ESET Endpoint Antivirus

Guide de l'utilisateur

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

Digital Security
Progress. Protected.

ESET Endpoint 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 Endpoint Antivirus 7

ESET Endpoint Antivirus 7 représente une nouvelle approche de sécurité informatique véritablement intégrée. La dernière version du moteur d'analyse ThreatSense® 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 Endpoint Antivirus 7 est une solution complète de sécurité, fruit d'efforts soutenus, qui associe protection maximale et encombrement minimal. Les technologies avancées basées sur l'intelligence artificielle sont capables de faire barrage de manière proactive à l'infiltration de virus, de logiciels espions, de chevaux de Troie, de vers, de logiciels publicitaires, de rootkits et d'autres attaques provenant d'Internet, sans réduire les performances ni perturber votre ordinateur.

ESET Endpoint Antivirus 7 est principalement destiné à être utilisé sur des postes de travail dans un environnement de petite entreprise.

Dans la section Utilisation d'ESET Endpoint Antivirus uniquement, des rubriques d'aide sont subdivisées en chapitres et sous-chapitres pour vous aider à trouver plus facilement les informations voulues, notamment sur le téléchargement, l'installation et l'activation.

L'utilisation de ESET Endpoint Antivirus avec ESET Security Management Center dans un environnement d'entreprise vous permet de facilement gérer des postes de travail client, quel que soit leur nombre, d'appliquer des règles et des stratégies, de surveiller les détections et de configurer les clients à distance à partir de n'importe quel ordinateur du réseau.

Le chapitre Questions courantes traite des questions et des problèmes les plus fréquents.

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 Endpoint Antivirus et propose automatiquement des contenus de support mis à jour.
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'antihameçonnage 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 Endpoint Antivirus.
Gestion à distance	ESET Security Management Center vous permet de gérer les produits ESET sur des stations de travail, des serveurs et des appareils mobiles dans un environnement en réseau à partir d'un emplacement central. À l'aide d'ESET Security Management Center Web Console (ESMC Web Console), vous pouvez déployer des solutions ESET, gérer des tâches, appliquer des stratégies de sécurité, surveiller l'état du système et résoudre rapidement les problèmes ou menaces sur les ordinateurs distants.
Protection contre les attaques réseau	Analyse le contenu du trafic réseau et protège contre les attaques réseau. Tout trafic considéré comme nuisible sera bloqué.
Filtrage web (ESET Endpoint Security uniquement)	Le Contrôle Web permet de bloquer les pages Web dont le contenu peut être choquant. En outre, les employés ou les administrateurs système peuvent interdire l'accès à plus de 27 catégories de sites Web prédéfinies et à plus de 140 sous-catégories.

Nouveautés de la version 7

ESET Endpoint Antivirus 7 a été publié et peut être téléchargé.

Nouveautés d'ESET Endpoint Antivirus 7.0

- Nouveau design de l'interface utilisateur graphique
- Analyse par glisser-déposer : vous pouvez analyser manuellement un fichier ou un dossier en le déplaçant vers la zone marquée.
- La protection contre les attaques réseau est maintenant disponible dans ESET Endpoint Antivirus. Pour plus d'informations, consultez Protection contre les attaques réseau.
- Dans État de la protection, le lien d'action rapide peut être désactivé par une stratégie ESET Security Management Center.
- Les règles de contrôle des appareils peuvent maintenant être appliquées à une certaine période. Pour plus d'informations, consultez Créneaux horaires.

Nouveautés d'ESET Endpoint Antivirus 7.1

- Nouveau type de journalisation : la journalisation avancée est maintenant disponible. Pour plus d'informations, consultez Journaux d'audit.

Nouveautés d'ESET Endpoint Antivirus 7.2

- L'apprentissage machine avancé est une 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. La configuration du moteur de détection ne propose plus les boutons bascules ACTIVER/DÉSACTIVER comme dans les versions 7.1 et antérieures. Ces boutons ont été remplacés par quatre seuils : Offensif, Équilibré, Prudent et Désactivé.
- Ajout de la localisation en letton.

- Modifications apportées aux exclusions. Les exclusions de performances permettent d'exclure des fichiers et des dossiers de l'analyse. Les exclusions de détection permettent d'exclure des objets du nettoyage à l'aide du nom de la détection, du chemin d'accès ou du hachage.

- Le nouveau module du programme HIPS comprend l'inspection comportementale approfondie qui analyse le comportement de tous les programmes en cours d'exécution sur l'ordinateur et vous avertit en cas de comportement de processus malveillant. Informations supplémentaires sur HIPS dans les pages d'aide.

- Les alertes interactives configurables permettent d'ajuster le comportement des alertes interactives configurables (par exemple, masquer l'alerte « Redémarrage recommandé » sur les ordinateurs endpoint).

Nouveautés d'ESET Endpoint Antivirus 7.3

- Cette version mineure contient plusieurs corrections de bogue et améliorations des performances.

Pour obtenir des informations et des captures d'écran supplémentaires sur les nouvelles fonctionnalités d'ESET Endpoint Antivirus, veuillez consulter l'article suivant de la base de connaissances ESET :

- Nouveautés d'ESET Endpoint Antivirus 7

Configuration système

Pour garantir le fonctionnement sans problème de ESET Endpoint Antivirus, le système doit répondre à la configuration matérielle et logicielle suivante (paramètres par défaut du produit) :

Processeurs pris en charge

Processeur 32 bits (x86) avec jeu d'instructions SSE2 ou 64 bits (x64), 1 GHz ou vitesse supérieure

Systèmes d’exploitation

Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8

Microsoft® Windows® 7 SP1 avec les dernières mises à jour de Windows (KB4474419 et KB4490628 au minimum)

Windows XP et Windows Vista ne sont plus pris en charge par la version 7.

Autre

- Respect de la configuration requise du système d'exploitation et des autres logiciels installés sur l'ordinateur

- 0,3 Go de mémoire système disponible (voir la remarque 1)

- 1 Go d'espace disque disponible (voir la remarque 2)

- Résolution graphique 1 024 x 768 (au minimum)
- Connexion Internet ou LAN à une source (voir la remarque 3) de mises à jour des produits

Bien qu'il soit possible d'installer et d'exécuter le produit sur des systèmes qui ne répondent pas à cette configuration, il est recommandé d'effectuer au préalable des tests d'utilisation selon les exigences de performances.

Remarque
(1) : Le produit peut utiliser plus de mémoire lorsque la mémoire est inutilisée sur un ordinateur infecté ou lorsque de grandes listes de données sont importées dans le produit (listes blanches d'URL, par exemple).
(2) : Espace disque nécessaire pour télécharger le programme d'installation, installer le produit et conserver une copie du package d'installation dans les données du programme ainsi que des sauvegardes des mises à jour du produit pour la fonctionnalité de restauration. Le produit peut utiliser davantage d'espace disque selon les paramètres (lorsque davantage de versions de sauvegarde du produit sont stockées ou que des grandes quantités d'entrées de journaux sont conservées, par exemple) ou sur un ordinateur infecté (en raison de la fonctionnalité de mise en quarantaine). Il est recommandé de conserver suffisamment d'espace disque pour prendre en charge les mises à jour du système et des produits ESET.
(3) : Bien que ce type de mise à jour ne soit pas recommandé, le produit peut être mis à jour manuellement à partir d'un support amovible.

Langues prises en charge

ESET Endpoint Antivirus peut être installé et téléchargé dans les langues ci-après.

Langue	Code de langue	LCID
Anglais (États-Unis)	en-US	1033
Arabe (Égypte)	ar-EG	3073
Bulgare	bg-BG	1026
Chinois simplifié	zh-CN	2052
Chinois traditionnel	zh-TW	1028
Croate	hr-HR	1050
Tchèque	cs-CZ	1029
Estonien	et-EE	1061
Finnois	fi-FI	1035
Français (France)	fr-FR	1036
Français (Canada)	fr-CA	3084
Allemand (Allemagne)	de-DE	1031
Grec	el-GR	1032
*Hébreu	he-IL	1037
Hongrois	hu-HU	1038
*Indonésien	id-ID	1057
Italien	it-IT	1040

Japonais	ja-JP	1041
Kazakh	kk-KZ	1087
Coréen	ko-KR	1042
*Letton	lv-LV	1062
Lituanien	lt-LT	1063
Norvégien	nb-NO	1044
Polonais	pl-PL	1045
Portugais (Brésil)	pt-BR	1046
Roumain	ro-RO	1048
Russe	ru-RU	1049
Espagnol (Chili)	es-CL	13322
Espagnol (Espagne)	es-ES	3082
Suédois (Suède)	sv-SE	1053
Slovaque	sk-SK	1051
Slovène	sl-SI	1060
Thaï	th-TH	1054
Turc	tr-TR	1055
*Vietnamien	vi-VN	1066

* ESET Endpoint Antivirus est disponible dans cette langue, mais le guide de l'utilisateur en ligne ne l'est pas (redirection vers la version anglaise).

Pour changer la langue de ce guide de l'utilisateur en ligne, utilisez la zone de sélection de la langue (dans le coin supérieur droit).

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

Télécharger les patchs de sécurité

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

Sauvegarder les données importantes

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

Rechercher régulièrement les virus sur votre ordinateur

La détection de virus, de vers, de chevaux de Troie et de rootkits, connus et inconnus, est gérée par le module de protection du système de fichiers en temps réel. Cela signifie qu'à chaque fois que vous accédez à un fichier ou que vous l'ouvrez, il est analysé afin de détecter toute trace de logiciels malveillants. Nous vous recommandons de lancer une analyse complète de l'ordinateur au moins une fois par mois, car les logiciels malveillants peuvent varier et 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 les fichiers d'aide ESET Endpoint Antivirus. Les informations fournies ici permettent de vous familiariser avec le produit et vous aident à sécuriser votre ordinateur.

Mise en route

Avant de commencer à utiliser ESET Endpoint Antivirus, notez que le produit présente les deux modes d'utilisation suivants : utilisateurs connectés via ESET Security Management Center ou utilisation unique. Nous vous recommandons également de vous familiariser avec les différents types de détections et attaques distantes auxquels vous êtes exposé lorsque vous utilisez votre ordinateur.

Consultez les nouvelles fonctionnalités pour découvrir les fonctionnalités ajoutées à cette version d'ESET Endpoint Antivirus. Nous avons également préparé un guide qui vous aidera à configurer et à personnaliser les paramètres de base ESET Endpoint Antivirus.

Utilisation des pages d'aide ESET Endpoint Antivirus

Pour vous aider à trouver plus facilement les informations voulues, les rubriques d'aide sont subdivisées en chapitres et sous-chapitres. Vous pouvez trouver des informations connexes en parcourant la structure des pages d'aide.

Pour obtenir des informations sur toute fenêtre du programme, appuyez sur **F1**. La page d'aide relative à la fenêtre actuellement affichée apparaîtra.

Vour pouvez effectuer des recherches dans les pages d'aide par mot-clé 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 les noms des paramètres ESET Endpoint Antivirus. Un ensemble uniforme de symboles est également utilisé pour souligner des informations importantes.

REMARQUE
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).

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

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

Exemple
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 indiquant les informations que vous devez fournir. 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.

Documentation pour les endpoints administrés à distance

Les produits pour les professionnels ESET ainsi qu'ESET Endpoint Antivirus peuvent être gérés à distance sur des postes de travail clients, des serveurs et des appareils mobiles dans un environnement en réseau à partir d'un emplacement central. Les administrateurs système qui administrent plus de 10 postes de travail clients peuvent envisager de déployer l'un des outils de gestion à distance ESET pour déployer des solutions ESET, gérer des tâches, appliquer des politiques de sécurité, surveiller l'état du système et résoudre rapidement les problèmes ou menaces sur les ordinateurs distants à partir d'un emplacement central.

Outils de gestion à distance ESET

ESET Endpoint Antivirus peut être géré à distance par ESET Security Management Center ou ESET PROTECT Cloud.

- Présentation de ESET Security Management Center
- Présentation de ESET PROTECT Cloud

Outils de gestion à distance tiers

- Surveillance et administration à distance (RMM)

Bonnes pratiques

- Connectez tous les endpoints avec ESET Endpoint Antivirus à ESET Security Management Center
- Protégez les paramètres des configurations avancées sur les ordinateurs clients connectés pour éviter toute modification non autorisée
- Appliquez une politique recommandée pour utiliser les fonctionnalités de sécurité disponibles
- Limitez l'utilisation de l'interface utilisateur pour réduire ou limiter l'interaction des utilisateurs avec ESET Endpoint Antivirus

Guides de procédure

- Utilisation du mode de remplacement
- Comment déployer ESET Endpoint Antivirus à l'aide de GPO ou SCCM

Présentation de ESET Security Management Center

ESET Security Management Center permet de gérer les produits ESET sur des postes de travail, des serveurs et des appareils mobiles dans un environnement en réseau à partir d'un emplacement central.

ESET Security Management Center (ESMC) est une nouvelle génération de système de gestion à distance, très différente des versions précédentes d'ESET Remote Administrator (ERA). Parce que son architecture est totalement différente, ESET Security Management Center 7 n'est que partiellement compatible avec ERA 6 et n'est pas rétrocompatible avec ERA 5. Toutefois, la compatibilité est maintenue avec les versions précédentes des produits de sécurité ESET.

Pour effectuer un déploiement complet du portefeuille de solutions de sécurité ESET, les composants suivants doivent être installés (plates-formes Windows et Linux) :

- ESMC Server
- ESMC Console Web
- ESET Management Agent

Bien que les composants de prise en charge suivants soient facultatifs, il est recommandé de les installer pour optimiser les performances de l'application sur le réseau :

- Capteur RD
- Apache HTTP Proxy
- Connecteur d'appareil mobile

À l'aide de la console web ESET Security Management Center Web Console (ESMC Web Console), vous pouvez déployer les solutions ESET, gérer des tâches, appliquer des politiques de sécurité, surveiller l'état du système et réagir rapidement aux problèmes ou aux menaces sur les ordinateurs distants.

Plus d'informations

Pour plus d'informations, consultez leguide de l'utilisateur en ligne de ESET Security Management Center.

Présentation de ESET PROTECT Cloud

ESET PROTECT Cloud vous permet de gérer les produits ESET sur des postes de travail et des serveurs dans un environnement en réseau à partir d'un emplacement central sans avoir besoin d'un serveur physique ou virtuel comme pour ESMC. À l'aide de la console Web ESET PROTECT Cloud, vous pouvez déployer des solutions ESET, gérer des tâches, appliquer des stratégies de sécurité, surveiller l'état du système et résoudre rapidement les

problèmes ou menaces sur les ordinateurs distants.

- Obtenez des informations supplémentaires dans le guide de l'utilisateur en ligne de ESET PROTECT Cloud.

Paramètres protégés par mot de passe

Afin de procurer une sécurité maximale à votre système, ESET Endpoint Antivirus doit être configuré correctement. Tout changement ou paramètre inapproprié peut réduire la sécurité du client et son niveau de protection. Pour limiter l'accès des utilisateurs aux paramètres avancés, un administrateur peut protéger les paramètres par mot de passe.

L'administrateur peut créer une politique de façon à protéger les paramètres de configuration avancée d'ESET Endpoint Antivirus par mot de passe sur les ordinateurs clients connectés. Pour créer une politique :

1. Dans ESMC Web Console, cliquez sur **Stratégies** dans le menu principal placé à gauche.

2. Cliquez sur **Nouvelle stratégie**.

3. Donnez un nom à votre nouvelle stratégie et ajoutez éventuellement une brève description. Cliquez sur le bouton **Continuer**.

4. Dans la liste des produits, sélectionnez **ESET Endpoint pour Windows**.

5. Cliquez sur **Interface utilisateur** dans la liste **Paramètres** et développez **Configuration de l'accès**.

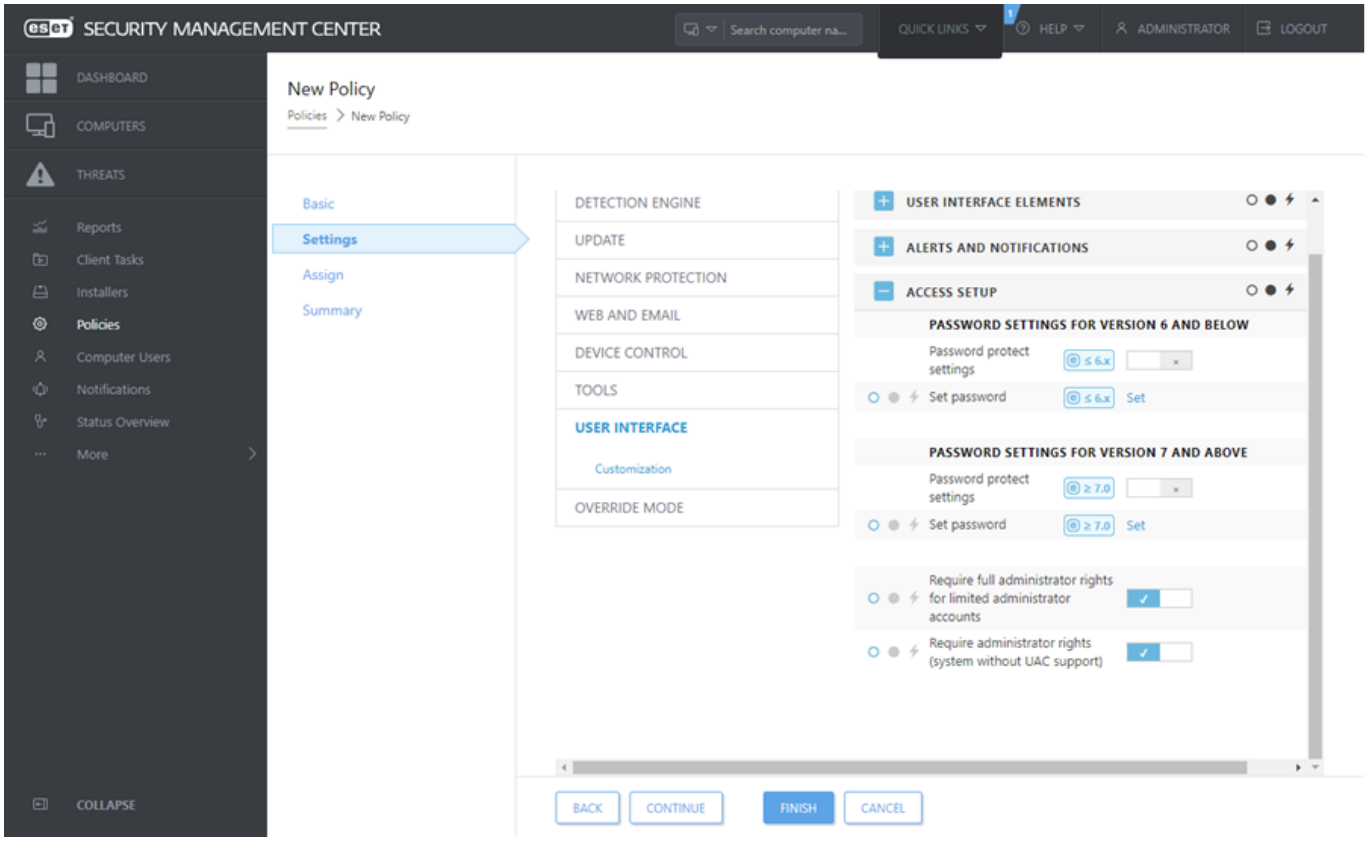
6. Selon la version de ESET Endpoint Antivirus, cliquez sur la barre du curseur afin d'activer **Mot de passe pour protéger les paramètres**. Notez que les produits ESET Endpoint offre une protection améliorée. Si vous disposez des versions 7 et 6 des produits Endpoint sur le réseau, définissez un mot de passe différent pour chacune des versions. Il est recommandé de ne pas définir de mot de passe uniquement dans le champ de la version 6, car cela affaiblit la sécurité des produits Endpoint de version 7.

7. Dans la fenêtre contextuelle, créez un mot de passe, confirmez-le et cliquez sur **OK**. Cliquez sur **Continuer**.

8. Affectez la politique aux clients. Cliquez sur **Affecter** et sélectionnez les ordinateurs ou les groupes d'ordinateurs à protéger par mot de passe. Cliquez sur **OK** pour confirmer.

9. Vérifiez que tous les ordinateurs clients souhaités se trouvent dans la liste cible et cliquez sur **Continuer**.

10. Passez en revue les paramètres de la stratégie dans le résumé et cliquez sur **Terminer** pour enregistrer votre nouvelle stratégie.



Présentation des politiques

L'administrateur peut transmettre des configurations spécifiques aux produits ESET s'exécutant sur les ordinateurs clients à l'aide de stratégies d'ESMC Web Console. Une stratégie peut être appliquée directement à des ordinateurs individuels ou à des groupes d'ordinateurs. Vous pouvez également affecter plusieurs stratégies à un ordinateur ou à un groupe.

Un utilisateur doit disposer des autorisations suivantes pour créer une stratégie : autorisation **Lire** afin de lire la liste de stratégies, autorisation **Utiliser** de façon à affecter des stratégies aux ordinateurs cibles et autorisation **Écrire** pour créer ou modifier les stratégies.

Les stratégies sont appliquées dans l'ordre dans lequel les groupes statiques sont disposés. Cela n'est pas le cas pour les groupes dynamiques, où les groupes dynamiques enfants sont d'abord parcourus. Vous pouvez ainsi appliquer des stratégies avec un plus grand impact au niveau supérieur de l'arborescence des groupes et des stratégies plus spécifiques pour les sous-groupes. À l'aide des indicateurs, un utilisateur ESET Endpoint Antivirus ayant accès aux groupes situés à un niveau supérieur de l'arborescence peut remplacer les stratégies des groupes de niveau inférieur. L'algorithme est expliqué en détail dans l'aide en ligne d'ESMC.

Affectation de stratégies plus génériques

Il est recommandé d'affecter des stratégies plus génériques (la stratégie de mise à jour du serveur, par exemple) aux groupes dont le niveau est supérieur dans l'arborescence des groupes. Les stratégies plus spécifiques (des paramètres de contrôle des appareils, par exemple) doivent être appliquées aux groupes de niveau inférieur. La stratégie de niveau inférieur remplace généralement les paramètres des stratégies de niveau supérieur lors de la fusion (à moins que des indicateurs de stratégie n'aient été définis autrement).

Fusion des politiques

Une stratégie appliquée à un client est généralement le résultat de plusieurs stratégies fusionnées en une seule stratégie finale. Les stratégies sont fusionnées une par une. Lors de la fusion des stratégies, la dernière stratégie remplace toujours les paramètres définis par la précédente. Pour modifier ce comportement, vous pouvez utiliser des indicateurs de stratégie (disponibles pour chaque paramètre).

Lors de la création des stratégies, vous pourrez constater que certains paramètres possèdent une règle supplémentaire (remplacer/ajouter à la fin/ajouter au début) que vous pouvez configurer.

- **Remplacer** : remplace toute la liste, ajoute de nouvelles valeurs et supprime toutes les valeurs précédentes.
- **Ajouter à la fin** : les éléments sont ajoutés en bas de la liste actuellement appliquée (il doit s'agir d'une autre stratégie, et la liste locale est toujours remplacée).
- **Ajouter au début** : les éléments sont ajoutés en haut de la liste (la liste locale est remplacée).

ESET Endpoint Antivirus prend en charge la fusion de paramètres locaux avec les stratégies distantes d'une nouvelle manière. Si le paramètre est une liste (par exemple, une liste de sites Web bloqués) et si une stratégie distante est en conflit avec un paramètre local existant, la stratégie distante le remplace. Vous pouvez choisir comment combiner des listes locales et distantes en sélectionnant les différentes règles de fusion afin de :

- Fusionner des paramètres pour les politiques distantes
- Fusionner des politiques distantes et locales : paramètres locaux avec la politique distante obtenue

Pour plus d'informations sur la fusion des politique, reportez-vous au guide de l'utilisateur en ligne ESMC et consultez l'exemple.

Fonctionnement des indicateurs

La stratégie appliquée à un ordinateur client est généralement le résultat de la fusion de plusieurs stratégies en une stratégie finale. Lors de la fusion de stratégies, vous pouvez ajuster le comportement attendu de la stratégie finale, en raison de l'ordre des stratégies appliquées, au moyen d'indicateurs de stratégies. Les indicateurs définissent la façon dont la stratégie gère un paramètre spécifique.

Pour chaque paramètre, vous pouvez sélectionner l'un des indicateurs suivants :

Ne pas appliquer	Ne pas appliquer : un paramètre associé à cet indicateur n'est pas défini par la stratégie. N'étant pas défini par la stratégie, il peut être modifié par les autres stratégies appliquées ultérieurement.
Appliquer	Les paramètres portant l'indicateur **Appliquer** sont appliqués sur l'ordinateur client. Toutefois, lors de la fusion des stratégies, il peut être remplacé par d'autres stratégies appliquées ultérieurement. Lorsqu'une stratégie est envoyée à un ordinateur client contenant des paramètres marqués avec cet indicateur, ces paramètres modifient la configuration locale de l'ordinateur client. Ce paramètre n'étant pas forcé, il peut être modifié par d'autres stratégies appliquées ultérieurement.

Forcer	Les paramètres portant l'indicateur **Forcer** sont prioritaires et ne peuvent être remplacés par aucune stratégie appliquée ultérieurement (même si elle est également marquée d'un indicateur **Forcer**). Cela assure que les autres stratégies appliquées ultérieurement ne pourront pas changer ce paramètre lors de la fusion. Lorsqu'une stratégie est envoyée à un ordinateur client contenant des paramètres marqués avec cet indicateur, ces paramètres modifient la configuration locale de l'ordinateur client.

Exemple : autoriser les utilisateurs à afficher toutes les stratégies

Scénario : l'*administrateur* veut autoriser l'utilisateur *John* à créer et modifier des stratégies dans son groupe parent et à afficher les stratégies créées par l'*administrateur*, y compris les stratégies marquées de l'indicateur Forcer. L'*administrateur* souhaite que *John* puisse voir toutes les stratégies, mais sans pouvoir modifier les stratégies existantes créées par l'*administrateur*. *John* peut uniquement créer ou modifier des stratégies au sein de son groupe parent, San Diego.
Solution : l'*administrateur* doit procéder comme suit :

Créer des groupes statiques et des jeux d'autorisations personnalisés

1. Il doit créer un groupe statique appelé *San Diego*.
2. Il doit créer un jeu d'autorisations appelé *Stratégie - Tous John* avec un accès au groupe statique *Tous* et une autorisation **Lire** pour **Stratégies**.
3. Il doit créer un jeu d'autorisations appelé *Stratégie John* avec un accès au groupe statique *San Diego* et une autorisation **Écrire** pour **Groupe et ordinateurs** et **Stratégies**. Ce jeu d'autorisations permet à *John* de créer ou modifier des stratégies dans son groupe parent *San Diego*.
4. Il doit créer l'utilisateur *John* et sélectionner dans la section **Jeux d'autorisations** *Stratégie - Tous John* et *Stratégie John*.

Créer les politiques

5. Il doit créer la stratégie *Tous - Activer le pare-feu*, développer la section **Paramètres**, sélectionner **ESET Endpoint pour Windows**, accéder à **Pare-feu personnel** > **Général** et appliquer tous les paramètres par l'indicateur **Forcer**. Il doit développer la section **Affecter** et sélectionner le groupe statique *Tous*.
6. Il doit créer la nouvelle stratégie *Groupe de John - Activer le pare-feu*, développer la section **Paramètre**, sélectionner **ESET Endpoint pour Windows**, accéder à **Pare-feu personnel** > **Général** et appliquer tous les paramètres par l'indicateur **Appliquer**. Il doit développer la section **Affecter** et sélectionner le groupe statique *San Diego*.

Résultat

Les stratégies créées par l'*administrateur* sont appliquées en premier, car les indicateurs **Forcer** ont été appliqués aux paramètres de la stratégie. Les paramètres portant l'indicateur Forcer sont prioritaires et ne peuvent être remplacés par aucune stratégie appliquée ultérieurement. Les stratégies créées par l'utilisateur *John* sont appliquées après celles créées par l'administrateur.
Pour afficher l'ordre de la stratégie finale, accédez à **Plus** > **Groupes** > **San Diego**. Sélectionnez l'ordinateur puis **Afficher les détails**. Dans la section **Configuration**, cliquez sur **Stratégies appliquées**.

Utilisation d'ESET Endpoint Antivirus uniquement

Cette section et la section Utilisation de ESET Endpoint Antivirus du guide de l'utilisateur est destinée aux utilisateurs qui emploient ESET Endpoint Antivirus sans ESET Security Management Center ou ESET PROTECT Cloud. Toutes les fonctions et fonctionnalités d'ESET Endpoint Antivirus sont entièrement accessibles selon les droits du compte de l'utilisateur.

Méthode d'installation

Vous pouvez utiliser plusieurs méthodes d'installation d'ESET Endpoint Antivirus version 7.x sur un poste de travail client, sauf si vous déployez ESET Endpoint Antivirus à distance sur des postes de travails clients via ESET Security Management Center ou ESET PROTECT Cloud.

- Cliquez ici si vous souhaitez installer ou mettre à niveau ESET Endpoint Antivirus vers la version 6.6.x

Méthodes	Objectif	Lien de téléchargement
Installation à l'aide d'ESET AV Remover	L'outil ESET AV Remover permet de supprimer presque tous les logiciels antivirus précédemment installés sur votre système avant de procéder à l'installation.	Télécharger la version 64 bits Télécharger la version 32 bits
Installation (.exe)	Installation sans ESET AV Remover.	N/A
Installation (.msi)	Dans les environnements d'entreprise, le programme d'installation .msi est le package d'installation préféré, principalement en raison des déploiements hors ligne et distants qui utilisent différents outils tels que ESET Security Management Center.	Télécharger la version 64 bits Télécharger la version 32 bits
Installation à l'aide d'une ligne de commande	ESET Endpoint Antivirus peut être installé localement à l'aide d'une ligne de commande ou à distance à l'aide d'une tâche client d'ESET Security Management Center.	N/A
Déploiement à l'aide de GPO ou SCCM	Utilisez des outils de gestion tels que GPO ou SCCM pour déployer ESET Management Agent et ESET Endpoint Antivirus sur les postes de travail clients.	N/A
Déploiement à l'aide des outils RMM	Les modules d'extension ESET DEM pour l'outil RMM permettent de déployer ESET Endpoint Antivirus sur des postes de travail clients.	N/A

ESET Endpoint Antivirus est disponible dans plus de 30 langues.

Installation à l'aide d'ESET AV Remover

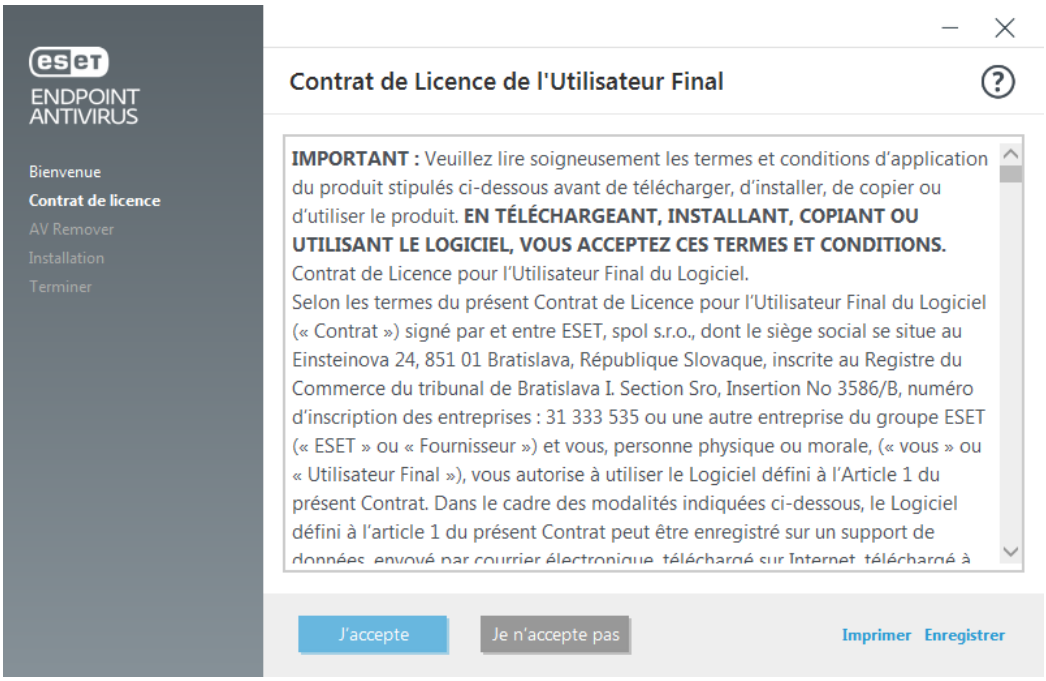
Avant de continuer la procédure d'installation, il est important de désinstaller toutes les applications de sécurité de l'ordinateur. Cochez la case en regard de l'option **Je souhaite désinstaller les applications antivirus indésirables à l'aide d'ESET AV Remover** pour qu'ESET AV Remover recherche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

ESET AV Remover

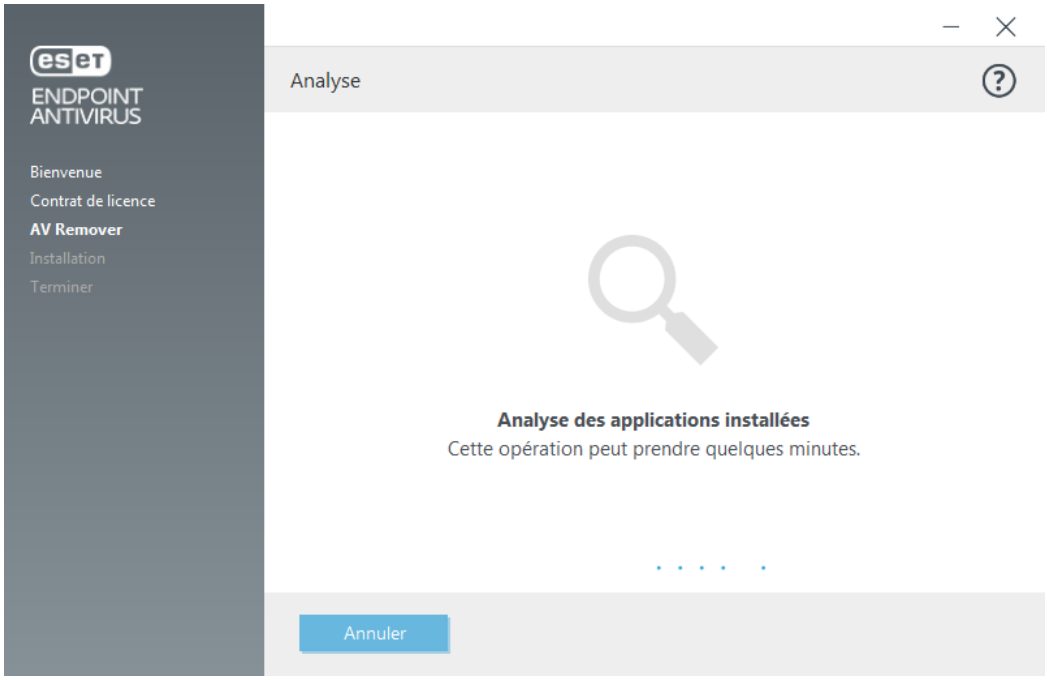
L'outil ESET AV Remover permet de supprimer presque tous les logiciels antivirus précédemment installés sur votre système. Pour supprimer un programme antivirus existant à l'aide d'ESET AV Remover, suivez les instructions ci-après.

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

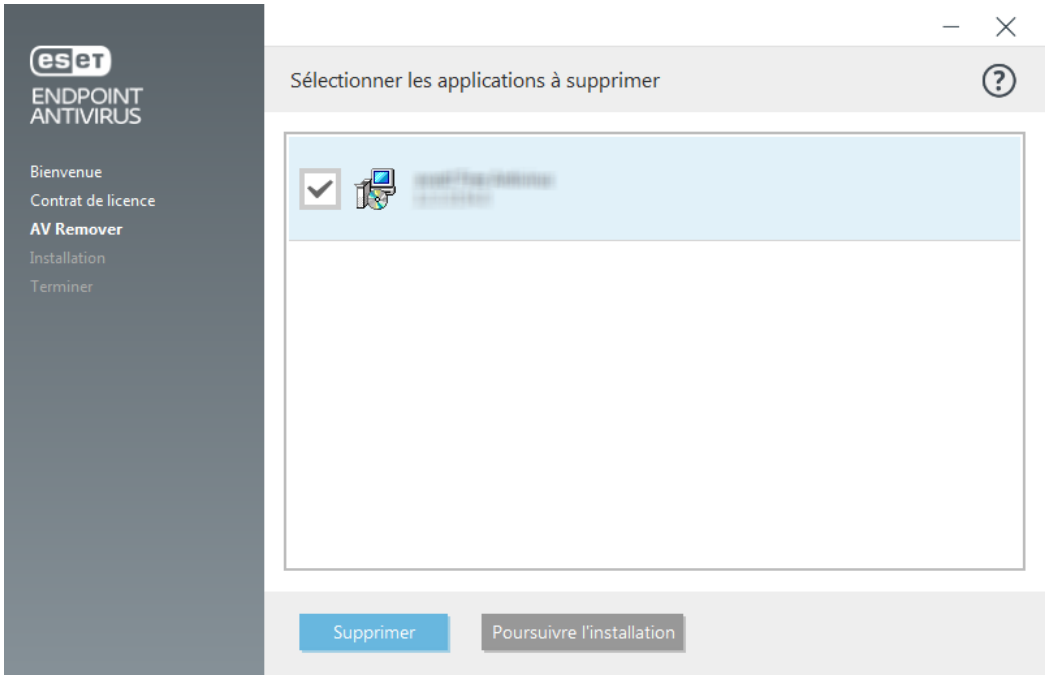
2. Lisez les termes du contrat de licence de l'utilisateur final, puis cliquez sur **Accepter** pour confirmer que vous les acceptez. Si vous cliquez sur **Refuser**, l'installation de ESET Endpoint Antivirus continue sans la suppression des applications de sécurité existantes sur l'ordinateur.



