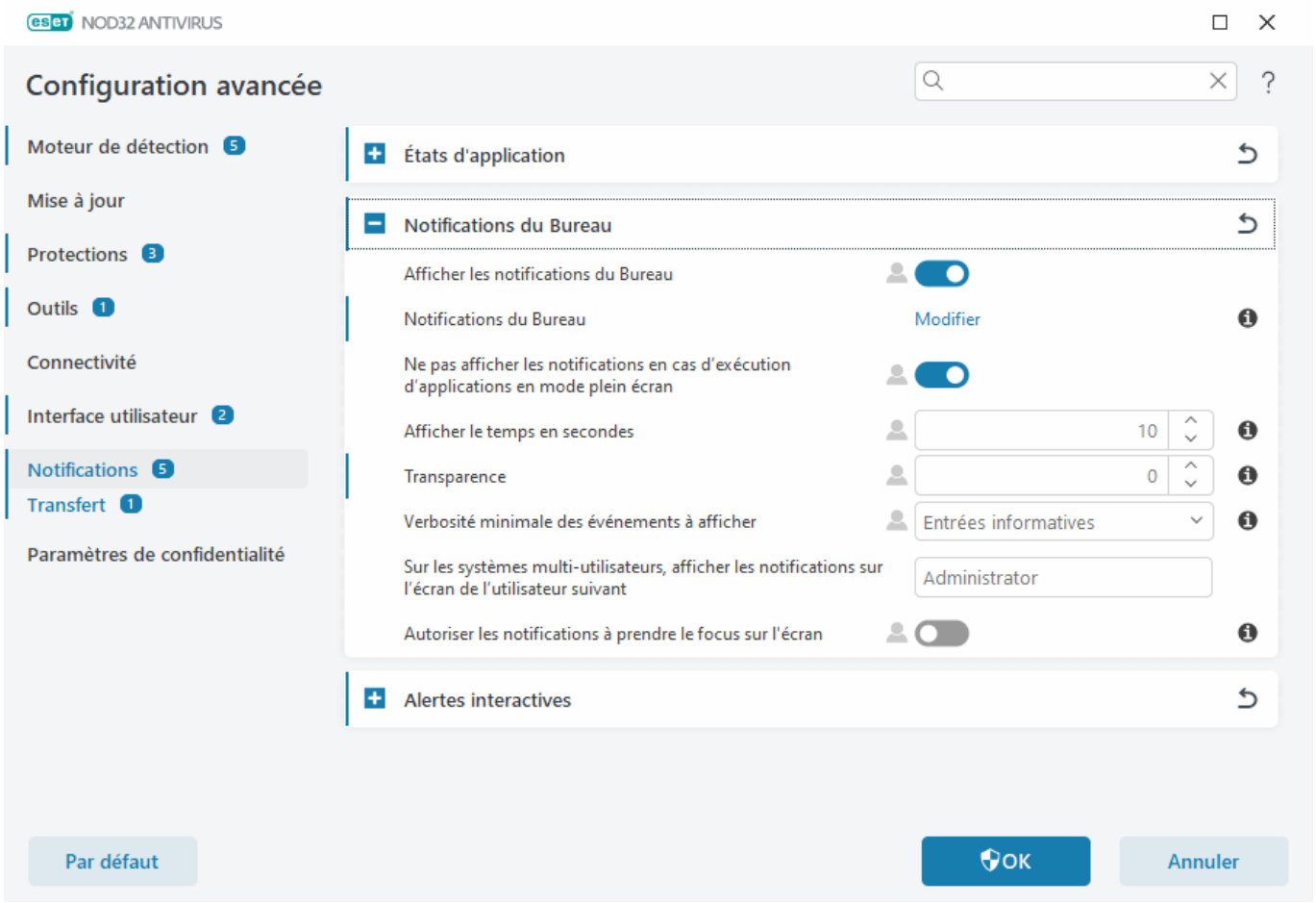
Boîtes de dialogue - États d'application

Cette boîte de dialogue permet de sélectionner les états d'application à afficher. Par exemple lorsque vous suspendez la protection antivirus et antispyware ou lorsque vous activez le mode joueur.

Un état d'application est également affiché si votre produit n'est pas activé ou si votre abonnement est arrivé à expiration.

Notifications du Bureau

Une notification du bureau est une petite fenêtre de notification située à côté de la barre des tâches système. Par défaut, elle est configurée pour s'afficher pendant 10 secondes et disparaître lentement. Les notifications sont les suivantes : mises à jour réussies du produit, nouveaux appareils connectés, achèvement des analyses antivirus ou découverte de nouvelles menaces.



Afficher les notifications sur le Bureau : il est recommandé de laisser cette option activée afin que le produit puisse vous informer lorsqu'un nouvel événement se produit.

Notifications du Bureau : cliquez sur **Modifier** pour activer ou désactiver des Notifications du Bureau spécifiques.

Ne pas afficher les notifications en cas d'exécution d'applications en mode plein écran : supprime toutes les notifications qui ne sont pas interactives lors de l'exécution d'applications en mode plein écran.

Afficher le temps en secondes – Définissez la durée de visibilité de la notification. La valeur doit être entre 3 et 30 secondes.

Transparence – Définissez le pourcentage de transparence de la notification. La plage prise en charge est comprise entre 0 (pas de transparence) et 80 (transparence très élevée).

Verbosité minimale des événements à afficher – Définissez le niveau de gravité de départ des notifications affichées. Dans le menu déroulant, sélectionnez l'une des options suivantes :

- **Diagnostic** – Affiche les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** – Affiche des messages d'information (les événements réseau non standard, par exemple), y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissements** – Affiche les messages d'avertissement, les erreurs et les erreurs critiques (par exemple, l'échec d'une mise à jour).
- **Erreurs** – Affiche les erreurs (par exemple, la protection des documents n'a pas démarré) et les erreurs

critiques.

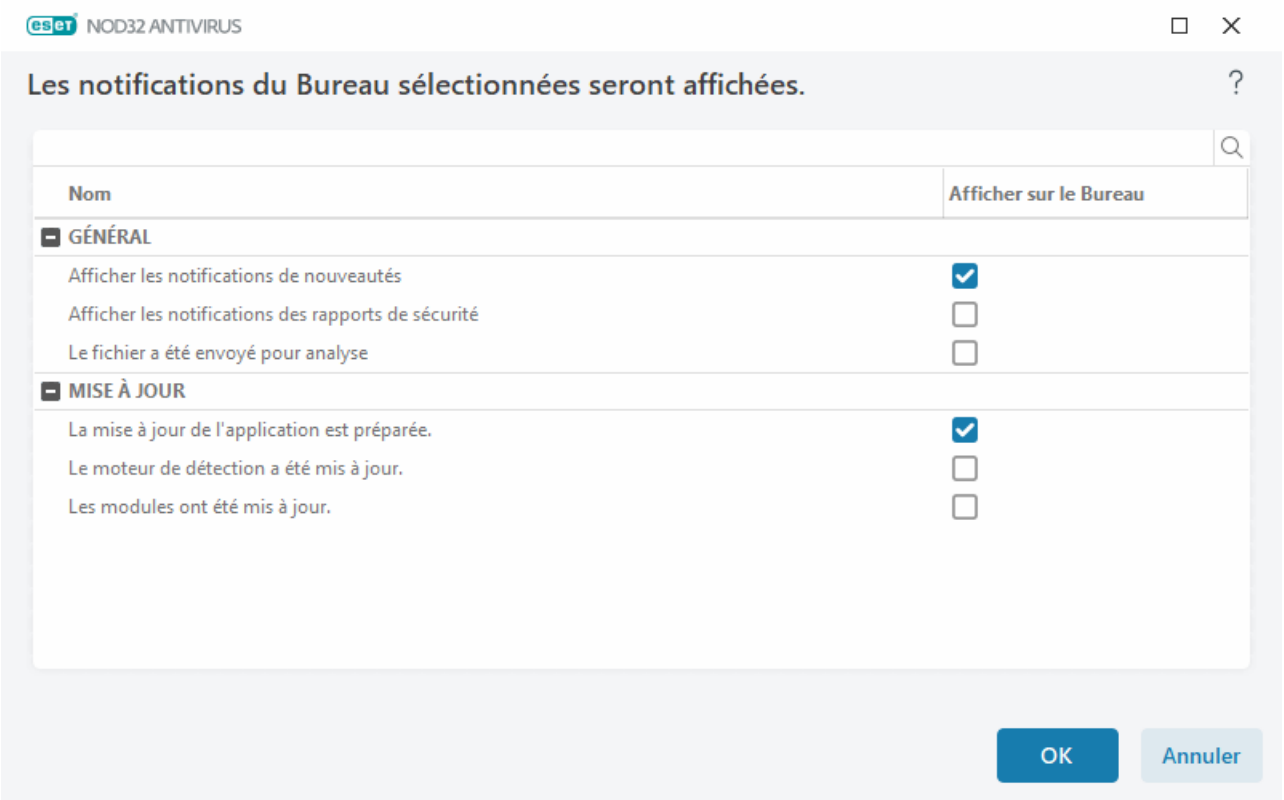
- **Critique** – Affiche uniquement les erreurs critiques (erreur de démarrage de la protection antivirus, système infecté, etc.).

Sur les systèmes multi-utilisateurs, afficher les notifications sur l'écran de l'utilisateur suivant – Permet au compte sélectionné de recevoir des notifications sur le Bureau. Par exemple, si vous n'utilisez pas le compte Administrateur, saisissez le nom complet du compte pour que les notifications du Bureau s'affichent pour ce compte. Seul un compte d'utilisateur peut recevoir les notifications sur le Bureau.

Autoriser les notifications à prendre le focus sur l'écran – Permet aux notifications de prendre le focus sur l'écran et d'être accessibles dans le menu **ALT + Tab**.

Liste des notifications du Bureau

Pour régler la visibilité des notifications du Bureau (affichées en bas à droite de l'écran), ouvrez les Configurations avancées > **Notifications** > **Notifications du Bureau**. Cliquez sur **Modifier** en regard de **Notifications du Bureau**, puis cochez la case **Afficher** appropriée.



Général

Afficher les notifications des rapports de sécurité : recevez une notification lorsqu'un nouveau rapport sur la sécurité est généré.

Afficher les notifications de nouveautés : notifications à propos de toutes les fonctionnalités nouvelles et améliorées de la dernière version du produit.

Le fichier a été envoyé pour analyse : recevez une notification chaque fois qu'ESET NOD32 Antivirus envoie un fichier pour analyse.

Inspecteur de réseau

Avertir lors de la détection de nouveaux appareils réseau : recevez une notification lorsqu'un nouvel appareil est connecté au réseau.

Protection du réseau

Profil de réseau modifié : recevez une notification lorsque le profil réseau est modifié.

Avertissements liés à la protection WiFi : recevez une notification lorsque vous essayez de vous connecter à un réseau Wi-Fi avec un mot de passe non complexe ou inexistant.

Mettre à jour

La mise à jour de l'application est préparée : recevez une notification lorsqu'une mise à jour vers une nouvelle version d'ESET NOD32 Antivirus est préparée.

Le moteur de détection a été mis à jour : recevez une notification lorsque le produit met à jour les modules du moteur de détection.

Modules correctement mis à jour : recevez une notification lorsque le produit met à jour les composants du programme.