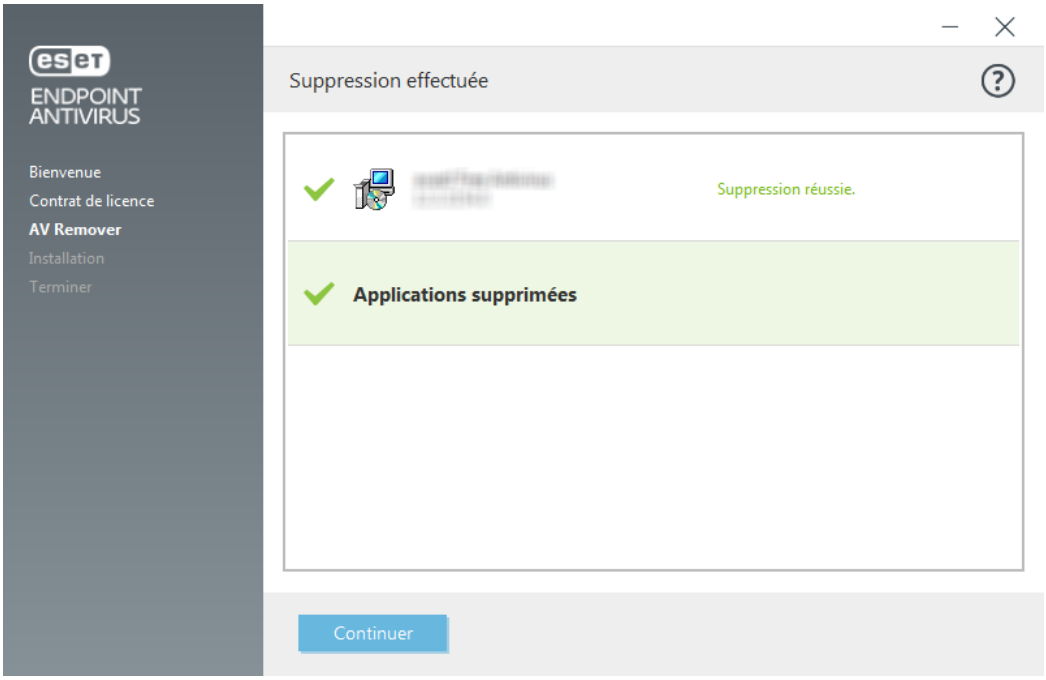
3. ESET AV Remover commence à rechercher les logiciels antivirus sur votre système.



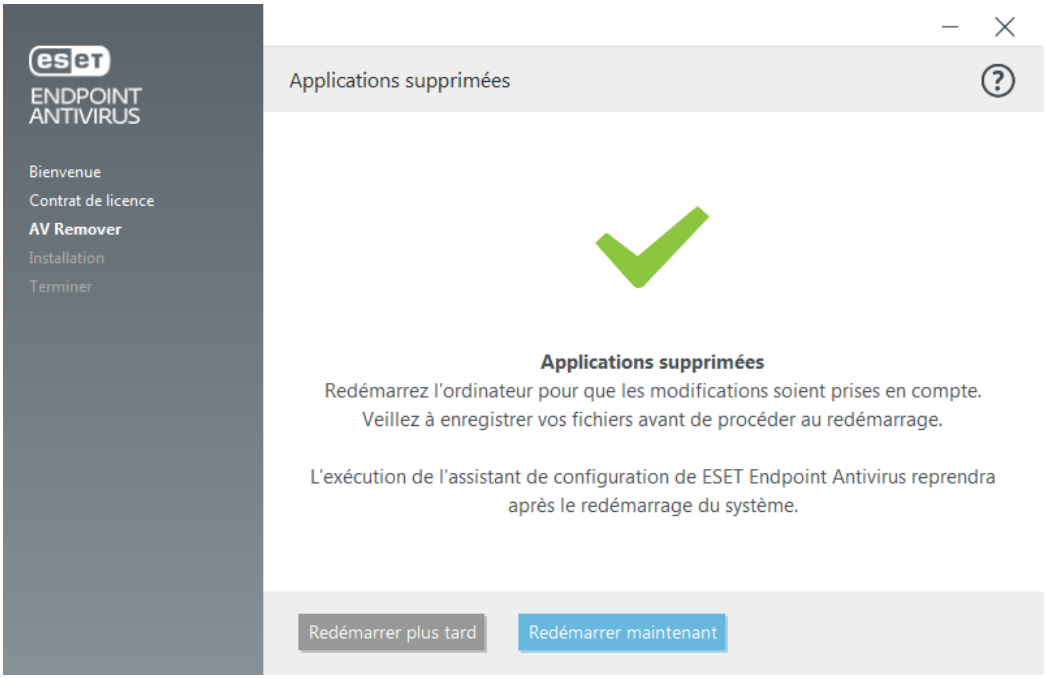
4. Sélectionnez les applications antivirus répertoriées, puis cliquez sur **Supprimer**. La suppression peut prendre quelques instants.



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



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



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

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

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

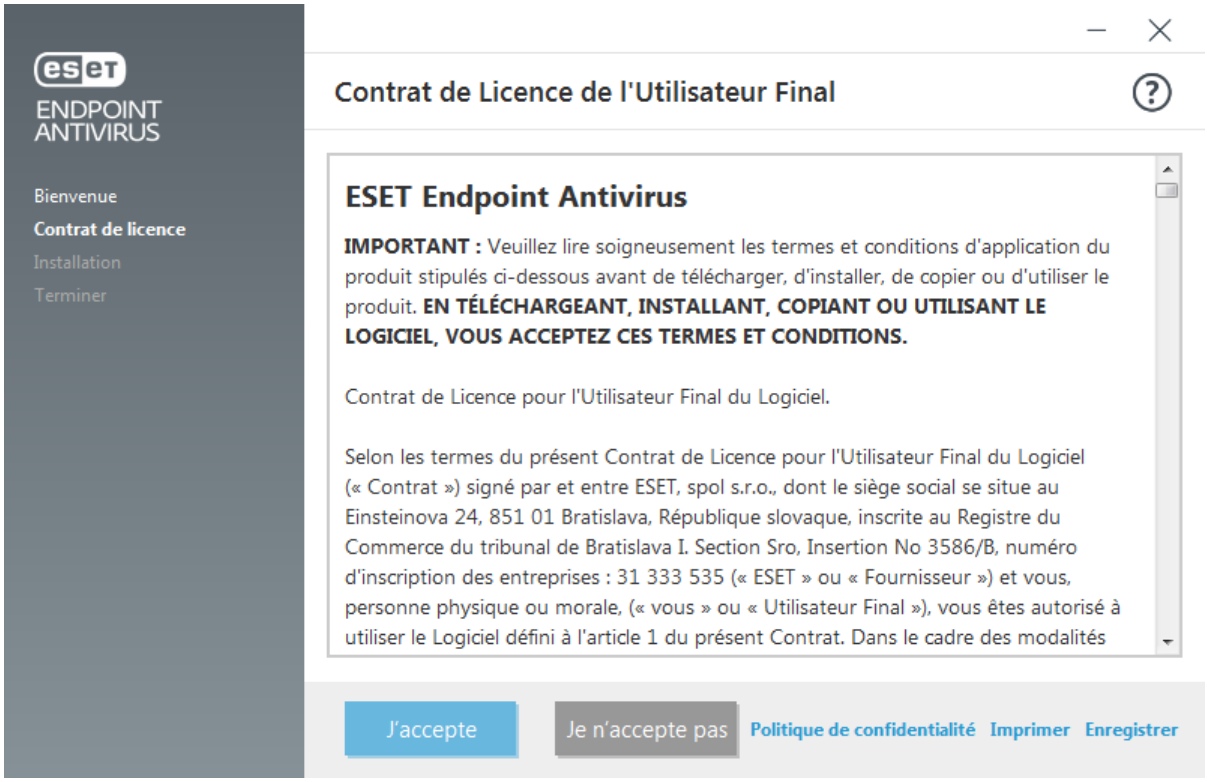
Si nécessaire, contactez le support technique ESET pour effectuer une demande d'assistance. Ayez à disposition le fichier **AppRemover.log** pour aider les techniciens ESET. Le fichier **AppRemover.log** est situé dans le dossier **eset**. Naviguez jusqu'au répertoire *%TEMP%* dans l'Explorateur Windows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

Installation (.exe)

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

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

1. Lisez le Contrat de Licence de l'utilisateur final et cliquez sur **J'accepte** pour confirmer que vous acceptez les clauses de celui-ci. Après avoir accepté les termes du contrat, cliquez sur **Suivant** pour poursuivre l'installation.

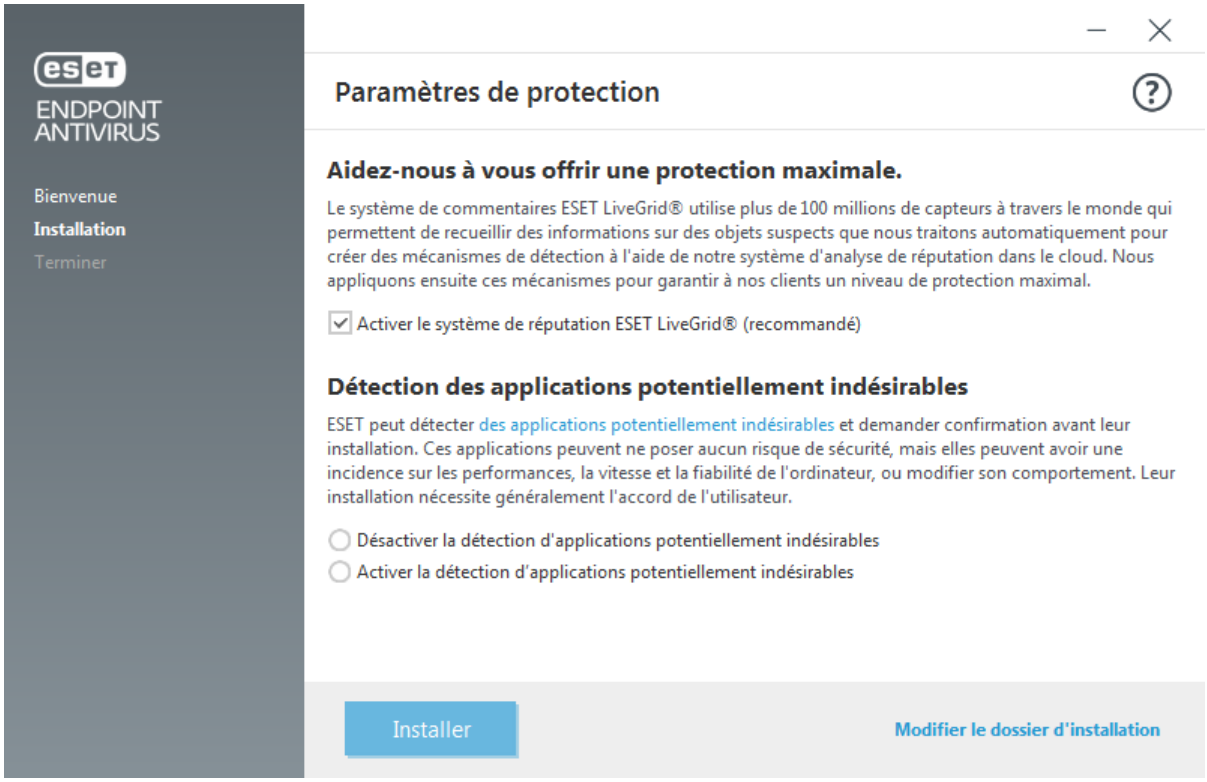


2. Indiquez si vous souhaitez activer le système de commentaire ESET LiveGrid®. ESET LiveGrid® contribue à garantir qu'ESET est informé immédiatement et en continu des nouvelles infiltrations, afin de mieux protéger ses clients. Le système permet de soumettre les nouvelles menaces au laboratoire ESET, où elles sont analysées, traitées, puis ajoutées au moteur de détection.

3. L'étape suivante de l'installation consiste à configurer la détection des applications potentiellement indésirables. Reportez-vous au chapitre Applications potentiellement indésirables pour plus d'informations.

Vous pouvez installer ESET Endpoint Antivirus dans un dossier spécifique en cliquant sur **Modifier le dossier d'installation**.

5. La dernière étape consiste à confirmer l'installation en cliquant sur **Installer**. Une fois l'installation terminée, vous êtes invité à activer ESET Endpoint Antivirus.



Modification du dossier d'installation (.exe)

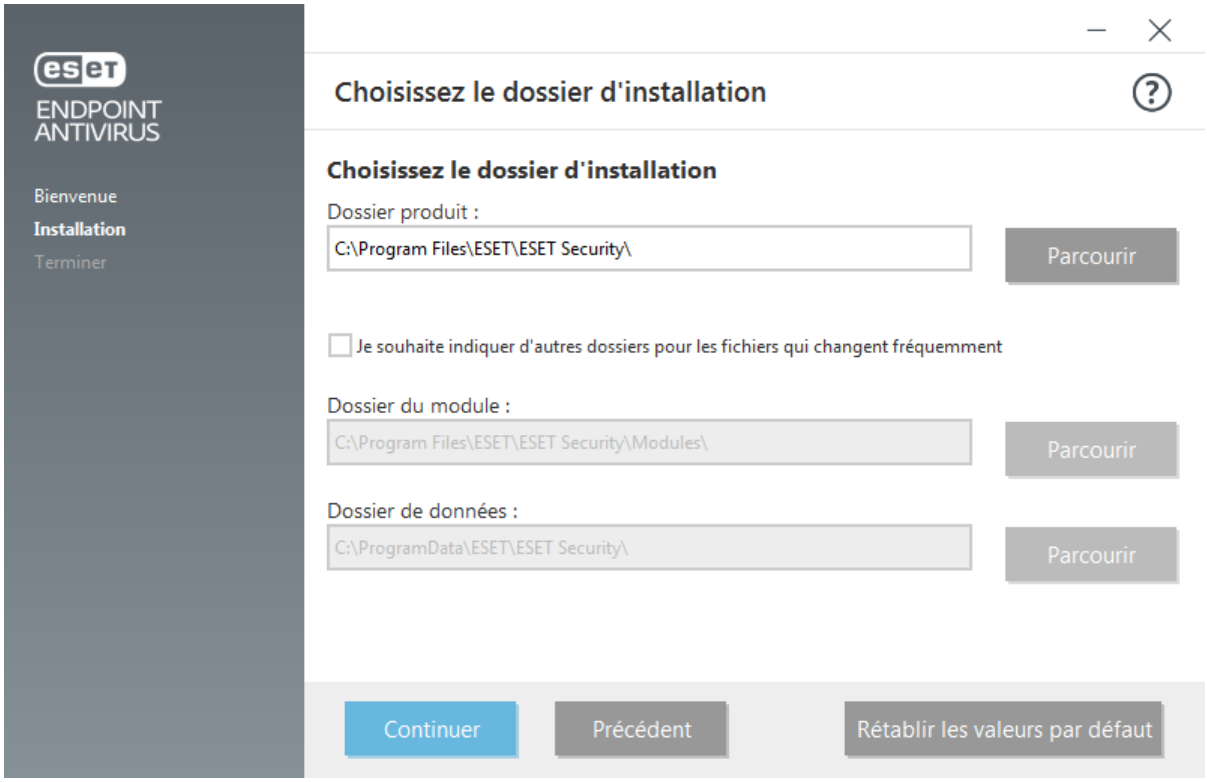
Une fois que vous avez sélectionné votre préférence pour la détection des applications potentiellement indésirables et que vous avez cliqué sur **Modifier le dossier d'installation**, vous êtes invité à sélectionner un emplacement pour le dossier d'installation du produit ESET Endpoint Antivirus. Par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

C:\Program Files\ESET\ESET Security

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

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

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



Cliquez sur **Continuer**, puis sur **Installer** pour démarrer l'installation.

Installation (.msi)

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

Objectif du programme d'installation .msi

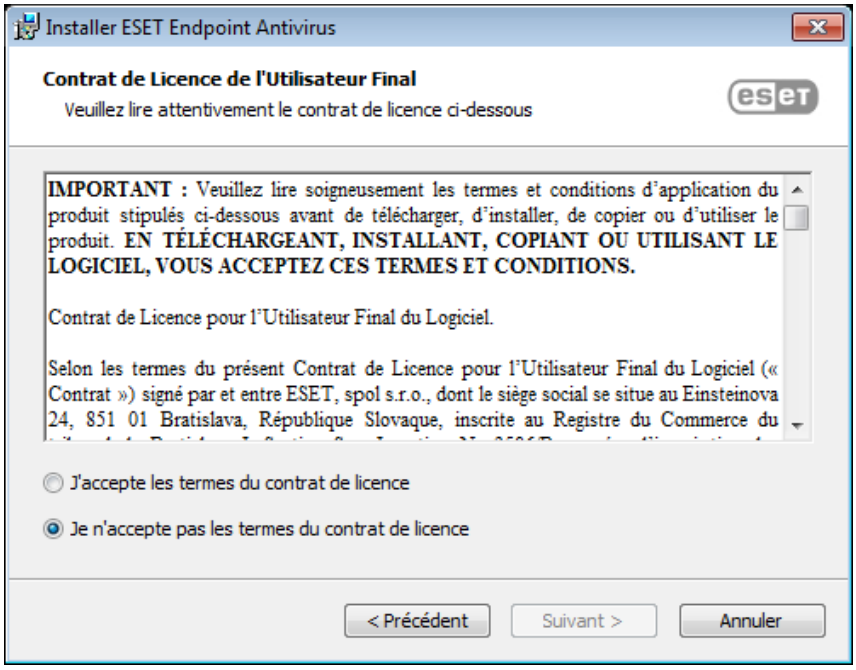
Dans les environnements d'entreprise, le programme d'installation .msi est le package d'installation préféré, principalement en raison des déploiements hors ligne et distants qui utilisent différents outils tels que ESET Security Management Center.

Important

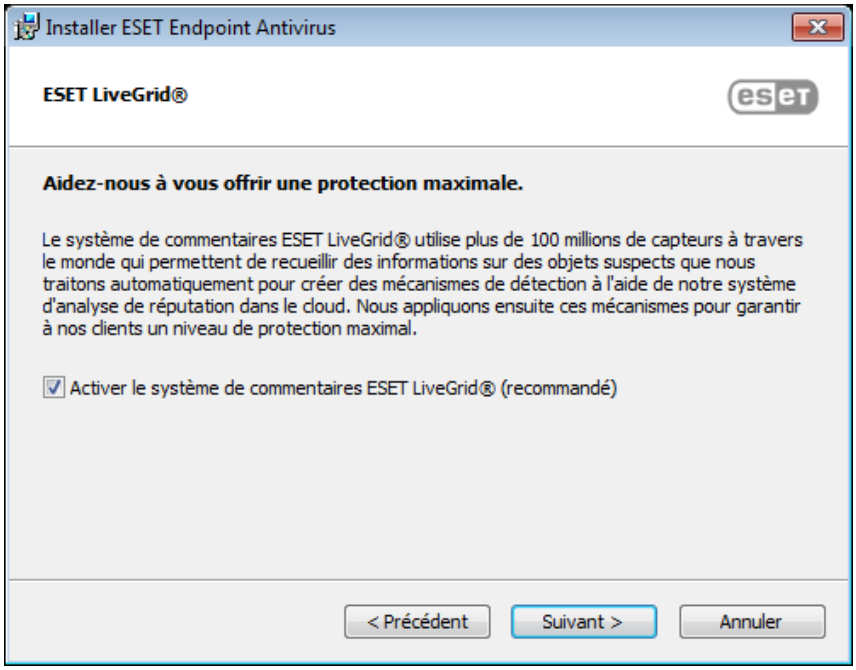
Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si plusieurs solutions antivirus sont installées sur un même ordinateur, elles risquent de provoquer des conflits. Nous recommandons de désinstaller tout autre antivirus de votre système. Reportez-vous à notre article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

1. Sélectionnez la langue souhaitée, puis cliquez sur **Suivant**.

2. Lisez le Contrat de Licence de l'utilisateur final et cliquez sur **J'accepte les termes du contrat de licence** pour confirmer que vous acceptez les clauses de celui-ci. Après avoir accepté les termes du contrat, cliquez sur **Suivant** pour poursuivre l'installation.

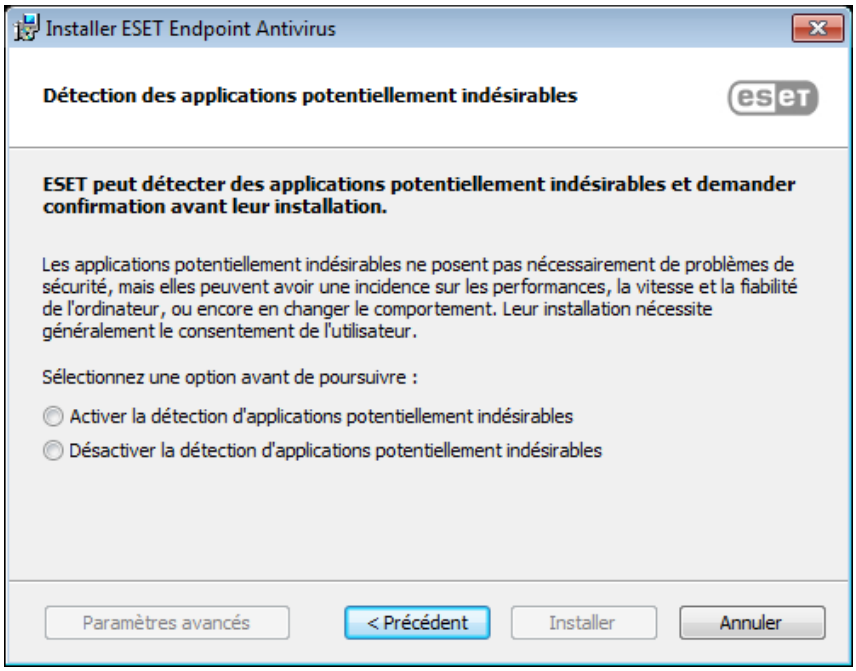


3. Sélectionnez votre préférence en ce qui concerne le système de commentaire ESET LiveGrid®. ESET LiveGrid® contribue à garantir qu'ESET est informé immédiatement et en continu des nouvelles infiltrations, afin de mieux protéger ses clients. Le système permet de soumettre les nouvelles menaces au laboratoire ESET, où elles sont analysées, traitées, puis ajoutées au moteur de détection.



4. L'étape suivante de l'installation consiste à configurer la détection des applications potentiellement indésirables. Reportez-vous au chapitre Applications potentiellement indésirables pour plus d'informations.

Cliquez sur **Paramètres avancés** si vous souhaitez effectuer une installation avancée (.msi).



5. La dernière étape consiste à confirmer l'installation en cliquant sur **Installer**. Une fois l'installation terminée, vous êtes invité à activer ESET Endpoint Antivirus.

Installation avancée (.msi)

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

5. Une fois que vous avez sélectionné votre préférence pour la détection des applications potentiellement indésirables et que vous avez cliqué sur **Paramètres avancés**, vous êtes invité à sélectionner un emplacement

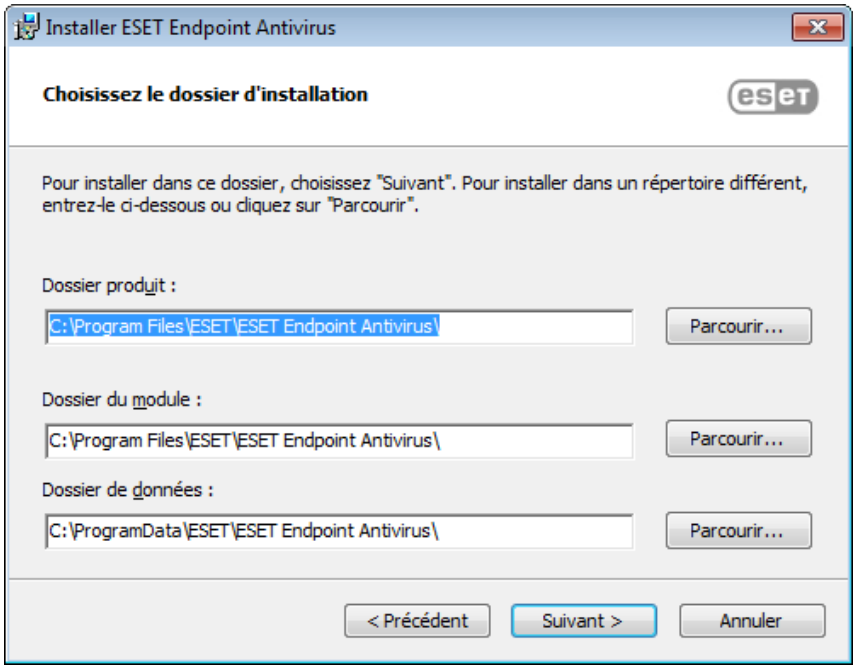
pour le dossier d'installation de ESET Endpoint Antivirus. Par défaut, le système installe le programme dans le répertoire suivant :

C:\Program Files\ESET\ESET Security

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

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

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



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

Installation à l'aide d'une ligne de commande

Vous pouvez installer ESET Endpoint Antivirus localement à l'aide de la ligne de commande ou à distance en utilisant une tâche client d'ESET Security Management Center.

Paramètres pris en charge

APPDIR=<chemin>

- Chemin : chemin d'accès valide au répertoire
- Répertoire d'installation de l'application.

APPDATADIR=<chemin>

- Chemin : chemin d'accès valide au répertoire
- Répertoire d'installation des données de l'application.

MODULEDIR=<chemin>

- Chemin : chemin d'accès valide au répertoire
- Répertoire d'installation du module.

ADDLOCAL=<liste>

- Installation du composant : liste des fonctionnalités non obligatoires à installer localement.
- Utilisation avec les packages .msi ESET : `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Pour plus d'informations sur la propriété **ADDLOCAL**, voir http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx

ADDEXCLUDE=<liste>

- La liste ADDEXCLUDE est séparée par des virgules et contient les noms de toutes les fonctionnalités à ne pas installer ; elle remplace la liste obsolète REMOVE.
- Lors de la sélection d'une fonctionnalité à ne pas installer, le chemin d'accès dans son intégralité (c.-à-d., toutes ses sous-fonctionnalités) et les fonctionnalités connexes invisibles doivent être explicitement inclus dans la liste.
- Utilisation avec les packages .msi ESET : `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

> **Remarque**
> **ADDEXCLUDE** ne peut pas être utilisée avec **ADDLOCAL**.

Consultez la documentation de la version de **msiexec** utilisée pour connaître les commutateurs de ligne de commande adéquats.

Règles

- La liste **ADDLOCAL** est une liste séparée par des virgules qui contient le nom de toutes les fonctionnalités à installer.
- Lors de la sélection d'une fonctionnalité à installer, le chemin d'accès entier (toutes les fonctionnalité parent) doit être explicitement inclus.
- Pour connaître l'utilisation correcte, reportez-vous aux règles supplémentaires.

Composants et fonctionnalités

> **Remarque**
> L'installation des composants à l'aide des paramètres ADDLOCAL/ADDEXCLUDE ne fonctionnera pas avec ESET Endpoint Antivirus.

Les fonctionnalités sont classées dans 4 catégories :

- **Obligatoire** : la fonctionnalité sera toujours installée.
- **Facultative** : la fonctionnalité peut être désélectionnée pour ne pas être installée.
- **Invisible** : fonctionnalité logique obligatoire pour que les autres fonctionnalités fonctionnent correctement.
- **Espace réservé** : fonctionnalité sans effet sur le produit, mais qui doit être répertoriée avec les sous-fonctionnalités.

L'ensemble de fonctionnalités d'ESET Endpoint Antivirus est le suivant :

Description	Nom de la fonctionnalité	Fonctionnalité parente	Présence
Composants de programme de base	`Computer`		Espace réservé
Moteur de détection	`Antivirus`	`Computer`	Obligatoire
Moteur de détection/Analyses des logiciels malveillants	`Scan`	`Computer`	Obligatoire
Moteur de détection/Protection en temps réel du système de fichiers	`RealtimeProtection`	`Computer`	Obligatoire
Moteur de détection/Analyses des logiciels malveillants/Protection des documents	`DocumentProtection`	`Antivirus`	Facultative
Contrôle de périphérique	`DeviceControl`	`Computer`	Facultative
Protection du réseau	`Network`		Espace réservé
Protection du réseau/Pare-feu	`Firewall`	`Network`	Facultative
Protection du réseau/Protection contre les attaques réseau/...	`IdsAndBotnetProtection`	`Network`	Facultative
Web et courier électronique	`WebAndEmail`		Espace réservé
Internet et messagerie/Filtrage des protocoles	`ProtocolFiltering`	`WebAndEmail`	Invisible
Web et courier électronique/Protection de l'accès Web	`WebAccessProtection`	`WebAndEmail`	Facultative
Web et courier électronique/Protection du client de messagerie	`EmailClientProtection`	`WebAndEmail`	Facultative
Internet et messagerie/Protection du client de messagerie/Clients de messagerie	`MailPlugins`	`EmailClientProtection`	Invisible
Web et courier électronique/Protection du client de messagerie/Protection antispam	`Antispam`	`EmailClientProtection`	Facultative
Web et courier électronique/Contrôle Web	`WebControl`	`WebAndEmail`	Facultative
Outils/ESET RMM	`Rmm`		Facultative

Mise à jour/Profils/Miroir de mise à jour	UpdateMirror		Facultative
Plug-in ESET Enterprise Inspector	EnterpriseInspector		Invisible

Ensemble de fonctionnalités :

Description	Nom de la fonctionnalité	Présence de la fonctionnalité
Toutes les fonctionnalités obligatoires	_Base	Invisible
Toutes les fonctionnalités disponibles	ALL	Invisible

Règles supplémentaires

- Si l'une des fonctionnalités **WebAndEmail** est sélectionnée pour l'installation, la fonctionnalité **ProtocolFiltering** invisible doit être incluse dans la liste.

- Les noms de toutes les fonctionnalités respectent la casse, par exemple UpdateMirror est différent de UPDATEMIRROR.

Liste des propriétés de configuration

Propriété	Valeur	Fonctionnalité
CFG_POTENTIALLYUNWANTED_ENABLED=	0 - Désactivé 1 - Activé	Détection des applications potentiellement indésirables
CFG_LIVEGRID_ENABLED=	Voir ci-dessous	Voir la propriété LiveGrid ci-dessous
FIRSTSCAN_ENABLE=	0 - Désactivé 1 - Activé	Planifiez et exécutez une analyse de l'ordinateur après l'installation
CFG_PROXY_ENABLED=	0 - Désactivé 1 - Activé	Paramètres du serveur proxy
CFG_PROXY_ADDRESS=	<ip>	Adresse IP du serveur proxy
CFG_PROXY_PORT=	<port>	Numéro du port du serveur proxy
CFG_PROXY_USERNAME=	<nom d'utilisateur>	Nom d'utilisateur pour l'authentification
CFG_PROXY_PASSWORD=	<mot de passe>	Mot de passe pour l'authentification
ACTIVATION_DATA=	Voir ci-dessous	Activation du produit, clé de licence ou fichier de licence hors ligne
ACTIVATION_DLG_SUPPRESS=	0 - Désactivé 1 - Activé	Lorsque ce paramètre est défini sur "1", ne pas afficher la boîte de dialogue d'activation du produit après le premier démarrage
ADMINCFG=	<chemin>	Chemin d'accès à la configuration XML exportée (valeur par défaut *cfg.xml*)

LiveGrid® propriété

Lors de l'installation d'ESET Endpoint Antivirus avec CFG_LIVEGRID_ENABLED, le comportement du produit après l'installation sera le suivant :

Fonctionnalité	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
Système de réputation ESET LiveGrid®	Activé	Activé
Système de réputation ESET LiveGrid®	Désactivé	Activé
Soumettre des statistiques anonymes	Désactivé	Activé

Propriété ACTIVATION_DATA

Format	Méthodes
`ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE`	Activation à l'aide de la clé de licence ESET (la connexion Internet doit être active)
`ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf`	Activation à l'aide d'un ficher de licence hors ligne

Propriétés de langue

Langue d'ESET Endpoint Antivirus (vous devez spécifier les deux propriétés).

Propriété	Valeur
`PRODUCT_LANG=`	Décimal LCID (ID de paramètres régionaux), par exemple 1033 pour l'anglais (États-Unis), voir la liste des codes de langue.
`PRODUCT_LANG_CODE=`	Chaîne LCID (nom de culture de la langue) en minuscules, par exemple en-us pour Anglais - États-Unis, voir la liste des codes de langue.

Exemples d'installation à l'aide d'une ligne de commande

Important
Veillez à lire le Contrat de Licence de l'utilisateur final et vérifiez que vous disposez de privilèges administratifs avant d'effectuer l'installation.

Exemple
Excluez la section **NetworkProtection** de l'installation (vous devez également spécifier toutes les fonctionnalités enfants) :
```
msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection
```

Exemple
Si vous souhaitez qu'ESET Endpoint Antivirus soit automatiquement configuré après l'installation, vous pouvez spécifier les paramètres de configuration de base dans la commande d'installation. Installez ESET Endpoint Antivirus avec ESET LiveGrid® activé :
```
msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1
```

Exemple
Effectuez l'installation dans un autre répertoire d'installation de l'application que celui par défaut.
```
msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\
```