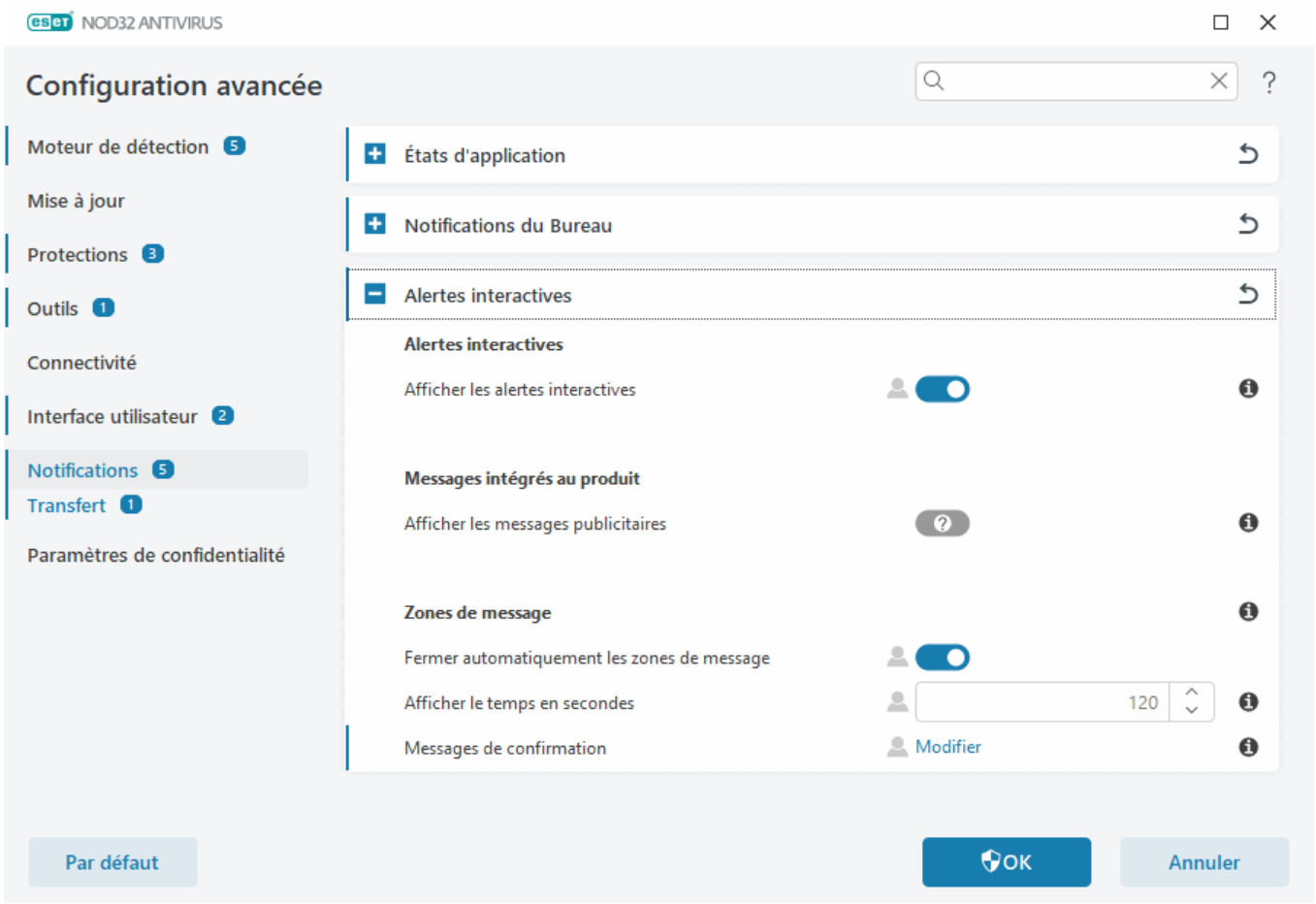
Pour définir les configurations générales des notifications sur le bureau, par exemple, la durée d'affichage d'un message ou la verbosité minimale des événements à afficher, accédez à Notifications du Bureau dans Configurations avancées > **Notifications**.

Alertes interactives

Vous recherchez des informations sur les alertes et les notifications courantes ?

- Menace détectée
- L'adresse a été bloquée.
- Produit non activé
- Passez à un produit avec des fonctionnalités supplémentaires
- Passez à un produit avec moins de fonctionnalités
- Une mise à jour est disponible
- Les informations de mise à jour ne sont pas cohérentes
- Résolution du message « Échec de la mise à jour des modules »
- Résoudre les erreurs de mise à jour des modules
- Certificat du site Web révoqué

La section **Alertes interactives** dans Configurations avancées > **Notifications** vous permet de configurer la manière dont ESET NOD32 Antivirus traite les boîtes de message et les alertes interactives pour les détections pour lesquelles une décision doit être prise par un utilisateur (par exemple, un site web d'hameçonnage potentiel).



Alertes interactives

Lorsque l'option **Afficher les alertes interactives** est désactivée, toutes les fenêtres et les boîtes de dialogue dans le navigateur sont masquées, ce qui ne convient qu'à un nombre limité de situations particulières. Nous recommandons de conserver cette option activée.

Messages intégrés au produit

Les messages intégrés au produit ont été conçus pour informer les utilisateurs des actualités et autres communications d'ESET. L'envoi de messages marketing nécessite le consentement de l'utilisateur. Par conséquent, les messages marketing ne sont pas envoyés à un utilisateur par défaut (affiché sous la forme d'un point d'interrogation). En activant cette option, vous acceptez de recevoir des messages marketing de la part d'ESET. Si vous ne souhaitez pas **recevoir de documents marketing ESET**, désactivez l'option.

Zones de message

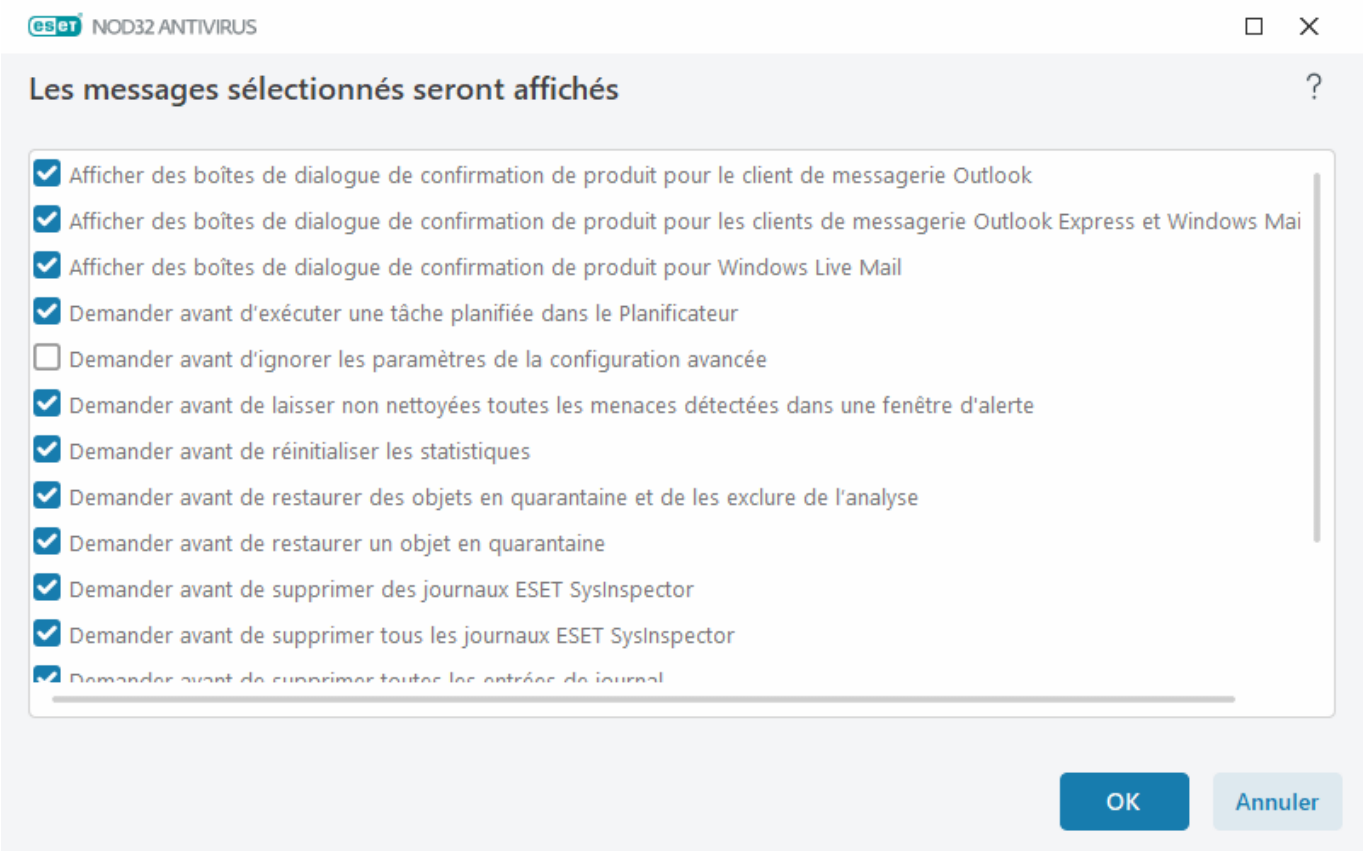
Pour fermer automatiquement les boîtes de message après un certain délai, sélectionnez **Fermer automatiquement les zones de message**. Si les fenêtres d'alerte ne sont pas fermées manuellement, le système les ferme automatiquement une fois le laps de temps écoulé.

Afficher le temps en secondes – Définit la durée de visibilité de l'alerte. La valeur doit être 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 non.

Messages de confirmation

Pour régler les messages de confirmation, accédez à Configurations avancées > **Notifications** > **Alertes interactives**, puis cliquez sur **Modifier** en regard de **Messages de confirmation**.



Cette boîte de dialogue contient les messages de confirmation qu'ESET NOD32 Antivirus affiche avant l'exécution de toute action. Activez ou désactivez la case à cocher en regard de chaque message de confirmation pour l'activer ou non.

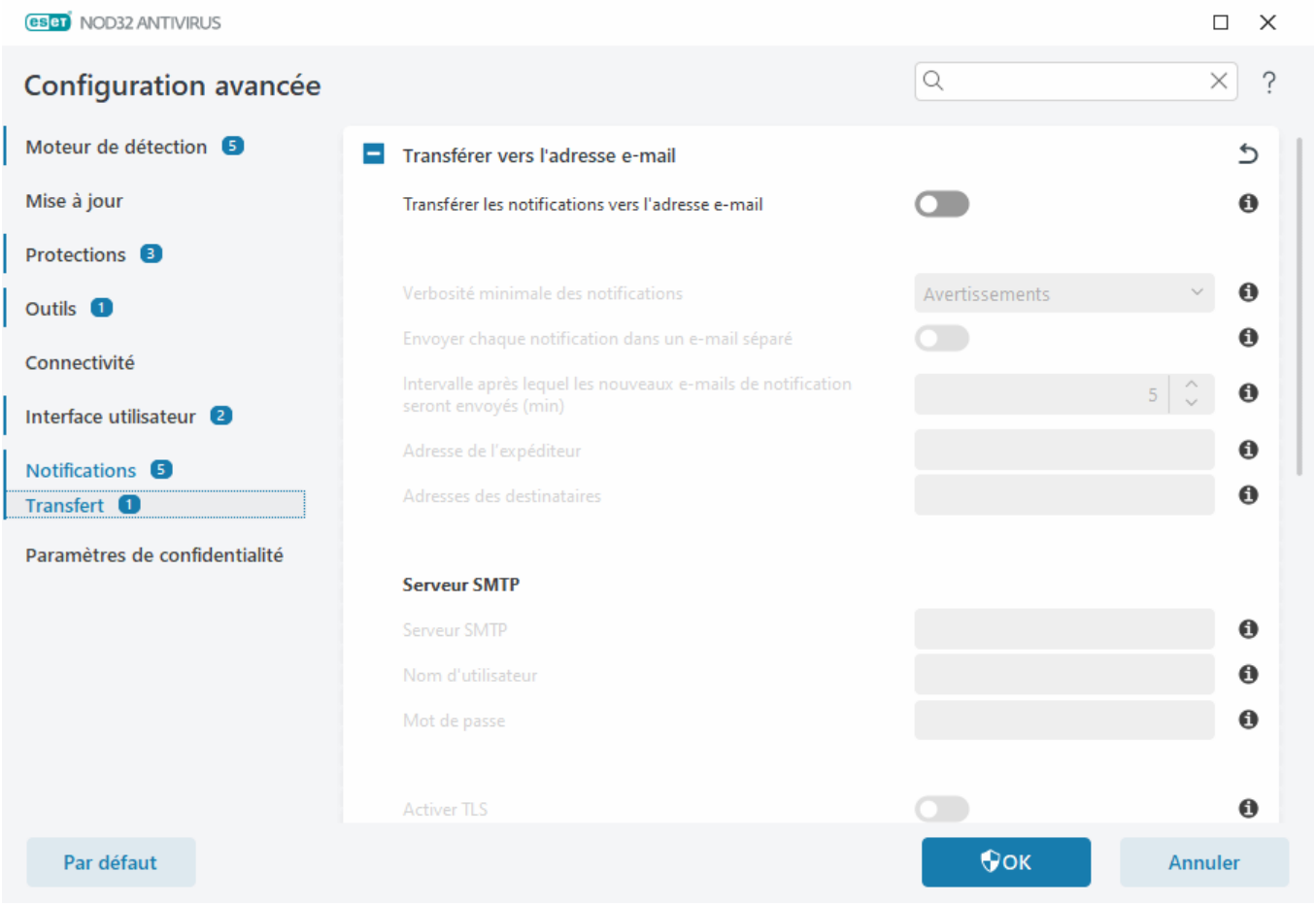
Découvrez la fonctionnalité spécifique liée aux messages de confirmation :

- Demander avant de supprimer les journaux ESET SysInspector
- Demander avant de supprimer tous les journaux ESET SysInspector
- Demander avant de supprimer un objet de quarantaine
- Demander avant d’ignorer les paramètres de la configuration avancée
- Demander avant de laisser non nettoyées toutes les menaces détectées dans une fenêtre d'alerte
- 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 des boîtes de dialogue de confirmation de produit pour les clients de messagerie Outlook Express et Windows Mail
- Afficher des boîtes de dialogue de confirmation de produit pour Windows Live Mail
- Afficher des boîtes de dialogue de confirmation de produit pour le client de messagerie Outlook

Transfert

ESET NOD32 Antivirus peut automatiquement envoyer des e-mails de notification si un événement avec le niveau de verbosité sélectionné se produit. Ouvrez les configurations avancées > **Notifications** > **Transfert** et activez **Transférer les notifications vers l'adresse e-mail** pour activer les notifications par e-mail.