Exemple
Installez et activez ESET Endpoint Antivirus à l'aide de votre clé de licence ESET.
```
msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```

Exemple
Installation silencieuse avec journalisation détaillée (utile pour le dépannage) et RMM uniquement avec les composants obligatoires :
```
msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm
```

Exemple
Installation complète silencieuse forcée avec une langue spécifiée.
```
msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us
```

Options de ligne de commande post-installation

- ESET CMD – importez un fichier de configuration .xml ou activez/désactivez une fonctionnalité de sécurité.
- Scanner de ligne de commande – exécutez une analyse de l'ordinateur depuis la ligne de commande.

Déploiement à l'aide de GPO ou SCCM

En plus d'installer ESET Endpoint Antivirus directement sur un poste de travail client ou de le déployer à distance à l'aide d'une tâche serveur d'ESMC, vous pouvez procéder à l'installation à l'aide d'outils de gestion comme GPO, SCCM, Symantec Altiris ou Puppet.

Géré (recommandé)

Pour les ordinateurs administrés, nous installons d'abord ESET Management Agent, puis nous déployons ESET Endpoint Antivirus via ESET Security Management Center (ESMC). ESMC doit être installé dans votre réseau.

1. Téléchargez le programme d'installation autonome pour ESET Management Agent.
2. Préparez le script de déploiement GPO/SCCM.
3. Déployez ESET Management Agent à l'aide de GPO ou SCCM.
4. Vérifiez que les ordinateurs clients ont été ajoutés à ESMC.
5. Déployez et activez ESET Endpoint Antivirus sur vos ordinateurs clients.

Instructions illustrées
Les articles suivants de la base de connaissances ESET peuvent être disponibles uniquement en anglais :
- Déployer ESET Management Agent via SCCM ou GPO (7.x)
- Déployer ESET Management Agent à l'aide d'un GPO

Mise à niveau vers une nouvelle version

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

1. Automatiquement, en utilisant ESET Security Management Center, ESET Remote Administrator (version 6.x des produits ESET Endpoint uniquement) ou ESET PROTECT Cloud.

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

Scénarios de mise à niveau recommandés

Mise à niveau à distance

Si vous administrez plus de 10 produits ESET Endpoint, envisagez de gérer les mises à niveau à l'aide de ESET Security Management Center ou ESET PROTECT Cloud . Veuillez consultez la documentation suivante :

- ESET Security Management Center | Création et dimensionnement d'une infrastructure
- ESET Remote Administrator | Procédures de mise à niveau, de migration et de réinstallation
- ESET Security Management Center | Procédures de mise à niveau, de migration et de réinstallation
- Présentation de ESET PROTECT Cloud

Mise à niveau manuelle sur un poste de travail client

Si vous envisagez de gérer manuellement les mises à niveau sur chaque poste de travail client :

1. Vérifiez d'abord les conditions préalables requises pour la mise à niveau d'ESET Endpoint Antivirus :

Mise à niveau depuis	Mise à niveau vers	Conditions préalables requises
6.x	7.x	• Aucune condition préalable requise • Remarque : ESET Endpoint Antivirus version 7 ne peut pas être géré par ESET Remote Administrator
6.x	6.6.x	• Aucune condition préalable requise
5.x	7.x	• Vérifiez que votre système d'exploitation est pris en charge. Par exemple, Windows XP ne l'est pas pour la version 7. • Vérifiez si les versions des produits endpoint ESET prennent en charge la mise à niveau depuis la version 5.x.
4.x	7.x	• Vérifiez que votre système d'exploitation est pris en charge. • Désinstallez ESET NOD32 Antivirus Business Edition ou ESET Smart Security Business Edition. N'installez pas la version 7 sur une version 4.x.

2. Téléchargez et installez une version plus récente par rapport à la version précédente.

Problèmes d'installation courants

Si des problèmes se produisent pendant l'installation, consultez la liste des erreurs d'installation communes et des résolutions pour trouver une solution à votre problème.

Échec de l'activation

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

- Clé de licence déjà utilisée
- Clé de licence non valide. Erreur du formulaire d'activation du produit
- Des informations supplémentaires nécessaires à l'activation sont manquantes ou non valides
- La communication avec la base de données d'activation a échoué. Veuillez réessayer dans 15 minutes
- Aucune connexion ou connexion aux serveurs d'activation ESET désactivée

Vérifiez que vous avez saisi la clé de licence correcte ou que vous avez associé une licence hors ligne. Assurez-vous également d'avoir réessayé l'activation du produit.

Si vous ne parvenez pas à procéder à l'activation, notre guide de bienvenue 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).

- Commencer le dépannage de l'activation des produits ESET

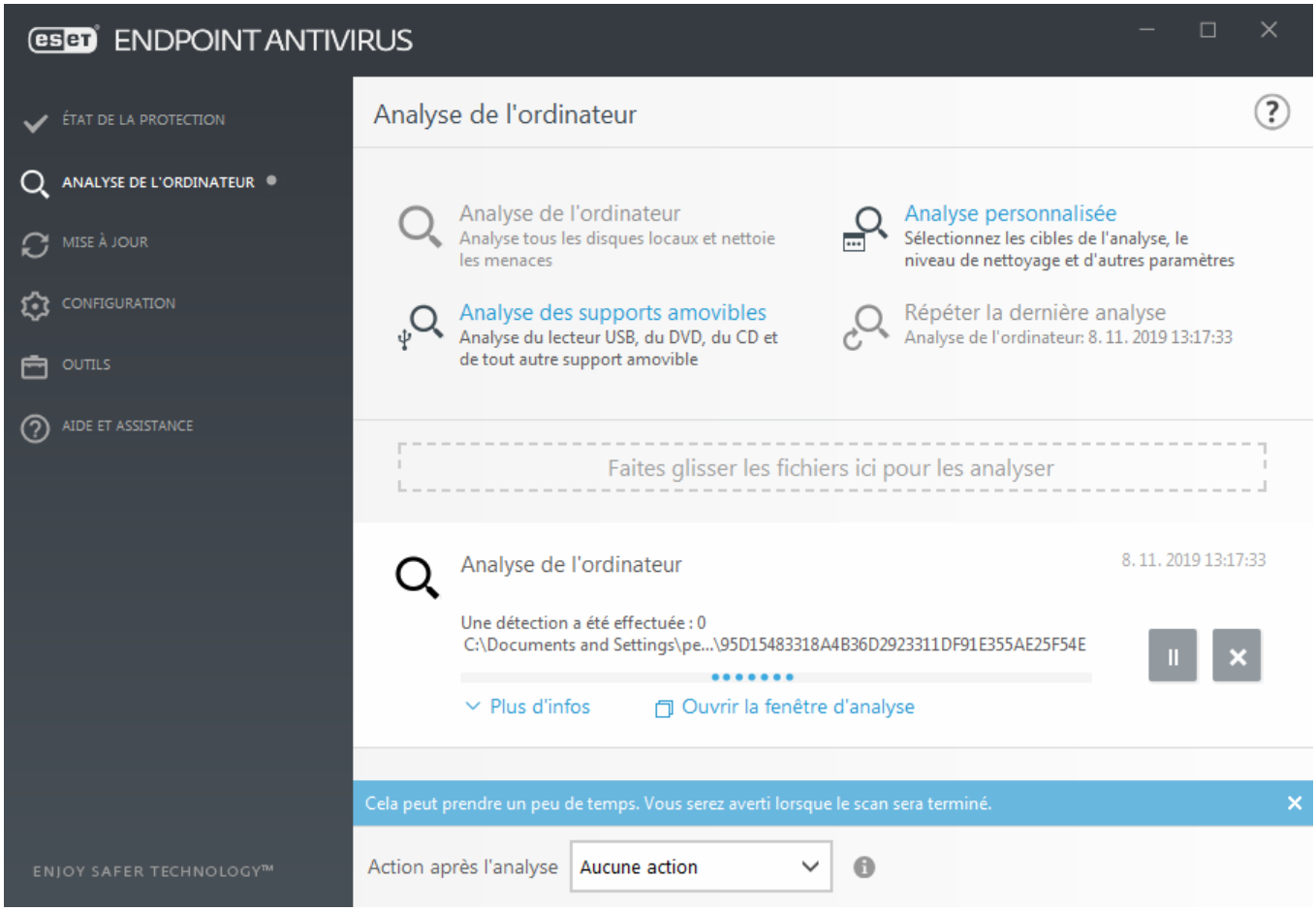
Activation du produit

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

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

Analyse d’ordinateur

Il est recommandé d'effectuer des analyses régulières de l'ordinateur ou de planifier une analyse régulière pour détecter les menaces éventuelles. Dans la fenêtre principale du programme, cliquez sur **Analyse d'ordinateur**, puis sur **Analyse intelligente**. Pour plus d'informations sur l'analyse d'ordinateur, reportez-vous à la section Analyse d'ordinateur.



Guide du débutant

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

Interface utilisateur

La fenêtre principale d'ESET Endpoint 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.

Voici une description des options disponibles dans le menu principal :

État de la protection – Fournit des informations sur l'état de protection d'ESET Endpoint Antivirus.

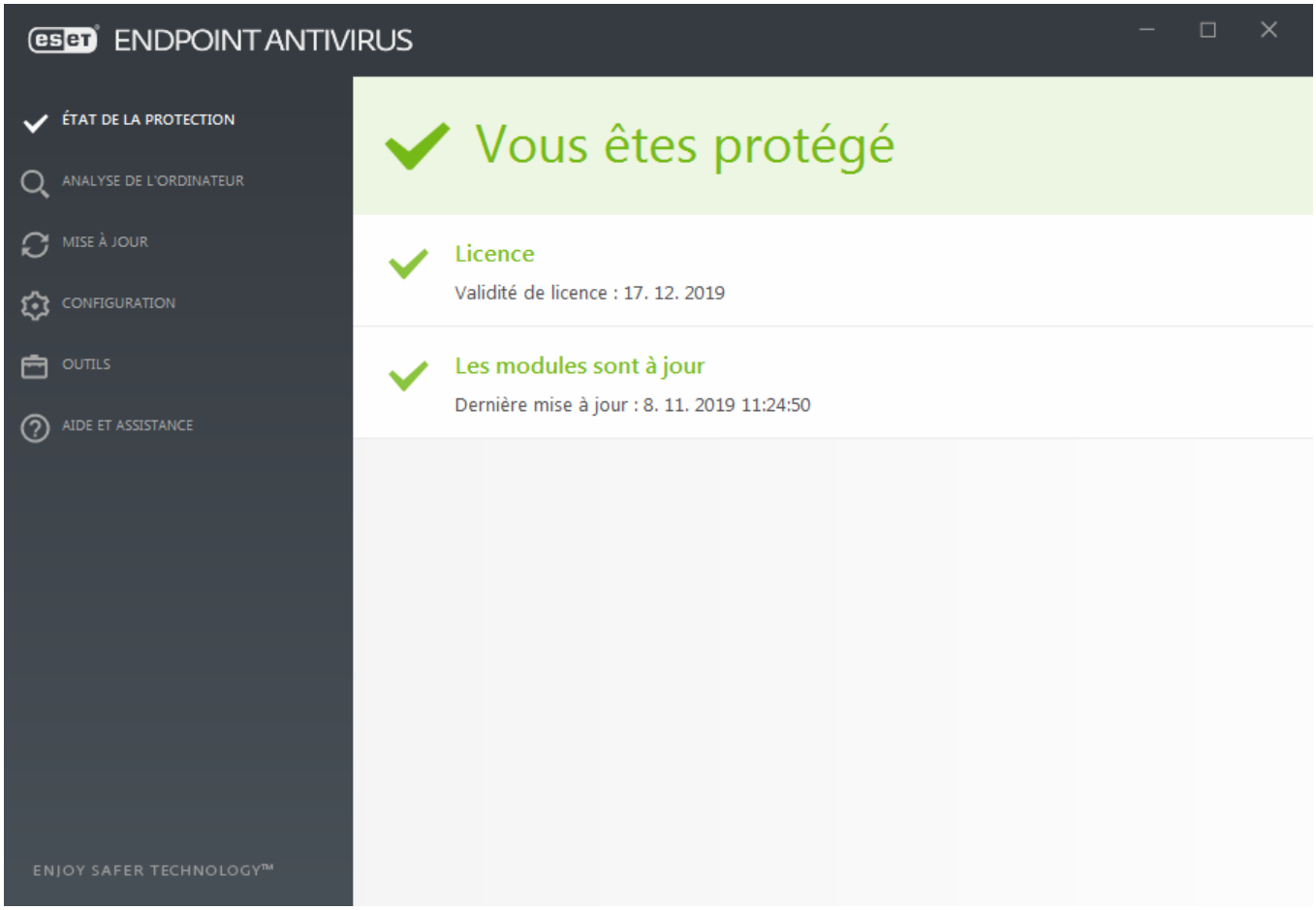
Analyse de l'ordinateur – Cette option permet de configurer et de lancer l'analyse intelligente, l'analyse personnalisée ou l'analyse de supports amovibles. Vous pouvez également répéter la dernière analyse effectuée.

Mise à jour – Affiche des informations sur le moteur de détection et permet de rechercher manuellement des mises à jour.

Configuration – Sélectionnez cette option pour régler les paramètres de sécurité de l'ordinateur ou de l'Internet et de la messagerie.

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

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

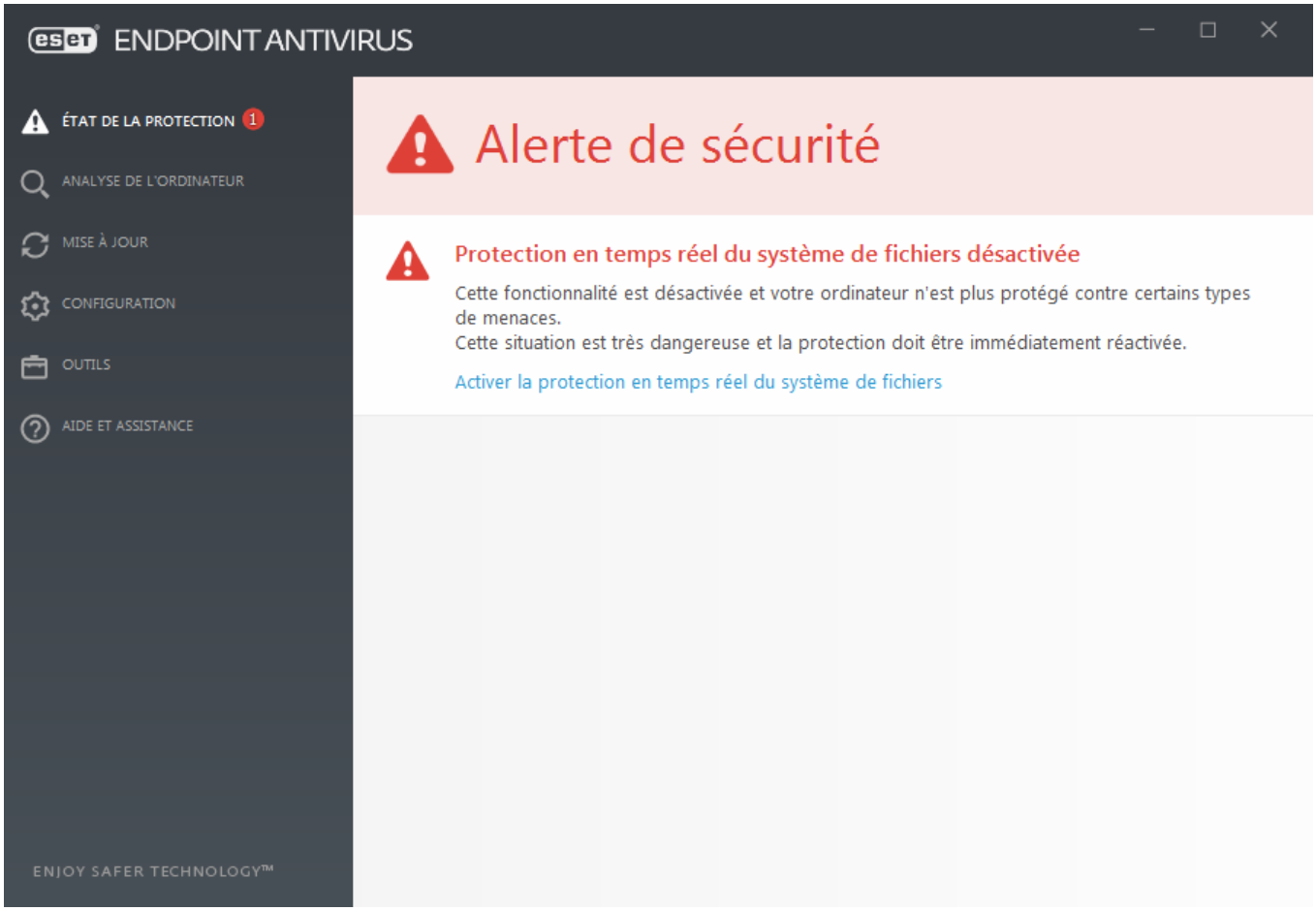


L'écran **État de la protection** vous informe sur le niveau actuel de sécurité et de protection de l'ordinateur. L'icône verte d'état **Protection maximale** indique qu'une protection maximale est assurée.

La fenêtre d'état contient également des liens rapides vers les fonctionnalités fréquemment utilisées dans ESET Endpoint Antivirus et des informations sur la dernière mise à jour.

Que faire lorsque le programme ne fonctionne pas correctement ?

Une coche verte s'affiche en regard de chaque module du programme qui fonctionne correctement. Un point d'exclamation rouge ou une icône de notification orange apparaît si un module requiert votre attention. Des informations supplémentaires sur le module, notamment des conseils pour son bon fonctionnement, s'affichent dans la partie supérieure de la fenêtre. Pour changer l'état d'un module, cliquez sur **Configuration** dans le menu principal, puis sur le module souhaité.



Un point d'exclamation rouge (!) indique que la protection maximale de votre ordinateur n'est pas assurée. Vous pouvez recevoir ce type de notification dans les situations suivantes :

- **La protection antivirus et antispyware est interrompue** – Cliquez sur **Démarrer tous les modules de protection antivirus et antispyware** pour réactiver la protection antivirus et antispyware dans le volet **État de la protection**. Vous pouvez également cliquer sur **Activer la protection antivirus et antispyware** dans le volet **Configuration** de la fenêtre principale du programme.
- **La protection antivirus ne fonctionne pas** – L'initialisation de l'analyseur de virus a échoué. La plupart des modules ESET Endpoint Antivirus ne fonctionneront pas correctement.
- **La protection antihameçonnage ne fonctionne pas** – Cette fonctionnalité n'est pas fonctionnelle, car d'autres modules requis du programme ne sont pas actifs.

- **Le moteur de détection n'est plus à jour** – Cette erreur apparaît après plusieurs tentatives infructueuses de mise à jour du moteur de détection (appelé auparavant base des signatures de virus). Nous vous conseillons de vérifier les paramètres de mise à jour. Cette erreur provient généralement de l'entrée incorrecte de données d'authentification ou de la configuration incorrecte des paramètres de connexion.

- **Le produit n'est pas activé** ou **Licence arrivée 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 la licence. Suivez les instructions de la fenêtre d'alerte pour renouveler la licence.

- **Le système HIPS (Host Intrusion Prevention System) est désactivé** – Ce problème est signalé lorsque le système HIPS est désactivé dans la configuration avancée. Votre ordinateur n'est plus protégé contre certains types de menace et la protection doit être réactivée immédiatement en cliquant sur **Activer HIPS**.

- **ESET LiveGrid® est désactivé** – Ce problème est signalé lorsque ESET LiveGrid® est désactivé dans la

confirguration avancée.

- **Aucune mise à jour régulière planifiée** – ESET Endpoint Antivirus ne recherche pas des mises à jour importantes ou ne les reçoit pas, sauf si vous planifiez une tâche de mise à jour.

- **Anti-Stealth est désactivé** – Cliquez sur **Activer Anti-Stealth** pour réactiver cette fonctionnalité.

- **Accès bloqué au réseau** – Ce message s'affiche lorsque la tâche client **Isoler l'ordinateur du réseau** de ce poste de travail est déclenchée depuis ESMC. Pour plus d'informations, contactez l'administrateur système.

- **La protection en temps réel du système de fichiers est interrompue** – 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** pour réactiver cette fonctionnalité.

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

- **La protection de l'accès Web est désactivée** – Cliquez sur la notification de sécurité pour réactiver la protection de l'accès Web, puis sur **Activer la protection de l'accès Web**.

- **Votre licence va arriver prochainement à expiration** – Cette information est donnée par l'icône d'état de protection qui affiche un point d'exclamation. Après l'expiration de votre licence, le programme ne peut plus se mettre à jour et l'icône d'état de la protection devient rouge.

- **La protection antispam est interrompue** – Cliquez sur **Activer la protection antispam pour réactiver cette fonctionnalité**.

- **Le contrôle web est interrompu** – Cliquez sur **Activer le contrôle web pour réactiver cette fonctionnalité**.

- **Remplacement de la stratégie active** – La configuration définie par la stratégie est remplacée de manière temporaire, probablement jusqu'à la fin du dépannage. Seul un utilisateur autorisé peut remplacer les paramètres de stratégie. Pour plus d'informations, voir Utilisation du mode de remplacement.

- **Le contrôle de périphérique est interrompu** – Cliquez sur **Activer le contrôle de périphérique** pour réactiver cette fonctionnalité.

Pour ajuster les états de visibilité du produit dans le premier volet d'ESET Endpoint Antivirus, consultez États d'application.

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 technique à ESET. Le support technique ESET répondra très rapidement à vos questions et vous permettra de trouver une solution.

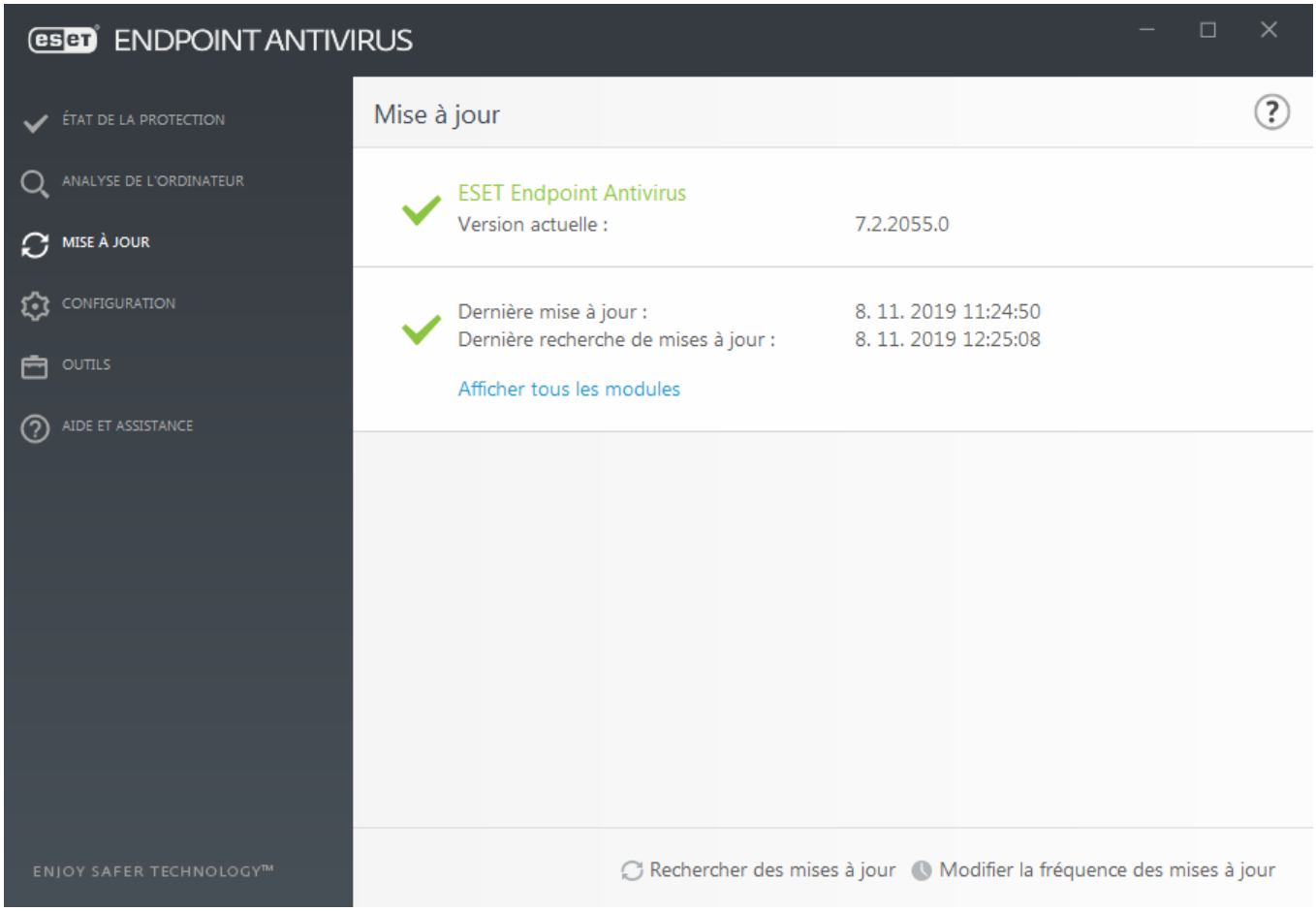
Remarque

Si l'état est associé à une fonctionnalité bloquée par la stratégie d'ESMC, il n'est pas possible de cliquer sur le lien.

Configuration des mises à jour

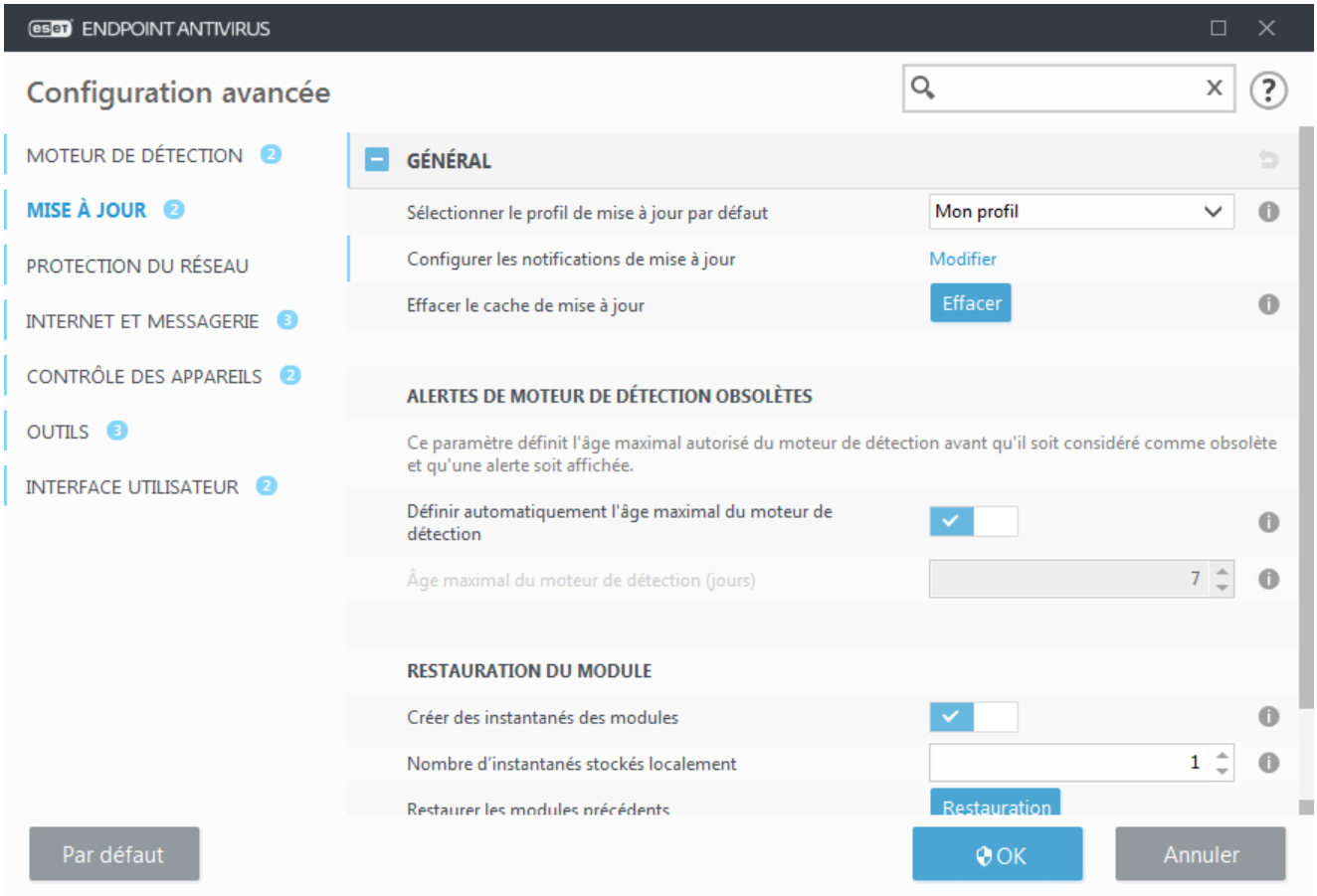
La mise à jour des modules est une opération importante qui assure la protection totale contre les attaques des codes malveillants. Il convient donc d'apporter une grande attention à la configuration et au fonctionnement des mises à jour. Dans le menu principal, sélectionnez **Mettre à jour** > **Rechercher des mises à jour** pour rechercher toute nouvelle mise à jour des modules.

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



La fenêtre Configurations avancées (cliquez sur **Configuration** > **Configurations avancées dans le menu principal** ou appuyez sur la touche **F5** de votre clavier) comporte d'autres options de mise à jour. Pour configurer les options avancées de mise à jour telles que le mode de mise à jour, l'accès au serveur proxy, les connexions LAN et les configurations de création de copie du moteur de détection, cliquez sur **Mise à jour** dans l'arborescence Configurations avancées.

- Si vous rencontrez des problèmes liés à une mise à jour, cliquez sur **Effacer** pour effacer le cache de mise à jour temporaire.



- L'option **Choisir automatiquement**, dans **Profils** > **Mises à jour** > **Mises à jour des modules**, est activée par défaut. Lorsque vous utilisez un serveur de mise à jour ESET pour recevoir des mises à jour, il est recommandé de laisser cette option activée.

- Si vous ne souhaitez pas que la notification de réussite de la mise à jour de la barre d'état système s'affiche dans le coin inférieur droit de l'écran, développez **Profils** > **Mises à jour**, cliquez sur **Modifier** en regard de l'option **Sélectionner les notifications de mises à jour reçues**, puis cochez/décochez les cases pour la notification **Mise à jour réussie du moteur de détection**.

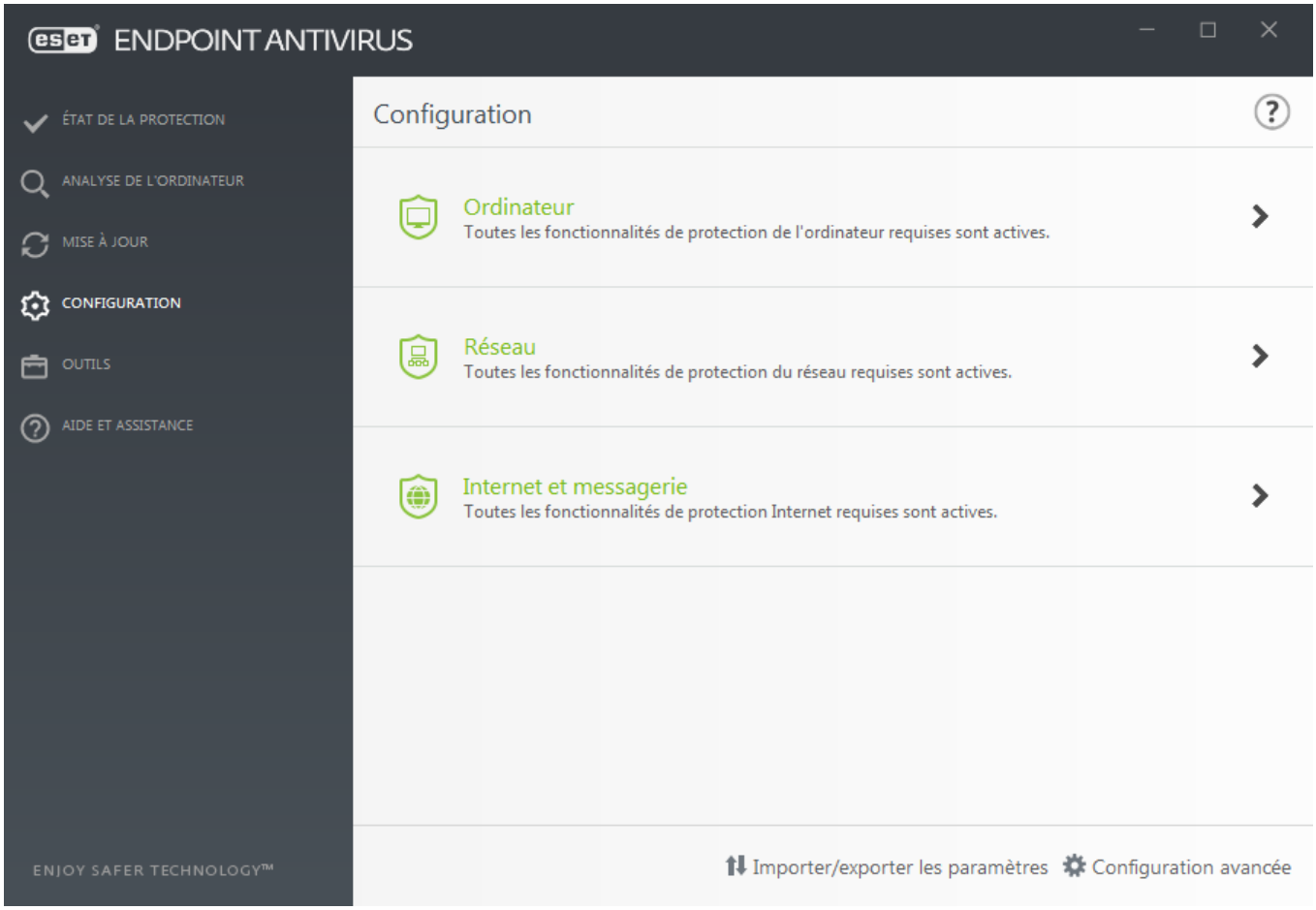
Le programme doit être mis à jour automatiquement pour assurer un fonctionnement optimal. Cela n'est possible que si la **clé de licence** correcte est entrée dans **Aide et assistance** > **Activer le produit**.

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

Utilisation d'ESET Endpoint Antivirus

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

> **Remarque**
> Lors de la création d'une stratégie à partir d'ESET Security Management Center Web Console, vous pouvez sélectionner l'indicateur de chaque paramètre. Les paramètres associés à l'indicateur Forcer sont prioritaires et ne peuvent pas être remplacés par une stratégie ultérieure (même si cette stratégie ultérieure est associée à un indicateur Forcer). Ces paramètres ne peuvent ainsi pas être modifiés (par un utilisateur ou des stratégies ultérieures lors d'une fusion, par exemple). Pour plus d'informations, voir la rubrique traitant des indicateurs dans l'aide en ligne d'ESMC.



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

- **Ordinateur**
- **Réseau**
- **Web et courier électronique**

La section **Ordinateur** permet d'activer ou de désactiver les composants suivants :

- **Protection en temps réel du système de fichiers** – Tous les fichiers ouverts, créés ou exécutés sont analysés pour y rechercher la présence éventuelle de code malveillant.
- **Contrôle des appareils** Permet un contrôle automatique des appareils (CD/DVD/USB/...). Ce module permet de bloquer ou d'ajuster les filtres étendus/autorisations, et de définir les autorisations des utilisateurs à accéder à un appareil et à l'utiliser.
- **Host Intrusion Prevention System (HIPS)** – Le système HIPS surveille les événements qui se produisent

dans le système d'exploitation et réagit en fonction d'un ensemble de règles personnalisées.

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

• **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.

• **Bouclier anti-ransomwares** constitue une 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®. Consultez d'autres informations sur ce type de protection.

• **Mode de présentation** – Fonctionnalité destinée aux utilisateurs qui ne veulent pas être interrompus lors de l'utilisation de leur logiciel. Ils ne souhaitent pas être dérangés par des fenêtres contextuelles et veulent réduire les contraintes sur l'UC. Vous recevez un message d'avertissement (risque potentiel de sécurité) et la fenêtre principale devient orange lorsque le mode de présentation est activé.

La section **Protection du réseau** permet de configurer la protection contre les attaques réseau (IDS) et la protection anti-botnet.

La configuration de la protection **Web et courier électronique** permet d'activer ou de désactiver les composants suivants :

• **Protection de l'accès Web** – Si cette option est activée, tout le trafic HTTP ou HTTPS est analysé afin d'y rechercher des codes malveillants.
• **Protection du client de messagerie** – Contrôle les communications reçues via les protocoles POP3 et IMAP.
• **Protection antihameçonnage** – Vous protège des tentatives d'acquisition de mots de passe, de données bancaires ou d'autres informations sensibles par des sites Web non légitimes se faisant passer pour des sites Web dignes de confiance.

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

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

Lorsque la stratégie ESMC/ERA est appliquée, l'icône représentant un verrou  s'affiche en regard d'un composant spécifique. La stratégie appliquée par ESET Security Management Center peut être remplacée localement après l'authentification par l'utilisateur connecté (l'administrateur, par exemple). Pour plus d'informations, reportez-vous à l'aide en ligne d'ESMC.

> **Remarque**
> toutes les mesures de protection désactivées de cette manière sont réactivées après le redémarrage de l'ordinateur.

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

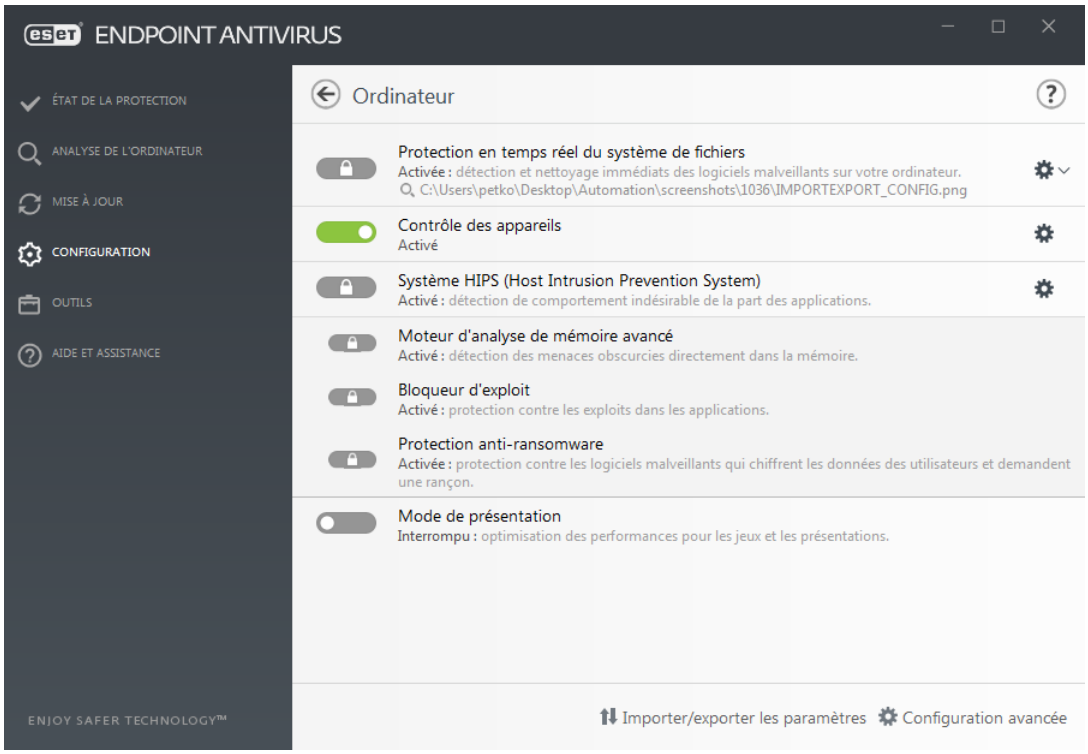
D'autres options sont disponibles au bas de la fenêtre de configuration. Pour charger les paramètres de configuration à l'aide d'un fichier de configuration *.xml* ou pour enregistrer les paramètres de configuration actuels dans un fichier de configuration, utilisez l'option **Importer/exporter les paramètres**.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

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

Ordinateur

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

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



La section **Ordinateur** permet d'activer ou de désactiver les composants suivants :

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

- **Contrôle des appareils** Permet un contrôle automatique des appareils (CD/DVD/USB/...). Ce module permet de bloquer ou d'ajuster les filtres étendus/autorisations, et de définir les autorisations des utilisateurs à accéder à un appareil et à l'utiliser.

- **Host Intrusion Prevention System (HIPS)** – Le système HIPS surveille les événements qui se produisent dans le système d'exploitation et réagit en fonction d'un ensemble de règles personnalisées.

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

plus sur ce type de protection, consultez le glossaire.

• **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.

• **Bouclier anti-ransomwares** constitue une 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®. Consultez d'autres informations sur ce type de protection.

• **Mode de présentation** – Fonctionnalité destinée aux utilisateurs qui ne veulent pas être interrompus lors de l'utilisation de leur logiciel. Ils ne souhaitent pas être dérangés par des fenêtres contextuelles et veulent réduire les contraintes sur l'UC. Vous recevez un message d'avertissement (risque potentiel de sécurité) et la fenêtre principale devient orange lorsque le mode de présentation est activé.

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

Moteur de détection (version 7.2 et versions ultérieures)

Le moteur de détection protège des attaques malveillantes 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. Le moteur de détection peut l'éliminer en le bloquant dans un premier temps, puis en le nettoyant, en le supprimant ou en le mettant en quarantaine.

Pour configurer en détail les paramètres du moteur de détection, cliquez sur **Configurations avancées** ou appuyez sur **F5**.

Dans cette section :

- Catégories de la protection en temps réel et par apprentissage machine
- Analyses des logiciels malveillants
- Configuration du signalement
- Configuration de la protection
- Bonnes pratiques

Modifications apportées à la configuration du scanner du moteur de détection

À partir de la version 7.2, la section Moteur de détection ne propose plus les boutons bascules ACTIVER/DÉSACTIVER comme dans les versions 7.1 et antérieures. Ces boutons ont été remplacés par quatre seuils : Offensif, Équilibré, Prudent et Désactivé.

Catégories de la protection en temps réel et par apprentissage machine

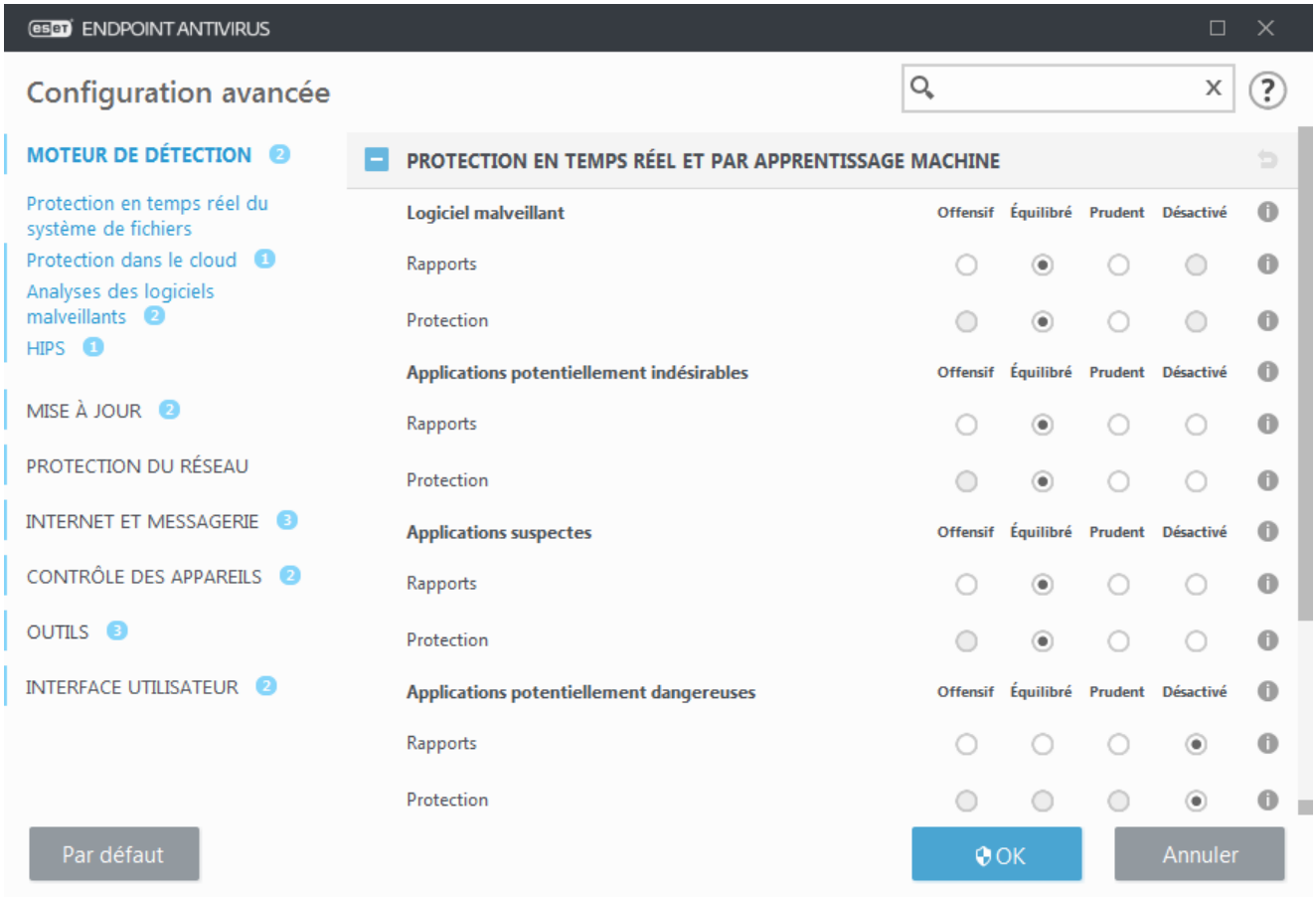
La **Protection en temps réel et par apprentissage machine** pour tous les modules de protection (protection en temps réel du système de fichiers, protection de l'accès web, etc.) permet de configurer les rapports et les niveaux de protection pour les catégories suivantes :

- **Logiciel malveillant** : un virus informatique 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 en savoir plus sur ces types d'applications, consultez le 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 en savoir plus sur ces types d'applications, consultez le glossaire.

- **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 en savoir plus sur ces types d'applications, consultez le glossaire.

- **Les applications suspectes** comprennent des programmes compressés par des compresseurs ou par des programmes de protection. Ces types de protections sont souvent exploités par des créateurs de logiciels malveillants pour contourner leur détection.



Amélioration de la protection

L'apprentissage machine avancé fait maintenant partie du moteur de détection 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.

Analyses des logiciels malveillants

Les paramètres de scanner peuvent être configurés séparément pour le scanner en temps réel et le scanner à la demande. Par défaut, l'option **Utiliser les configurations de protection en temps réel** est activée. Lorsque cette option est activée, les paramètres d'analyse à la demande pertinents sont hérités de la section **Protection en temps réel et par apprentissage machine**.

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 Endpoint Antivirus.

Le seuil de signalement est configuré pour chaque catégorie (appelée « CATÉGORIE ») :

1. 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. Il est possible de 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 Endpoint 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

* Disponible dans ESET Endpoint Antivirus versions 7.2 et ultérieure.
** 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 Endpoint 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.
- Le seuil **Prudent** représente un niveau de protection comparable à celui des versions précédentes d'ESET Endpoint Antivirus (versions 7.1 et antérieures). Il est recommandé pour les environnements pour lesquels la priorité est de minimiser les objets identifiés à tort par un logiciel de sécurité.
- 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 Endpoint 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.

Tableau de conversion des politiques d'ESMC pour ESET Endpoint Antivirus 7.1 et versions antérieures

L'éditeur de politiques ESMC pour les paramètres de scanner ne contient plus les boutons bascules ACTIVÉ/DÉSACTIVÉ pour chaque CATÉGORIE. Le tableau suivant présente une conversion entre le seuil de protection et l'état final du bouton bascule dans ESET Endpoint Antivirus 7.1 et les versions antérieures.

Etat des seuils CATÉGORIE	Offensif	Équilibré	Prudent	Désactivé
Bouton bascule de catégorie appliqué	✓	✓	✓	✗

Lors de la mise à niveau des versions 7.1 et antérieures vers les versions 7.2 et ultérieures, le nouvel état de seuil sera comme suit :

Bouton bascule de catégorie avant la mise à niveau		
Nouveau seuil de CATÉGORIE après la mise à niveau	Équilibré	Désactivé

Bonnes pratiques

NON ADMINISTRÉ (poste de travail client distinct)

Conservez les valeurs recommandées par défaut telles quelles.

ENVIRONNEMENT ADMINISTRÉ

Ces paramètres sont généralement appliqués aux postes de travail via une politique.

1. Phase initiale

Cette phase peut prendre jusqu'à une semaine.

- Définissez tous les seuils des **Rapports** sur **Équilibré**.
REMARQUE : si nécessaire, définissez les seuils des rapports sur **Offensif**.
- Définissez ou conservez la **protection** contre les logiciels malveillants sur **Équilibré**.
- Définissez la **protection** des autres CATÉGORIES sur **Prudent**.
REMARQUE : Il n'est pas recommandé de définir le seuil de **protection** sur **Offensif** pendant cette phase, car toutes les détections effectuées seraient corrigées, même celles identifiées à tort.
- Trouvez les objets identifiés à tort dans le journal Détections et ajoutez-les d'abord aux exclusions de détection.

2. Phase de transition

- Mettez en œuvre la « phase de production » sur certains postes de travail à titre de test (pas pour tous les postes de travail du réseau).

3. Phase de production

- Définissez tous les seuils de **protection** sur **Équilibré**.
- En cas d'administration à distance, utilisez une politique prédéfinie d'antivirus appropriée pour ESET Endpoint Antivirus.
- Le seuil de protection **Offensif** peut être défini si des taux de détection les plus élevés sont requis et si les objets identifiés à tort sont acceptés.
- Consultez le journal Détections ou les rapports ESMC pour rechercher une détection manquante éventuelle.

Options avancées du moteur de détection

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

Activer l'analyse avancée via AMSI – L'outil Microsoft Antimalware Scan Interface permet aux développeurs d'applications de créer de nouvelles défenses contre les logiciels malveillants (Windows 10 uniquement).

Moteur de détection (version 7.1 et versions antérieures)

Le moteur de détection protège des attaques malveillantes 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. Le moteur de détection peut l'éliminer en le bloquant dans un premier temps, puis en le nettoyant, en le supprimant ou en le mettant en quarantaine.

Pour configurer en détail les paramètres du moteur de détection, cliquez sur **Configurations avancées** ou appuyez sur **F5**.

> **Modifications apportées à la configuration du scanner du moteur de détection**
> À partir de la version 7.2, la section Moteur de détection a un aspect différent.

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

- **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 en savoir plus sur ces types d'applications, consultez le glossaire.

- **Les applications potentiellement dangereuses** sont des logiciels commerciaux légitimes susceptibles d'être utilisés à des fins malveillantes. Cette catégorie comprend les programmes d'accès à distance, les applications de décodage des mots de passe ou les keyloggers (programmes qui enregistrent chaque frappe au clavier de l'utilisateur). Cette option est désactivée par défaut.
  Pour en savoir plus sur ces types d'applications, consultez le glossaire.

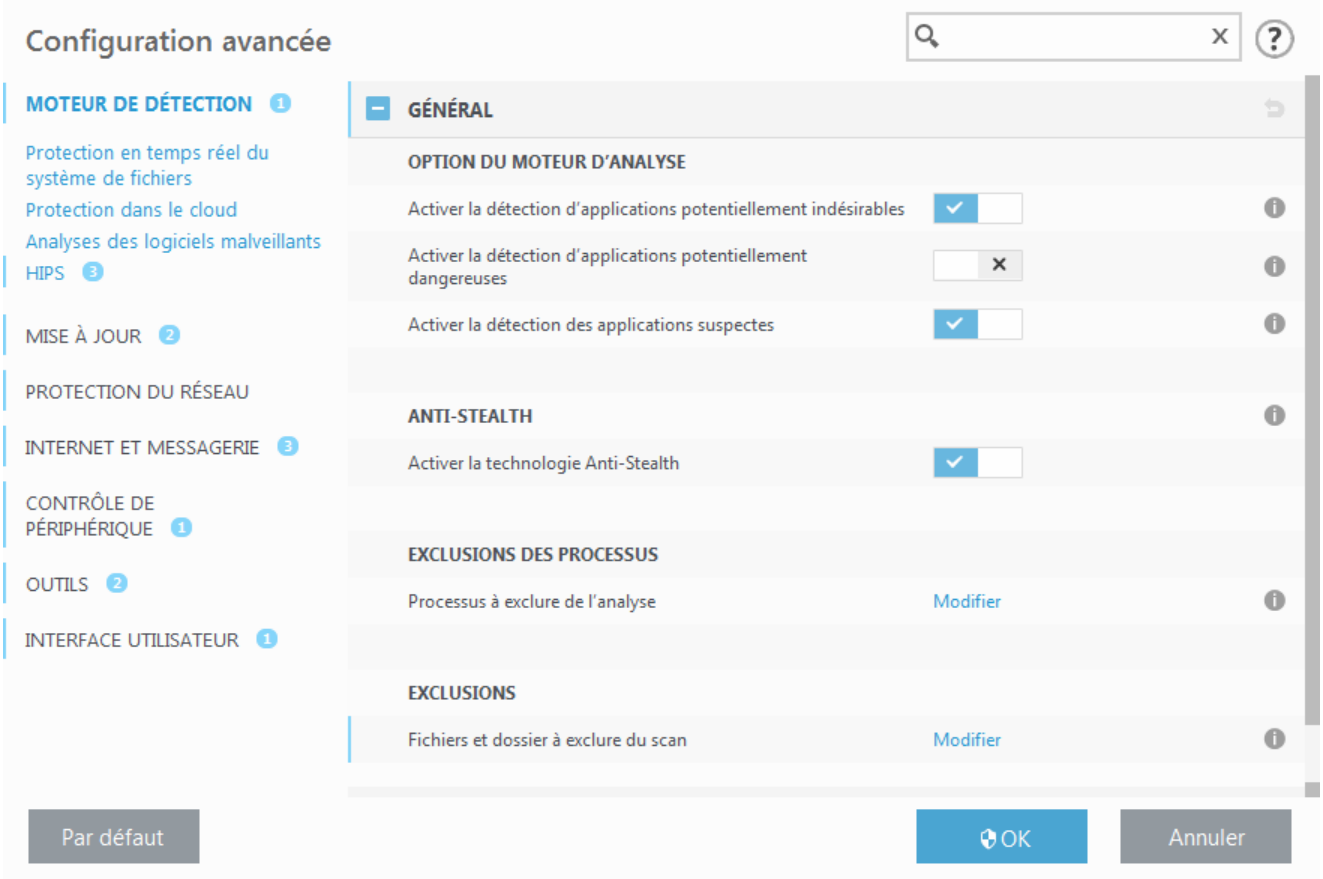
- **Les applications suspectes** comprennent des programmes compressés par des compresseurs ou par des programmes de protection. Ces types de protections sont souvent exploités par des créateurs de logiciels malveillants pour contourner leur détection.

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

techniques de test ordinaires.

Les **exclusions** permettent d'exclure des objets de l'analyse. Pour plus d'informations, consultez Exclusions.

Activer l'analyse avancée via AMSI – L'outil Microsoft Antimalware Scan Interface permet aux développeurs d'applications de créer de nouvelles défenses contre les logiciels malveillants (Windows 10 uniquement).



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.).

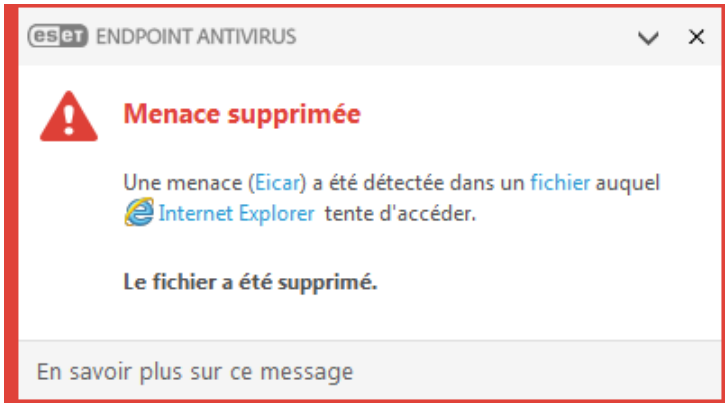
Comportement standard

Pour illustrer de manière générale la prise en charge des infiltrations par ESET Endpoint 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

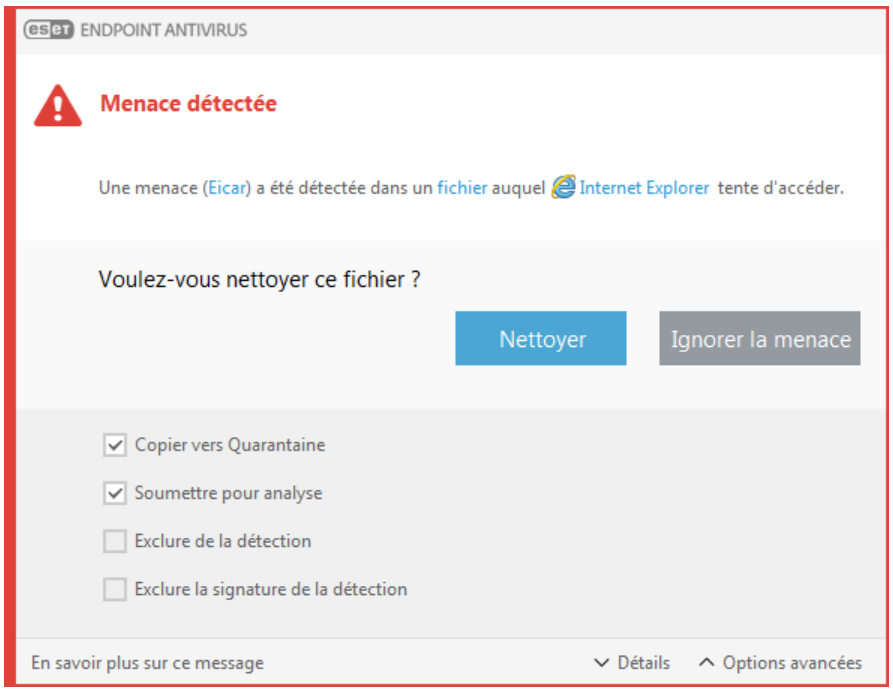
Chaque fonction utilise le niveau de nettoyage standard et tente de nettoyer le fichier et de le déplacer en Quarantaine ou met fin à la connexion. Une fenêtre de notification s'affiche dans la zone de notification, dans

l'angle inférieur droit de l'écran. Pour plus d'informations sur les niveaux et le comportement de nettoyage, voir Nettoyage.



Nettoyage et suppression

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



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

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

Menaces multiples

Si des fichiers infectés n'ont pas été nettoyés durant une analyse de l'ordinateur (ou si le niveau de nettoyage a

été défini sur **Pas de nettoyage**), une fenêtre d'alerte s'affiche ; elle vous invite à sélectionner une action pour ces fichiers.

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.

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

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

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

Cache local partagé

Shared Local Cache peut améliorer les performances dans les environnements isolés (par exemple, les machines virtuelles) en éliminant les analyses en double sur le réseau. Chaque fichier ne sera ainsi analysé qu'une seule fois et stocké dans le cache partagé.

ESET Shared Local Cache doit être d'abord installé et configuré.

- Téléchargez ESET Shared Local Cache.
- Pour plus d'informations, consultez le manuel ESET Shared Local Cache.

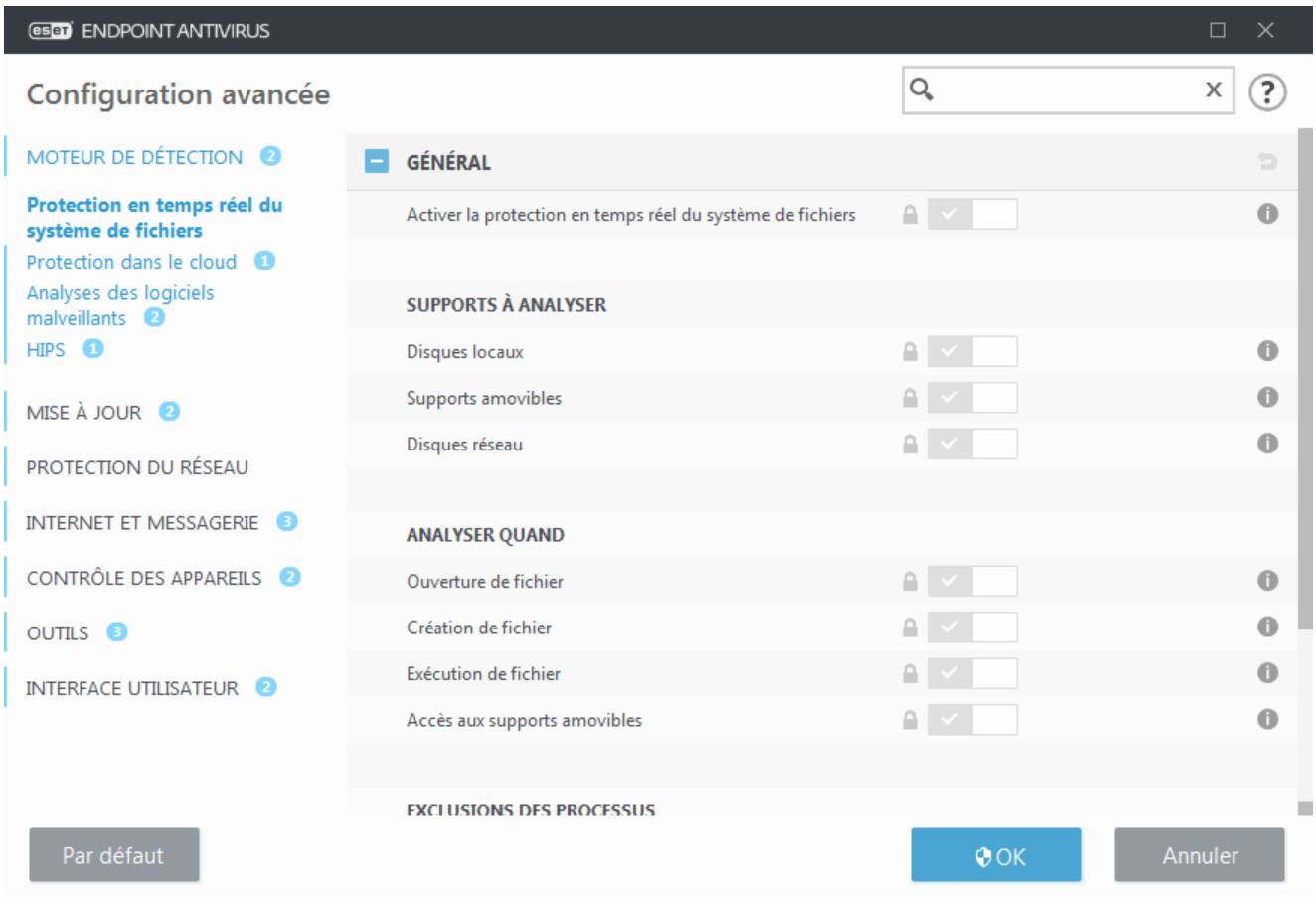
Activez le bouton bascule **Options de mise en cache** pour enregistrer les informations relatives aux analyses des fichiers et des dossiers de votre réseau dans ESET Shared Local Cache. Si vous effectuez une nouvelle analyse, ESET Endpoint Antivirus recherche les fichiers analysés dans ESET Shared Local Cache. Si les fichiers correspondent, ils seront exclus de l'analyse.

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

- **Nom d'hôte** – Nom d'hôte ou adresse IP de l'ordinateur sur lequel se trouve ESET Shared Local Cache.
- **Port** – Numéro de port utilisé pour les communications (identique à celui défini dans ESET Shared Local Cache).
- **Mot de passe** – Spécifiez le mot de passe pour ESET Shared Local Cache si nécessaire.

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** sous **Moteur de détection** > **Protection en temps réel du système de fichiers** > **Général** dans **Configuration avancée**.

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 appareils amovibles** fonctionne correctement, gardez l'option **Secteurs d'amorçage/UEFI** activée dans les paramètres ThreatSense.

Processus à exclure de l'analyse – Obtenez des informations supplémentaires sur ce type d'exclusion dans le chapitre Exclusions de processus.

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

Pour garantir un impact minimal de la protection en temps réel sur le système, les fichiers déjà analysés ne sont pas analysés plusieurs fois (sauf s'ils ont été modifiés). Les fichiers sont immédiatement réanalysés après chaque mise à jour 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, appuyez sur **F5** pour ouvrir la configuration avancée, puis développez **Moteur de détection** > **Protection en temps réel du système de fichiers**. Cliquez ensuite sur **Paramètres ThreatSense** > **Autre**, puis sélectionnez ou désélectionnez **Activer l'optimisation intelligente**.

Vérification de la protection en temps réel

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

Le fichier 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.

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

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

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

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

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

La protection en temps réel est désactivée

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

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

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

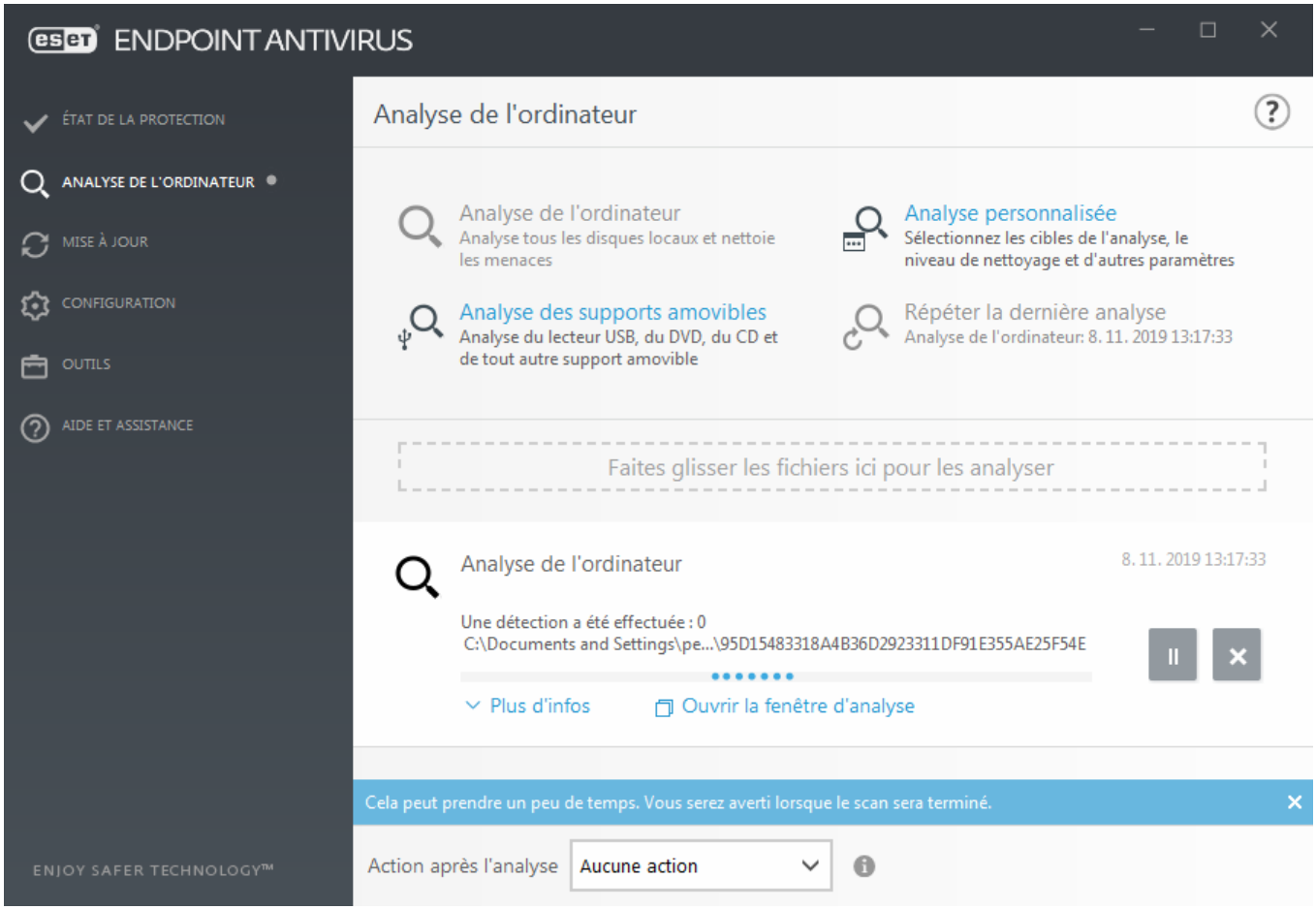
Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si deux programmes de protection en temps réel sont activés en même temps, il peut y avoir un conflit entre les deux. Nous recommandons de désinstaller tout autre antivirus de votre système avant d'installer ESET.

La protection en temps réel ne démarre pas

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

Analyse d’ordinateur

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



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

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

Analyse intelligente

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

Analyse personnalisée

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

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

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

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.

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.

Vous pouvez sélectionner **Aucune action**, **Arrêt** ou **Redémarrage** dans le menu déroulant **Action après l'analyse**. 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. L'action sélectionnée débutera une fois que toutes les analyses en cours d'exécution seront terminées. Lorsque l'action **Arrêt** est sélectionnée, une boîte de dialogue de confirmation d'arrêt affiche un compte à rebours de 30 secondes.(cliquez sur **Annuler** pour désactiver le compte à rebours demandé). Pour plus d'informations, consultez Options d'analyse avancées.

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

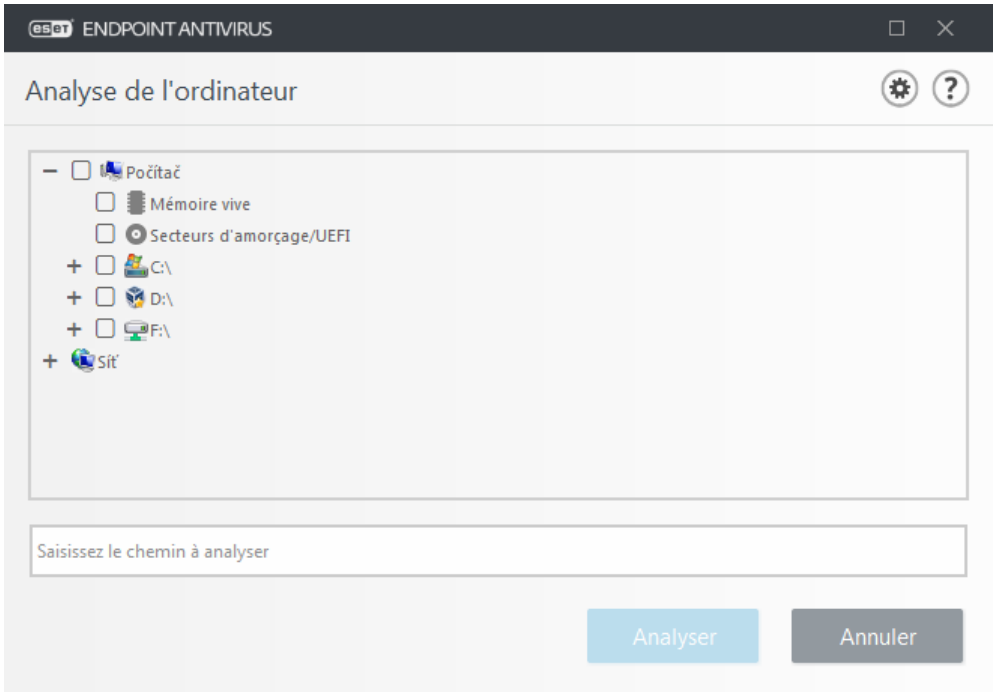
Lanceur d'analyses personnalisées

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

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

- **Par les paramètres de profil** – Permet de sélectionner les cibles indiquées dans le profil d'analyse sélectionné.
- **Supports amovibles** – Permet de sélectionner les disquettes, les périphériques USB, les CD/DVD, etc.
- **Disques locaux** – Permet de sélectionner tous les disques durs du système.
- **Disques réseau** – Analyse tous les lecteurs réseau mappés.
- **Sélection personnalisée** – Permet à l'utilisateur de créer une sélection personnalisée de cibles.

Pour accéder rapidement à une cible à analyser ou ajouter un dossier ou des fichiers cibles, saisissez le répertoire cible dans le champ vide sous la liste des dossiers. Aucune cible ne doit avoir été sélectionnée dans la structure arborescente et le menu **Cibles à analyser** doit être défini sur **Aucune sélection**.



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

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

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

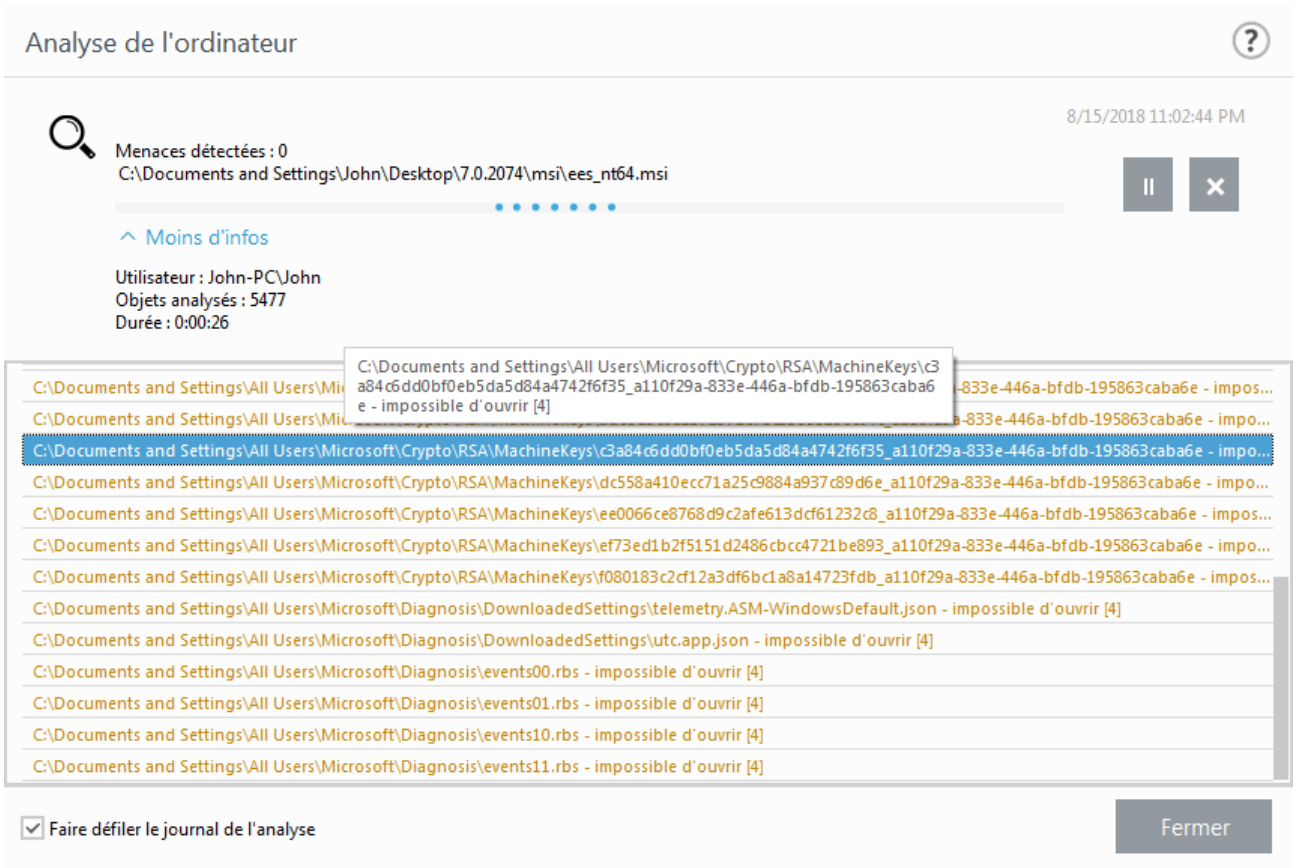
Cliquez sur **Analyser** pour exécuter l'analyse avec les paramètres personnalisés que vous avez définis.

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

> **Remarque**
> 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.



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

Progression de l'analyse – La barre de progression indique l'état des objets déjà analysés par rapport aux objets qui ne sont pas encore analysés. L'état de progression de l'analyse est dérivé du nombre total d'objets intégrés dans l'analyse.

Cible – Nom de l'élément analysé et emplacement.

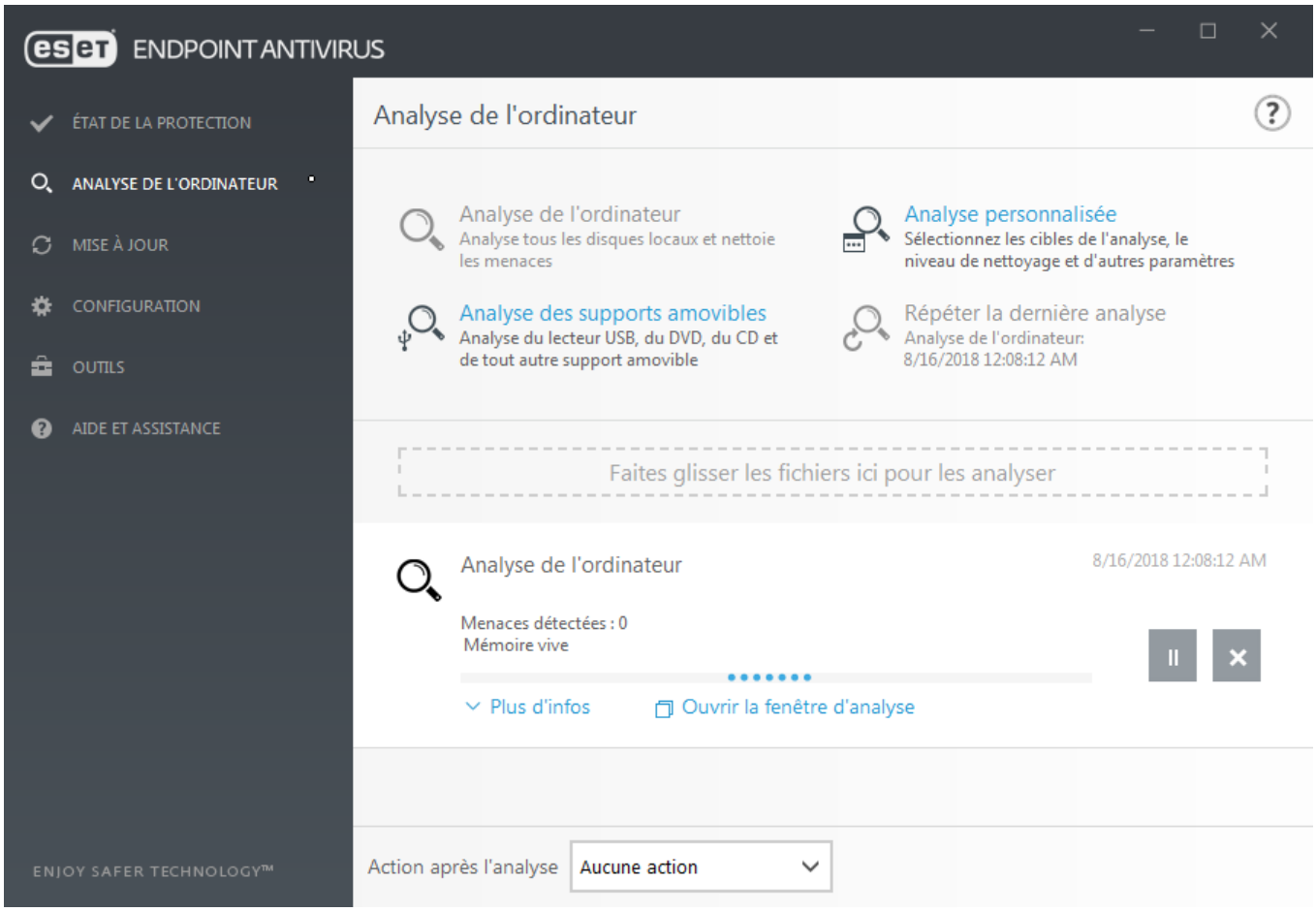
Menaces détectées – Indique le nombre total de menaces détectées pendant une analyse.

Interrompre – Interrompt une analyse.

Reprendre – Cette option est visible lorsque l'analyse est interrompue. Cliquez sur **Reprendre** pour poursuivre l'analyse.

Arrêter – Met fin à l'analyse.

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



Journal d'analyse de l'ordinateur

Le journal d'analyse de l'ordinateur fournit des informations générales sur l'analyse, notamment les informations suivantes :

- Date et heure de l'analyse
- Disques, dossiers et fichiers analysés
- Nombre d'objets analysés
- Nombre de menaces détectées
- Heure d’achèvement
- Durée totale de l'analyse

Analyses des logiciels malveillants

La section **Analyses des logiciels malveillants** est accessible dans le menu Configuration avancée. Appuyez sur la touche **F5**, cliquez sur **Moteur de détection** > **Analyses des logiciels malveillants**. Elle propose des options pour sélectionner des configurations d'analyse :

- **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.
- **Protection à la demande et par apprentissage machine** – Consultez la section Moteur de détection (version 7.2 et versions ultérieures).
- **Cibles à analyser** – Si vous souhaitez uniquement analyser une cible spécifique, vous pouvez cliquer sur **Modifier** en regard de **Cibles à analyser**, puis sélectionner une option dans le menu déroulant ou choisir des cibles spécifiques dans la structure (arborescence) des dossiers. Pour plus d'informations, consultez Cibles à analyser.
- **Configurations de ThreatSense** – Cette section contient des options de configuration avancées, telles que les extensions des fichiers que vous souhaitez contrôler, les méthodes de détection utilisées, etc. Cliquez sur cette option pour afficher un onglet contenant les options avancées d'analyse.

Analyse en cas d'inactivité

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

Analyse en cas d'inactivité

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

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

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

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.

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

Profils d'analyse

Vos paramètres d'analyse préférés peuvent être enregistrés pour les prochaines analyses. Il est recommandé de créer autant de profils (avec différentes cibles et méthodes, et d'autres paramètres d'analyse) que d'analyses utilisées régulièrement.

Pour créer un profil, ouvrez la fenêtre Configuration avancée (F5) et cliquez sur **Moteur de détection** > **Analyses des logiciels malveillants** > **Analyse à la demande** > **Liste des profils**. 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 la section ThreatSenseConfiguration du moteur ; vous y trouverez une description de chaque paramètre de configuration de l'analyse.

Remarque

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 **nettoyage strict**. Entrez le nom du nouveau profil dans la fenêtre **Gestionnaire de profils**, puis cliquez sur **Ajouter**. Sélectionnez le nouveau profil dans le menu déroulant **Profil sélectionné** et réglez les paramètres restants selon vos besoin. Cliquez sur **OK** pour enregistrer le nouveau profil.

Cibles à analyser

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

- **Par les paramètres de profil** – Permet de sélectionner les cibles indiquées dans le profil d'analyse sélectionné.

- **Supports amovibles** – Permet de sélectionner les disquettes, les périphériques USB, les CD/DVD, etc.
- **Disques locaux** – Permet de sélectionner tous les disques durs du système.
- **Disques réseau** – Analyse tous les lecteurs réseau mappés.
- **Sélection personnalisée** – Permet à l'utilisateur de créer une sélection personnalisée de cibles.

Options d'analyse avancées

Cette fenêtre permet de définir des options avancées pour une opération d'analyse de l'ordinateur planifiée. Vous pouvez définir l'exécution automatique d'une action au terme d'une analyse à l'aide du menu déroulant :

- **Arrêter** – L'ordinateur est mis hors tension à la fin d'une analyse.
- **Redémarrer** – Ferme tous les programmes ouverts 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.
- **Aucune action** – Aucune action n'est exécutée à la fin d'une analyse.

> **Remarque**
> Notez 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.

Sélectionnez **L'action ne peut pas être annulée par l'utilisateur** 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.

Reportez-vous également au chapitre Progression de l'analyse.

Contrôle de périphérique

ESET Endpoint Antivirus permet un contrôle automatique des périphériques (CD/DVD/USB/...). 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
- Stockage FireWire
- Périphérique Bluetooth
- Lecteur de carte à puce
- Périphérique d'image
- Modem
- Port LPT/COM
- Périphérique portable
- Tous les types de périphérique

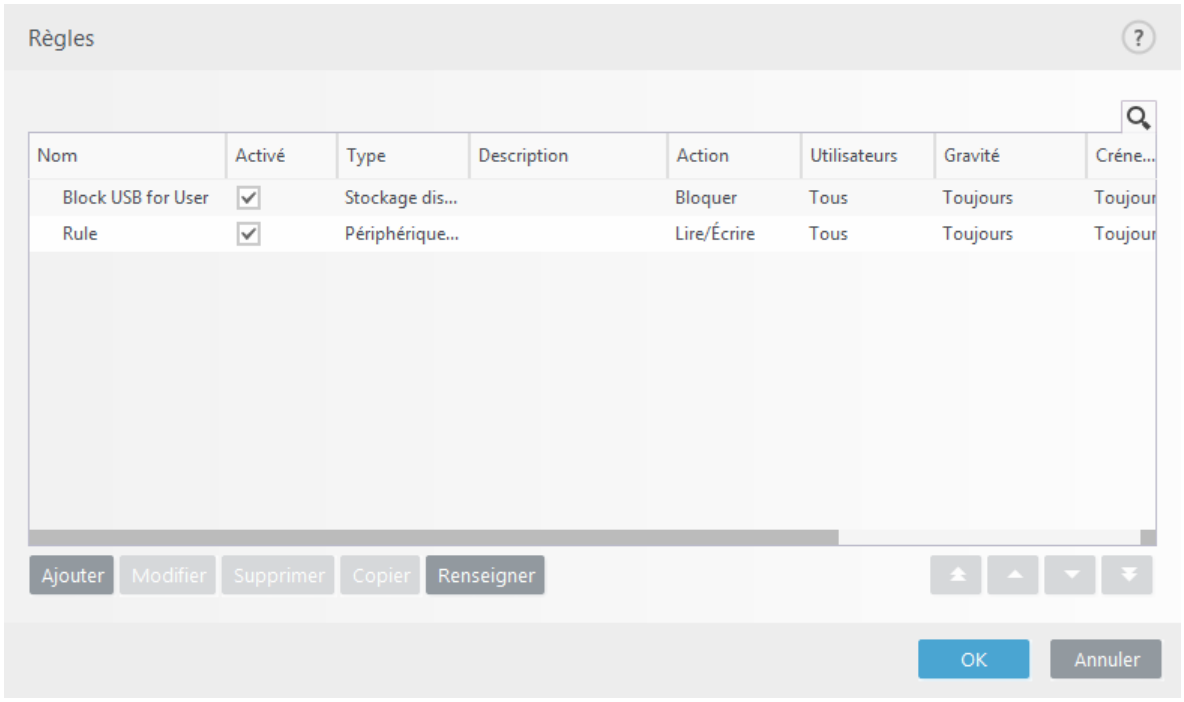
Les options de configuration du contrôle de périphérique peuvent être modifiées dans **Configuration avancée** (F5) > **Contrôle de périphérique**.

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

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

Éditeur de règles de contrôle de périphérique

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



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

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

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

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

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

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

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 sélectionnez un périphérique (dans la liste des périphériques détectés) et cliquez sur **OK** , une fenêtre d'éditeur de règles s'affiche avec des informations prédéfinies (tous les paramètres peuvent être réglés).

Groupe de périphériques

> **Avertissement**
> 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 le groupe avec la liste des périphériques que vous souhaitez afficher 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 un périphérique dans la liste renseignée, puis cliquez sur **OK** pour l'ajouter au groupe.

Éléments de commande

Ajouter : vous pouvez ajouter un groupe en saisissant son nom ou un périphérique à un groupe existant. Vous pouvez éventuellement indiquer des informations détaillées (le nom du fabricant, le modèle et le numéro de série, par exemple) 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 de périphériques à partir d'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).

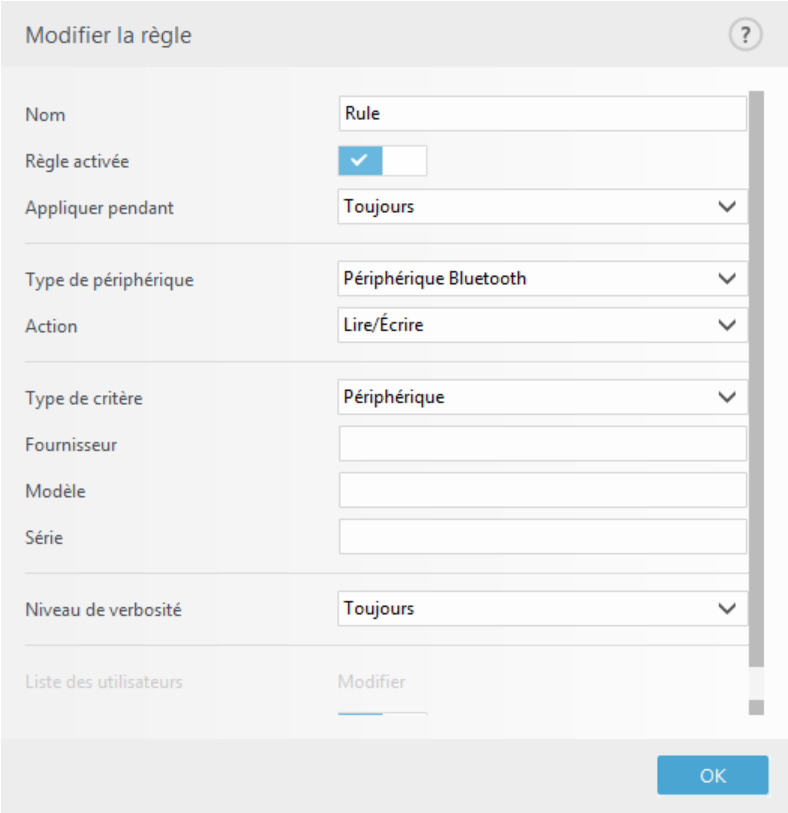
Une fois la personnalisation terminée, cliquez sur **OK**. Cliquez sur **Annuler** si vous souhaitez fermer la fenêtre **Groupes de périphériques** sans enregistrer les modifications.

> **Exemple**
> vous pouvez créer des groupes de périphériques différents auxquels différentes règles sont appliquées. Vous pouvez également créer un seul groupe de périphériques auquel la règle avec l'action **Lire/Écrire** ou **Lecture seule** sont appliquées. Les périphériques non reconnus sont ainsi bloqués par le contrôle de périphérique lorsqu'ils sont connectés à votre ordinateur.

Il convient de noter que toutes les actions (autorisations) ne sont pas disponibles pour tous les types de périphériques. S'il s'agit d'un périphérique de stockage, les quatre actions sont disponibles. Pour les périphériques autres que les périphériques de stockage, seules trois actions sont disponibles (par exemple, l'action **Lecture seule** n'étant pas disponible pour Bluetooth, un tel périphérique ne peut être qu'autorisé ou sujet à un avertissement).

Ajout de règles de contrôle de périphérique

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



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

Appliquer pendant – Permet d'appliquer la règle créée pendant un certain temps. Dans le menu déroulant, sélectionnez le créneau horaire créé. Pour plus d'informations, cliquez ici.

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.

> **Remarque**
> la liste des utilisateurs n'est pas disponible pour les modems. La règle sera appliquée pour tous les utilisateurs et la liste des utilisateurs actuelle sera supprimée.

Action

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

- **Lire/Écrire** – L'accès complet au périphérique est autorisé.
- **Bloquer** – L'accès au périphérique est bloqué.
- **Lecture seule** – 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 périphériques ne sont pas mémorisés, une notification continuera de s'afficher lors des connexions suivantes d'un même périphérique.

Il convient de noter que toutes les actions (autorisations) ne sont pas disponibles pour tous les types de périphériques. S'il s'agit d'un périphérique de stockage, les quatre actions sont disponibles. Pour les périphériques autres que les périphériques de stockage, seules trois actions sont disponibles (par exemple, l'action **Lecture seule** n'étant pas disponible pour Bluetooth, un tel périphérique ne peut être qu'autorisé ou sujet à un avertissement).

Type de critère – Sélectionnez Groupe de périphériques ou Périphérique.

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

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

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

> **Remarque**
> 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.

Niveau de verbosité

- **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 et les envoie à ERA Server.
- **Aucun** – Aucun journal n'est enregistré.

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

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

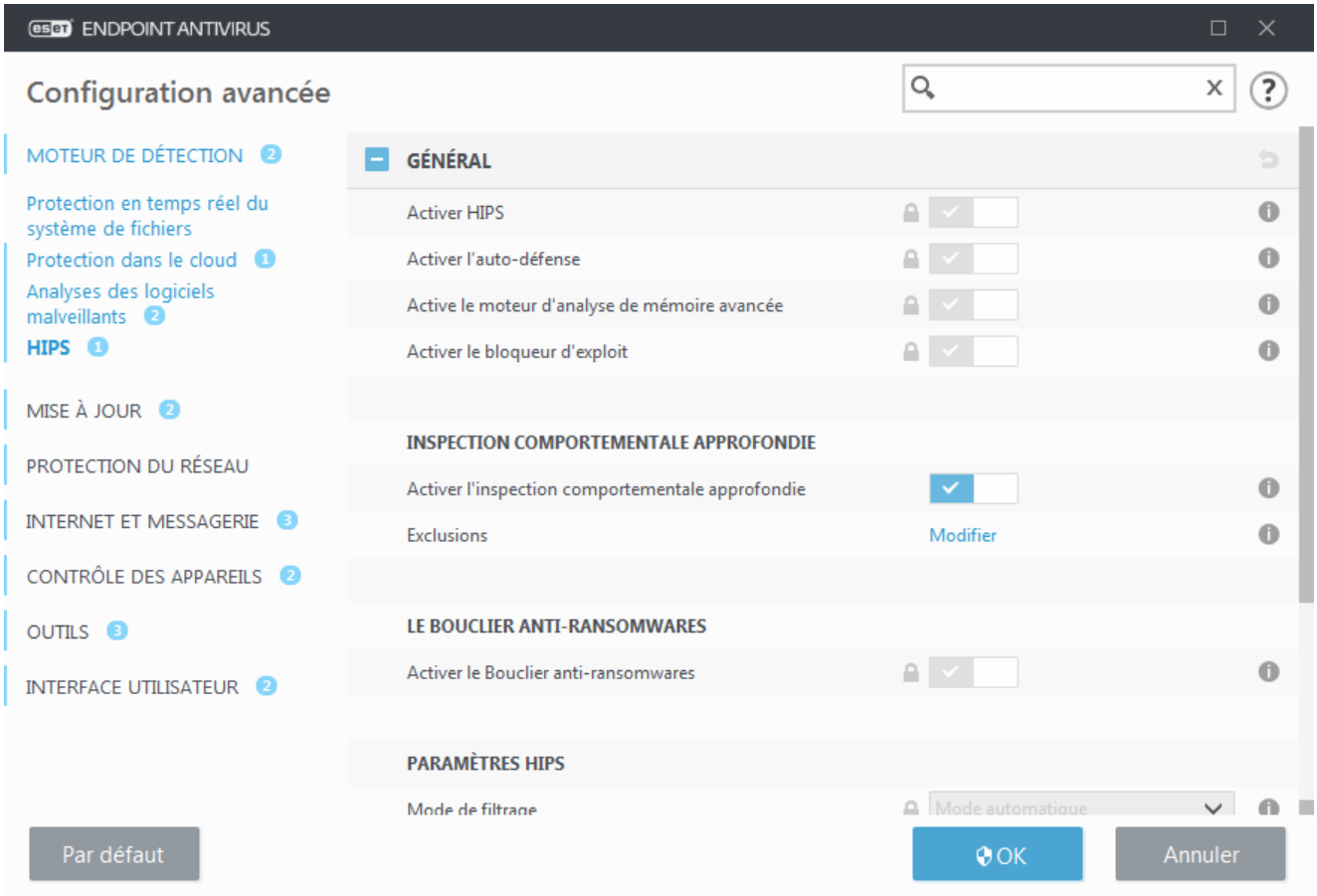
Remarque
Tous les périphériques ne peuvent pas être filtrés par les règles de l'utilisateur (par exemple, les périphériques d'image ne fournissent pas d'informations sur les utilisateurs, uniquement sur les actions effectuées).

Système HIPS

Avertissement
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.

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



Général

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

Activer l'auto-défense – ESET Endpoint 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. ESET Management Agent est également protégé lorsqu'il est installé.

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. Cette option est disponible dans Windows 8.1 et Windows 10.

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 le mode d'audit – Tous les éléments détectés par le Bouclier anti-ransomwares ne sont pas automatiquement bloqués. Ils sont consignés avec une gravité d'avertissement et envoyés à la console de gestion avec l'indicateur « MODE AUDIT ». L'administrateur peut choisir d'exclure ce type de détection pour empêcher toute détection ultérieure ou la garder active (ce qui signifie qu'une fois le mode d'audit terminé, elle sera bloquée et supprimée). L'activation et la désactivation du mode d'audit seront également consignées dans ESET Endpoint Antivirus. Cette option est uniquement disponible dans ESMC ou l'éditeur de configuration de politique ESET PROTECT Cloud.

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 consultées 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.

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).

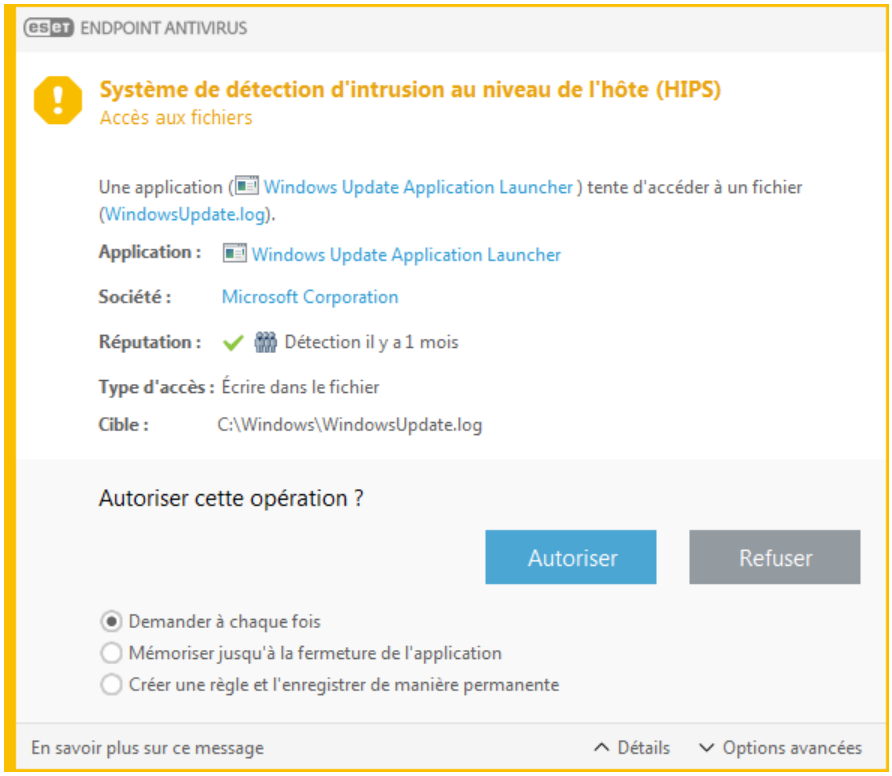
Cliquez sur **Détails** en bas pour déterminer quelle application déclenche l'opération, quelle est la réputation du fichier ou quel type d'opération il vous est demandé d'autoriser ou de refuser.

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** – Sélectionnez 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 **Mode automatique** dans **Configuration avancée** (F5) > **Moteur de détection** > **HIPS** > **Général**.



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**.

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

Gestion des règles HIPS

Il s'agit de la liste des règles définies par l'utilisateur et ajoutées automatiquement dans le système HIPS. Vous trouverez des informations détaillées sur la création de règles et sur les opérations HIPS au chapitre Configurations des règles HIPS. Consultez également Principe général HIPS.

Colonnes

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

Activé – Désactivez ce 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.

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

Notifier – Une petite notification contextuelle 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).

Paramètres de règle HIPS

Consultez d'abord la 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 ce bouton bascule si vous souhaitez conserver la règle dans la liste, mais ne souhaitez pas l'appliquer.

Journaliser – Si vous activez cette option, les informations sur cette règle sont indiquées dans le journal HIPS.

Avertir l'utilisateur – Une petite fenêtre contextuelle 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 – 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 ajouter de nouveaux fichiers ou dossiers. Vous pouvez également sélectionner **Toutes les entrées** dans le menu déroulant pour ajouter toutes les entrées.

Remarque
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 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.

> **Remarque**
> Il n'est pas possible d'intercepter des opérations de processus sur la version 64 bits de Windows XP.

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.

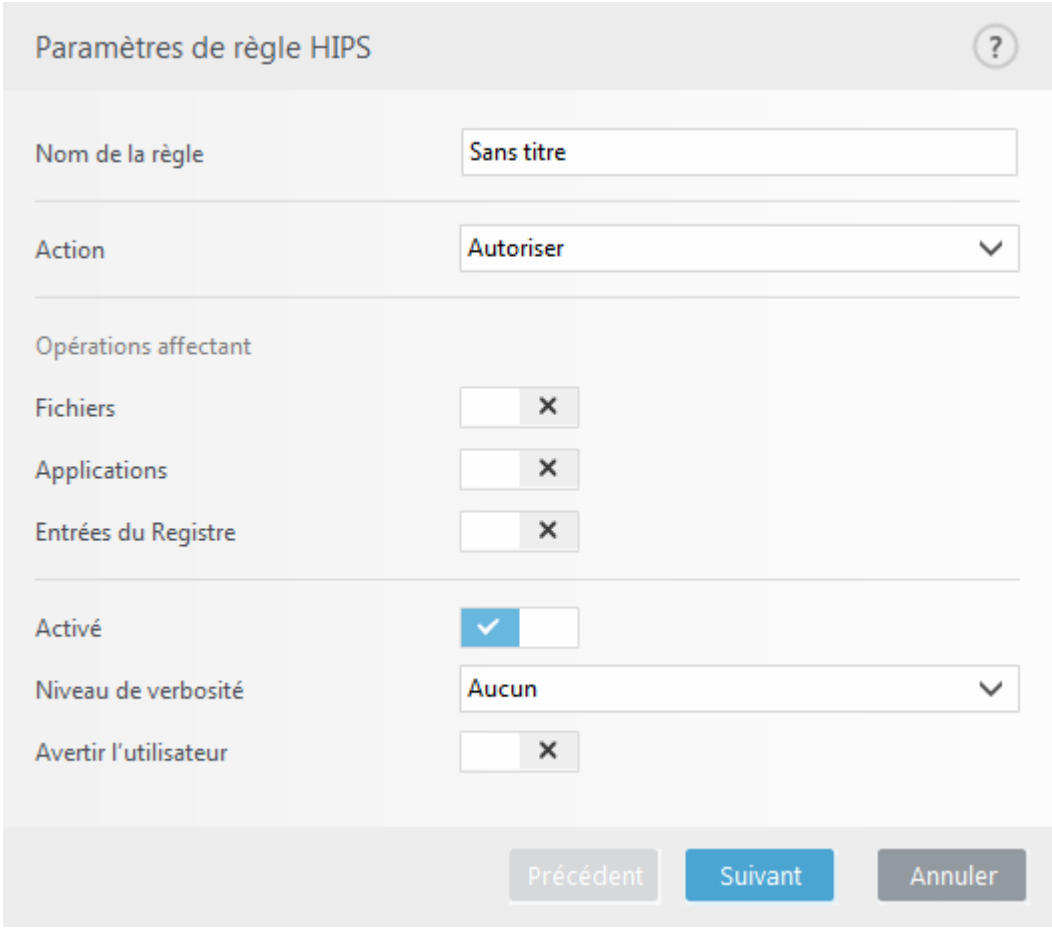
> **Remarque**
> Utilisation des caractères génériques dans les règles
> L'astérisque peut uniquement être utilisé dans les règles afin de remplacer une clé particulière, par exemple « HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start ». Les autres utilisations des caractères génériques ne sont pas prises en charge.
> Création de règles ciblant la clé HKEY_CURRENT_USER
> Cette clé n'est qu'un lien vers la sous-clé appropriée de HKEY_USERS spécifique à l'utilisateur identifié par SID (identifiant sécurisé). Pour créer une règle pour l'utilisateur actuel uniquement, utilisez un chemin pointant sur HKEY_USERS\%SID%, plutôt qu'un chemin menant vers HKEY_CURRENT_USER. Vous pouvez en effet utiliser un astérisque en tant que SID de façon à rendre la règle applicable à l'ensemble des utilisateurs.

> **Avertissement**
> 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 **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.



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.

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.

> **Remarque**
> 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.

Mode de présentation

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

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

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

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

Analyse au démarrage

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

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

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

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 fixes pour chaque groupe précité.

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

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

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 la fenêtre **Configuration avancée** (appuyez sur F5) > **Moteur de détection** > **Analyses des logiciels malveillants** > **Protection des documents**, puis cliquez sur le commutateur **Intégrer dans le système**.

Remarque
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).

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 nettoyage 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.

Dans la version 7.1 et les versions antérieures, les exclusions de performances et les exclusions de détection ont été fusionnées.

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

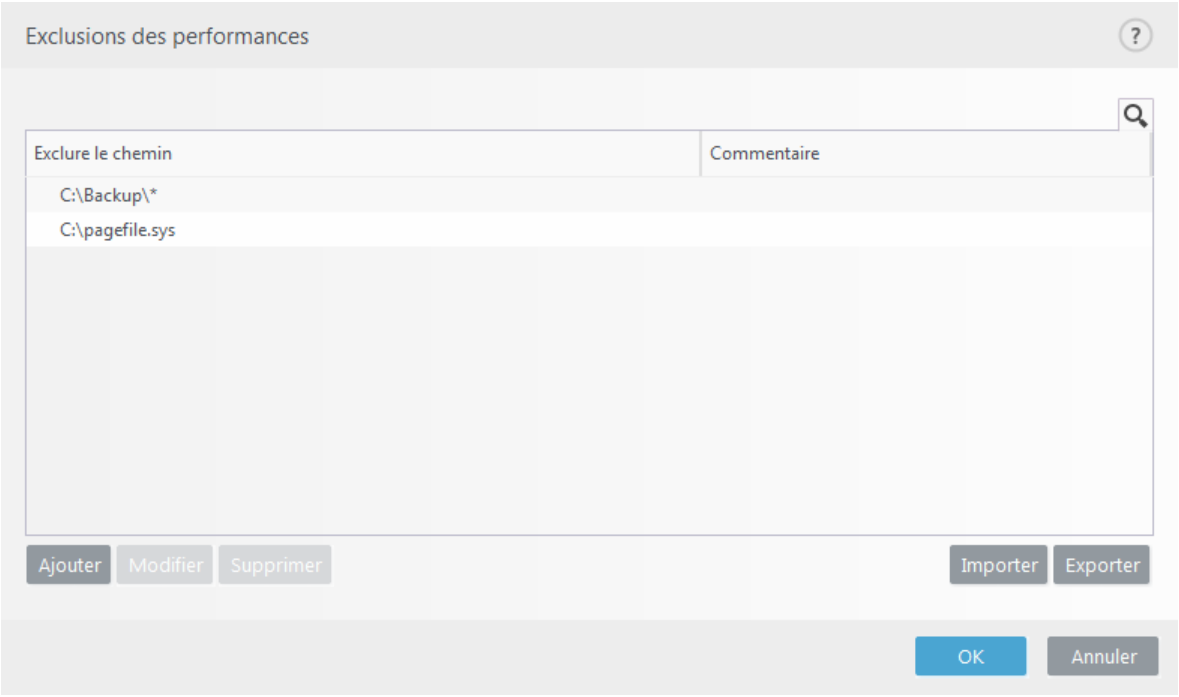
Les exclusions de performances permettent d'exclure des fichiers et dossiers de l'analyse.

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** (**F5**) > **Moteur de détection** > **Exclusions** > **Exclusions des performances** > **Modifier**.

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.



REMARQUE

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** – Permet d'ajouter une nouvelle entrée pour exclure des objets de l'analyse.
- **Modifier** – Permet de modifier des entrées sélectionnées.
- **Retirer** – Retire les entrées sélectionnées (CTRL + clic pour sélectionner plusieurs entrées.
- **Importer/Exporter** – Ces opérations sont utiles si vous devez sauvegarder les exclusions actuelles pour les utiliser ultérieurement. L'option Exporter les paramètres est également pratique pour les utilisateurs des environnements non gérés qui souhaitent utiliser leur configuration préférée sur plusieurs systèmes. Il leur suffit d'importer un fichier .txt pour transférer ces paramètres.

Exemple du format de fichier d'importation/exportation

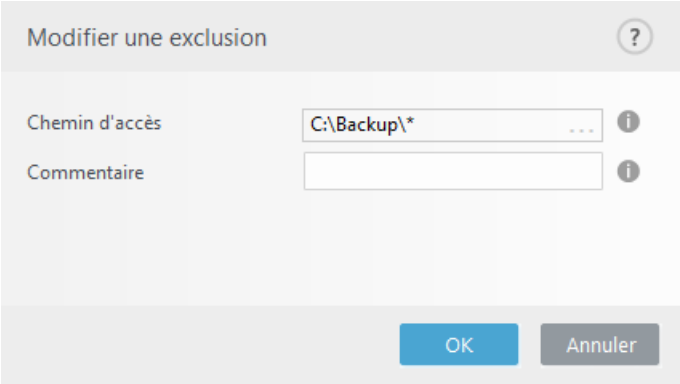
```
# {"product":"endpoint","version":"7.2.2055","path":"plugins.01000600.settings.Perfo
rmanceExclusions","columns":["Path","Description"]}