Dans le menu déroulant **Verbosité minimale des notifications**, vous pouvez sélectionner le niveau de gravité de départ des notifications à envoyer.

- **Diagnostic** – Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** – Enregistre tous les messages d'information (les événements réseau non standard,

par exemple), y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.

• **Avertissements** – Enregistre les erreurs critiques et les messages d'avertissement (par exemple, l'échec d'une mise à jour).

• **Erreurs** – Enregistre les erreurs (la protection des documents n'a pas démarré) et les erreurs critiques.

• **Critique** – Enregistre uniquement les erreurs critiques (erreur de démarrage de la protection antivirus ou menace détectée, par exemple).

Envoyer chaque notification dans un e-mail séparé – Lorsque cette option est activée, le destinataire recevra un nouvel e-mail pour chaque notification. Cela peut se traduire par la réception de nombreux e-mails dans une courte période.

Intervalle après lequel les nouveaux e-mails de notification seront envoyés (min) – Intervalle en minutes après lequel de nouvelles notifications seront envoyées par e-mail. Si vous définissez cette valeur sur 0, les notifications sont envoyées immédiatement.

Adresse de l'expéditeur – Définit l'adresse de l'expéditeur qui apparaît dans l'en-tête des notifications.

Adresses des destinataires – Définit les adresses des destinataires qui apparaissent dans l'en-tête des notifications. Plusieurs valeurs sont prises en charge. Utilisez un point-virgule comme séparateur.

SMTP server

Serveur SMTP – Serveur SMTP utilisé pour envoyer des notifications (smtp.provider.com:587, le port prédéfini est le port 25).

Les serveurs SMTP avec chiffrement TLS sont pris en charge par ESET NOD32 Antivirus.

Nom d'utilisateur et **mot de passe** – Si le serveur SMTP exige une authentification, ces champs doivent être remplis avec un nom d'utilisateur et un mot de passe valides donnant accès au serveur SMTP.

Activer TLS – Alerte de sécurité et notifications utilisant le chiffrement TLS.

Tester la connexion SMTP – Un e-mail de test sera envoyé à l'adresse e-mail du destinataire. Le serveur SMTP, le nom d'utilisateur, le mot de passe, l'adresse de l'expéditeur et les adresses des destinataires doivent être renseignés.

Format des messages

Les communications entre le programme et l'utilisateur ou l'administrateur système distants se font via 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'événement qui s'affichent sur les ordinateurs distants.

Format des messages d'avertissement de menace – Messages d'alerte et de notification de menace dont le format par défaut est prédéfini. Nous recommandons de conserver ce format prédéfini. Toutefois, dans certaines

circonstances (par exemple, si vous avez un système automatisé de traitement des messages), vous serez peut-être amené à modifier le format des messages.

Jeu de caractères – Convertit un e-mail en codage ANSI sur la base des paramètres régionaux de Windows (windows-1250, Unicode (UTF-8), ACSII 7-bit ou (ISO-2022-JP) japonais). Ainsi, "á" sera remplacé par "a" et un symbole inconnu par "?".

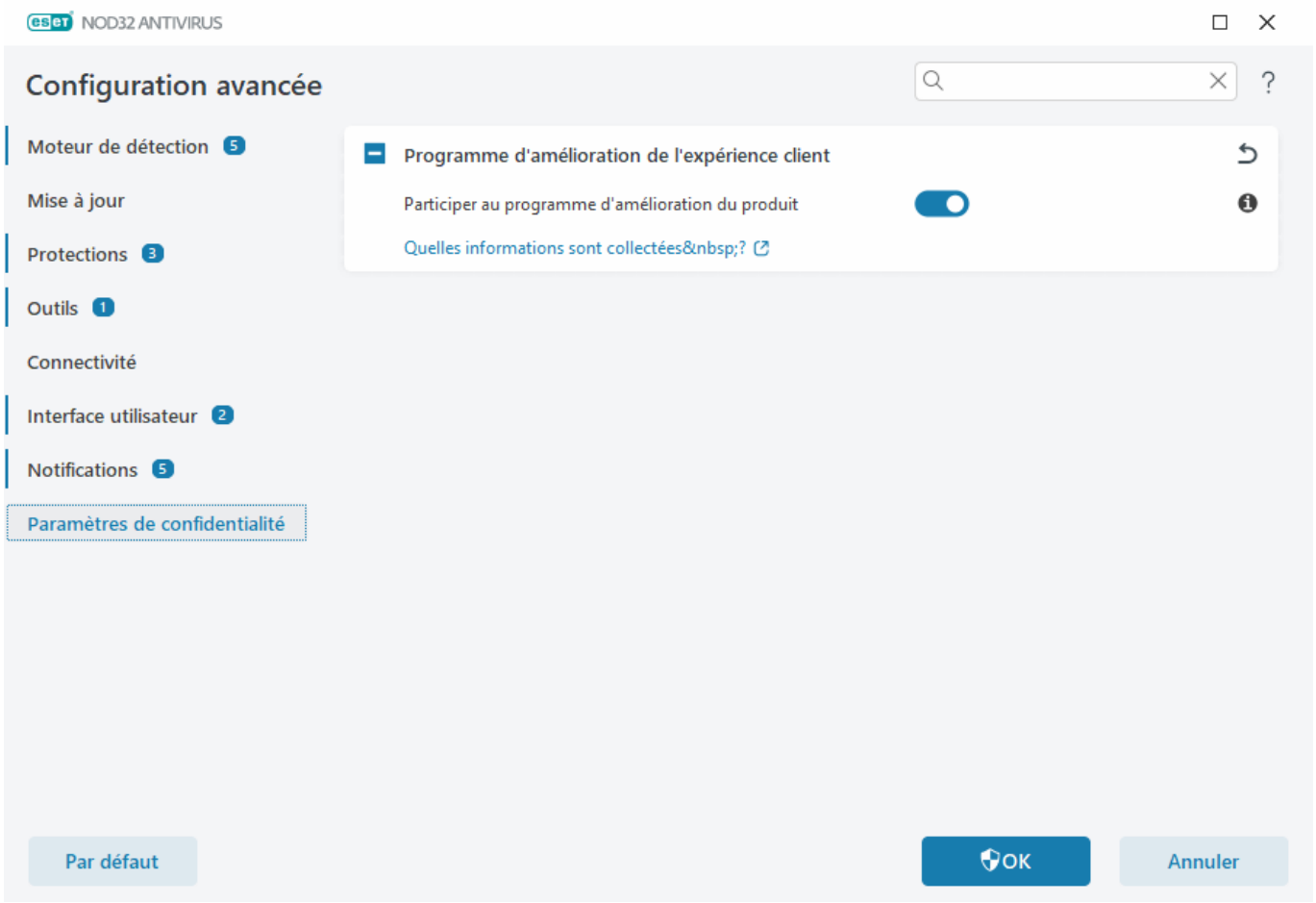
Utiliser l'encodage Quoted-printable – Le message électronique source est codé au format Quoted-printable (QP) qui utilise les caractères ASCII et peut correctement transmettre les caractères spéciaux par e-mail au format 8 bits (áéíóú).

- **%TimeStamp%** – Date et heure de l'événement
- **%Scanner%** – Module concerné
- **%ComputerName%** – Nom de l'ordinateur sur lequel l'alerte s'est produite
- **%ProgramName%** – Programme ayant généré l'alerte
- **%InfectedObject%** – Nom du fichier, message infecté, etc.
- **%VirusName%** – Identification de l'infection
- **%Action%** – Action exécutée sur 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 Configurations avancées > **Paramètres de confidentialité**.



Programme d\'amélioration du produit

Pour rejoindre le programme d'amélioration du produit, activez le bouton bascule en regard de l'option **Participer au programme d'amélioration du produit**. En participant à ce programme, vous fournissez à ESET des informations anonymes relatives à l'utilisation des produits ESET. Les données collectées permettent à ESET d'améliorer votre expérience. Elles ne seront jamais partagées avec des tiers. Quelles informations sont collectées ?

Rétablir les paramètres par défaut

Pour rétablir tous les paramètres du programme, pour tous les modules, cliquez sur **Par défaut** dans les Configurations avancées. Ils sont rétablis dans l'état qu'ils auraient après une nouvelle installation.

Consultez également Importer et exporter les paramètres.

Rétablir tous les paramètres de la section actuelle

Cliquez sur la flèche courbée pour rétablir les paramètres par défaut définis par ESET de tous les paramètres de la section actuelle.

Notez que les modifications apportées après avoir cliqué sur **Rétablir les paramètres par défaut** sont perdues.

Rétablir le contenu des tables – Lorsque cette option est activée, les tâches ou les profils ajoutés automatiquement ou manuellement sont perdus.

Consultez également Importer et exporter les paramètres.

Erreur lors de l’enregistrement de la configuration

Ce message d'erreur indique que, à la suite 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 :

- possède des droits d'accès insuffisants ou ne dispose pas des privilèges nécessaires du système d'exploitation pour modifier les fichiers de configuration et le registre du système.
  > Pour apporter 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 aux Configurations avancées.
  > Pour enregistrer la configuration et éviter tout conflit de configuration, fermez les Configurations avancées sans procéder à l'enregistrement et réessayez d'apporter les modifications souhaitées.

Sinon, il est également possible que le programme ne fonctionne plus correctement, qu'il soit endommagé et qu'il doive donc être réinstallé.

Analyseur de ligne de commande

Le module antivirus d'ESET NOD32 Antivirus peut être lancé depuis la ligne de commande, manuellement (avec la commande « ecls ») ou au moyen d'un fichier de commandes (« bat »).

Utilisation de l’analyseur de ligne de commande ESET :

```
ecls [OPTIONS..] FILES..
```

Les paramètres suivants peuvent être utilisés lors de l'exécution de l'analyseur à la demande, à partir de la ligne de commande :

Options

/base-dir=DOSSIER	charger les modules depuis le DOSSIER
/quar-dir=DOSSIER	DOSSIER de quarantaine
/exclude=MASK	exclure les fichiers correspondant à MASQUE de l'analyse
/subdir	analyser les sous-dossiers (valeur par défaut)
/no-subdir	ne pas analyser les sous-dossiers
/max-subdir-level=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	journaliser les résultats dans un FICHIER
/log-rewrite	écraser le fichier de résultats (valeur par défaut – append)

/log-console	journaliser les résultats sur la console (valeur par défaut)
/no-log-console	ne pas journaliser les résultats sur la console
/log-all	journaliser également les fichiers nettoyés
/no-log-all	ne pas journaliser les fichiers nettoyés (valeur par défaut)
/aind	afficher l'indicateur d'activité
/auto	analyser et nettoyer automatiquement tous les disques locaux

Options de l'analyseur

/files	analyser les fichiers (valeur par défaut)
/no-files	ne pas analyser les fichiers
/memory	analyser la mémoire
/boots	analyser les secteurs d'amorçage
/no-boots	ne pas analyser les secteurs d'amorçage (valeur par défaut)
/arch	analyser les archives (valeur par défaut)
/no-arch	ne pas analyser les archives
/max-obj-size=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 auto-extractible que s'ils sont plus petits que TAILLE Mo (valeur par défaut 0 = illimité)
/mail	analyser les fichiers des courriers électroniques (valeur par défaut)
/no-mail	ne pas analyser les fichiers des courriers électroniques
/mailbox	analyser les boîtes aux lettres (valeur par défaut)
/no-mailbox	ne pas analyser les boîtes aux lettres
/sfx	analyser les archives auto-extractibles (valeur par défaut)
/no-sfx	ne pas analyser les archives auto-extractibles
/rtp	analyser les fichiers exécutables compressés par un compresseur d'exécutables (valeur par défaut)
/no-rtp	ne pas analyser les fichiers exécutables compressés
/unsafe	rechercher les applications potentiellement dangereuses
/no-unsafe	ne pas rechercher les applications potentiellement dangereuses (valeur par défaut)
/unwanted	rechercher les applications potentiellement indésirables
/no-unwanted	ne pas rechercher les applications potentiellement indésirables (valeur par défaut)
/suspicious	rechercher les applications suspectes (valeur par défaut)
/no-suspicious	ne pas rechercher les applications suspectes
/pattern	utiliser les signatures (valeur par défaut)
/no-pattern	ne pas utiliser les signatures
/heur	activer l'heuristique (valeur par défaut)

/no-heur	désactiver l'heuristique
/adv-heur	activer l'heuristique avancée (valeur par défaut)
/no-adv-heur	désactiver l'heuristique avancée
/ext-exclude=EXTENSIONS	exclure de l'analyse les EXTENSIONS de fichier délimitées par deux-points
/clean-mode=MODE	utiliser le MODE de nettoyage pour les objets infectés Les options disponibles sont les suivantes : • `none` (par défaut) – Aucun nettoyage automatique ne se produit. • `standard` – ecls.exe tente automatiquement de nettoyer ou de supprimer les fichiers infectés. • `nettoyage strict` – ecls.exe tente automatiquement de nettoyer ou de supprimer les fichiers infectés sans intervention de l'utilisateur (vous ne recevez pas d'invite avant la suppression des fichiers). • `nettoyage rigoureux` – ecls.exe supprime les fichiers sans tenter de les nettoyer, quel que soit leur type. • `suppression` – ecls.exe supprime les fichiers sans tenter de les nettoyer, mais s'abstient de supprimer les fichiers sensibles tels que les fichiers système de Windows.
/quarantine	copier les fichiers infectés (si nettoyés) vers Quarantaine (complète l'action effectuée lors du nettoyage)
/no-quarantine	ne pas copier les fichiers infectés vers Quarantaine

Options générales

/help	afficher l'aide et quitter
/version	afficher les informations de version et quitter
/preserve-time	conserver la date et l'heure du dernier accès

Codes de sortie

0	aucune menace détectée
1	menace détectée et nettoyée
10	certains fichiers n'ont pas pu être analysés (peuvent être des menaces)
50	menace détectée
100	erreur

Un code sortie supérieur à 100 signale un fichier non analysé qui est potentiellement infecté.

FAQ

Vous trouverez ci-dessous les questions et les problèmes les plus fréquents. Cliquez sur l'intitulé d'une rubrique pour savoir comment résoudre le problème :

- Comment mise à jour ESET NOD32 Antivirus
- ESET NOD32 Antivirus a détecté une menace

- Comment éliminer un virus de mon PC
- Comment créer une tâche dans le Planificateur
- Comment planifier une tâche d'analyse (hebdomadaire)
- Comment déverrouiller la configuration avancée
- Comment résoudre les problèmes liés à la désactivation du produit depuis ESET HOME

Si votre problème n'est pas abordé dans la liste ci-dessus, consultez l'aide en ligne d'ESET NOD32 Antivirus.

Si vous ne trouvez pas une solution à votre problème/question dans l'aide en ligne d'ESET NOD32 Antivirus, vous pouvez consulter notre base de connaissances ESET en ligne qui est régulièrement mise à jour. Des liens vers les articles les plus populaires de notre base de connaissances sont répertoriés ci-dessous :

- Comment renouveler mon abonnement ?
- J'ai reçu un message d'erreur d'activation pendant l'installation de mon produit ESET. Qu'est-ce que cela signifie ?
- Activer mon produit ESET Windows pour les particuliers à l'aide de la clé d'activation
- Désinstaller ou réinstaller mon produit ESET pour les particuliers
- Un message m'indique que l'installation de mon produit ESET s'est terminée prématurément.
- Que dois-je faire après avoir renouvelé ma abonnement ? (utilisateurs de la version familiale)
- Que faire si je change d'adresse de messagerie ?
- Transférer mon produit ESET vers un nouvel ordinateur ou appareil
- Comment démarrer Windows en mode sans échec ou en mode sans échec avec réseau
- Exclure un site web fiable du blocage
- Autoriser l'accès des lecteurs d'écran à l'interface utilisateur graphique d'ESET

Au besoin, vous pouvez contacter notre support technique pour soumettre vos questions ou problèmes.

Comment mise à jour ESET NOD32 Antivirus

La mise à jour de ESET NOD32 Antivirus peut être effectuée manuellement ou automatiquement. Pour déclencher la mise à jour, cliquez sur **Mise à jour** dans la fenêtre principale du programme, puis sur **Rechercher des mises à jour**.

Les paramètres d'installation par défaut créent une tâche de mise à jour automatique qui s'exécute chaque heure. Pour changer l'intervalle, accédez à **Outils** > Planificateur.

Comment éliminer un virus de mon PC

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

1. Dans la fenêtre principale du programme, cliquez sur **Analyse de l'ordinateur**.

2. Cliquez sur **Analyse intelligente** pour démarrer l'analyse de votre système.

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

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

Pour plus d'informations, voir :

- Article de la base de connaissances ESET
- Quarantaine

Comment créer une tâche dans le Planificateur

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

- **Exécuter une application externe** – Permet de programmer l'exécution d'une application externe.
- **Maintenance des journaux** – Les fichiers journaux contiennent également des éléments provenant d'enregistrements supprimés. Cette tâche optimise régulièrement les entrées des fichiers journaux pour garantir leur efficacité.
- **Contrôle des fichiers de démarrage du système** – Vérifie les fichiers autorisés à s'exécuter au démarrage du système ou lors de l'ouverture de session de l'utilisateur.
- **Créer un rapport de l'état de l'ordinateur** – Crée un instantané ESET SysInspector de l'ordinateur et collecte des informations détaillées sur les composants système (pilotes, applications) et évalue le niveau de risque de chacun de ces composants.
- **Analyse de l'ordinateur à la demande** – Effectue une analyse des fichiers et des dossiers de votre ordinateur.
- **Mise à jour** – Planifie une tâche de mise à jour en mettant à jour les modules.

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

Dans le menu déroulant **Tâche planifiée**, sélectionnez **Mise à jour**. Saisissez le nom de la tâche dans le champ **Nom de la tâche**, puis cliquez sur **Suivant**. Sélectionnez la fréquence de la tâche. Les options disponibles sont les suivantes : **Une fois**, **Plusieurs fois**, **Quotidienne**, **Hebdomadaire** et **Déclenchée par un événement**. Sélectionnez

Ignorer la tâche en cas d'alimentation par batterie pour diminuer les ressources système lorsque l'ordinateur portable fonctionne sur batterie. Cette tâche est exécutée à l'heure et au jour spécifiées dans les champs **Exécution de tâche**. Vous pouvez définir ensuite l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée. Les options disponibles sont les suivantes :

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

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

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

Comment programmer une analyse hebdomadaire de l'ordinateur

Pour planifier une tâche régulière, ouvrez la fenêtre principale du programme et cliquez sur **Outils** > **Planificateur**. Vous trouverez ci-dessous un guide abrégé indiquant comment planifier une tâche qui analyse les disques locaux toutes les semaines. Consultez notre article de base de connaissances pour obtenir des instructions plus détaillées.

Pour programmer une tâche d'analyse :

1. Cliquez sur **Ajouter** dans l'écran principal du planificateur.
2. Saisissez un nom pour la tâche, puis sélectionnez **Analyse de l'ordinateur à la demande** dans le menu déroulant **Type de tâche**.
3. Sélectionnez **Hebdomadaire** comme fréquence de tâche.
4. Choisissez le jour et l'heure d'exécution de la tâche.
5. Sélectionnez **Exécuter la tâche dès que possible** pour exécuter la tâche plus tard si la tâche programmée ne s'exécute pas pour quelque raison que ce soit (par exemple, si l'ordinateur a été mis hors tension).
6. Passez en revue le résumé de la tâche planifiée, puis cliquez sur **Terminer**.
7. Dans le menu déroulant **Cibles**, sélectionnez **Lecteurs locaux**.
8. Cliquez sur **Terminer** pour appliquer la tâche.

Comment déverrouiller la configuration avancée protégée par mot de passe

Lorsque vous souhaitez accéder à la configuration avancée protégée, la fenêtre de saisie du mot de passe s'affiche. Si vous avez oublié ou perdu votre mot de passe, cliquez sur **Restaurer le mot de passe**, puis saisissez l'adresse e-mail utilisée pour l'enregistrement de l'abonnement. ESET vous envoie alors un e-mail contenant le code de vérification. Saisissez le code de vérification, puis tapez le nouveau mot de passe et confirmez-le. Le code de vérification est valable pendant 7 jours.

Restaurer le mot de passe via votre compte ESET HOME : choisissez cette option si l'abonnement utilisé pour l'activation est associé à votre compte ESET HOME. Saisissez l'adresse e-mail que vous utilisez pour vous connecter à votre compte ESET HOME.

Si vous avez oublié votre adresse e-mail ou si vous ne parvenez pas à restaurer le mot de passe, cliquez sur **Contacter l'assistance technique**. Vous êtes alors redirigé vers le site web ESET afin de contacter rapidement l'assistance technique.

Générer le code pour l'assistance technique : cette option permet de générer un code pour l'assistance technique. Copiez le code fourni par l'assistance technique et cliquez sur **Je possède un code de vérification**. Saisissez le code de vérification, puis tapez le nouveau mot de passe et confirmez-le. Le code de vérification est valable pendant 7 jours.

Pour plus d'informations, voir Déverrouiller le mot de passe de paramètres dans les produits ESET Windows pour les particuliers.

Comment résoudre les problèmes liés à la désactivation du produit depuis ESET HOME

Produit non activé

Ce message d'erreur s'affiche lorsque le titulaire de l'abonnement désactive ESET NOD32 Antivirus depuis le portail ESET HOME ou que l'abonnement partagé avec votre compte ESET HOME n’est plus partagé. Pour résoudre ce problème :

- Cliquez sur **Activer** et utilisez l’une des méthodes d’activation pour activer ESET NOD32 Antivirus.
- Contactez le titulaire de l'abonnement pour l'informer que ESET NOD32 Antivirus a été désactivé par lui ou que l'abonnement n'est plus partagé avec vous. Il peut résoudre le problème sur le ESET HOME.

Produit désactivé, appareil déconnecté

Ce message d’erreur s’affiche après la suppression d’un appareil du ESET HOME. Pour résoudre ce problème :

- Cliquez sur **Activer** et utilisez l’une des méthodes d’activation pour activer ESET NOD32 Antivirus.
- Contactez le titulaire de l'abonnement pour l'informer que ESET NOD32 Antivirus a été désactivé et que l'appareil a été déconnecté de ESET HOME.

• Si vous êtes le titulaire de l'abonnement et que vous n'êtes pas conscient de ces modifications, examinez le flux d'activités ESET HOME. Si vous détectez une activité suspecte, modifiez le mot de passe de votre compte ESET HOME et contactez l'assistance technique ESET.

Produit désactivé, appareil déconnecté

Ce message d'erreur s'affiche après la suppression d'un appareil du ESET HOME. Pour résoudre ce problème :

• Cliquez sur **Activer** et utilisez l'une des méthodes d'activation pour activer ESET NOD32 Antivirus.

• Contactez le titulaire de l'abonnement pour l'informer que ESET NOD32 Antivirus a été désactivé et que l'appareil a été déconnecté de ESET HOME.

• Si vous êtes le titulaire de l'abonnement et que vous n'êtes pas conscient de ces modifications, examinez le flux d'activités ESET HOME. Si vous détectez une activité suspecte, modifiez le mot de passe de votre compte ESET HOME et contactez l'assistance technique ESET.

Produit non activé

Ce message d'erreur s'affiche lorsque le titulaire de l'abonnement désactive ESET NOD32 Antivirus depuis le portail ESET HOME ou que l'abonnement partagé avec votre compte ESET HOME n'est plus partagé. Pour résoudre ce problème :

• Cliquez sur **Activer** et utilisez l'une des méthodes d'activation pour activer ESET NOD32 Antivirus.