C:\Backup\*,custom comment

C:\pagefile.sys,
```

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 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 (le point d'interrogation remplace les caractères manquants/inconnus)

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 de chemin faisant appel à un astérisque

Voici d'autres exemples d'exclusion faisant appel à un astérisque :

*C:\Tools** – Le chemin doit se terminer par une barre oblique inverse et un astérisque pour indiquer qu'un dossier et tous ses sous-dossiers sont en cours d'exclusion.

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.

Exception pour les exclusions de performances :

C:\Tools.** – Même comportement que *C:\Tools** (le masque `*.*` exclut uniquement les fichiers dotés d'extension dans le dossier *Tools*).

Exemple d'exclusion saisie manuellement de façon incorrecte :

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 – N'oubliez pas d'ajouter un astérisque à la fin du chemin : *C:\Tools**

Caractères génériques au milieu d'un chemin

Il est vivement recommandé de ne pas utiliser de caractères génériques au milieu d'un chemin (*C:\Tools*\Data\file.dat*, par exemple), sauf si votre infrastructure système le demande. Pour plus d'informations, consultez cet article de la base de connaissances.

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 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 (le point d'interrogation remplace les caractères manquants/inconnus)

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%*

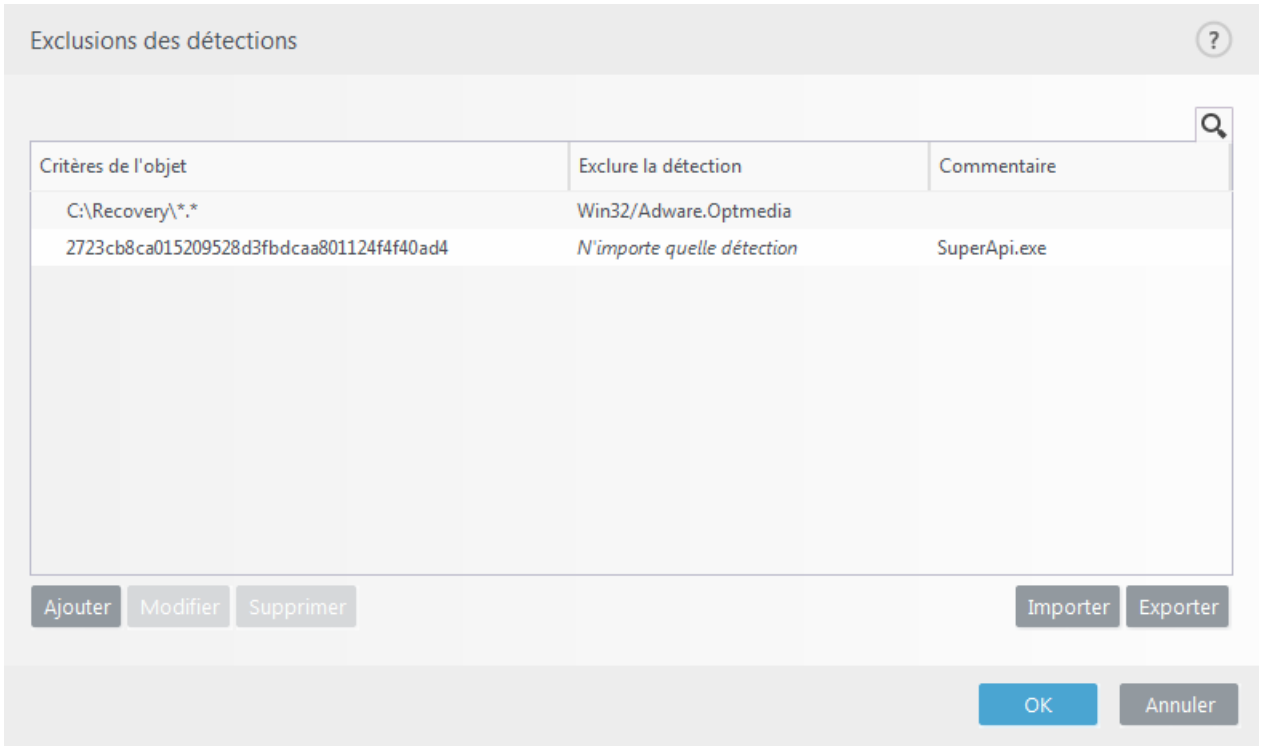
Les variables système spécifiques à l'utilisateur (comme *%TEMP%* ou *%USERPROFILE%*) et les variables d'environnement (comme *%PATH%*) ne sont pas prises en charge.

Exclusions des détections

Les exclusions de détection permettent d'exclure des objets du nettoyage 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** (**F5**) > **Moteur de détection** > **Exclusions** > **Exclusions des détections** > **Modifier**.

Pour exclure un objet (par son nom de détection ou par son hachage) du nettoyage, cliquez sur **Ajouter**.

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 se trouve en regard d'un fichier exclu, cela signifie que ce fichier n'est exclu que pour cette détection et non pas complètement. Si le fichier est infecté ultérieurement par un autre logiciel malveillant, il est détecté. Ce type d'exclusion ne peut être utilisé que pour certains types d'infiltrations. Il peut être créé soit dans la fenêtre des alertes qui signale l'infiltration (cliquez sur **Afficher les options avancées** et sélectionnez **Exclure de la détection**), soit en cliquant sur **Outils** > **Quarantaine** à l'aide d'un clic droit sur le fichier placé en quarantaine et en sélectionnant **Restaurer et exclure de l'analyse** dans le menu contextuel.
- **Hachage** – Permet d'exclure un fichier selon le hachage spécifié (SHA1), indépendamment du type de fichier, de l'emplacement ou de l'extension de celui-ci.

Éléments de commande

- **Ajouter** – Permet d'ajouter une nouvelle entrée pour exclure des objets du nettoyage.
- **Modifier** – Permet de modifier des entrées sélectionnées.
- **Retirer** – Retire les entrées sélectionnées (CTRL + clic pour sélectionner plusieurs entrées.
- **Importer/Exporter** – Ces opérations sont utiles si vous devez sauvegarder les exclusions actuelles pour les utiliser ultérieurement. L'option Exporter les paramètres est également pratique pour les utilisateurs

des environnements non gérés qui souhaitent utiliser leur configuration préférée sur plusieurs systèmes. Il leur suffit d'importer un fichier .txt pour transférer ces paramètres.

Exemple du format de fichier d'importation/exportation

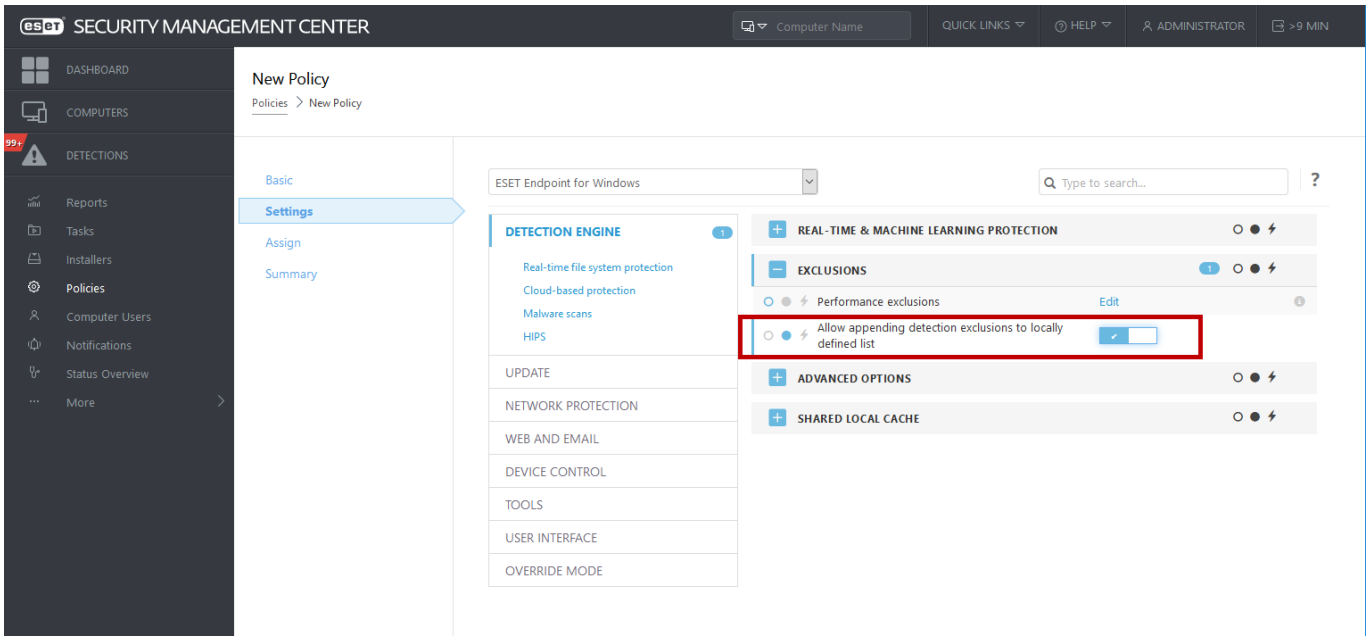
```
# {"product":"endpoint","version":"7.2.2055","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","FileHash"]}