• Contactez le titulaire de l'abonnement pour l'informer que ESET NOD32 Antivirus a été désactivé par lui ou que l'abonnement n'est plus partagé avec vous. Il peut résoudre le problème sur le ESET HOME.

0

Programme d\'amélioration du produit

En participant au programme d'amélioration du produit, vous fournissez à ESET des informations anonymes relatives à l'utilisation de ses produits. Des informations supplémentaires sur le traitement des données figurent dans la Politique de confidentialité d'ESET.

Votre consentement

La participation au programme est volontaire et repose sur votre consentement. Après avoir rejoint le programme, la participation est passive, ce qui signifie que vous n'avez plus rien à faire. Vous pouvez revenir à tout moment sur votre consentement en modifiant les configurations du produit. ESET ne pourra plus alors poursuivre le traitement de vos données anonymes.

Vous pouvez revenir à tout moment sur votre consentement en modifiant les configurations du produit:

- Modifier les configurations du programme d'amélioration du produit dans les produits pour les particuliers ESET Windows

Quels types d'informations sont collectés ?

Données d'interaction avec le produit

Ces informations permettent d'en savoir plus sur l'utilisation des produits ESET. Ainsi, ESET peut déterminer par exemple quelles sont les fonctionnalités souvent utilisées, quelles sont les configurations modifiées par les utilisateurs ou combien de temps les utilisateurs utilisent le produit.

Données concernant les appareils

ESET collecte ces informations pour déterminer où et sur quels appareils ses produits sont utilisés. Des exemples types comprennent notamment le modèle de l'appareil, le pays, la version et le nom du système d'exploitation.

Données de diagnostics d'erreurs

Des informations sur les erreurs et les défaillances sont également collectées, comme le type d'erreur s'étant produit et les actions l'ayant provoqué.

Pourquoi collections-nous ces informations ?

Ces informations anonymes permettent à ESET d'améliorer ses produits pour ses utilisateurs. Elles aident ESET à rendre ses produits aussi pertinents, conviviaux et parfaits que possible.

Qui contrôle ces informations ?

ESET, spol. s r.o. est le contrôleur de données exclusif des données collectées dans le programme. Ces informations ne sont pas transmises à des tiers.

Contrat de licence de l'utilisateur final

En vigueur à compter du 19 octobre 2021.

IMPORTANT : Veuillez lire soigneusement les termes et conditions d'application du produit stipulés ci-dessous avant de télécharger, d'installer, de copier ou d'utiliser le produit. **EN TÉLÉCHARGEANT, INSTALLANT, COPIANT OU UTILISANT LE LOGICIEL, VOUS ACCEPTEZ CES TERMES ET CONDITIONS ET RECONNAISSEZ AVOIR PRIS CONNAISSANCE DE LA POLITIQUE DE CONFIDENTIALITÉ.**

Contrat de licence de l'utilisateur final

Selon les termes du présent Contrat de Licence pour l'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 de Bratislava I. Section Sro, Insertion No 3586/B, numéro d'inscription des entreprises : 31333532 (« ESET » ou « Fournisseur ») et vous, personne physique ou morale, (« vous » ou « Utilisateur Final »), vous êtes autorisé à utiliser le Logiciel défini à l'article 1 du présent Contrat. Dans le cadre des modalités indiquées ci-dessous, le Logiciel défini à l'article 1 du présent Contrat peut être enregistré sur un support de données, envoyé par courrier électronique, téléchargé sur Internet, téléchargé à partir de serveurs du Fournisseur ou obtenu à partir d'autres sources.

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, installez, copiez ou utilisez le Logiciel, vous acceptez les termes et conditions du présent Contrat et reconnaissez avoir pris connaissance de la Politique de confidentialité. Si vous n'êtes pas d'accord avec tous les termes et conditions du présent Contrat et/ou de la Politique de confidentialité, cliquez immédiatement sur l'option d'annulation, annulez le téléchargement ou l'installation, détruisez ou renvoyez le Logiciel, le support d'installation, la documentation connexe et une facture au Fournisseur ou à l'endroit où vous avez obtenu 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 TERMES ET CONDITIONS.

1. **Logiciel.** Dans le cadre du présent Contrat, le terme « Logiciel » désigne : (i) le programme informatique et tous ses composants ; (ii) le contenu des disques, des CD-ROM, des DVD, des courriers électroniques et de leurs pièces jointes, ou de tout autre support auquel le présent Contrat est attaché, dont le formulaire de code objet fourni sur un support de données, par courrier électronique ou téléchargé par le biais d'Internet ; (iii) tous documents explicatifs écrits et toute documentation relative au Logiciel, en particulier, toute description du Logiciel, ses caractéristiques, description des propriétés, description de l'utilisation, description de l'interface du système d'exploitation sur lequel le Logiciel est utilisé, guide d'installation ou d'utilisation du Logiciel ou description de l'utilisation correcte du Logiciel (« Documentation ») ; (iv) les copies du Logiciel, les correctifs d'erreurs du Logiciel, les ajouts au Logiciel, ses extensions, ses versions modifiées et les mises à jour des parties du Logiciel, si elles sont fournies, au titre desquels le Fournisseur vous octroie la Licence conformément à l'article 3 du présent Contrat. Le Logiciel est fourni exclusivement sous la forme d'un code objet exécutable.

2. **Installation, Ordinateur et Clé de licence**. Le Logiciel fourni sur un support de données, envoyé par courrier électronique, téléchargé à partir d'Internet ou de serveurs du Fournisseur ou obtenu à partir d'autres sources nécessite une installation. Vous devez installer le Logiciel sur un Ordinateur correctement configuré, qui doit au moins satisfaire les exigences spécifiées dans la Documentation. La méthode d'installation est décrite dans la Documentation. L'Ordinateur sur lequel le Logiciel sera installé doit être exempt de tout programme ou matériel susceptible de nuire au bon fonctionnement du Logiciel. Le terme Ordinateur désigne le matériel, notamment les ordinateurs personnels, ordinateurs portables, postes de travail, ordinateurs de poche, smartphones, appareils électroniques portatifs ou autres appareils électroniques, pour lequel le Logiciel a été conçu et sur lequel il sera installé et/ou utilisé. Le terme Clé de licence désigne la séquence unique de symboles, lettres, chiffres ou signes spéciaux fournie à l'Utilisateur Final afin d'autoriser l'utilisation légale du Logiciel, de sa version spécifique ou de l'extension de la durée de la Licence conformément au présent Contrat.

3. **Licence**. Sous réserve que vous ayez accepté les termes du présent Contrat et que vous respectiez tous les termes et conditions stipulés 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 « 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 un courrier électronique par le biais d'un client de messagerie. Si le client de messagerie accepte du courrier électronique 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 courrier électronique est distribué. Si un serveur de messagerie joue le rôle de passerelle de courriel, le nombre

d’Utilisateurs Finaux est égal au nombre de serveurs 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 n'est autorisé à saisir la Clé de licence du Logiciel que dans la mesure où il a le droit d'utiliser le Logiciel conformément à la limite découlant du nombre de licences accordées par le Fournisseur. La Clé de licence est confidentielle. Vous ne devez pas partager la Licence avec des tiers ni autoriser des tiers à utiliser la Clé de licence, sauf si le présent Contrat ou le Fournisseur le permet. Si votre Clé de licence est endommagée, informez-en immédiatement le Fournisseur.

c) **Home/Business Edition.** Une version Home Edition du Logiciel doit être utilisée exclusivement dans des environnements privés et/ou non commerciaux, pour un usage domestique et familial uniquement. Une version Business Edition du Logiciel est requise pour l'utiliser dans un environnement commercial ainsi que pour utiliser le Logiciel sur des serveurs de messagerie, relais de messagerie, passerelles de messagerie ou 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 achetés à un fabricant d'équipement informatique 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 est en droit de mettre fin au droit de l'Utilisateur final à l'utilisation des fonctions du Logiciel, qui nécessitent une connexion aux serveurs du Fournisseur ou à des serveurs tiers.

4. **Fonctions avec des exigences en matière de connexion Internet et de collecte de données.** Pour fonctionner correctement, le Logiciel nécessite une connexion Internet et doit se connecter à intervalles réguliers aux serveurs du Fournisseur ou à des serveurs tiers et collecter des données en conformité avec la Politique de confidentialité. Une connexion Internet et une collecte de données sont requises pour les fonctions suivantes du Logiciel :

a) **Mises à jour du Logiciel.** Le Fournisseur est autorisé de temps à autre à publier des mises à jour ou des mises à niveau du Logiciel (« Mises à jour »), 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. Pour la mise à disposition de Mises à jour, une vérification de l'authenticité de la Licence est requise. Elle comprend notamment la collecte d'informations sur l'Ordinateur et/ou la plate-forme sur lesquels le Logiciel est installé, en conformité avec la Politique de confidentialité.

La fourniture des mises à jour peut être soumise à la Politique de fin de vie (« Politique de fin de vie »), qui est disponible à l'adresse suivante : https://go.eset.com/eol_home. Aucune mise à jour ne sera fournie après que le Logiciel ou l'une de ses fonctionnalités ait 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 collectent des échantillons de virus, d'autres programmes informatiques également nuisibles et d'objets problématiques, suspects, potentiellement indésirables ou dangereux tels que des fichiers, des URL, des paquets

IP et des trames Ethernet (« Infiltrations »), puis les envoient au Fournisseur, en incluant, sans s'y limiter, des informations sur le processus d'installation, l'Ordinateur ou la plateforme hébergeant le Logiciel et des informations sur les opérations et fonctions du Logiciel (« Informations »). Les Informations et les Infiltrations sont susceptibles de contenir des données (y compris des données personnelles obtenues par hasard ou accidentellement) concernant l'Utilisateur final et/ou d'autres usagers de l'ordinateur sur lequel le Logiciel est installé et les fichiers affectés par les Infiltrations et les métadonnées associées.

Les informations et les infiltrations peuvent être collectées pat les fonctions suivantes du Logiciel :

i. La fonction Système de réputation LiveGrid collecte et envoie les hachages unidirectionnelles liés aux Infiltrations au Fournisseur. Cette fonction est activée dans les paramètres standard du Logiciel.

ii. La fonction Système de commentaires LiveGrid collecte et envoie les Infiltrations avec les Informations et les métadonnées associées au Fournisseur. Cette fonction peut être activée par l'Utilisateur Final pendant le processus d'installation du Logiciel.

Le Fournisseur utilisera les Informations et Infiltrations reçues uniquement pour effectuer des analyses et des recherches sur les Infiltrations et améliorer le Logiciel et la vérification de l'authenticité de la Licence. Il prendra en outre les mesures adéquates afin de protéger les Infiltrations et Informations reçues. Si vous activez cette fonction du Logiciel, les Infiltrations et Informations peuvent être collectées et traitées par le Fournisseur, comme stipulé dans la Politique de confidentialité et conformément aux réglementations en vigueur. Vous pouvez désactiver ces fonctions à tout moment.

Aux fins du présent Contrat, il est nécessaire de collecter, traiter et stocker des données permettant au Fournisseur de vous identifier conformément à la Politique de confidentialité. Vous acceptez que le Fournisseur vérifie à l'aide de ses propres moyens si vous utilisez le Logiciel conformément aux dispositions du présent Contrat. Vous reconnaissez qu'aux fins du présent Contrat, il est nécessaire que vos données soient transférées pendant les communications entre le Logiciel et les systèmes informatiques du Fournisseur ou de ceux de ses partenaires commerciaux, dans le cadre du réseau de distribution et de support du Fournisseur, afin de garantir les fonctionnalités du Logiciel, l'autorisation d'utiliser le Logiciel et la protection des droits du Fournisseur.

Après la conclusion du présent Contrat, le Fournisseur et ses partenaires commerciaux, dans le cadre du réseau de distribution et de support du Fournisseur, sont autorisés à transférer, à traiter et à stocker des données essentielles vous identifiant, aux fins de facturation, d'exécution du présent Contrat et de transmission de notifications sur votre Ordinateur.

Des informations détaillées sur la vie privée, la protection des données personnelles et Vos droits en tant que personne concernée figurent dans la Politique de confidentialité, disponible sur le site Web du Fournisseur et directement accessible à partir de l'installation. Vous pouvez également la consulter depuis 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 Ordinateurs ou systèmes informatiques pour lesquels vous avez obtenu une Licence.

6. **Restrictions des 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, modifier, traduire, reproduire ou 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 rétroconcevoir, 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 acceptez de n'utiliser le Logiciel et ses fonctions que de façon à ne pas entraver la possibilité des autres Utilisateurs Finaux à accéder à ces services. Le Fournisseur se réserve le droit de limiter l'étendue des services fournis à chacun des Utilisateurs Finaux, pour permettre l'utilisation des services au plus grand nombre possible d'Utilisateurs Finaux. Le fait de limiter l'étendue des services implique aussi la résiliation totale de la possibilité d'utiliser toute fonction du Logiciel ainsi que la suppression des Données et des informations présentes sur les serveurs du Fournisseur ou sur des serveurs tiers, qui sont afférentes à une fonction particulière du Logiciel.

g) Vous acceptez de ne pas exercer d'activités impliquant l'utilisation de la Clé de licence, qui soit contraire aux termes du présent Contrat, ou conduisant à fournir la Clé de licence à toute personne n'étant pas autorisée à utiliser le logiciel (comme le transfert d'une Clé de licence utilisée ou non utilisée ou la distribution de Clés de licence dupliquées ou générées ou l'utilisation du Logiciel suite à l'emploi d'une Clé de licence obtenue d'une source autre que le Fournisseur).

7. **Droit 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. ESET est protégée 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 rétroconcevez, 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 termes du présent Contrat en tant qu'Utilisateur final du Logiciel.

9. **Versions multilingues, logiciel sur plusieurs supports, copies multiples**. 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 remise 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. Lorsque le logiciel ou l'une de ses fonctionnalités atteint la date de fin de vie définie dans la Politique de fin de vie, votre droit d'utiliser le logiciel prend 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 ait 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, d'autres informations et des données conformes à la Politique de confidentialité peuvent être requises en vue de fournir une 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'utiliser le 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 présentant un courrier électronique envoyé au Fournisseur contenant tous les renseignements sur la licence (nom d'utilisateur et mot de passe). Des informations de licence et des données d'identification de l'Utilisateur Final conformes à la Politique de confidentialité peuvent être requises en vue de vérifier 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 en aucun cas, directement ou indirectement, exporter, réexporter, transférer ou mettre le Logiciel à la disposition de quiconque, ou l'utiliser d'une manière ou participer à un acte qui pourrait entraîner ESET ou ses sociétés de holding, ses filiales et les filiales de l'une de ses sociétés de holding, ainsi que les entités contrôlées par ses sociétés de holding (« Sociétés affiliées ») à enfreindre ou faire l'objet des conséquences négatives de l'enfreinte des Lois sur le contrôle à l'exportation, qui comprennent

i. les lois qui contrôlent, limitent ou imposent des exigences en matière de licence pour l'exportation, la réexportation ou le transfert de marchandises, de logiciels, de technologies ou de services, émises ou adoptées 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 tout pays dans lequel les obligations au titre de l'accord doivent être exécutées, ou dans lequel ESET ou l'une de ses filiales est établie ou mène ses activités et

ii. toute sanction économique, financière, commerciale ou autre, 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 tout pays dans lequel les obligations au titre de l'accord doivent être exécutées, ou dans lequel ESET ou l'une de ses filiales est établie ou mène ses activités.

(les actes juridiques mentionnés aux points i, et ii. ci-dessus étant appelés ensemble « Lois sur le contrôle à l'exportation »).

b) ESET a le droit de suspendre ses obligations en vertu des présentes Conditions ou d'y mettre fin avec effet immédiat dans le cas où :

i. ESET estime raisonnablement que l'Utilisateur a enfreint ou est susceptible d'enfreindre la disposition de l'Article 19 a) du Contrat ; ou

ii. l'Utilisateur final et/ou le Logiciel deviennent soumis aux Lois sur le contrôle à l'exportation et, par conséquent, ESET estime raisonnablement que l'exécution continue de ses obligations en vertu de l'accord pourrait entraîner ESET ou ses affiliés à enfreindre ou faire l'objet des conséquences négatives de l'enfreinte des Lois sur le contrôle à l'exportation.

c) Rien dans le Contrat ne vise, et rien ne doit être interprété comme incitant ou obligeant l'une des parties à agir ou à s'abstenir d'agir (ou à accepter d'agir ou à s'abstenir d'agir) d'une manière qui soit incompatible, pénalisée

ou interdite en vertu de toute loi sur le contrôle à l'exportation applicable.

20. **Avis**. Tous les avis, les renvois du Logiciel et 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 e-mails, des notifications intégrés à l'application via le 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 particulières ou des Politiques de confidentialité, toute proposition/acceptation de contrat ou invitation à traiter, avis ou autres communications légales. Ces communications électroniques sont réputées avoir été reçues par écrit, sauf si les lois applicables exigent spécifiquement une autre forme de communication.

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. 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. Si une traduction du Contrat est préparée pour des raisons de commodité ou pour toute autre raison, ou en cas de discordance entre les versions linguistiques du présent Contrat, seule la version en langue anglaise fait foi.

ESET se réserve le droit d'apporter des modifications au Logiciel ainsi que de réviser les conditions du présent Contrat, des Annexes, des Addendums, de la Politique de confidentialité, de la Politique de fin de vie et de la Documentation ou toute partie de celle-ci à tout moment en mettant à jour le document approprié (i) pour refléter les modifications apportées au Logiciel ou dans la façon dont ESET mène ses activités, (ii) pour des raisons légales, réglementaires ou de sécurité, ou (iii) pour éviter tout abus ou dommage. Vous serez averti de toute révision du Contrat par e-mail, par le biais d'une notification intégrée à 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'une notification de la modification. À moins que Vous ne résiliez le Contrat dans ce délai, les modifications proposées seront considérées comme acceptées et prendront effet à Votre égard à la date à laquelle vous avez reçu une notification de la modification.

Cela constitue l'intégralité du Contrat entre le Fournisseur et vous en relation avec le Logiciel, et il remplace toute représentation, discussion, entreprise, communication ou publicité antérieure en relation avec le Logiciel.

ADDENDUM AU CONTRAT

Évaluation de la sécurité des appareils connectés au réseau. Des dispositions supplémentaires s'appliquent à l'Évaluation de la sécurité des appareils connectés au réseau comme suit :

Le logiciel contient une fonction de contrôle de la sécurité du réseau local de l'utilisateur final et de la sécurité des appareils du réseau local, qui nécessite le nom du réseau local et des informations sur les appareils du réseau local, telles que la présence, le type, le nom, l'adresse IP et l'adresse MAC de l'appareil sur le réseau local, en relation avec les informations de licence. Les informations comprennent également le type de sécurité sans fil et le type de chiffrement sans fil pour les périphériques de routeur. Cette fonction peut également fournir des informations sur la disponibilité de la solution logicielle de sécurité pour protéger les appareils du réseau local.

Protection contre l'utilisation abusive des données. Des dispositions supplémentaires s'appliquent à la

Protection contre l'utilisation abusive des données comme suit :

Le Logiciel contient une fonction qui empêche la perte ou l'utilisation abusive de données critiques relatives au vol d'un Ordinateur. Cette fonction est désactivée dans les paramètres par défaut du Logiciel. Un Compte ESET HOME doit être créé afin de l'activer, ce qui entraîne la collecte de données par la fonction dans l'éventualité d'un vol de l'ordinateur. Si vous activez cette fonction du Logiciel, les données concernant l'Ordinateur volé sont collectées et envoyées au Fournisseur. Ces données peuvent notamment comprendre l'emplacement réseau de l'Ordinateur, les données sur le contenu affiché à l'écran de l'Ordinateur, les données concernant la configuration de l'ordinateur et/ou les données enregistrées par une caméra branchée à l'ordinateur (« Données »). L'Utilisateur Final est autorisé à utiliser les Données obtenues par cette fonction et fournies par le biais du Compte ESET HOME exclusivement pour réparer une situation défavorable entraînée par le vol d'un Ordinateur. À la seule fin de cette fonction, le Fournisseur traite les Données, comme stipulé dans la Politique de confidentialité et conformément aux réglementations en vigueur. Le Fournisseur autorise l'Utilisateur final à accéder aux Données pendant la période requise pour atteindre le but pour lequel les données ont été obtenues, période qui ne doit pas dépasser celle de rétention indiquée dans la Politique de confidentialité. La protection contre l'utilisation abusive des données doit être utilisée exclusivement avec les Ordinateurs et les comptes pour lesquels l'Utilisateur final dispose d'un accès légitime. Toute utilisation interdite sera signalée à l'autorité compétente. Le Fournisseur respectera la législation applicable et assistera les forces de l'ordre en cas d'utilisation abusive. Vous acceptez et reconnaissez être responsable de la protection du mot de passe permettant d'accéder au Compte ESET HOME. Vous acceptez également de ne pas divulguer votre mot de passe à des tiers. L'Utilisateur final est responsable de toute activité, autorisée ou non, utilisant la fonction de Protection contre l'utilisation abusive des données et le Compte ESET HOME. Si un Compte ESET HOME est corrompu, avertissez-en immédiatement le Fournisseur. Les dispositions supplémentaire pour la Protection contre l'utilisation abusive des données doivent être exclusivement applicables aux Utilisateurs Finaux d'ESET Internet Security et ESET Smart Security Premium.

ESET Secure Data. Des dispositions supplémentaires s'appliquent à ESET Secure Data comme suit :

1. Définitions. Dans les présentes dispositions supplémentaires d'ESET Secure Data, les termes suivants sont définis comme suit :

a) « Information » les informations ou les données chiffrées ou déchiffrées à l'aide du logiciel ;

b) “Produits”ESET Secure Datale logiciel et la documentation ;

« ESET Secure Data » le ou les logiciels utilisés pour le chiffrement et le déchiffrement des données électroniques ;

Les termes employés au pluriel s'entendent également au singulier et les termes employés au masculin s'entendent également au féminin, et inversement. Les termes 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) vous êtes responsable de la protection, gestion et sauvegarde des Informations ;

b) vous devez effectuer une sauvegarde complète de toutes les Informations et données (y compris les informations et données critiques) stockées sur votre Ordinateur avant d'installer le ESET Secure Data ;

c) Vous devez conserver en lieu sûr les mots de passe et toute autre information utilisés pour configurer et utiliser ESET Secure Data ; vous devez également créer des copies de sauvegarde de toutes les clés de chiffrement, de tous les codes de licence et fichiers de clé, ainsi que des autres données générées sur des supports de stockage distincts ;

d) Vous êtes responsable de l'utilisation des Produits. Le Fournisseur ne pourra pas être tenu responsable de toutes pertes, réclamations ou dommages résultant d'un chiffrement ou d'un déchiffrement non autorisé ou erroné d'Informations ou de données, quels que soient l'emplacement et la méthode de stockage de ces Informations ou données ;

e) Bien que le Fournisseur ait pris toutes les mesures raisonnables pour garantir l'intégrité et la sécurité d'ESET Secure Data, les Produits (ou l'un d'entre eux) ne doivent pas être utilisés dans des environnements à risques ou potentiellement dangereux, y compris, de manière non limitative, les installations nucléaires, la navigation aérienne ou les systèmes de communications aériennes, le contrôle du trafic aérien, les systèmes de défense et d'armement ou les appareils de réanimation ou de surveillance médicale ;

f) Il vous incombe de vous assurer que le niveau de sécurité et de chiffrement fourni par les produits correspond à vos besoins ;

g) Vous êtes responsable de l'utilisation des Produits (ou de l'un d'entre eux), y compris de vous assurer que celle-ci respecte les réglementations en vigueur en République slovaque ou dans tout autre pays, région ou état dans lequel les Produits sont utilisés. Vous devez vérifier avant toute utilisation des Produits qu'ils ne sont pas contraires à tout embargo gouvernemental (en République slovaque) ;

h) ESET Secure Data peut contacter de temps en temps les serveurs du Fournisseur afin de vérifier la présence d'informations de licence, de correctifs, de Service Packs et d'autres mises à jour pouvant améliorer, maintenir et modifier le fonctionnement d'ESET Secure Data. ESET Secure Data peut envoyer des informations système générales relatives à son fonctionnement conformément à la Politique de confidentialité.

i) le Fournisseur ne pourra être tenu responsable de toute perte, dommage, frais ou réclamation résultant de la perte, du vol, du mauvais usage, de l'endommagement ou de la destruction des mots de passe, des informations de configuration, des clés de chiffrement, des codes d'activation de licence et des autres données générées ou stockées pendant l'utilisation du logiciel.