4c59cd02-357c-4b20-a0ac-ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF

2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,,
```

Configuration des exclusions de détection dans ESMC

ESMC 7.1 contient un nouvel assistant pour la gestion des exclusions de détection. Il permet de créer une exclusion de détection et l'appliquer à d'autres ordinateurs/groupes.

Remplacement possible des exclusions de détection d'ESMC

En présence d'une liste locale d'exclusions de détection, l'administrateur doit appliquer une politique avec l'option **Autoriser l'ajout des exclusions de détection à la liste définie localement**. Après, l'ajout des exclusions de détection d'ESMC fonctionnera comme prévu.



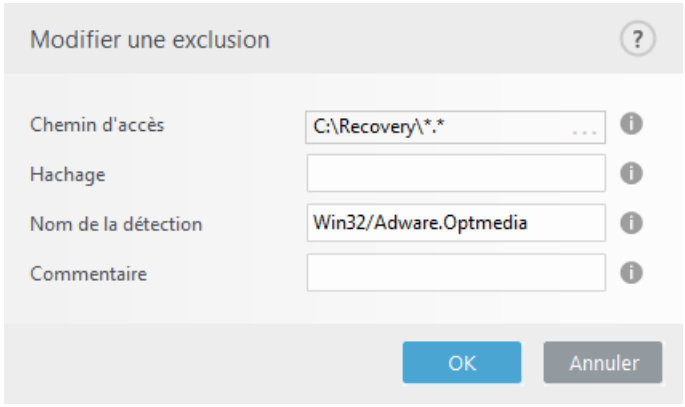
Ajout ou modification d'une exclusion de détection

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 Endpoint 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.

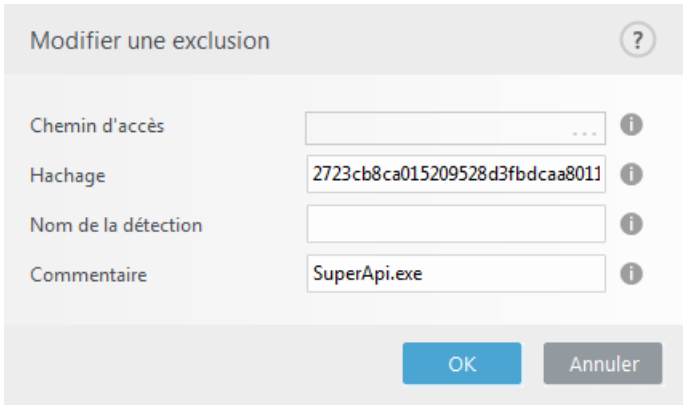
Consultez également Format d'exclusion de chemin.



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

Exclure le hachage

Permet d'exclure un fichier selon le hachage spécifié (SHA1), 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 Endpoint 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** :

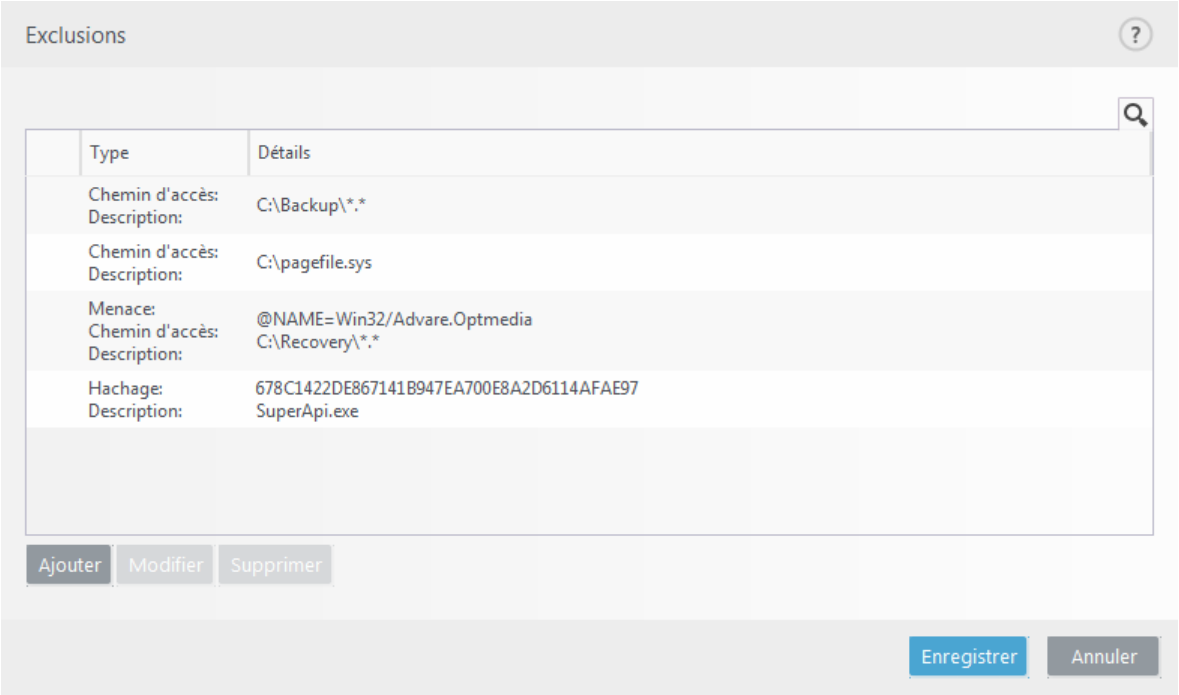
- **Fichiers exacts** – Exclure chaque fichier par son hachage SHA-1.
- **Détection** – Exclure chaque fichier par son nom de détection.
- **Chemin et détection** – Exclure chaque fichier par nom de détection et chemin, notamment le nom de fichier (*file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*,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

Exclusions (version 7.1 et version antérieure)

Dans la version 7.1 et les versions antérieures, les exclusions de performances et les exclusions de détection ont été fusionnées.



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. Des problèmes similaires peuvent se produire lors d'une migration dynamique de machines virtuelles. 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. Nous vous recommandons de faire preuve de prudence lors de la création d'exclusions. Un outil de sauvegarde exclu peut accéder aux fichiers infectés sans déclencher d'alerte. C'est pourquoi les autorisations étendues ne sont autorisées que dans le module de protection en temps réel.

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 dans la liste des processus exclus des fichiers exécutables via **Configuration avancée** (**F5**) > **Moteur de détection** > **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.

Exemple

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 Endpoint Antivirus et aucune analyse n'est effectuée sur les opérations de fichier effectuées par celui-ci.

Important

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.

Remarque

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*).

Exemple

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 Endpoint Antivirus et aucune analyse n'est effectuée sur les opérations de fichier effectuées par celui-ci.

Important

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.

Exclusions HIPS

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

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.

Paramètres ThreatSense

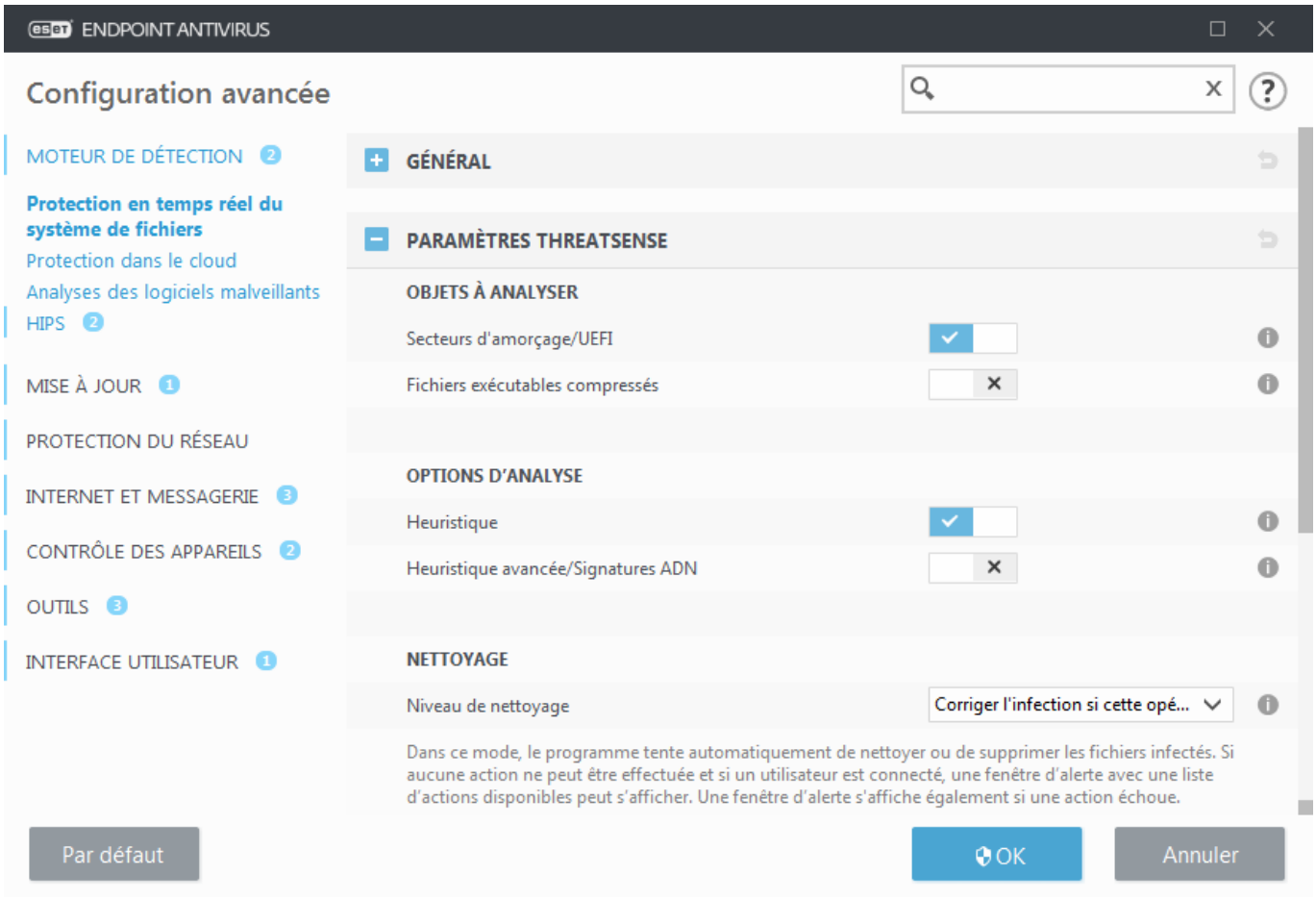
ThreatSense est constitué de nombreuses méthodes complexes de détection de menaces. C'est une technologie proactive : elle fournit une protection dès le début de la propagation d'une nouvelle menace. Elle utilise une combinaison d'analyse de code, d'émulation de code, de signatures génériques et de signatures 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 du moteur ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

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

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

- Protection en temps réel du système de fichiers
- Analyse en cas d’inactivité
- Analyse au démarrage
- Protection des documents
- Protection du client de messagerie
- Protection de l’accès 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.

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

Options d'analyse

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

Heuristique – La méthode heuristique utilise un algorithme d'analyse de l'activité (malveillante) des programmes. Elle présente l'avantage d'identifier un code malveillant qui n'existait pas ou qui n'était pas connu par la 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 Endpoint Antivirus lors du nettoyage des objets.

Exclusions

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

Autre

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

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

Exécuter les analyses en arrière-plan avec une priorité faible – Toute séquence d'analyse consomme une

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

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

Configuration de l'analyse d'archive

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

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

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

Niveaux de nettoyage

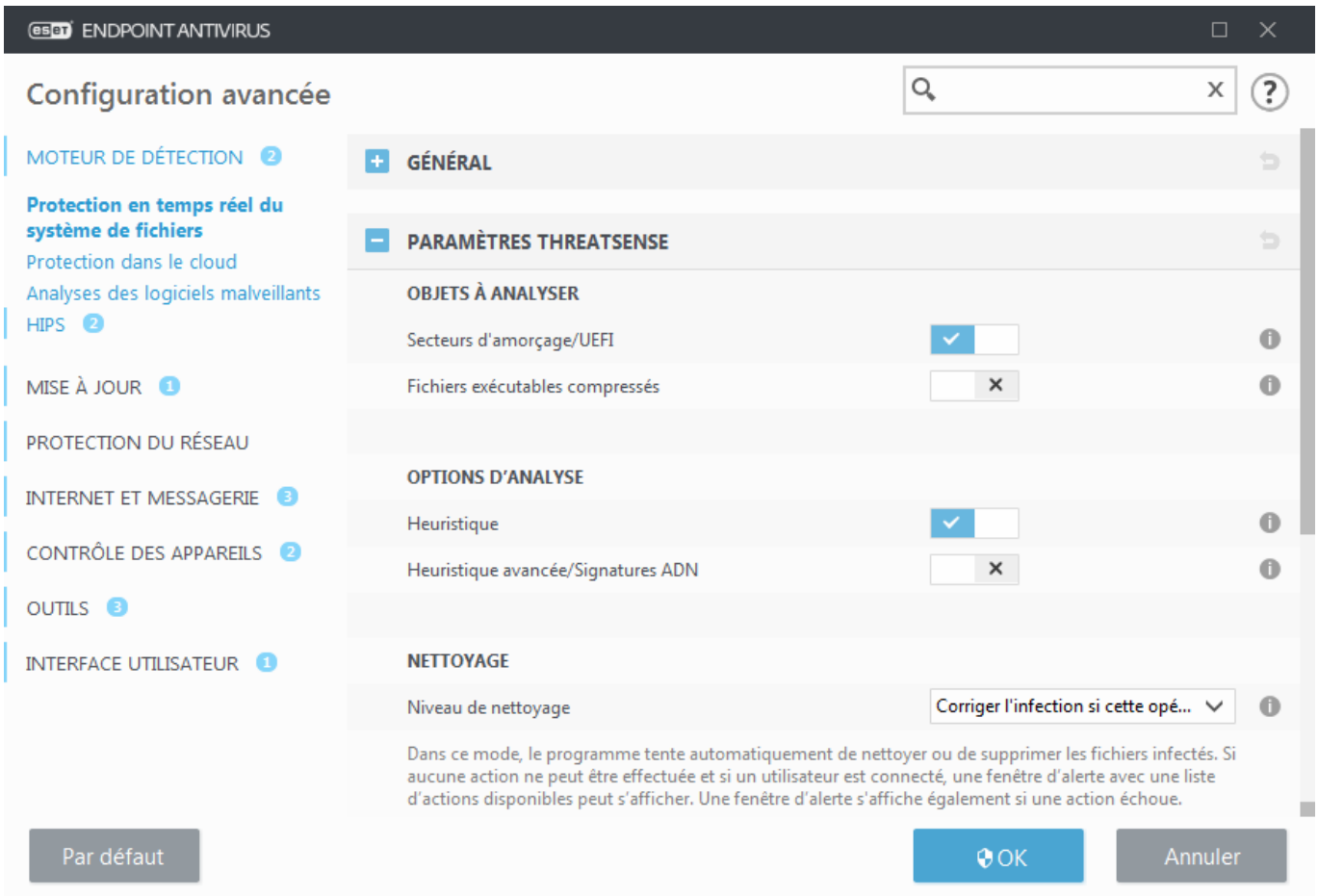
Pour accéder aux paramètres de niveaux de nettoyage d'un module de protection de votre choix, développez **paramètres ThreatSense** (**Protection en temps réel du système de fichiers**, par exemple), puis cliquez sur

Nettoyage.

La protection en temps réel et d'autres modules de protection ont les niveaux de correction (c.-à-d. de nettoyage) ci-après.

Correction dans ESET Endpoint Antivirus 7.2 et les versions ultérieures

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. **Toujours corriger la détection** est le paramètre par défaut recommandé dans un environnement administré.
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.



Niveaux de nettoyage dans ESET Endpoint Antivirus 7.1 et les versions antérieures

Niveau de nettoyage	Description
Pas de nettoyage	Les détections ne sont pas nettoyées automatiquement. Le programme affiche alors une fenêtre d'avertissement et laisse l'utilisateur choisir une action. Ce niveau a été conçu pour les utilisateurs expérimentés qui connaissent les mesures à prendre en cas de détection.
Nettoyage normal	Le programme tente de nettoyer ou de supprimer automatiquement tout fichier sur la base d'une action prédéfinie (dépendant du type d'infiltration). La détection et la suppression d'un fichier infecté sont signalées par une notification affichée dans l'angle inférieur droit de l'écran. S'il n'est pas possible de sélectionner automatiquement l'action correcte, le programme propose plusieurs actions de suivi. C'est le cas également si une action prédéfinie ne peut pas être menée à bien.
Nettoyage strict	Le programme nettoie ou supprime toutes les détections. Les seules exceptions sont les fichiers système. S'il n'est pas possible de les nettoyer, l'utilisateur est invité à sélectionner une action dans une fenêtre d'avertissement.

Le niveau de nettoyage mentionné est appliqué lors de la configuration d'une politique ESMC pour les versions antérieures d'ESET Endpoint Antivirus :

Niveau de nettoyage dans la politique ESMC	Niveau de nettoyage appliqué
Toujours corriger la détection	Nettoyage strict
Corriger la détection si cette opération est sûre. Sinon, conserver	Nettoyage normal
Corriger la détection si cette opération est sûre. Sinon, demander à l'utilisateur*	Nettoyage normal
Toujours demander à l'utilisateur final	Pas de nettoyage

* Valeur par défaut lors de la mise à niveau vers les versions 7.2 et ultérieures avec l'option **Nettoyage normal** définie dans ESET Endpoint Antivirus.

Extensions de fichier exclues de l'analyse

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

> **Remarque**
> Ne pas confondre avec d'autres types d'Exclusions :

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.

Exemple

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`).

Remarque

Pour connaître l'extension exacte (le cas échéant) d'un fichier sous un système d'exploitation Windows, vous devez décocher l'option **Masquer les extensions des fichiers dont le type est connu**, dans **Panneau de configuration** > **Options des dossiers** > **Affichage** (onglet), et appliquer cette modification.

Autres paramètres ThreatSense

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

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

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

Réseau

La section **Réseau** permet d'accéder rapidement aux composants et aux configurations suivants dans les configurations avancées :

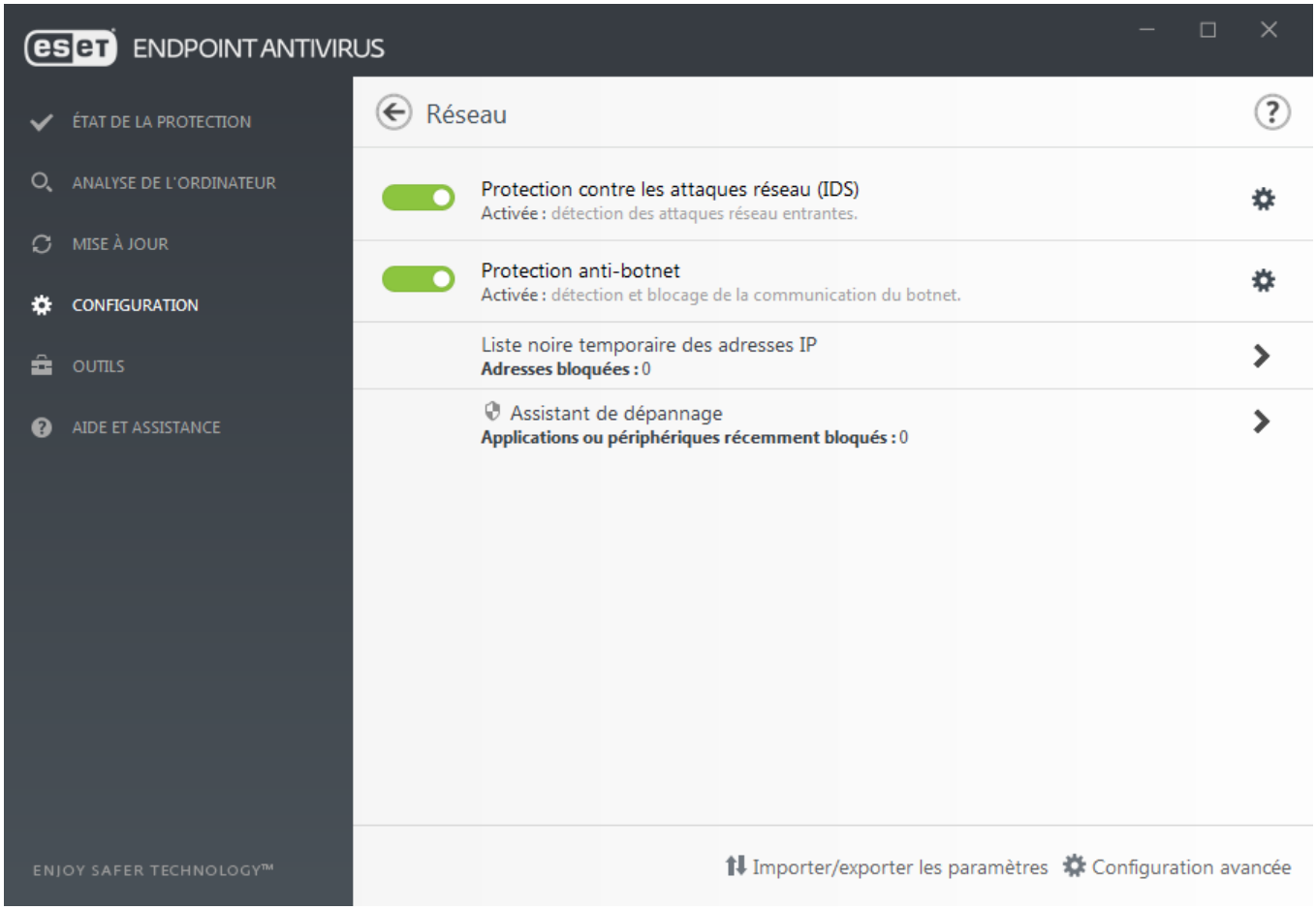
- **Protection contre les attaques réseau (IDS)** – Analyse le contenu du trafic réseau et protège contre les attaques réseau. Tout trafic considéré comme nuisible sera bloqué. ESET Endpoint Antivirus vous informe lorsque vous vous connectez à un réseau sans fil non protégé ou un réseau avec une protection faible.

- **Protection anti-botnet** – Identifie rapidement et précisément les logiciels malveillants sur le système. Pour désactiver la protection anti-botnet pendant une période spécifique, cliquez sur  . (non recommandé)

- **Liste noire temporaire des adresses IP** – Affichez la liste des adresses IP qui ont été détectées comme

source d'attaques et ajoutées à la liste noire pour bloquer les connexions pendant une certaine période. Pour plus d'informations, cliquez sur cette option et appuyez sur F1.

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



Protection contre les attaques réseau

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

Activer la protection anti-botnet – Détecte et bloque les communications avec des serveurs de contrôle et de commande malveillants selon les modèles classiques lorsque l'ordinateur est infecté et qu'un robot tente de communiquer.Pour en savoir plus sur la protection anti-botnet, consultez le glossaire.

Règles IDS : cette option permet de configurer les options de filtrage avancées visant à détecter plusieurs types d'attaques et exploits pouvant être utilisés pour porter atteinte à votre ordinateur.

Options de filtrage avancées

La section Protection contre les attaques réseau permet de configurer des options de filtrage avancées pour détecter plusieurs types d'attaques et de vulnérabilités pouvant être perpétrés contre votre ordinateur.

Notifications et consignation

Dans certains cas, vous ne recevrez pas de notification de menace sur les communications bloquées. Pour obtenir des instructions afin d'afficher toutes les communications bloquées dans le journal du pare-feu, consultez la section Consignation et création de règles ou d'exceptions à partir du journal.

Disponibilité d'options spécifiques dans cette page d'aide

La disponibilité d'options spécifiques dans Configurations avancées (**F5**) > **Protection du réseau** > **Protection contre les attaques réseau** peut varier selon le type ou la version de votre produit ESET Endpoint et du module de pare-feu et de celle de votre système d'exploitation. Certaines options peuvent être uniquement disponibles pour ESET Endpoint Security.

Détection d'intrusion

- **Protocole SMB** – Détecte et bloque divers problèmes de sécurité dans le protocole SMB, notamment :
  - **Détection d'authentification par falsification de challenge** – Protège contre une attaque utilisant un challenge falsifié durant l'authentification, dans le but d'obtenir les identifiants de l'utilisateur.
  - **Évasion IDS pendant la détection d'ouverture d'un canal nommé** – Détection de techniques d'évasion connues et utilisées pour l'ouverture de canaux nommés MSRPC dans le protocole SMB.
  - **Détections CVE** (Common Vulnerabilities and Exposures) – Méthodes de détection mises en œuvre de diverses attaques, formes, trous de sécurité et exploits sur le protocole SMB. Reportez-vous au site Web CVE cve.mitre.org pour plus de détails sur les identificateurs CVE (CVE).
- **Protocole RPC** – Détecte et bloque divers CVE dans le système d'appel des procédures à distance développé pour l'environnement Distributed Computing Environment (DCE).
- **Protocole RDP** – Détecte et bloque divers CVE dans le protocole RDP (voir ci-dessus).
- **Bloquer l'adresse non sûre après une détection d'attaque** – Les adresses IP qui ont été identifiées comme sources d'attaques sont ajoutées à la liste noire pour prévenir toute connexion pendant une certaine période.
- **Afficher une notification après la détection d'une attaque** – Active les notifications qui apparaissent dans la barre d'état système, dans l'angle inférieur droit de l'écran.
- **Afficher également des notifications pour les attaques entrantes contre les trous de sécurité** – Vous avertit si des attaques contre des trous de sécurité sont détectées ou si une menace tente d'accéder au système de cette manière.

Vérification des paquets

- **Autoriser les connexions entrantes aux partages administratifs du protocole SMB** : les partages administratifs sont les partages réseau par défaut qui partagent les partitions de disque dur (*C$*, *D$*, ...) au sein du système, ainsi que le répertoire système (*ADMIN$*). Désactiver la connexion aux partages administratifs peut limiter de nombreux risques de sécurité. Par exemple, le ver Conficker effectue des attaques par dictionnaire afin de se connecter aux partages administratifs.
- **Refuser les dialectes SMB anciens (non pris en charge)** – Refuse des sessions SMB qui utilisent un ancien dialecte SMB non pris en charge par IDS. Les systèmes d'exploitation Windows modernes prennent en charge

les anciens dialectes SMB en raison de la rétrocompatibilité avec les anciens systèmes d'exploitation tels que Windows 95. Le pirate peut utiliser un ancien dialecte dans une session SMB dans le but d'échapper à l'inspection du trafic. Refusez les anciens dialectes SMB si votre ordinateur n'a pas besoin de partager des fichiers (ou utiliser des communications SMB en général) avec un ordinateur équipé d'une ancienne version de Windows.

- **Refuser les sessions SMB sans sécurité étendue** – La sécurité étendue peut être utilisée au cours de la négociation de session SMB, afin de fournir un mécanisme d'authentification plus sécurisé que l'authentification par challenge/réponse du gestionnaire LAN (LM). Le schéma LM est considéré comme faible et son utilisation n'est pas recommandée.

- **Autoriser la communication avec le service Security Account Manager** : pour plus d'informations sur ce service, voir [MS-SAMR].

- **Autoriser la communication avec le service Local Security Authority** : pour plus d'informations sur ce service, voir [MS-LSAD] et [MS-LSAT].

- **Autoriser la communication avec le service Remote Registry** : pour plus d'informations sur ce service, voir [MS-RRP].

- **Autoriser la communication avec le service Service Control Manager** : pour plus d'informations sur ce service, voir [MS-SCMR].

- **Autoriser la communication avec le service Server** : pour plus d'informations sur ce service, voir [MS-SRVS].

- **Autoriser la communication avec les autres services** – Le protocole MSRPC est l'implémentation par Microsoft du mécanisme DCE RPC. De plus, MSRPC peut utiliser des canaux nommés transportés (ncacn_np transport) par le protocole SMB (partage de fichiers en réseau). Les services MSRPC fournissent des interfaces d'accès et de gestion à distance pour les systèmes Windows. Plusieurs vulnérabilités ont été découvertes et exploitées librement dans le système Windows MSRPC (vers Conficker et Sasser, …). Désactivez la communication avec les services MSRPC que vous ne devez pas fournir, afin de limiter de nombreux risques de sécurité (tels que l'exécution de code à distance ou les attaques par déni de service).

- **Vérifier l'état de la connexion TCP** – Vérifie si tous les paquets TCP appartiennent à une connexion existante. Si un paquet n'existe pas dans une connexion, il est ignoré.

- **Maintenir les connexions TCP inactives** – Pour fonctionner, certaines applications exigent que la connexion TCP qu'elles établissent soit maintenue, même si elle peut être inactive. Sélectionnez cette option pour éviter de mettre fin à des connexions TCP inactives.

- **Détection de surcharge du protocole TCP** – Le principe de cette méthode consiste à soumettre l'ordinateur/serveur à plusieurs demandes. Voir également Attaques par déni de service (DoS).

- **Vérification des messages par protocole ICMP** – Empêche les attaques qui exploitent les faiblesses du protocole ICMP, ce qui peut provoquer une absence de réponse de l'ordinateur. Voir également Attaques par déni de service (DoS).

- **Détection de données cachées dans le protocole ICMP** – Vérifie si le protocole ICMP n'est pas utilisé pour le transfert de données. De nombreuses techniques malveillantes utilisent le protocole ICMP pour contourner le pare-feu.

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

Règles IDS

Dans certaines situations, le service IDS (Intrusion Detection Service) peut détecter des communications entre des box Internet ou d'autres périphériques réseau internes comme des attaques potentielles. Par exemple, vous pouvez ajouter l'adresse sécurisée connue aux adresses exclues de la zone IDS pour contourner le service IDS.

> **Instructions illustrées**
> Les articles suivants de la base de connaissances ESET peuvent être disponibles uniquement en anglais :
> - Créer des exclusions IDS sur les postes de travail clients dans ESET Endpoint Antivirus
> - Créer des exclusions IDS pour les postes de travail clients dans ESET Security Management Center

Colonnes

- **Alerte** : type d'alerte.
- **Application** : 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.
- **Adresse IP distante** : liste des adresses IPv4 ou IPv6 distantes/plages/sous-réseaux. Plusieurs adresses doivent être séparées par des virgules.
- **Bloquer** : chaque processus système possède son propre comportement et une action affectée (bloquer ou autoriser). Pour remplacer le comportement par défaut de ESET Endpoint Antivirus, vous pouvez choisir de le bloquer ou de l'autoriser à l'aide du menu déroulant.
- **Notifier** : sélectionnez **Oui** pour afficher les notifications du Bureau sur votre ordinateur. Sélectionnez **Non** si vous ne souhaitez pas les afficher. Les valeurs disponibles sont **Par défaut**/**Oui**/**Non**.
- **Consigner** : sélectionnez **Oui** pour consigner les événements dans les fichiers journaux de ESET Endpoint Antivirus. Sélectionnez **Non** si vous ne souhaitez pas consigner les événements. Les valeurs disponibles sont **Par défaut**/**Oui**/**Non**.

Gestion des exceptions IDS

- **Ajouter** : cliquez sur cette option pour ajouter une nouvelle exception IDS.
- **Modifier** : cliquez sur cette option pour modifier une exception IDS existante.
- **Supprimer** : cliquez sur cette option si vous souhaitez supprimer une exception de la liste des exceptions IDS.
-  **Haut/Monter/Bas/Descendre** : permet d'ajuster le niveau de priorité des exceptions (les exceptions sont évaluées du haut vers le bas).

Exemple

Vous souhaitez afficher une notification et créer un journal chaque fois que l'événement se produit :

1.Cliquez sur **Ajouter** pour ajouter une exception IDS.
2.Sélectionnez une alerte spécifique dans le menu déroulant **Alerte**.
3.Cliquez sur**...** et sélectionnez le chemin d'accès au fichier de l'application à laquelle vous souhaitez appliquer la notification.
4.Conservez l'option **Par défaut** dans le menu déroulant **Bloquer**. Cela permet d'hériter l'action par défaut appliquée par ESET Endpoint Antivirus.
5.Définissez les menus déroulants **Notifier** et **Consigner** sur **Oui**.
6.Cliquez sur **OK** pour enregistrer cette notification.

Exemple