Les dispositions supplémentaires pour ESET Secure Data doivent s'appliquer exclusivement aux Utilisateurs finaux d'ESET Smart Security Premium.

Password Manager Logiciel. Des dispositions supplémentaires s'appliquent au Logiciel Password Manager comme suit :

1. Déclaration supplémentaire de l'Utilisateur Final. Vous reconnaissez et acceptez que vous n'êtes pas autorisé à :

a) utiliser le Logiciel Password Manager dans l'exploitation d'une application critique dans laquelle des vies humaines ou des biens peuvent être en jeu. Vous comprenez que le Logiciel Password Manager n'est pas conçu pour de telles applications, que sa défaillance dans de telles applications serait susceptible d'entraîner la mort, des blessures ou des dommages importants aux biens ou à l'environnement et que le Fournisseur ne saurait être tenu responsable d'aucune de ces conséquences.

LE LOGICIEL PASSWORD MANAGER N'EST PAS CONÇU, DESTINÉ OU CONCÉDÉ SOUS LICENCE POUR ÊTRE UTILISÉ DANS DES ENVIRONNEMENTS À RISQUES DONT LES PERFORMANCES NE DOIVENT SUBIR AUCUNE DÉFAILLANCE, Y COMPRIS, SANS LIMITATION, DANS LA CONCEPTION, LA CONSTRUCTION, LA MAINTENANCE OU LE FONCTIONNEMENT DE CENTRALES NUCLÉAIRES, LA NAVIGATION AÉRIENNE OU LES SYSTÈMES DE COMMUNICATION, LE CONTRÔLE AÉRIEN ET LES SYSTÈMES D'ASSISTANCE VITALE OU LES SYSTÈMES D'ARMEMENT. LE FOURNISSEUR DÉCLINE EXPRESSÉMENT TOUTE GARANTIE EXPRESSE OU IMPLICITE DE CONVENANCE À DE TELLES APPLICATIONS.

b) utiliser le logiciel Password Manager d'une manière qui enfreint le présent contrat ou les lois de la République

slovaque ou de votre juridiction. Plus précisément, vous n'êtes pas autorisé à utiliser le Logiciel Password Manager pour mener ou promouvoir des activités illégales, notamment télécharger des données de contenu nuisible ou de contenu pouvant être utilisé pour des activités illégales ou qui enfreint de quelque manière que ce soit la loi ou les droits d'un tiers (notamment tous les droits de propriété intellectuelle), y compris, mais sans s'y limiter, toute tentative d'accès aux comptes dans l'espace de Stockage (aux fins des présentes conditions supplémentaires relatives au Logiciel Password Manager, « Stockage » désigne l'espace de stockage des données géré par le Fournisseur ou un tiers autre que le Fournisseur et l'utilisateur dans le but de permettre la synchronisation et la sauvegarde des données utilisateur) ou aux comptes et aux données d'autres utilisateurs du logiciel Password Manager ou de l'espace de Stockage. Si vous ne respectez pas l'une de ces dispositions, le Fournisseur est en droit de résilier immédiatement le présent 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 « EN L'ÉTAT » SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE. VOUS UTILISEZ LE LOGICIEL À VOS RISQUES ET PÉRILS. LE FOURNISSEUR NE PEUT ÊTRE TENU RESPONSABLE DES PERTES DE DONNÉES, DES DOMMAGES, DE LA LIMITATION DE LA DISPONIBILITÉ DU SERVICE, Y COMPRIS DE L'ENVOI DE DONNÉES PAR LE LOGICIEL PASSWORD MANAGER À UN SYSTÈME DE STOCKAGE EXTERNE À DES FINS DE SYNCHRONISATION ET DE SAUVEGARDE DES DONNÉES. LE CHIFFREMENT DES DONNÉES À L'AIDE DU LOGICIEL PASSWORD MANAGER N'IMPLIQUE AUCUNE RESPONSABILITÉ DU FOURNISSEUR EN CE QUI CONCERNE LA SÉCURITÉ DE CES DONNÉES. VOUS RECONNAISSEZ EXPRESSÉMENT QUE LES DONNÉES ACQUISES, UTILISÉES, CHIFFRÉES, STOCKÉES, SYNCHRONISÉES OU ENVOYÉES À L'AIDE DU LOGICIEL PASSWORD MANAGER PEUVENT ÉGALEMENT ÊTRE STOCKÉES SUR DES SERVEURS TIERS (S'APPLIQUE UNIQUEMENT À L'UTILISATION DU LOGICIEL PASSWORD MANAGER POUR LAQUELLE LES SERVICES DE SYNCHRONISATION ET DE SAUVEGARDE ONT ÉTÉ ACTIVÉS). SI LE FOURNISSEUR CHOISIT D'UTILISER UN TEL SYSTÈME DE STOCKAGE, SITE WEB, PORTAIL WEB, SERVEUR OU SERVICE, IL NE PEUT ÊTRE TENU RESPONSABLE DE LA QUALITÉ, SÉCURITÉ OU DISPONIBILITÉ D'UN TEL SERVICE TIERS. LE FOURNISSEUR N'EST AUCUNEMENT RESPONSABLE DE TOUTE VIOLATION DES OBLIGATIONS CONTRACTUELLES OU LÉGALES PAR LE TIERS NI DES DOMMAGES, PERTE DE BÉNÉFICES, PRÉJUDICES FINANCIERS OU MORAUX OU TOUT AUTRE TYPE DE PERTE LIÉ À L'UTILISATION DE CE LOGICIEL. LE FOURNISSEUR NE PEUT ÊTRE TENU RESPONSABLE DU CONTENU DES DONNÉES ACQUISES, UTILISÉES, CHIFFRÉES, STOCKÉES, SYNCHRONISÉES OU ENVOYÉES À L'AIDE DU LOGICIEL PASSWORD MANAGER OU DANS LE SYSTÈME DE STOCKAGE. VOUS RECONNAISSEZ QUE LE FOURNISSEUR N'A PAS ACCÈS AU CONTENU DES DONNÉES STOCKÉES ET NE PEUT PAS LE SURVEILLER NI SUPPRIMER LÉGALEMENT LE CONTENU NUISIBLE.

Le Fournisseur détient tous les droits sur les améliorations, les mises à niveau et les correctifs relatifs au Logiciel Password Manager (« Améliorations »), même si de telles améliorations ont été conçues à partir des commentaires, des idées ou des suggestions dont vous nous avez fait part sous n'importe quelle forme. Vous n'avez droit à aucune rémunération ni redevances pour de telles Améliorations.

LES ENTITÉS ET LES CONCÉDANTS DU FOURNISSEUR NE POURRONT ÊTRE TENUS RESPONSABLES DES RÉCLAMATIONS ET RESPONSABILITÉS DE QUELQUE NATURE QUE CE SOIT DÉCOULANT DE VOTRE UTILISATION DU LOGICIEL PASSWORD MANAGER OU DE CELLE DE TIERS, DE L'UTILISATION OU DE LA NON-UTILISATION D'UNE SOCIÉTÉ DE COURTAGE OU D'UN MARCHAND OU DE LA VENTE OU L'ACHAT DE TITRES, QUELQUE SOIT LE RÉGIME DE RESPONSABILITÉ.

LES ENTITÉS ET CONCÉDANTS DU FOURNISSEUR NE POURRONT EN AUCUN CAS ÊTRE TENUS RESPONSABLES DE TOUT DOMMAGE DIRECT, ACCESSOIRE, SPÉCIAL, INDIRECT OU CONSÉCUTIF RÉSULTANT OU LIÉ À UN LOGICIEL TIERS, À DES DONNÉES AYANT FAIT L'OBJET D'UN ACCÈS VIA LE LOGICIEL PASSWORD MANAGER, À VOTRE UTILISATION OU INCAPACITÉ D'UTILISER OU ACCÉDER AU LOGICIEL PASSWORD MANAGER OU AUX DONNÉES FOURNIES VIA LE LOGICIEL PASSWORD MANAGER, QUEL QUE SOIT LE RÉGIME DE RESPONSABILITÉ. LES DOMMAGES EXCLUS DE CETTE CLAUSE COMPRENNENT, SANS LIMITATION, CEUX POUR PERTE DE BÉNÉFICES, DOMMAGES COPORELS OU MATÉRIELS, INTERRUPTION D'ACTIVITÉ ET PERTE D'INFORMATIONS

PROFESSIONNELLES OU PERSONNELLES. CERTAINES JURIDICTIONS NE PERMETTENT PAS DE LIMITER LA RESPONSABILITÉ POUR LES DOMMAGES ACCESSOIRES ET INDIRECTS. DANS CE CAS, LA RESPONSABILITÉ DU FOURNISSEUR CORRESPONDRA AU MINIMUM PRÉVU PAR LA LOI.

LES INFORMATIONS FOURNIES PAR LE BIAIS DU LOGICIEL PASSWORD MANAGER, NOTAMMENT LES COTATIONS BOURSIÈRES, LES ANALYSES, LES INFORMATIONS SUR LE MARCHÉ, LES ACTUALITÉS ET LES DONNÉES FINANCIÈRES PEUVENT ÊTRE RETARDÉES, INEXACTES OU CONTENIR DES ERREURS OU OMISSIONS, ET LES ENTITÉS ET CONCÉDANTS DU FOURNISSEUR N'AURONT AUCUNE RESPONSABILITÉ À CET ÉGARD. LE FOURNISSEUR PEUT MODIFIER OU INTERROMPRE À TOUT MOMENT TOUT ASPECT OU FONCTIONNALITÉ DU LOGICIEL PASSWORD MANAGER OU L'UTILISATION DE TOUT OU PARTIE DES FONCTIONNALITÉS OU DE LA TECHNOLOGIE DU LOGICIEL PASSWORD MANAGER SANS NOTIFICATION PRÉALABLE.

SI LES DISPOSITIONS DU PRÉSENT ARTICLE SONT JUGÉES NULLES POUR QUELQUE RAISON QUE CE SOIT OU SI LE FOURNISSEUR EST CONSIDÉRÉ COMME RESPONSABLE DES PERTES, DOMMAGES OU AUTRE EN VERTU DES LOIS APPLICABLES, LES PARTIES CONVIENNENT QUE LA RESPONSABILITÉ DU FOURNISSEUR ENVERS VOUS SERA LIMITÉE AU MONTANT TOTAL DES FRAIS DE LICENCE QUE VOUS AVEZ PAYÉS.

VOUS ACCEPTEZ DE DÉFENDRE, D'INDEMNISER ET DE SOUTENIR LE FOURNISSEUR ET SES EMPLOYÉS, FILIALES, SOCIÉTÉS AFFILIÉES ET AUTRES PARTENAIRES CONTRE LES RÉCLAMATIONS, RESPONSABILITÉS, DOMMAGES, PERTES, COÛTS, DÉPENSES ET FRAIS DE TIERS (Y COMPRIS LES POSSESSEURS DE L'APPAREIL OU LES PARTIES DONT LES DROITS ONT ÉTÉ AFFECTÉS PAR LES DONNÉES UTILISÉES DANS LE LOGICIEL PASSWORD MANAGER) QUE CES PARTIES PEUVENT ENCOURIR EN RAPPORT AVEC VOTRE UTILISATION DU LOGICIEL PASSWORD MANAGER.

3. Données du Logiciel Password Manager. Sauf sélection 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 sous une forme chiffrée sur votre ordinateur ou sur tout autre périphérique de stockage défini. Vous comprenez qu'en cas de suppression ou d'endommagement d'une base de données ou d'autres fichiers du Logiciel Password Manager, toutes les données qui y sont contenues sont perdues de manière irréversible. Vous comprenez et acceptez le risque d'une telle perte. Le fait que vos données personnelles soient stockées sous une forme chiffrée sur l'ordinateur n'implique pas que les informations ne puissent pas être volées ou utilisées par toute personne découvrant le mot de passe principal ou obtenant un accès au périphérique d'activation défini par le client pour l'ouverture de la base de données. Vous êtes responsable de la sécurité des méthodes d'accès.