Vous souhaitez supprimer les notifications récurrentes pour un type d'alerte que vous ne considérez pas comme une menace :

1.Cliquez sur **Ajouter** pour ajouter une exception IDS.
2.Sélectionnez une alerte spécifique dans le menu déroulant **Alerte**, par exemple **Session SMB sans extensions de sécurité**.
3.Sélectionnez **Entrant** dans le menu déroulant de la direction s'il s'agit d'une communication entrante.
4.Définissez le menu déroulant **Notifier** sur **Non**.
5.Définissez le menu déroulant **Consigner** sur **Oui**.
6.Laissez le champ **Application** vide.
7.Si la communication ne provient pas d'une adresse IP particulière, laissez le champ **Adresses IP distantes** vide.
8.Cliquez sur **OK** pour enregistrer cette notification.

Menace soupçonnée bloquée

Cette situation peut se produire lorsqu'une application sur votre ordinateur tente de transmettre du trafic malveillant à un autre ordinateur du réseau, en exploitant une faille de la sécurité, ou lorsqu'une personne tente d'analyser les ports de votre réseau.

Menace – Nom de la menace.

Source – Adresse réseau source.

Cible – Adresse réseau cible.

Arrêter le blocage – Crée une exception IDS pour la menace soupçonnée avec des paramètres permettant les communications.

Continuer le blocage – Bloque la menace détectée. Pour créer une exception IDS pour cette menace avec des paramètres permettant de bloquer les communications, sélectionnez **Ne plus m'informer**.

Remarque
Les informations affichées dans cette fenêtre de notification peuvent varier selon le type de la menace détectée.
Pour plus d'informations sur les menaces et d'autres termes associés, reportez-vous aux sections Types d'attaques distantes ou Types de détections.

Dépannage de la protection du réseau

L'assistant de dépannage permet de résoudre les problèmes de connectivité liés au pare-feu ESET. Dans le menu déroulant, sélectionnez une période pendant laquelle la communication a été bloquée. La liste des communications bloquées récemment vous donne un aperçu du type d'application ou d'appareil, de la réputation, ainsi que du nombre total d'applications et d'appareils bloqués pendant cette période. Pour plus d'informations sur la communication bloquée, cliquez sur **Détails**. L'étape suivante consiste à débloquer l'application ou l'appareil pour lesquels vous constatez des problèmes de connexion.

Lorsque vous cliquez sur **Débloquer**, la communication précédemment bloquée est autorisée. Si vous continuez à rencontrer des problèmes avec une application ou si votre appareil ne fonctionne pas comme prévu, cliquez sur **L'application ne fonctionne toujours pas** et toutes les communications précédemment bloquées sont autorisées. Si le problème persiste, redémarrez l'ordinateur.

Cliquez sur **Afficher les modifications** pour afficher les règles créées par l'assistant. Par ailleurs, vous pouvez afficher les règles créées par l'assistant en sélectionnant **Configuration avancée** > **Protection du réseau** > **Pare-feu** > **Avancé** > **Règles**.

Cliquez sur **Débloquer un(e) autre pour résoudre les problèmes de communication avec un autre appareil ou une autre application.**

Ajout temporaire d'une adresse IP à la liste noire

Pour afficher les adresses IP qui ont été détectées comme source d'attaques et ajoutées à la liste noire pour bloquer les connexions pendant une certaine période, dans ESET Endpoint Antivirus, accédez à **Configuration** > **Protection du réseau** > **Liste noire temporaire des adresses IP**.

Colonnes

Adresse IP – Indique une adresse IP ayant été bloquée.

Raison du bloquage – Indique le type d'attaque qui a été évité depuis cette adresse (par exemple, attaque par analyse de ports TCP).

Expiration – Indique l'heure et la date d'expiration du maintien de l'adresse sur la liste noire.

Éléments de commande

Supprimer – Cliquez sur cette option pour supprimer une adresse de la liste noire avant son expiration.

Supprimer tout – Cliquez sur cette option pour supprimer immédiatement toutes les adresses de la liste noire.

Ajouter une exception – Cliquez pour ajouter une exception de pare-feu au filtrage IDS.

Résolution des problèmes liés au pare-feu ESET

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

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

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

Assistant de dépannage

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

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

Par défaut, le pare-feu ESET ne consigne pas toutes les connexions bloquées. Si vous voulez examiner les éléments bloqués par le pare-feu, activez la journalisation avancée de la protection du réseau dans la section **Diagnostics** de **Configurations avancées** sous **Outils** > **Diagnostics**. Si vous voyez dans le journal un élément que vous ne voulez pas voir bloqué par le pare-feu, vous pouvez créer une règle ou une exception IDS pour celui-ci en cliquant dessus avec le bouton droit et en sélectionnant **Ne plus bloquer les événements semblables**. Notez que le journal de toutes les connexions bloquées peut contenir des milliers d'éléments. Il peut donc être difficile de trouver une connexion spécifique dans le journal. Vous pouvez désactiver la consignation une fois le problème résolu.

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

Remarque

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

Créer une règle à partir du journal

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

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

- définition de la verbosité minimale des journaux sur **Diagnostic** dans **Configuration avancée** (F5) > **Outils** > **Fichiers journaux**,

- activation de **Afficher également des notifications pour les attaques entrantes contre les trous de sécurité** dans **Configuration avancée** (F5) > **Protection du réseau** > **Protection contre les attaques réseau** > **Options avancées** > **Détection d'intrusion**.

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

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

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

Journalisation PCAP avancée

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

1. Accédez à **Configuration avancée** > **Outils** > **Diagnostics** et activez l'option **Activer la journalisation avancée du filtrage des protocoles**.

2. Essayez de reproduire le problème que vous rencontrez.

3. Désactivez la journalisation PCAP avancée.

4. Le fichier journal PCAP se trouve dans le même répertoire où sont générés les fichiers d'image mémoire de diagnostic :

- Microsoft Windows Vista ou version ultérieure

C:\ProgramData\ESET\ESET Security\Diagnostics

- Microsoft Windows XP

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

Résolution des problèmes liés au filtrage des protocoles

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

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

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

- Si le filtrage du protocole SSL est activé, essayez de le désactiver temporairement. Vous pouvez conserver le filtrage SSL et effectuer la mise à jour en excluant la communication qui pose problème :
  Changez le mode de filtrage du protocole SSL en mode interactif. Réexécutez la mise à jour. Une boîte de dialogue doit s'afficher pour vous fournir des informations sur le trafic réseau chiffré. Vérifiez que l'application correspond à celle que vous dépannez et que le certificat semble provenir du serveur à partir duquel il effectue la mise à jour. Choisissez ensuite de mémoriser l'action pour ce certificat et cliquez sur Ignorer. Si aucune boîte de dialogue ne s'affiche, vous pouvez rechanger le mode de filtrage en mode automatique. Le problème doit être résolu.

- Si l'application concernée ne correspond pas à un navigateur ou un client de messagerie, vous pouvez complètement l'exclure du filtrage des protocoles (procéder ainsi avec un navigateur ou un client de messagerie expose votre ordinateur à des risques). Les applications dont les communications ont déjà été filtrées doivent figurer dans la liste fournie lors de l'ajout de l'exception. Il n'est donc pas nécessaire d'ajouter une application manuellement.

Problème d'accès à un périphérique sur le réseau

Si vous ne parvenez pas à utiliser les fonctionnalités d'un périphérique sur le réseau (ouvrir une page Web de la webcam ou lire une vidéo sur un lecteur multimédia domestique, par exemple), essayez d'ajouter ses adresses Pv4 et IPv6 à la liste des adresses exclues.

Problème lié à un site Web spécifique

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

Erreur « Certaines applications aptes à importer un certificat racine sont

toujours en cours d’utilisation »

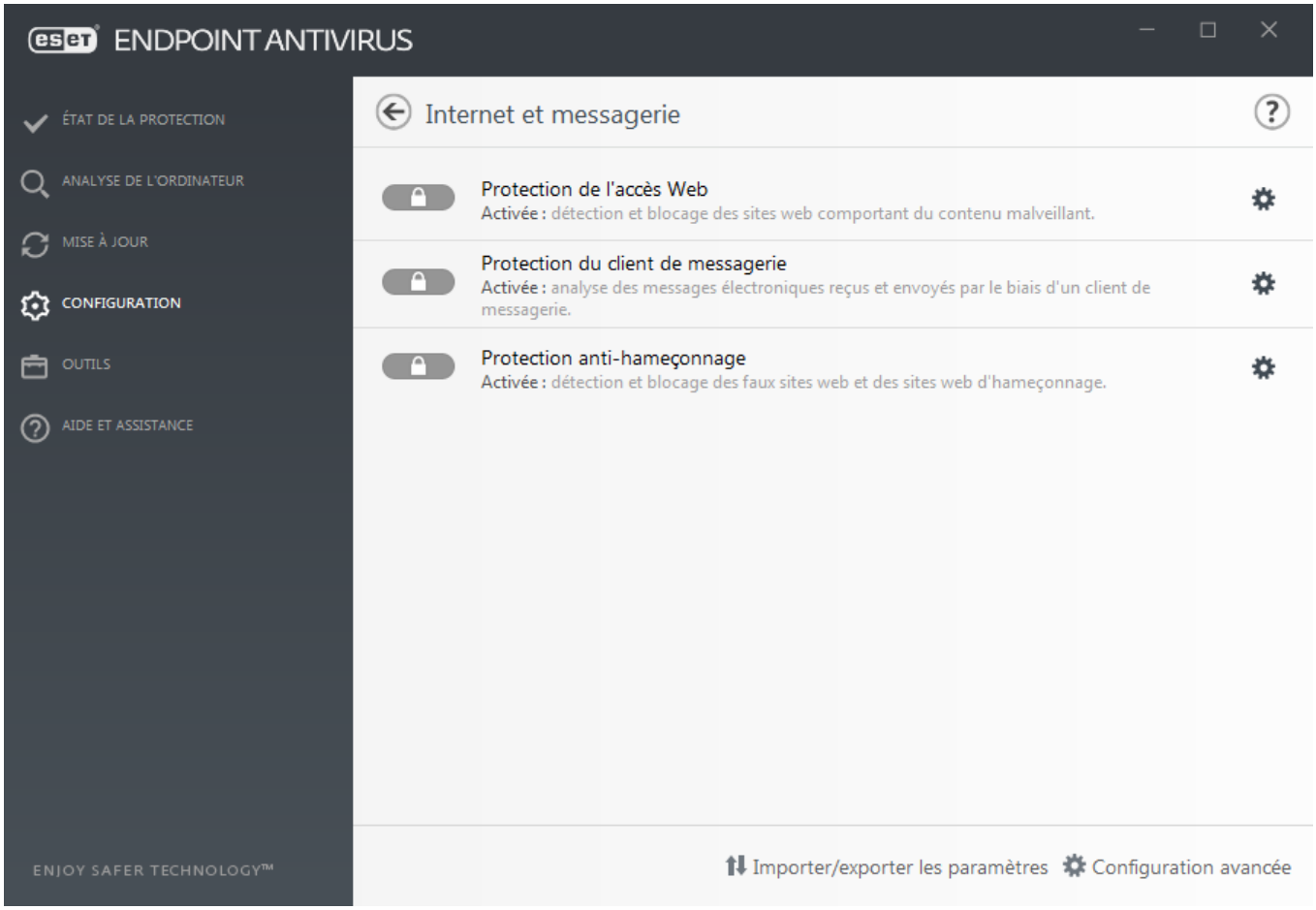
Lorsque vous activez le filtrage du protocole SSL, ESET Endpoint Antivirus vérifie que les applications installées approuvent le filtrage du protocole SSL en important un certificat dans leur magasin de certificats. Cette opération n'est pas possible lorsque certaines applications sont en cours d'exécution.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

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

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

Web et courier électronique

La configuration d'Web et courier électronique est accessible sous **Configuration** > **Web et courier électronique**. Elle permet d’accéder à des paramètres plus détaillés du programme.



La connectivité Internet est une fonctionnalité standard des ordinateurs personnels. Internet est malheureusement devenu le principal mode de transfert des codes malveillants. Il est donc essentiel de prêter une grande attention aux paramètres de **protection de l'accès Web**.

La **protection du client de messagerie** permet de contrôler les communications par courrier électronique reçues

via les protocoles POP3(S) et IMAP(S). ESET Endpoint Antivirus utilise le plugin de votre client de messagerie pour contrôler toutes les communications concernant le client de messagerie.

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

Vous pouvez désactiver temporairement le module de protection Wem/messagerie/antihameçonnage en cliquant sur  .

Filtrage des protocoles

La protection antivirus des protocoles d'application est fournie par le moteur d'analyse ThreatSense qui intègre en toute transparence toutes les techniques avancées d'analyse des logiciels malveillants. Le filtrage des protocoles fonctionne automatiquement, indépendamment du navigateur Internet ou du client de messagerie utilisés. Pour modifier les paramètres chiffrés (SSL), accédez à **Configuration avancée** (F5) > **Internet et messagerie** > **SSL/TLS**.

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

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

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

Exemple d'adresses IP exclues

Adresses IPv4 et masque :

- *192.168.0.10* – Ajoute l'adresse IP d'un ordinateur auquel appliquer la règle.
- *192.168.0.1* à *192.168.0.99* – Saisissez l'adresse IP de début et de fin pour définir la plage IP (de plusieurs ordinateurs) à laquelle la règle doit être appliquée.
- Le sous-réseau (groupe d'ordinateurs) est défini par une adresse IP et un masque. Par exemple, *255.255.255.0* est le masque réseau du préfixe *192.168.1.0/24*, ce qui signifie que la plage d'adresses est comprise entre *192.168.1.1* à 192.168.1.254.

Adresses IPv6 et masque :

- *2001:718:1c01:16:214:22ff:fec9:ca5* – Ajoute l'adresse Ipv6 d'un ordinateur auquel appliquer la règle.
- *2002:c0a8:6301:1::1/64* – Adresse IPv6 avec une longueur de préfixe de 64 octets, c'est-à-dire *2002:c0a8:6301:0001:0000:0000:0000:0000 en 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

Applications exclues

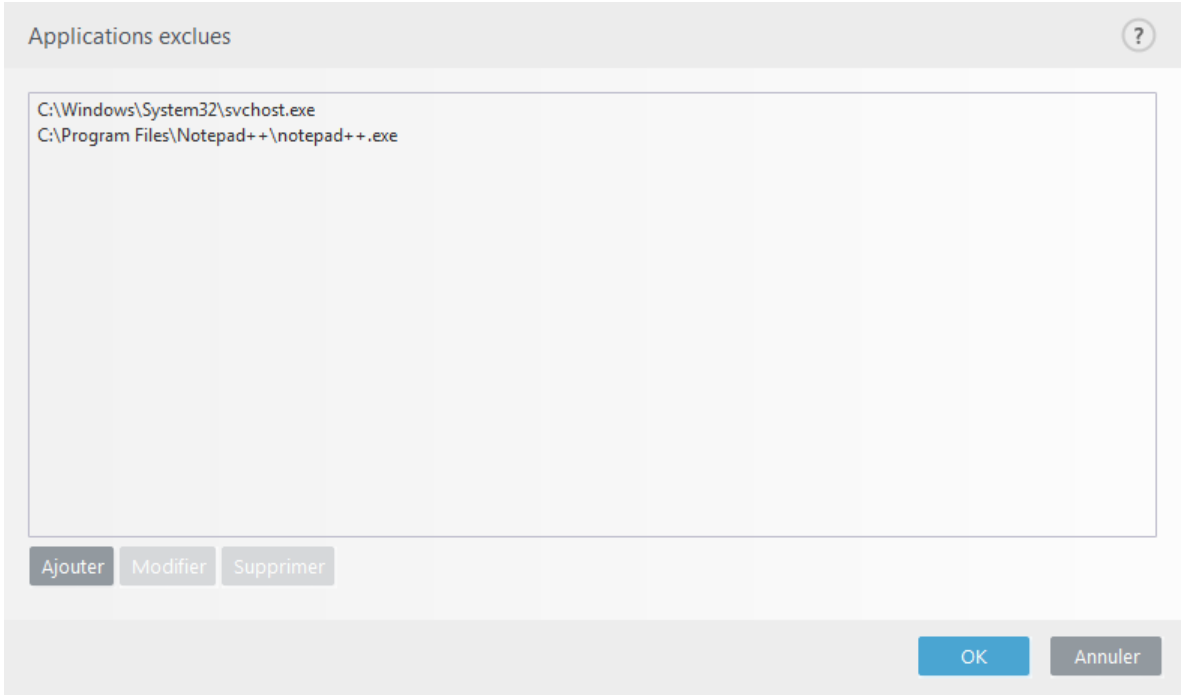
Pour exclure du filtrage des protocoles les communications de certaines applications sensibles au réseau, ajoutez-les à la liste. Les communications HTTP/POP3/IMAP des applications sélectionnées ne font pas l'objet d'une détection des menaces. Il est recommandé d'utiliser uniquement cette technique si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

fonctionnent pas correctement lorsque le filtrage des protocoles est activé.

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

Modifier – Modifie les entrées sélectionnées de la liste.

Supprimer – Supprime les entrées sélectionnées de la liste.



Adresses IP exclues

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

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

Modifier – Modifie les entrées sélectionnées de la liste.

Supprimer – Supprime les entrées sélectionnées de la liste.

SSL/TLS

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

Activer le filtrage du protocole SSL/TSL : le filtrage des protocoles est activé par défaut. Vous pouvez désactiver le filtrage du protocole SSL/TSS dans **Configurations avancées** > **Internet et messagerie** > **SSL/TLS** ou via une politique. Si le filtrage des protocoles est désactivé, le programme n'analyse pas les communications sur le protocole SSL.

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

Mode de filtrage	Description
Mode automatique	Ce mode par défaut n'analyse que les applications appropriées telles que les navigateurs Web et les clients de messagerie. Vous pouvez l'ignorer en sélectionnant les applications dont les communications seront analysées.
Mode interactif	Si vous entrez un nouveau site protégé par SSL (avec un certificat inconnu), une boîte de dialogue de sélection d'action s'affiche. Ce mode vous permet de créer la liste des certificats SSL/applications qui seront exclus de l'analyse.
Mode de stratégie	Mode de stratégie : 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.

La **liste des applications filtrées par le protocole SSL** peut être utilisée afin de personnaliser le comportement d'ESET Endpoint Antivirus pour des applications spécifiques.

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

Exclure la communication avec les domaines approuvés : lorsque cette option est activée, la communication avec les domaines approuvés est exclue de la vérification. L'approbation des domaines est déterminée par la liste blanche intégrée.

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

> **Remarque**
> Les adresses ne sont pas filtrées si le paramètre **Exclure la communication avec les domaines approuvés** est activé et que le domaine est considéré comme fiable.

Certificat racine

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

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

Validité du certificat

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

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

> **Exemples illustrés**
> Les articles suivants de la base de connaissances ESET peuvent être disponibles uniquement en anglais :
> - Notifications de certificat dans les produits ESET
> - Le message « Trafic réseau chiffré : certificat non approuvé » s'affiche lors de la consultation de pages web

Certificats

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

Dans certains cas, il est impossible de vérifier le certificat à l'aide du magasin d'Autorités de certification racine de confiance (VeriSign par exemple). Cela signifie que le certificat est signé automatiquement par un utilisateur (l'administrateur d'un server Web ou une petite entreprise) et que le fait de le considérer comme fiable n'est pas toujours un risque. La plupart des grandes entreprises (les banques par exemple) utilisent un certificat signé par TRCA. Si **Interroger sur la validité du certificat** est activé (sélectionné par défaut), l'utilisateur est invité à sélectionner une action à entreprendre lorsque la communication chiffrée est établie. Une boîte de dialogue de sélection d'action apparaît ; vous pouvez décider de 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 vérifié.

Si le certificat n'est pas valide ou est endommagé, cela signifie qu'il est arrivé à expiration ou que sa signature automatique est incorrecte. Dans ce cas, il est recommandé de bloquer la communication qui utilise le certificat.

Trafic réseau chiffré

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

Lorsqu'un site Web utilise un certificat non valide ou ne pouvant pas être vérifié et qu'ESET Endpoint 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 de filtrage du protocole SSL** est définie sur **Mode interactif**, une boîte de dialogue demande pour chaque site Web d'**analyser** ou d'**ignorer** le trafic. Certaines applications vérifient que le trafic SSL n'est ni modifié ni inspecté par quelqu'un. Dans ce cas, ESET Endpoint 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 ESET
- Le message « 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 la liste des certificats connus.

Liste des certificats connus

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

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

Colonnes

Nom : nom du certificat.

Émetteur du certificat : nom du créateur du certificat.

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

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

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

Éléments de commande

Ajouter : il est possible de charger manuellement un certificat en tant que fichier doté de l'extension *.cer*, *.crt* ou *.pem*. Pour charger un certificat local, cliquez sur **Fichier**. Pour indiquer l'emplacement d'un certificat en ligne, cliquez sur **URL**.

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**.

Liste des applications filtrées par le protocole SSL/TLS

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

La fenêtre **Liste des applications filtrées SSL/TLS** contient les éléments suivants :

Colonnes

Application – Nom de l'application.

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.

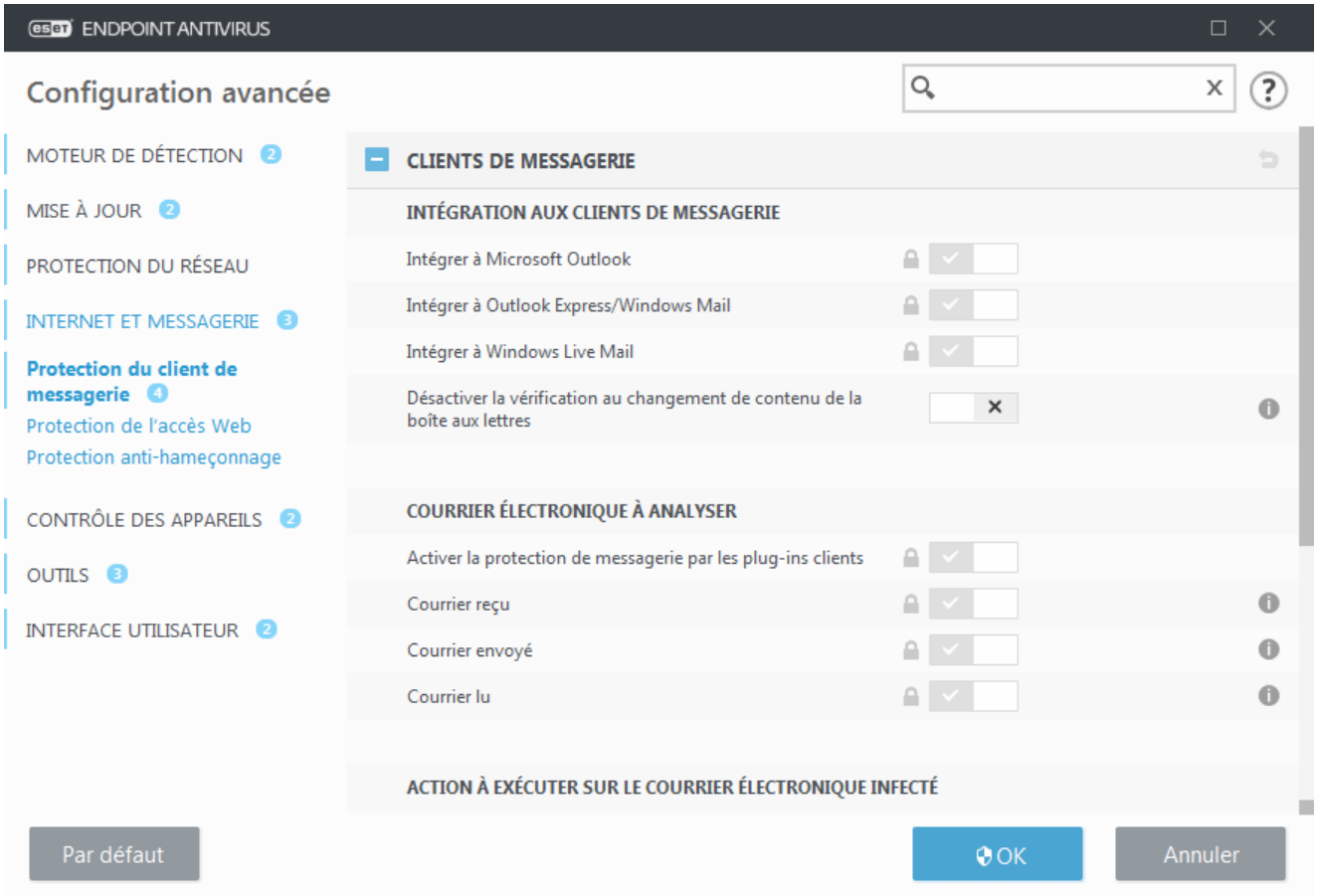
Modifier – Sélectionnez le certificat à configurer, puis cliquez sur **Modifier**.

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.

Protection du client de messagerie

L'intégration d'ESET Endpoint Antivirus à votre client de messagerie augmente le niveau de protection active contre les codes malveillants dans les messages électroniques. Si votre client de messagerie est pris en charge, l'intégration peut être activée dans ESET Endpoint Antivirus. Une fois le produit intégré à votre client de messagerie, la barre d'outils d'ESET Endpoint Antivirus est insérée directement dans le client de messagerie, ce qui permet une protection plus efficace des messages. Les paramètres d'intégration sont situés dans **Configuration avancée** (F5) > **Internet et messagerie** > **Protection du client de messagerie** > **Clients de messagerie**.



Intégration aux clients de messagerie

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

Activez l'option **Désactiver la vérification au changement de contenu de la boîte aux lettres** si vous constatez un ralentissement du système lors de la récupération des e-mails.

Courrier électronique à analyser

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.

E-mail reçu – Lorsque cette option est activée, elle vérifie les messages reçus.

E-mail envoyé – Lorsque cette option est activée, elle vérifie les messages envoyés.

E-mail lu – Lorsque cette option est activée, elle vérifie les messages lus.

> **Remarque**
> 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 le filtrage des protocoles (IMAP/IMAPS et POP3/POP3S).

Action à exécuter sur le courrier électronique infecté

Aucune action – Si cette option est activée, le programme identifie les pièces jointes infectées, mais n'entreprend aucune action sur les messages concernés.