4. Transmission des Données personnelles au Fournisseur ou au système de Stockage. À des fins de stockage et de synchronisation des données uniquement et si vous le spécifiez, le logiciel Password Manager transmet ou envoie les données personnelles de la base de données du Logiciel Password Manager, à savoir les mots de passe, les informations de connexion, les comptes et les identités, au système de Stockage via Internet. Les données sont transmises de manière chiffrée. L'utilisation du Logiciel Password Manager afin de renseigner des formulaires en ligne avec des mots de passe, données de connexion ou autres peut nécessiter l'envoi d'informations au site web que vous avez identifié via Internet. Cette transmission de données n'est liée au Logiciel Password Manager. Par conséquent, le Fournisseur ne peut être tenu responsable de la sécurité de ces interactions avec les sites web pris en charge par divers fournisseurs. Toute transaction sur Internet, que ce soit ou non avec le logiciel Password Manager, sont effectuées à votre entière discrétion et à vos propres risques Vous serez seul responsable de tout dommage de votre système informatique ou de toute perte de données résultant du téléchargement et/ou de l'utilisation de ce type de matériel ou service. Afin de limiter le risque de perte de données précieuses, le Fournisseur recommande que les clients effectuent des sauvegardes régulières de la base de données et d'autres fichiers sensibles sur des lecteurs externes. Le Fournisseur n'est pas en mesure de vous aider pour récupérer des données perdues ou endommagées. Si le Fournisseur propose un service de sauvegarde des fichiers de base de données en cas de dommages ou de suppression de ceux-ci sur le PC client alors un tel service est sans garantie et n'implique en aucun cas la responsabilité du Fournisseur envers vous.

En utilisant le Logiciel Password Manager, vous acceptez que le logiciel puisse contacter de temps en temps les serveurs du Fournisseur afin de vérifier la présence d'informations de licence, de correctifs, de Service Packs et

d'autres mises à jour pouvant améliorer, maintenir ou modifier le fonctionnement du Logiciel Password Manager. Le logiciel peut envoyer des informations système générales relatives au fonctionnement du Logiciel Password Manager en conformité avec la Politique de confidentialité.

5. Informations et instructions de désinstallation. Les informations que vous souhaitez conserver de la base de données doivent être exportées avant de désinstaller le Logiciel Password Manager.

Les dispositions supplémentaires pour le Logiciel Password Manager doivent s'appliquer exclusivement aux Utilisateurs finaux d'ESET Smart Security Premium.

ESET LiveGuard. Des dispositions supplémentaires 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 conformément à la Politique de confidentialité et aux dispositions légales applicables.

Les dispositions supplémentaires pour ESET LiveGuard doivent s'appliquer exclusivement aux Utilisateurs finaux d'ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Politique de confidentialité

La protection des données personnelles revêt une importance particulière pour ESET, spol. s r.o., dont le siège social est établi au Einsteinova 24, 851 01 Bratislava, Slovak Republic, inscrite au registre du commerce administré par le Tribunal de district de Bratislava I, Section Sro, Entrée No 3586/B, Numéro d'identification de l'entreprise : 31333532 en tant que Responsable du traitement des données ("ESET" ou « Nous"). Nous souhaitons nous conformer à l'exigence de transparence telle qu'elle est légalement normalisée par le Règlement général sur la protection des données de l'UE ("RGPD"). Pour atteindre cet objectif, nous publions la présente Politique de confidentialité dans le seul but d'informer notre client ("Utilisateur final" ou "Vous"), en tant que personne concernée, des 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 de Vos données personnelles
- Coordonnées.

Base juridique du traitement des données personnelles

Il n'existe que quelques bases juridiques en matière de traitement des données que nous utilisons conformément au cadre législatif applicable en ce qui concerne la protection des données à caractère personnel. Le traitement des données personnelles chez ESET est principalement nécessaire pour l'exécution du Contrat de licence de l'utilisateur final ("CLUF") avec l'Utilisateur final (Article 6 (1) (b) RGPD), qui est applicable pour la fourniture des produits ou des services ESET, sauf indication contraire explicite, par exemple :

- La base juridique de l'intérêt légitime (Article 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 les meilleures protection, assistance et expérience possibles. Puisque le marketing est également reconnu comme un intérêt légitime par la législation applicable, Nous nous appuyons généralement sur celui-ci pour nos communications marketing avec nos clients.

- Le consentement (Article 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 des obligations légales (Article 6 (1) (c) RGPD), par exemple en stipulant des exigences en matière de communication électronique, de conservation pour les documents de facturation.

Partage des données et confidentialité

Nous ne partageons pas vos données avec des tiers. Cependant, ESET est une entreprise présente dans le monde entier par le biais de sociétés affiliées et de partenaires du réseau de vente, de service et d'assistance ESET. Les informations relatives aux licences, à la facturation et à l'assistance technique traitées par ESET peuvent être transférées depuis et vers les sociétés affiliées ou les partenaires dans le but de respecter le Contrat de licence pour l'utilisateur final (pour la fourniture de services ou l'assistance, par exemple).

ESET préfère traiter ses données dans l’Union européenne (EU). Toutefois, en fonction de votre localisation (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 situé en dehors de l'UE. Nous utilisons par exemple des services tiers dans le cadre du cloud computing. 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 nous mettons d'accord sur les clauses contractuelles types de l'UE et, si nécessaire, sur 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 ou accord particulier.

Sécurité des données

ESET met en place des mesures techniques et organisationnelles adéquates pour assurer un niveau de sécurité adapté aux risques potentiels. Nous faisons tout notre possible pour garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes 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 informer l'autorité de contrôle compétente ainsi que les utilisateurs finaux concernés en tant que personnes concernées.

Droits des personnes concernées

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 ci-après garantis chez ESET. Pour exercer les droits de la personne concernée, vous pouvez nous contacter par le biais du formulaire d'assistance ou par e-mail à l'adresse suivante : dpo@eset.sk. À des fins d'identification, nous vous demandons les informations suivantes : Nom, adresse e-mail et - le cas échéant - clé de licence ou numéro de client et affiliation à la société. Veuillez vous abstenir de nous envoyer d'autres données personnelles, telles que votre 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 retirer le consentement. Le droit de retirer le consentement est applicable en cas de traitement fondé sur le consentement uniquement. Si Nous traitons vos données personnelles sur la base de 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 nommé par nous et au traitement de vos données personnelles à tout moment. Votre opposition n'a d'effet que pour l'avenir et n'affecte pas la licéité des données traitées avant l'opposition. Si nous traitons vos données personnelles à des fins de marketing direct, il n'est pas nécessaire de motiver votre objection. Il en est de même pour le profilage, dans la mesure où il est lié au 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 sur la base d'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 l'effacement 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. Si nous traitons vos données personnelles, par exemple avec votre consentement, que vous le retirez et qu'il n'existe pas d'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 inclurons vos coordonnées dans notre liste noire interne afin d'éviter tout contact non sollicité. Dans le cas contraire, vos données personnelles seront supprimées.

Veuillez noter que Nous pouvons être tenus de conserver vos données jusqu'à l'expiration des obligations et 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.

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 porter plainte. En tant que personne concernée, Vous avez le droit de déposer une plainte auprès d'une autorité de contrôle à tout moment. ESET est soumise à la réglementation des lois slovaques et est tenue de respecter la législation en matière de protection des données de l'Union européenne. L'autorité de contrôle des données compétente est l'Office pour la protection des données personnelles de la République slovaque, situé à Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Traitement de Vos données personnelles

Les services ESET qui sont implémentés dans le produit sont fournis selon les termes du CLUF, mais certains d'entre eux peuvent nécessiter une attention particulière. Nous souhaitons Vous donner plus de détails sur la collecte de données liée à la fourniture de nos services. Nous proposons différents services qui sont décrits dans le Contrat de Licence de l'utilisateur final et la documentation. Pour que tous ces services soient fonctionnels, Nous devons collecter les informations suivantes :

Données de licence et de facturation. Le nom, l'adresse e-mail, la clé de licence et (si applicable) l'adresse, l'affiliation de la société et les données de paiement sont collectées et traitées par ESET afin de faciliter l'activation de la licence, la remise de la clé de licence, les rappels sur l'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 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 concernant l'installation et votre ordinateur, notamment la plate-forme sur laquelle notre produit est installé, et des informations sur les opérations et fonctionnalités de nos produits (système d'exploitation, informations matérielles, identifiants d'installation, identifiants de licence, adresse IP, adresse MAC, 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 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®. Les hachages unidirectionnels liés à l'infiltration sont traités aux fins du système de réputation ESET LiveGrid® qui améliore l'efficacité de nos solutions de protection contre les programmes malveillants en comparant les fichiers analysés à une base de données d'éléments en liste blanche et liste noire dans le cloud. L'Utilisateur final n'est pas identifié au cours de ce processus.

Système de commentaires ESET LiveGrid®. Échantillons suspects et métadonnées génériques dans le cadre du système de commentaires ESET LiveGrid® qui permet à ESET de réagir immédiatement face aux besoins des utilisateurs finaux et de rester réactifs face aux dernières menaces. Nous dépendons de Vous pour l'envoi

- D'infiltrations (échantillons potentiels de virus et d'autres programmes malveillants et suspects), d'objets problématiques, potentiellement indésirables ou potentiellement dangereux (fichiers exécutables), de messages électroniques que Vous avez signalés comme spam ou détectés par notre produit ;

- D'informations concernant l'utilisation d'Internet, telles que l'adresse IP et des informations géographiques, les paquets IP, les URL et les trames Ethernet ;

- De fichiers de vidage sur incident et des informations qu'ils contiennent.

Nous ne souhaitons pas collecter vos données en dehors de ce cadre, mais cela s'avère parfois impossible. Des données collectées accidentellement peuvent être incluses dans des logiciels malveillants (informations collectées à votre insu ou sans votre consentement) ou dans des noms de fichier ou des URL. Nous ne souhaitons pas que ces données fassent partie de nos systèmes ni qu'elles soient traitées dans le but déclaré dans la présente Politique de confidentialité.

Toutes les informations obtenues et traitées par le système de commentaires ESET LiveGrid® sont destinées à

être utilisées sans l'identification de l'Utilisateur final.

Évaluation de la sécurité des appareils connectés au réseau. Pour fournir la fonction d'évaluation de la sécurité, Nous traitons le nom du réseau local et les informations sur les appareils de votre réseau local, telles que la présence, le type, le nom, l'adresse IP et l'adresse MAC de l'appareil dans votre réseau local en relation avec les informations sur la licence. Les informations comprennent également le type de sécurité sans fil et le type de chiffrement sans fil pour les périphériques de routeur. Les informations relatives à la licence identifiant l'Utilisateur final seront rendues anonymes au plus tard 12 mois après l'expiration de la licence.

Assistance technique. Les informations et données de contact et de licence contenues dans vos demandes d'assistance peuvent être requises pour fournir le service d'assistance. Selon le canal que Vous choisissez pour nous contacter, Nous pouvons collecter votre adresse e-mail, votre numéro de téléphone, des informations sur la licence, des détails sur le produit et la description de votre demande d'assistance. Nous pouvons Vous demander de nous fournir d'autres informations pour faciliter la fourniture du service d'assistance. Les données traitées pour l'assistance technique sont conservées pendant 4 ans.

Protection contre l'utilisation abusive des données. Si le Compte ESET HOME sur https://home.eset.com st créé et que la fonction est activée par l'Utilisateur final dans le cadre du vol de l'ordinateur, les informations suivantes seront collectées et traitées : les données de localisation, les captures d'écran, les données sur 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 de Password Manager, les données relatives à vos informations de connexion sont stockées sous forme chiffrée uniquement sur votre ordinateur ou autre appareil désigné. Si Vous activez le service de synchronisation, les données chiffrées sont stockées sur nos serveurs ou sur les serveurs de nos prestataires de services afin d'assurer la fourniture de ce service. Ni ESET ni le prestataire de services n'a accès aux données chiffrées. Vous êtes la seule personne à détenir la clé permettant de 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 exige la soumission d'échantillons tels que des fichiers prédéfinis et sélectionnés par l'Utilisateur final. Les échantillons que Vous choisissez pour l'analyse à distance seront chargés sur le service ESET, et le résultat de l'analyse sera renvoyé sur Votre ordinateur. Tout échantillon suspect est traité à la manière des informations recueillies par le système de commentaires ESET LiveGrid®.

Programme d'amélioration du produit. Si Vous avez choisi d'activer le Programme d'amélioration du produit , des informations de télémétrie anonymes relatives à l'utilisation de Nos produits seront collectées et utilisées, sur la base de Votre consentement.

Veuillez noter que si la personne utilisant nos produits et services n'est pas l'Utilisateur final qui a acheté le produit ou le service et conclu le Contrat de licence pour l'utilisateur final 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 Contrat de licence pour l'utilisateur final, 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 fournis par Nous conformément au Contrat de licence pour l'utilisateur final.

Coordonnées

Si vous souhaitez exercer vos droits en tant que personne concernée ou si vous avez une question ou un doute, 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