Supprimer les courriers – Le programme avertit l'utilisateur à propos d'une infiltration et supprime le message.

Déplacer les courriers vers le dossier Éléments supprimés – Les courriers infectés sont automatiquement placés dans le dossier Éléments supprimés.

Déplacer les courriers vers le dossier (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.

Répéter l'analyse après mise à jour – Lorsque cette option est activée, elle effectue une nouvelle analyse des messages infectés après la mise à jour du moteur de détection.

Accepter les résultats d'analyse d'autres modules – Permet au module de protection de messages d'utiliser les résultats d'analyse reçus d'autres modules de protection au lieu d'effectuer une nouvelle analyse.

Protocoles de messagerie

Les protocoles IMAP et POP3 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.

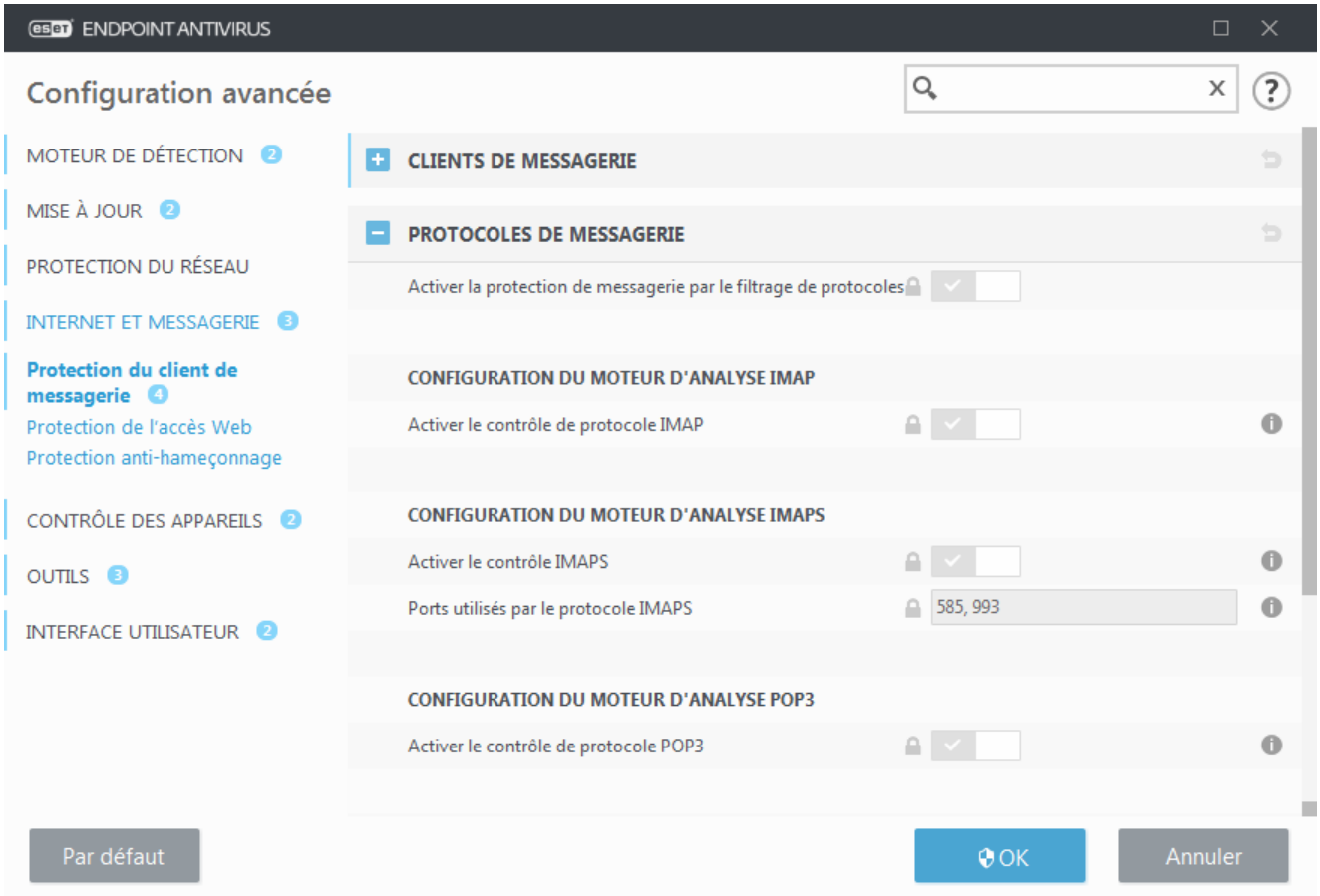
ESET Endpoint Antivirus protège ces protocoles, quel que soit le client de messagerie utilisé, sans avoir à reconfigurer le client de messagerie. Par défaut, toutes les communications via les protocoles POP3 et IMAP sont analysées, quels que soient les numéros de port POP3/IMAP par défaut.
Le protocole 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.

Il est recommandé de conserver l'option **Activer la protection de la messagerie par filtrage des protocoles** activée**.** Pour configurer le contrôle des protocoles IMAP/IMAPS et POP3/POP3S, accédez à Configurations avancées > **Internet et messagerie** > **Protection du client de messagerie** > **Protocoles de messagerie**.

ESET Endpoint 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 Endpoint Antivirus contrôle la communication à l'aide des protocoles SSL (Secure Socket Layer) et TLS (Transport Layer Security). Le programme analyse uniquement le trafic sur les ports définis dans **Ports utilisés par le protocole IMAPS/POP3S**, quelle que soit la version du système d'exploitation. D'autres ports de communication peuvent être ajoutés au besoin. Les différents numéros de ports doivent être séparés par une virgule.

La communication chiffrée est analysée par défaut. Pour afficher la configuration de l'analyseur, accédez à l'option SSL/TLS dans la section Configuration avancée, cliquez sur **Internet et messagerie** > **SSL/TLS** et activez

l'option **Activer le filtrage du protocole SSL/TLS**.



Notifications et alertes sur les e-mails

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

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 n'est 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 envoyé – Désactivez cette option si vous ne souhaitez pas que la protection de la messagerie ajoute un avertissement de virus dans l'objet d'un message infecté. Cette fonctionnalité permet tout simplement de filtrer les courriers infectés en fonction de leur objet (si elle est prise en charge par le programme de messagerie). Elle augmente également la crédibilité du destinataire et, en cas de détection d'une infiltration, fournit des informations précieuses sur le niveau de menace d'un message ou d'un expéditeur.

Texte ajouté à l'objet des messages 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.

Intégration aux clients de messagerie

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

Barre d'outils Microsoft Outlook

La protection Microsoft Outlook fonctionne comme un module plugin. Après l'installation de ESET Endpoint Antivirus, cette barre d'outils contenant les options de protection antivirus est ajoutée à Microsoft Outlook :

ESET Endpoint Antivirus – Cliquez sur l'icône pour ouvrir la fenêtre principale du programme ESET Endpoint 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 la section Protection du client de messagerie.

Configuration du moteur d'analyse – Affiche les options de configuration de la Protection du client de messagerie.

Barre d'outils Outlook Express et Windows Mail

La protection pour Outlook Express et Windows Mail fonctionne comme un module plugin. Après l'installation de ESET Endpoint Antivirus, cette barre d'outils contenant les options de protection antivirus est ajoutée à Outlook Express ou à Windows Mail :

ESET Endpoint Antivirus – Cliquez sur l'icône pour ouvrir la fenêtre principale du programme ESET Endpoint 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 la section Protection du client de messagerie.

Configuration du moteur d'analyse – Affiche les options de configuration de la Protection du client de messagerie.

Interface utilisateur

Personnaliser l'apparence – Vous pouvez modifier l'apparence de la barre d'outils pour votre client de messagerie. Désactivez cette option pour personnaliser l'apparence indépendamment des paramètres du programme de messagerie.

Afficher le texte – Affiche des descriptions des icônes.

Texte à droite – Les descriptions d'options sont déplacées du bas vers le côté droit des icônes.

Grandes icônes – Affiche des icônes de grande taille pour les options de menu.

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 Endpoint 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.

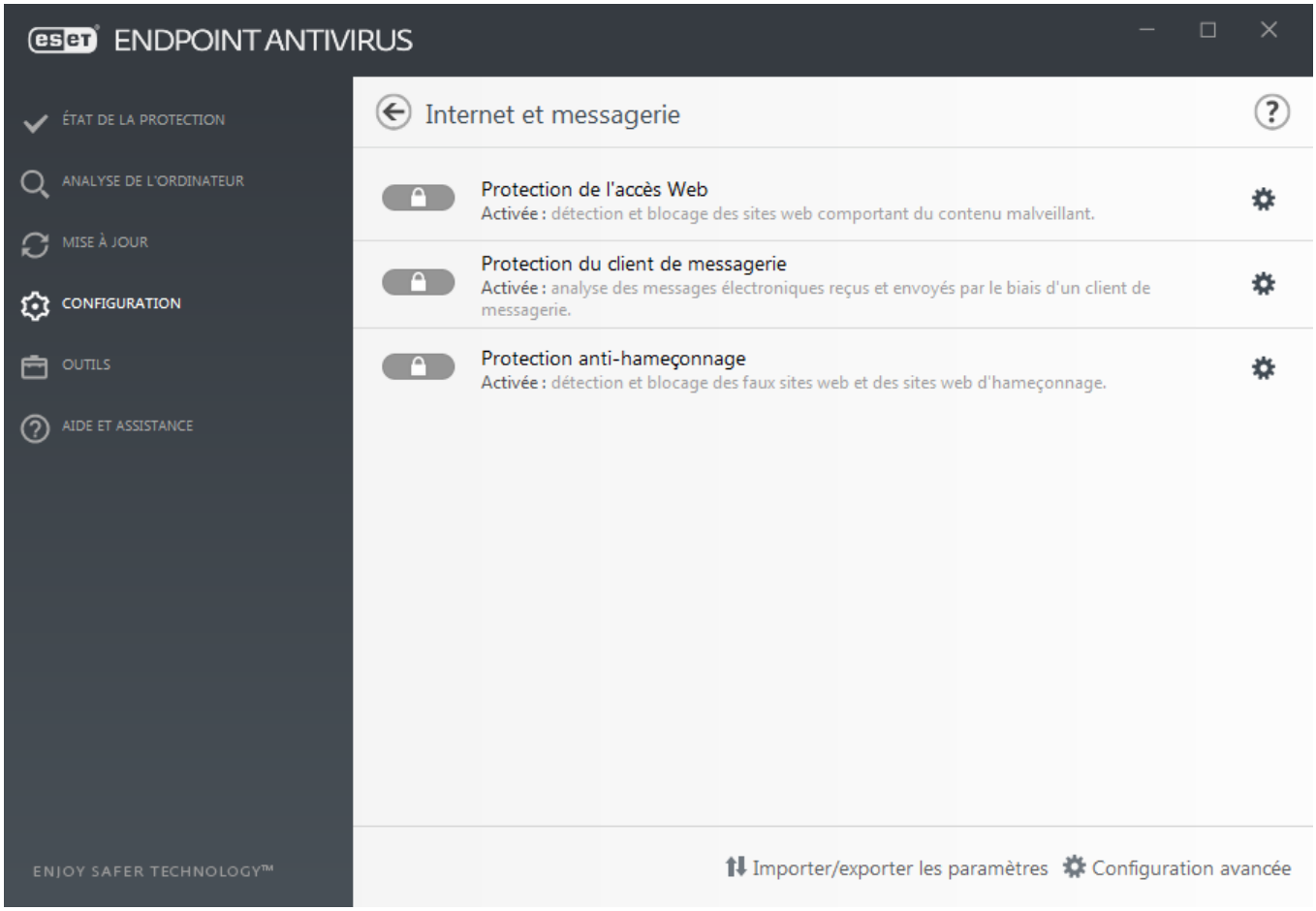
La case à cocher **Réanalyser les messages déjà analysés** permet d'exécuter une autre analyse sur des messages déjà analysés.

Protection de l'accès Web

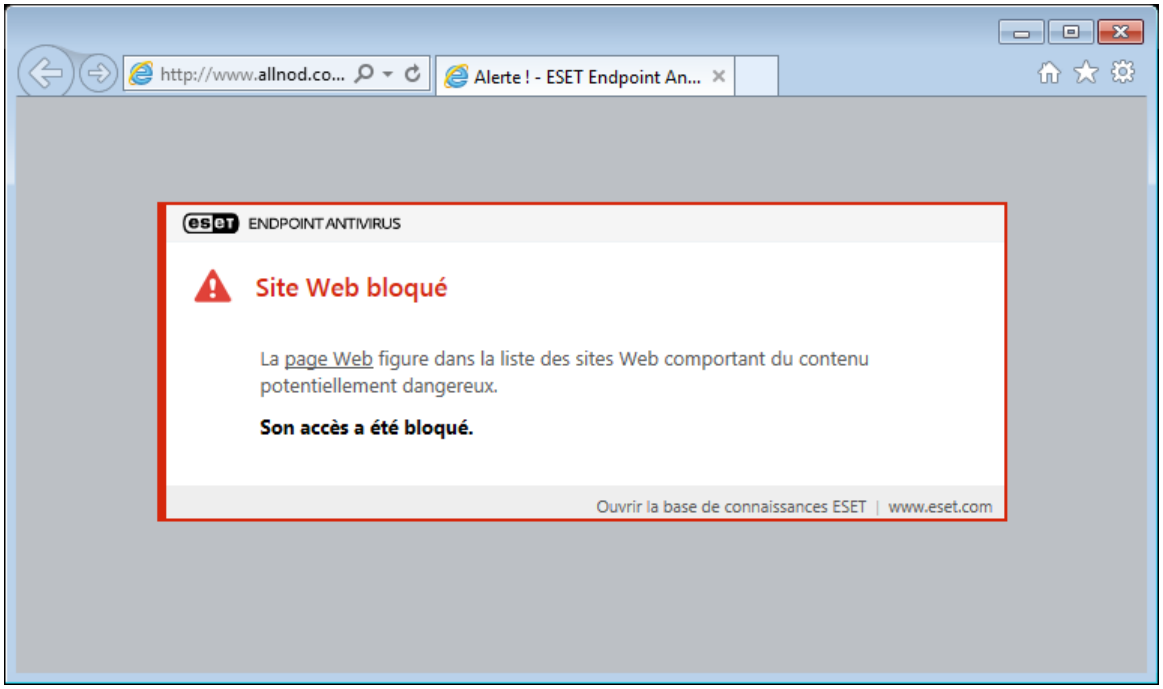
La connectivité Internet est une fonctionnalité standard des ordinateurs personnels. Elle est malheureusement devenue le principal mode de transfert des codes malveillants. La protection de l'accès au Web opère par surveillance des communications entre les navigateurs Internet et les serveurs distants,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

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

Nous vous recommandons vivement d'activer l'option de protection de l'accès au Web. Cette option est accessible à partir de la fenêtre principale de ESET Endpoint Antivirus en accédant à **Configuration** > **Protection Internet** > **Protection de l'accès Web**.



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 :

- Débloquer un site web fiable sur un poste de travail dans ESET Endpoint Antivirus
- Débloquer un site web fiable sur un endpoint à l'aide d'ESET Security Management Center

---

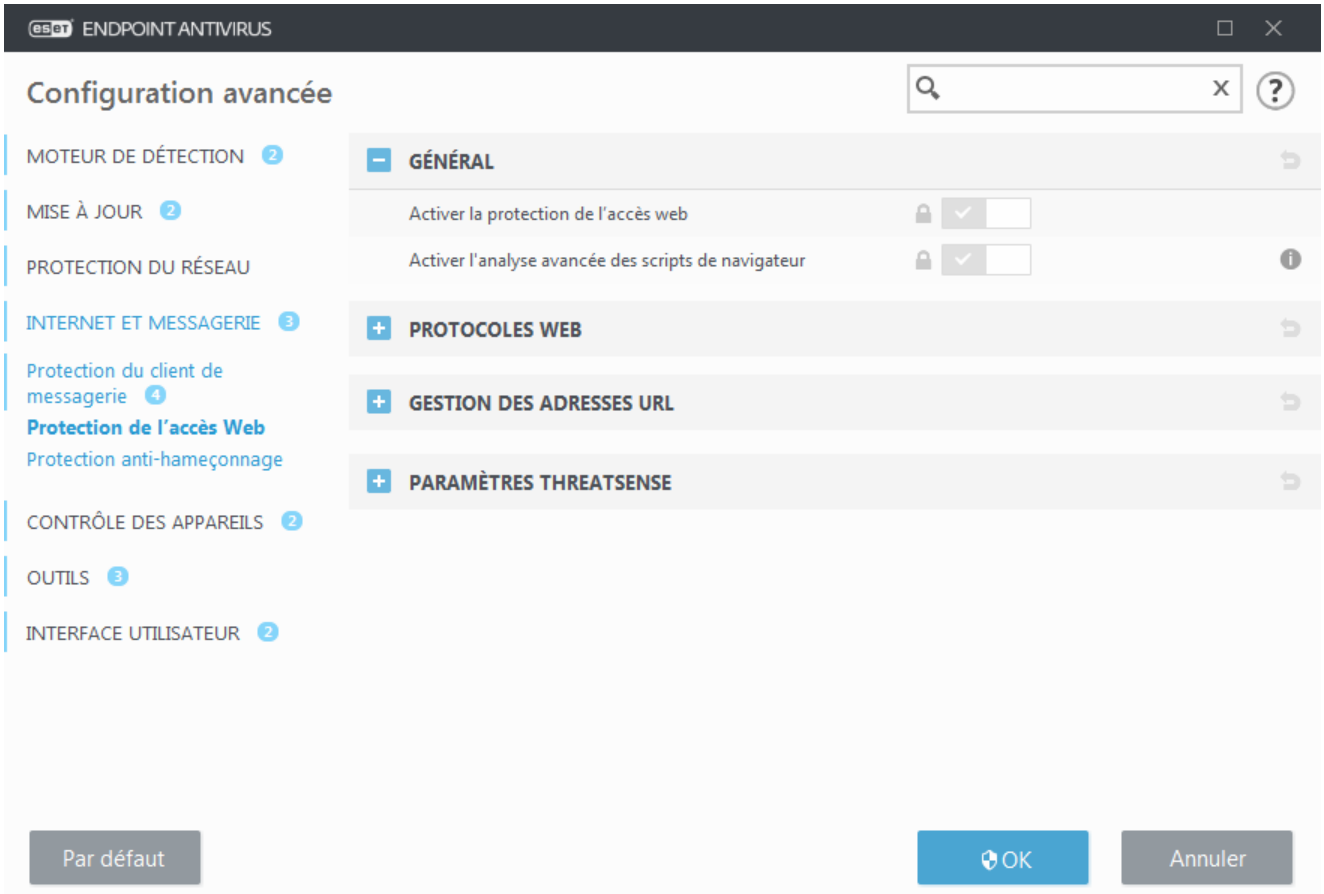
Les options suivantes sont disponibles dans **Configuration avancée** (F5) > **Web et courier électronique** > **Protection de l'accès Web** :

- **Général** – Permet d'activer ou de désactiver cette fonctionnalité depuis les Configurations avancées.

- **Protocoles Web** : permet de configurer le contrôle de ces protocoles standard qui sont utilisés par la plupart des navigateurs Internet.

- **Gestion des adresses URL** : permet de spécifier des listes d'adresses URL qui seront bloquées, autorisées ou exclues de la vérification.

- **Paramètres ThreatSense** : la configuration avancée de l'analyseur de virus permet de configurer des paramètres tels que les types d'objet à analyser (courriers électroniques, archives, etc.), les méthodes de détection pour la protection de l'accès Web, etc.



Configuration avancée de la protection de l'accès web

Les options suivantes sont disponibles dans **Configurations avancées** (F5) > **Internet et messagerie** > **Protection de l'accès web**> **Général** :

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.

Activer l'analyse avancée des scripts de navigateur – Lorsque cette option est activée, tous les programmes JavaScript exécutés par les navigateurs web sont vérifiés par le moteur de détection.

> **Remarque**
> Il est vivement recommandé de conserver l'option de protection de l'accès Web activée.

Protocoles Web

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

Configuration du scanner HTTP

Le trafic HTTP est toujours contrôlé sur tous les ports pour toutes les applications.

Configuration du scanner HTTPS

ESET Endpoint Antivirus prend également en charge le contrôle de protocole HTTPS. Les communications HTTPS utilisent un canal chiffré pour transférer des informations entre un serveur et un client. ESET Endpoint 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 (443, 0-65535) définis dans **Ports utilisés par le protocole HTTPS**, quelle que soit la version du système d'exploitation.

La communication chiffrée est analysée par défaut. Pour afficher la configuration de l'analyseur, accédez à l'option SSL/TLS dans la section Configuration avancée, cliquez sur **Internet et messagerie** > **SSL/TLS** et activez l'option **Activer le filtrage du protocole SSL/TLS**.

Gestion d'adresse URL

La section Gestion des adresses URL permet de spécifier des listes d'adresses HTTP qui seront bloquées, autorisées ou exclues de l'analyse du contenu.

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

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.

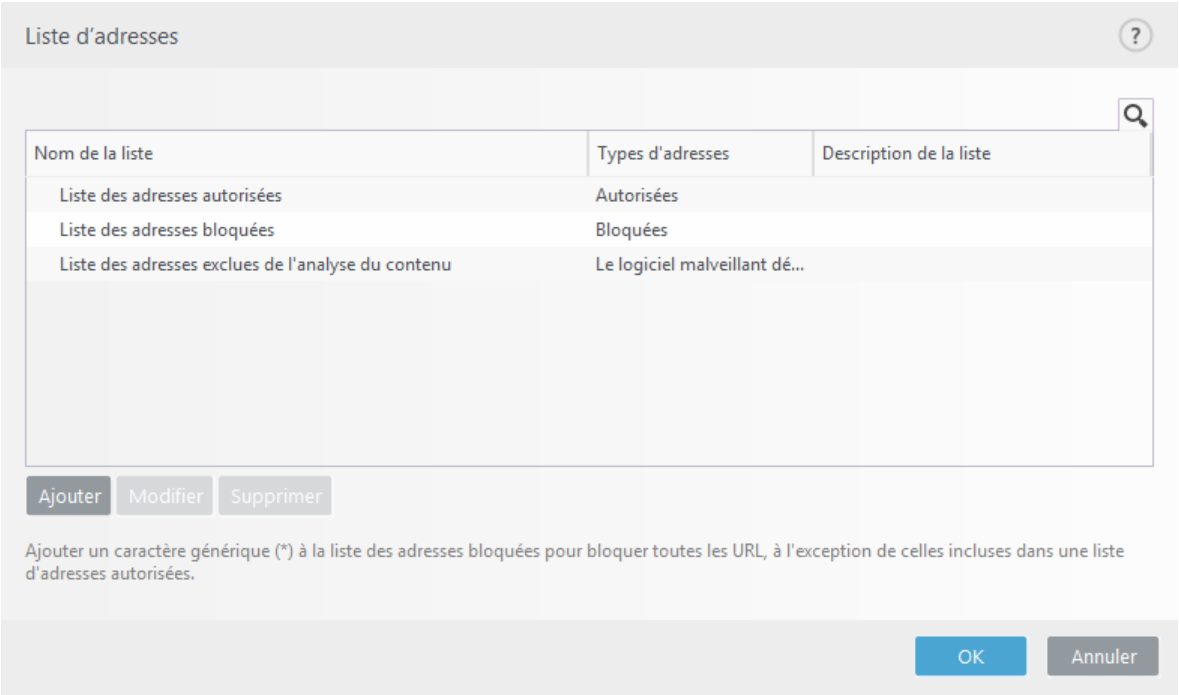
Vous ne pouvez pas utiliser le symbole « * » (astérisque) et le caractère « ? » (point d'interrogation) dans les listes. L'astérisque remplace n'importe quelle chaîne de caractères, tandis que le point d'interrogation remplace n'importe quel caractère. Soyez particulièrement prudent dans la définition 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**.

Bloquer ou autoriser des extensions de fichier spécifiques

la gestion des adresses URL vous permet également de bloquer ou d'autoriser l'ouverture de types de fichiers spécifiques pendant la navigation sur Internet. Par exemple, si vous souhaitez que les fichiers exécutables ne soit pas ouverts, sélectionnez dans le menu déroulant la liste dans laquelle vous souhaitez bloquer ces fichiers, puis saisissez le masque « "**.exe" ».

Domaines approuvés

Les adresses ne sont pas filtrées si le paramètre **Internet et messagerie** > **SSL/TLS** > **Exclure la communication avec les domaines approuvés** est activé et que le domaine est considéré comme fiable.



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.

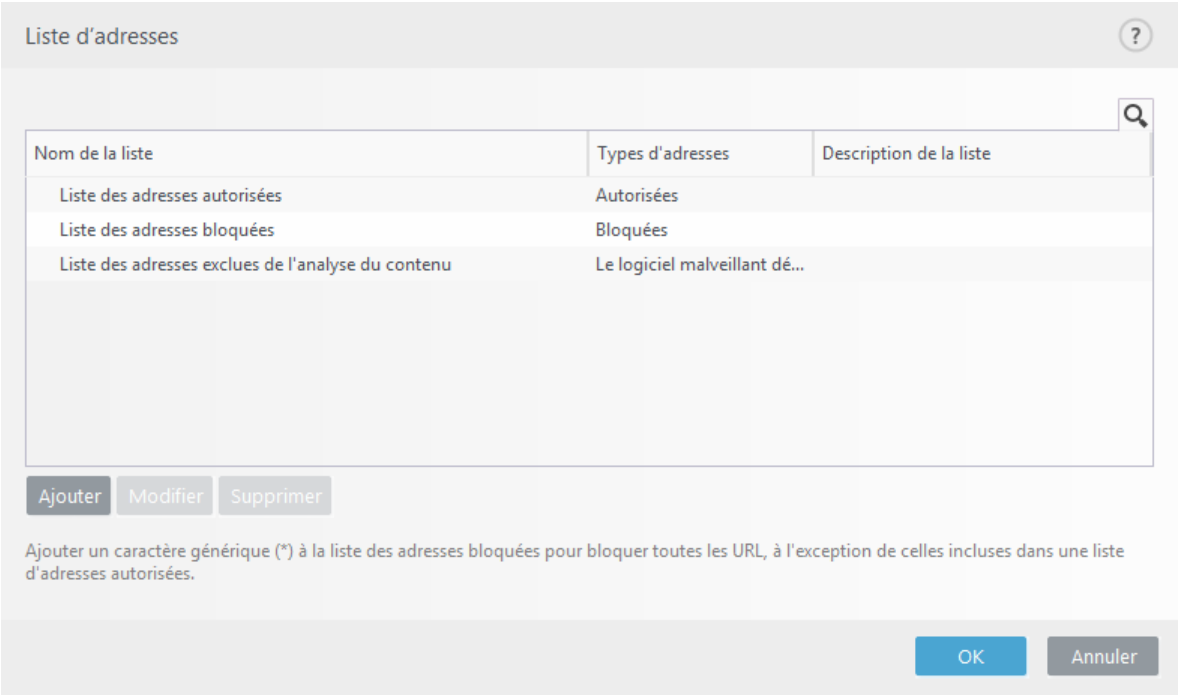
Liste des adresses URL

Dans cette section, vous pouvez spécifier des listes d'adresses HTTP 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 :

- Débloquer un site web fiable sur un poste de travail dans ESET Endpoint Antivirus
- Débloquer un site web fiable sur un endpoint à l'aide d'ESET Security Management Center

Pour plus d'informations, reportez-vous à Gestion des adresses URL.

Création d'une liste d'adresses URL

Cette section permet de spécifier des listes d'adresses URL/masques qui seront bloqués, autorisés ou exclus de la vérification.

Lors de la création d'une liste, vous pouvez configurer les options suivantes :

Type de liste d'adresses – Trois types de liste sont disponibles :

- **Exclues de la vérification** – Aucune vérification de la présence de code malveillant n'est effectuée pour les adresses répertoriées dans la liste.
- **Bloquées** - L'utilisateur n'est pas autorisé à accéder aux adresses répertoriées dans cette liste.
- **Autorisées** – Si votre stratégie est configurée pour utiliser cette fonctionnalité et que la valeur du caractère générique (*) est ajoutée à la liste, vous êtes autorisé à accéder aux adresses de la liste même si celles-ci figurent également dans la liste des adresses bloquées.

Nom de liste – Spécifiez le nom de la liste. Ce champ n'est pas disponible lorsque vous modifiez l'une des trois listes prédéfinies.

Description de la liste – Tapez une brève description de la liste (facultatif). Ce champ n'est pas disponible lorsque vous modifiez l'une des trois listes prédéfinies.

Liste active – Sélectionnez la barre du curseur pour activer la liste.

Notifier lors de l'application – Sélectionnez la barre du curseur si vous souhaitez être averti lorsque cette liste est utilisée pour l'évaluation d'un site HTTP visité. Par exemple, une notification est émise lorsqu'un site Web est bloqué ou autorisé en raison de son inclusion dans la liste des adresses bloquées ou autorisées. La notification indique le nom de la liste qui spécifie le site Web.

Niveau de verbosité – Sélectionnez le niveau de verbosité dans le menu déroulant. Les entrées avec la verbosité Avertissement peuvent être collectées par Remote Administrator.

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. Il est possible uniquement de supprimer les adresses créées à l'aide de l'option **Ajouter**.

Supprimer – Permet de supprimer des adresses existantes de la liste. Il est possible uniquement de supprimer les adresses créées à l'aide de 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 Endpoint 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*.

Protection antihameçonnage

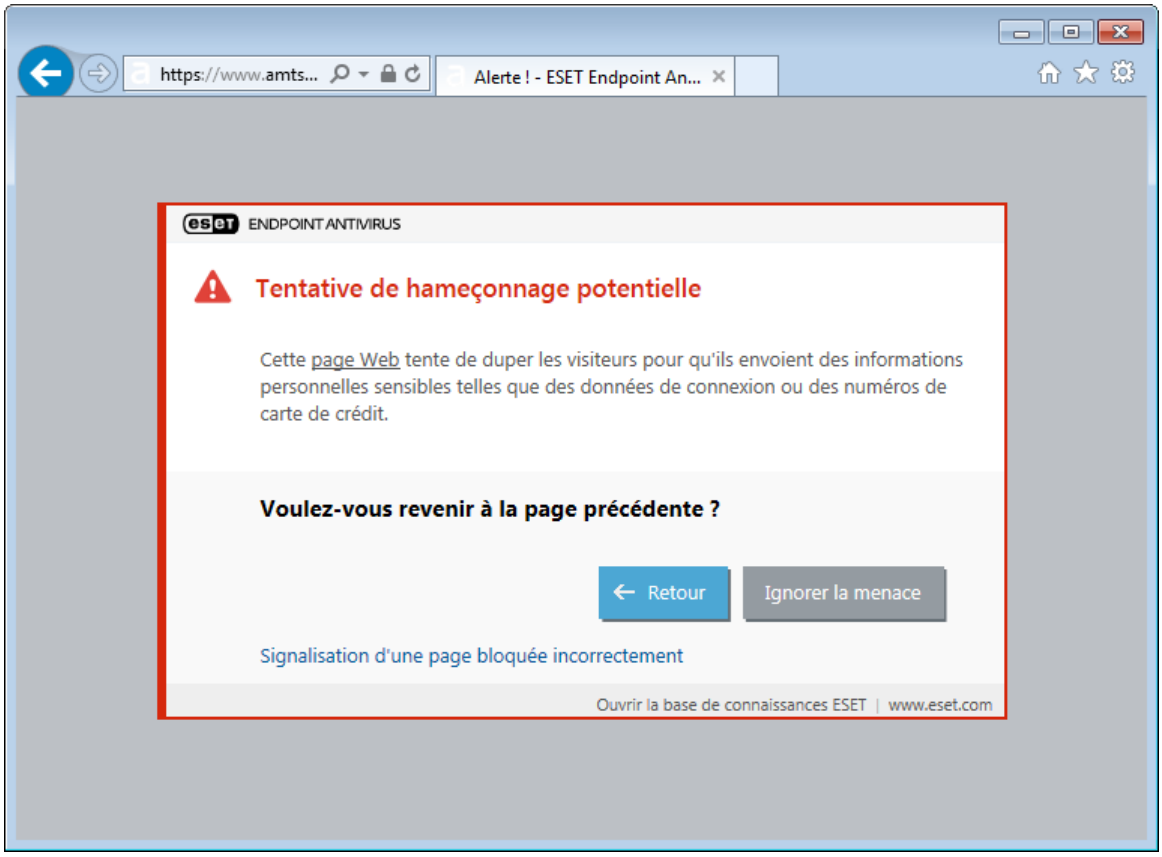
Le terme d'hameçonnage (phishing en anglais) désigne une activité frauduleuse utilisant des techniques de piratage psychologique qui consistent à manipuler les utilisateurs pour obtenir des informations confidentielles. L'hameçonnage est souvent utilisé pour accéder à des données sensibles, telles que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

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

Pour plus d'informations sur la protection antihameçonnage d'ESET Endpoint 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, la boîte de dialogue suivante s'affiche dans votre navigateur Web. Si vous souhaitez toujours accéder au site Web, cliquez sur **Accéder au site** (non recommandé).



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

Signalement d'un site de hameçonnage

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

Remarque
Avant de soumettre un site Web à ESET, assurez-vous qu'il répond à au moins l'un des critères suivants :
- le site Web n'est pas du tout détecté,
- le site Web est, à tort, détecté comme une menace. Dans ce cas, vous pouvez Signaler un site faux positif de hameçonnage.

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

Mise à jour du programme

La mise à jour régulière d'ESET Endpoint Antivirus est la meilleure méthode pour bénéficier du niveau maximum de sécurité sur votre ordinateur. Le module de mise à jour veille à ce que le programme soit toujours à jour de

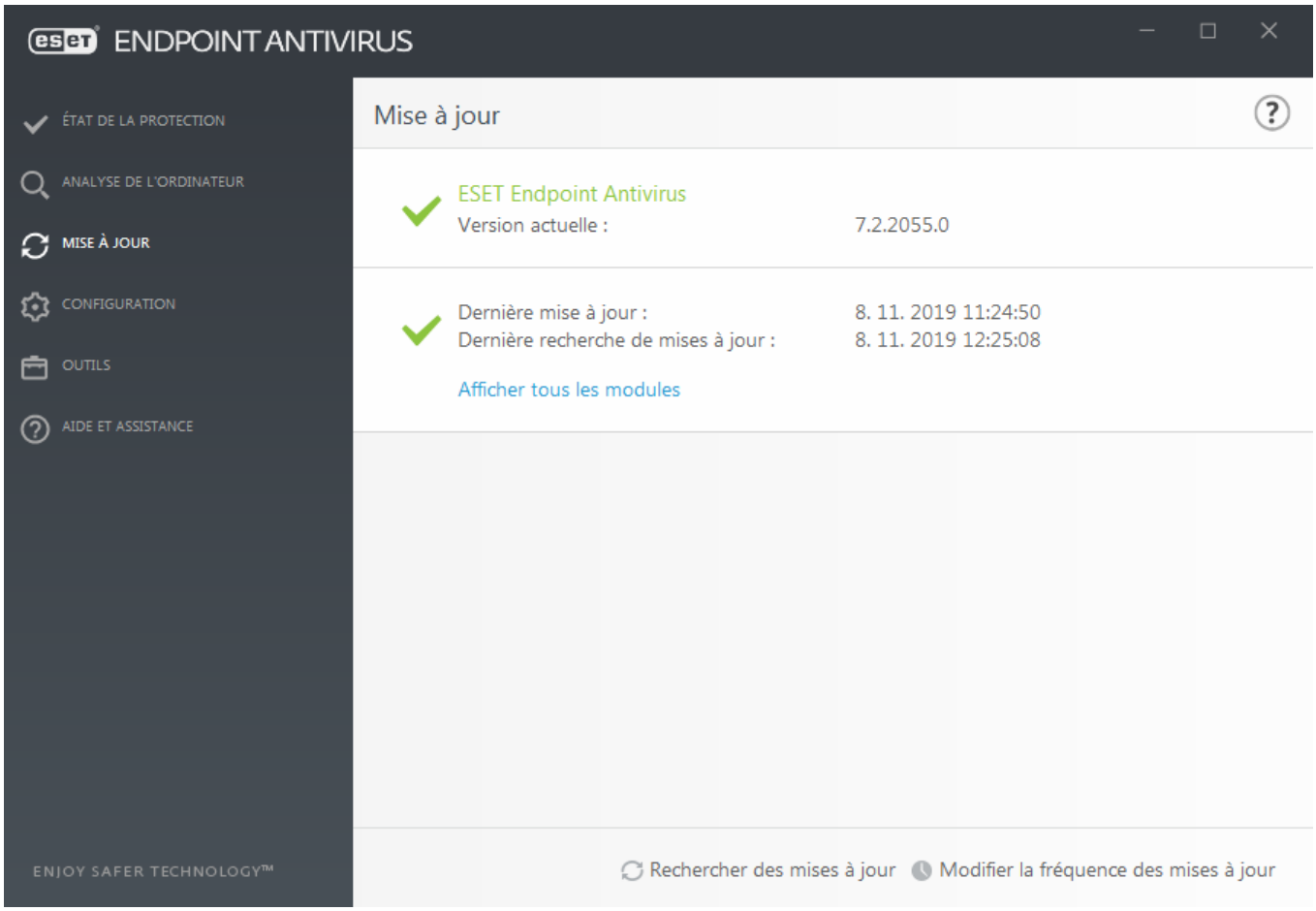
deux façons : en mettant à jour le moteur de détection et en mettant à jour les composants système. Lorsque le programme est activé, les mises à jour sont automatiques par défaut.

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. Vous pouvez aussi cliquer sur le lien **Afficher tous les modules** pour ouvrir la liste des modules installées et vérifier la version et la dernière mise à jour d'un module.

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

Si vous activez ESET Endpoint Antivirus à l'aide d'une licence hors ligne et sans nom d'utilisateur ni mot de passe et si vous essayez d'effectuer une mise à jour, le message **Échec de la mise à jour des modules** indique que vous pouvez télécharger les mises à jour à partir du miroir uniquement.

> **Remarque**
> la clé de licence est fournie par ESET après l'achat d'ESET Endpoint Antivirus.



Version actuelle : numéro de version de ESET Endpoint Antivirus.

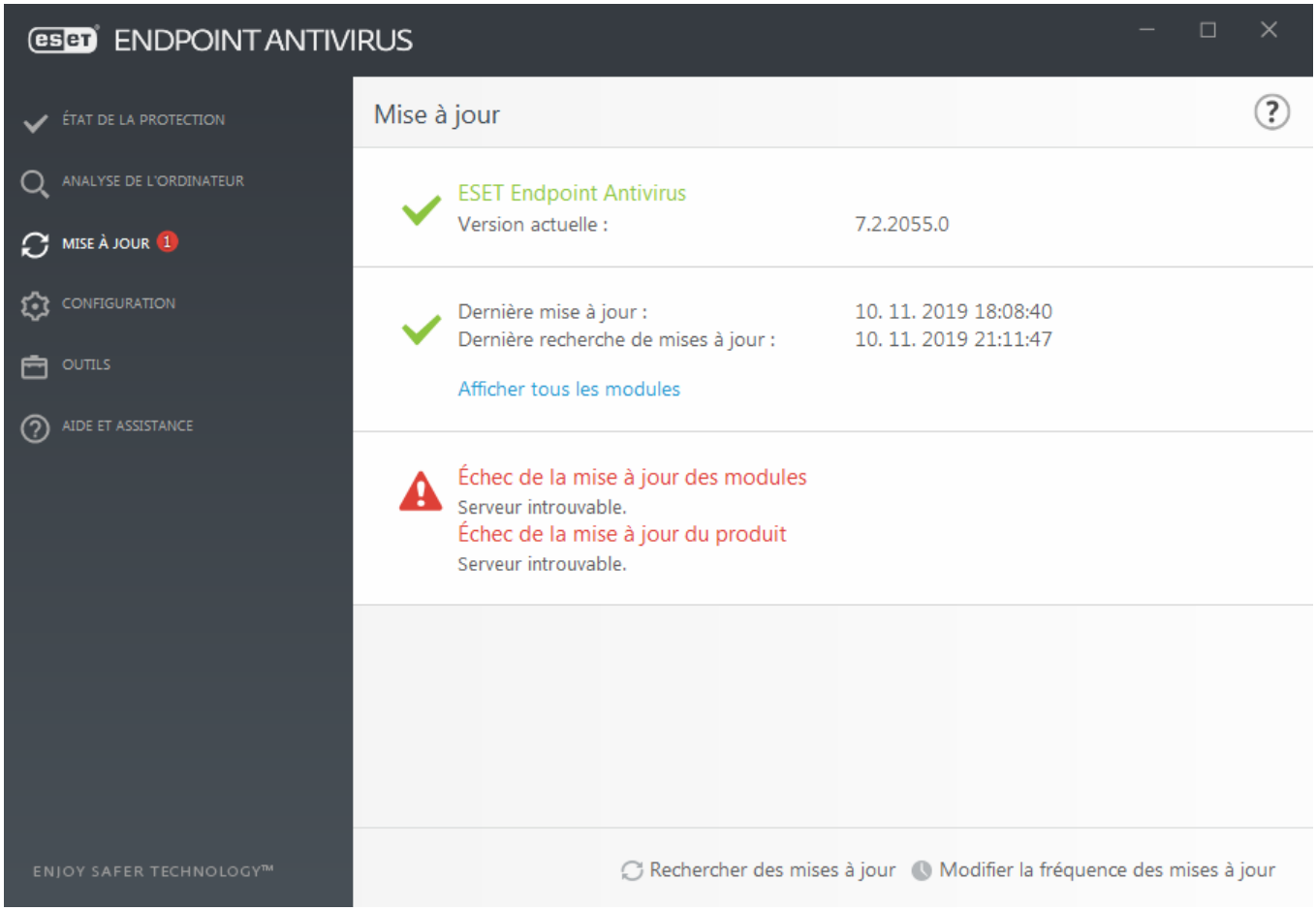
Dernière mise à jour réussie – Date et heure de la dernière mise à jour réussie. Vérifiez qu'il s'agit d'une date récente indiquant que le moteur de détection est à jour.

Dernière recherche de mises à jour – Date et heure de la dernière tentative réussie de mise à jour des modules.

Afficher tous les modules – Cliquez sur ce lien pour ouvrir la liste des modules installés et vérifier la version et la dernière mise à jour d'un module.

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**.



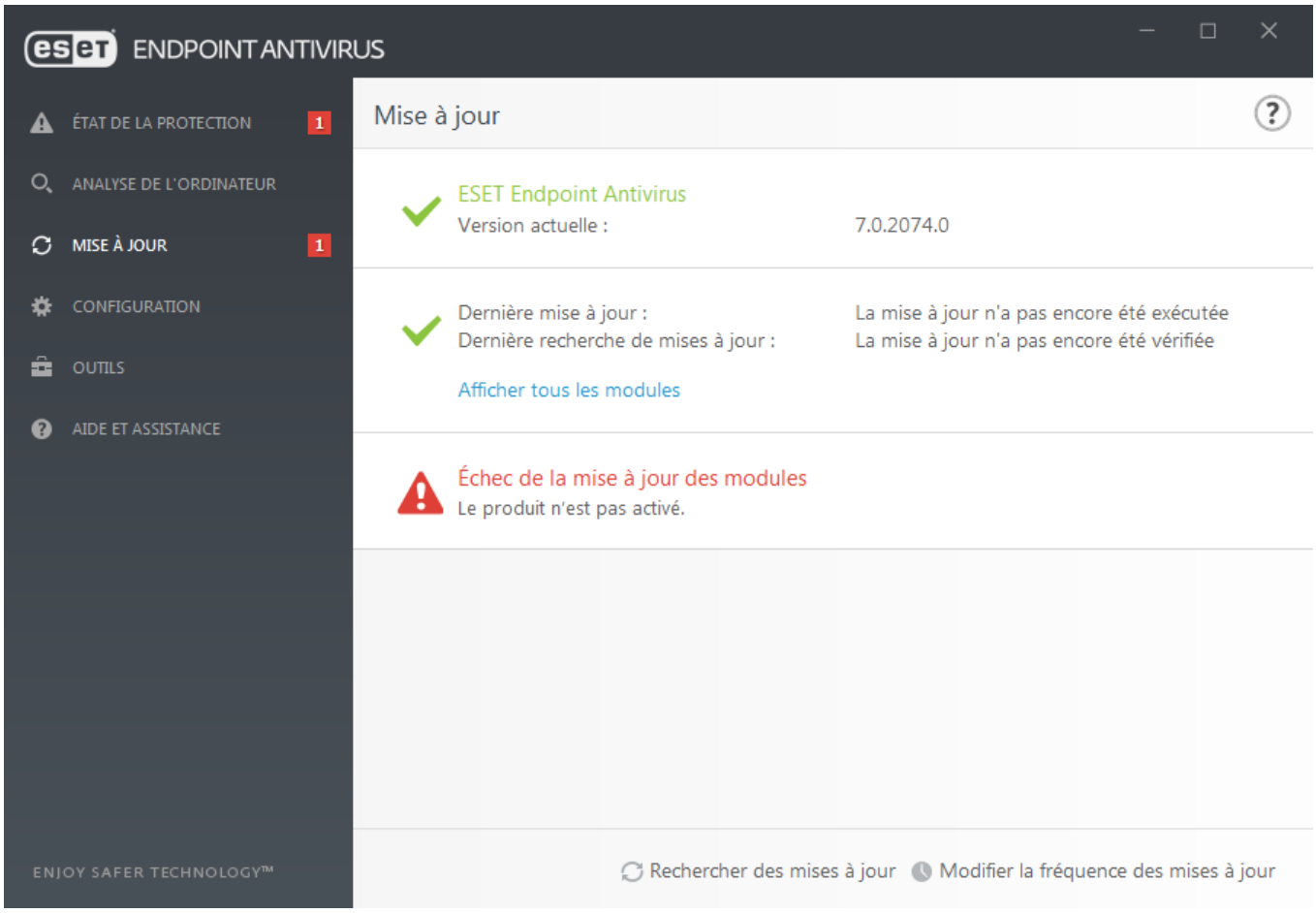
Important
Dans des circonstances normales, les modules se mettent à jour plusieurs fois par jour. Si ce n'est pas le cas, le programme n'est pas à jour et le risque d'infection est accru. Veillez à mettre à jour les modules dès que possible.

Le moteur de détection n'est plus à jour – Cette erreur apparaît après plusieurs tentatives infructueuses de mise à jour des modules. 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 configurations de connexion.

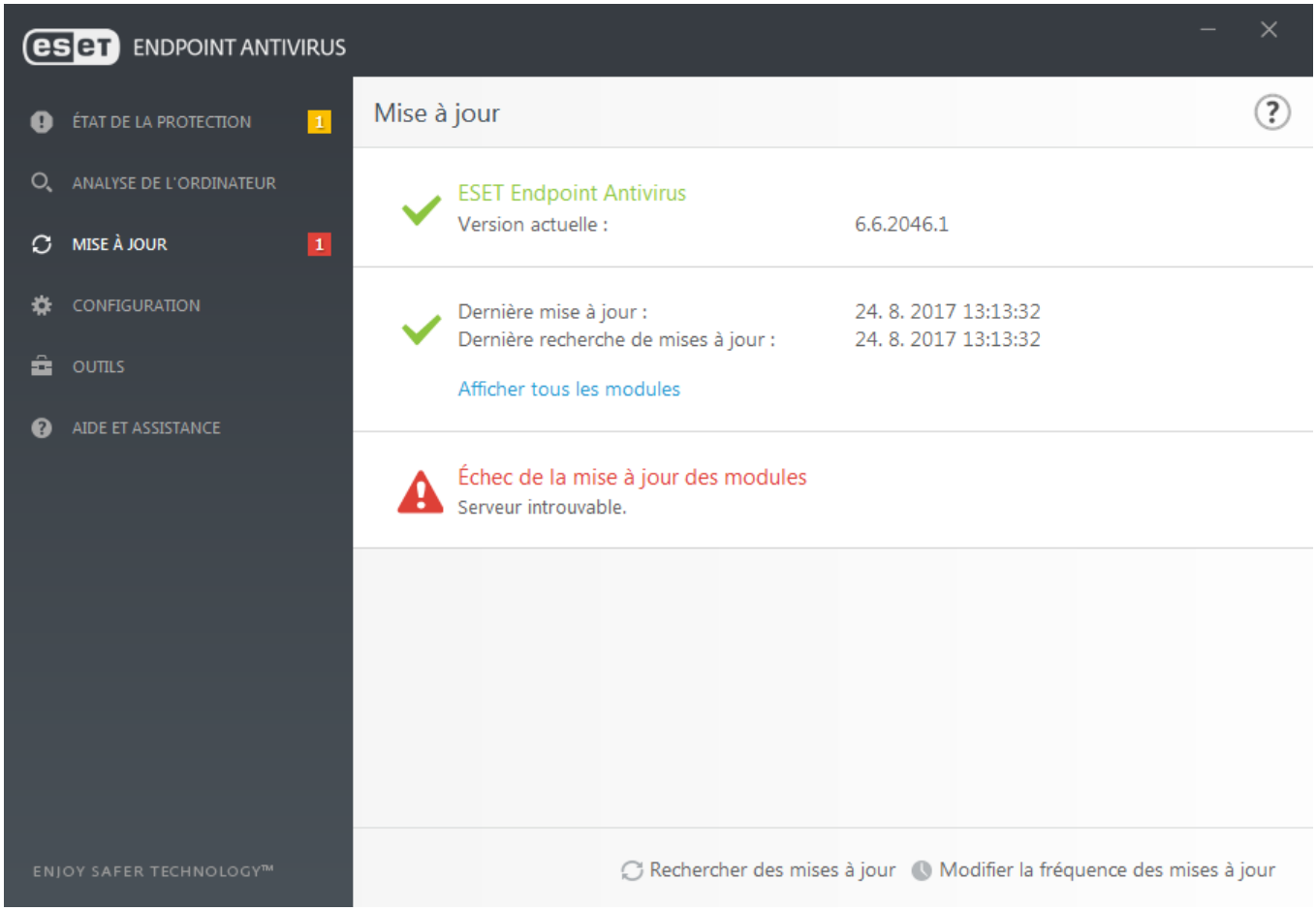
La notification précédente concerne les deux messages **Échec de la mise à jour des modules** sur les mises à jour infructueuses :

1. **Licence non valide** – La clé de licence n'a pas été correctement saisie lors de la configuration des mises à

jour. Nous vous recommandons de vérifier vos données d'authentification. La fenêtre Configuration avancée (cliquez sur **Configuration** dans le menu principal et sur **Configuration avancée**, ou appuyez sur la touche F5 de votre clavier) comporte d'autres options de mise à jour. Dans le menu principal, cliquez sur **Aide et assistance** > **Modifier la licence** pour saisir une nouvelle clé de licence.



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



Remarque
Pour plus d'informations, consultez cet article de la base de connaissances ESET.

Configuration des mises à jour

Les options de configuration des mises à jour sont accessibles dans l'arborescence **Configuration avancée** (F5), sous **Mise à jour**. 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.

Ajuster correctement les configurations des mises à jour
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 HTTPS, par exemple).

Général

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.

Configurer les notifications de mise à jour (option appelée précédemment **Sélectionner les notifications de mises à jour reçues**) – Cliquez sur **Modifier** pour sélectionner les notifications de l'application à afficher. Vous

pouvez choisir les options suivantes pour les notifications : **Afficher sur un bureau** et/ou **Envoyer par e-mail**.

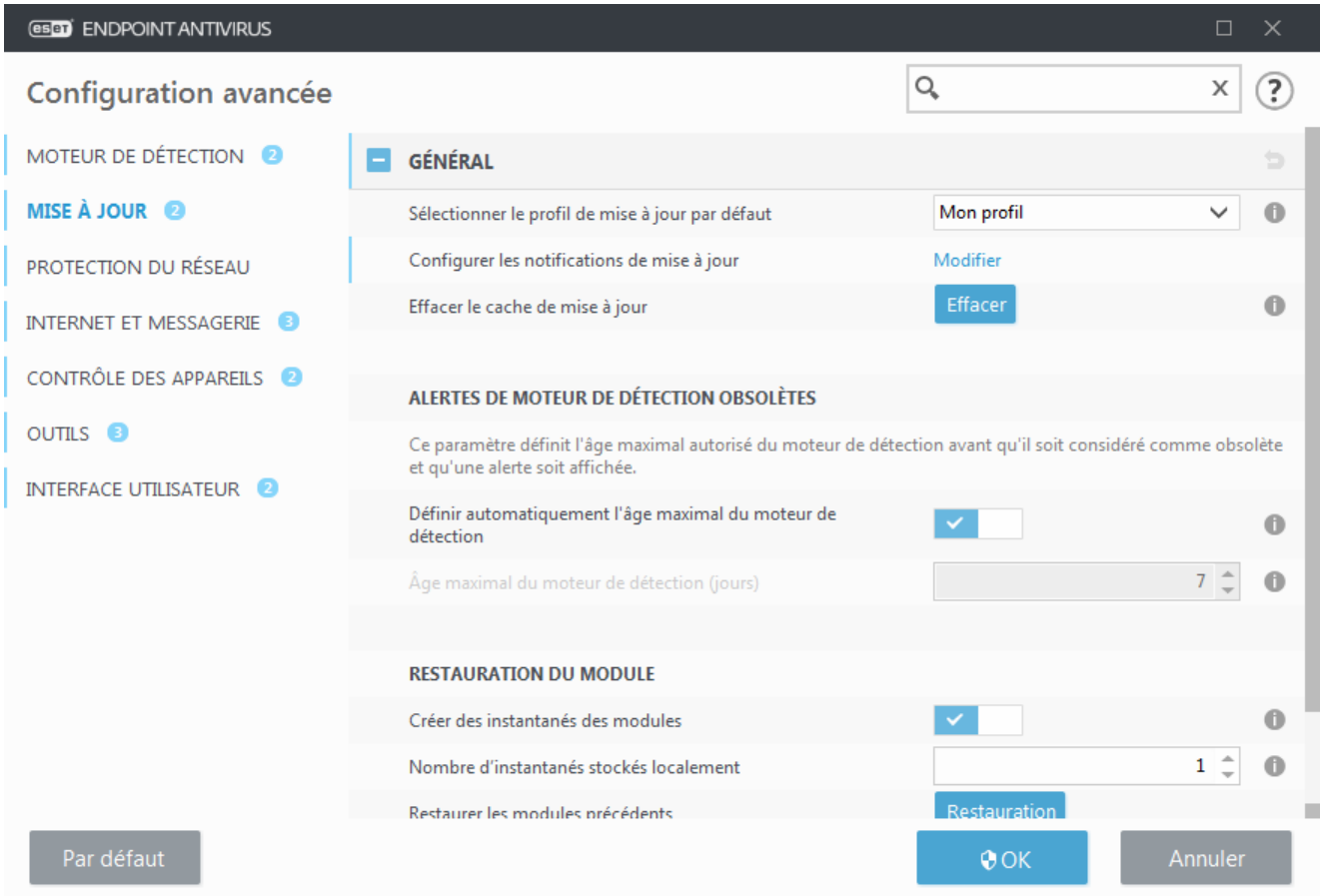
Si vous rencontrez des problèmes lors du téléchargement des mises à jour des modules, cliquez sur **Effacer** en regard de l'option **Vider le cache de mise à jour** pour supprimer les fichiers de mise à jour/le cache temporaires.

Alertes : moteur de détection obsolète

Définir automatiquement l'âge maximal du moteur de détection – Permet de définir la durée maximale (en jours) au terme de laquelle le moteur de détection est signalé comme étant obsolète. La valeur par défaut de l'option **Âge maximal du moteur de détection (jours)** est 7.

Restauration du module

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.



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**.

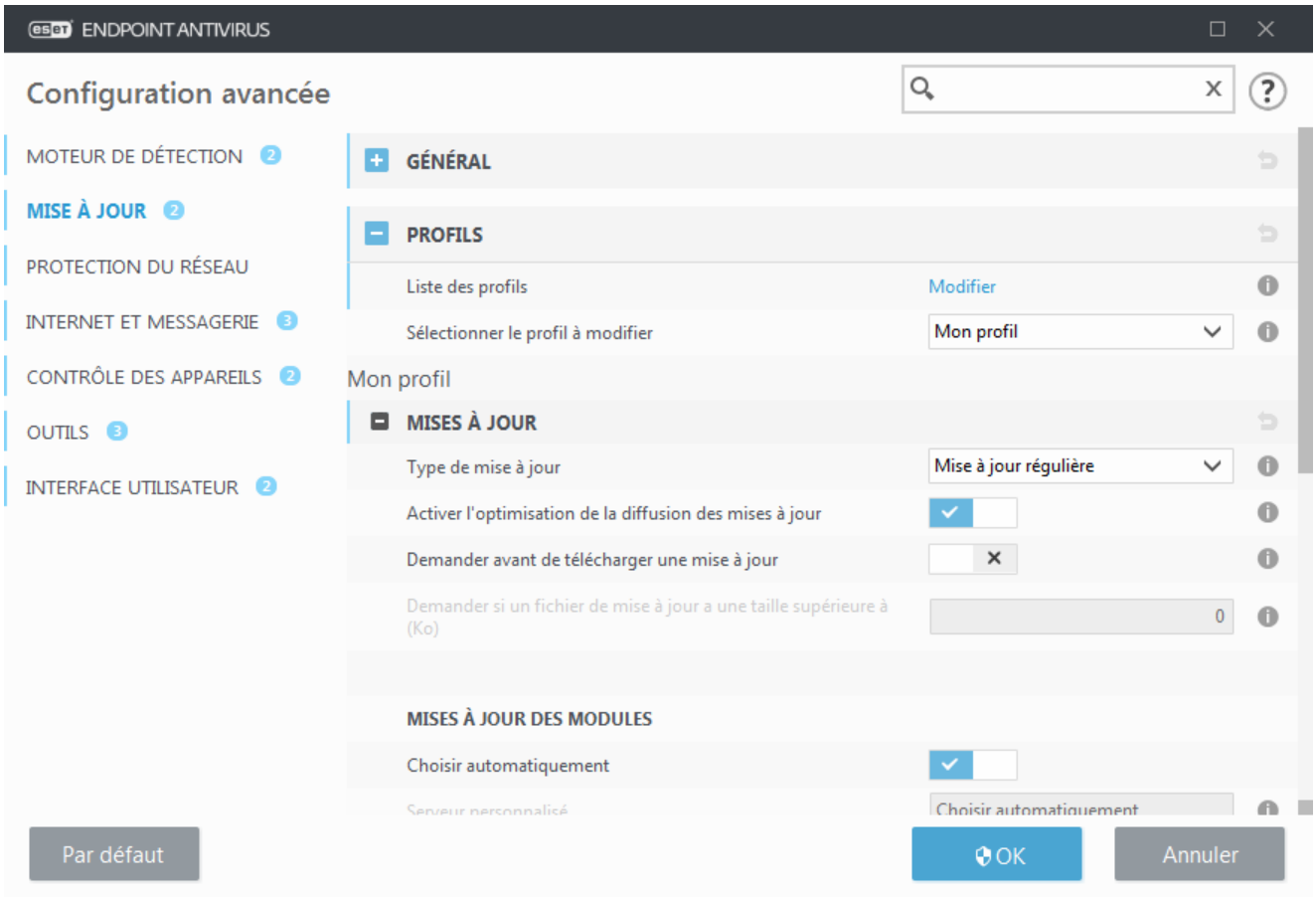
Pour créer un profil, cliquez sur **Modifier** en regard de **Liste des profils**, saisissez un nom dans **Nom du profil**, puis cliquez sur **Ajouter**.

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. L'option **Mise à jour retardée** permet d'effectuer la mise à jour à partir de serveurs de mise à jour spéciaux fournissant les nouvelles versions de bases de virus après un délai d'au moins X heures (bases testées dans un environnement réel et donc considérées comme stables).

Activer l'optimisation de la diffusion des mises à jour – Lorsque cette option est activée, les fichiers de mise à jour peuvent être téléchargés à partir du CDN (réseau de distribution de contenu). La désactivation de ce paramètre peut entraîner des interruptions de téléchargement et des ralentissements lorsque les serveurs de mise à jour ESET dédiés sont surchargés. Elle est utile lorsqu'un pare-feu est limité à l'accès uniquement aux adresses IP du serveur de mise à jour ESET ou qu'une connexion aux services CDN ne fonctionne pas.

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

L'option **Choisir automatiquement** est activée par défaut. L'option **Serveur personnalisé** correspond à l'emplacement où sont stockées les mises à jour. Si vous utilisez un serveur de mise à jour ESET, il est recommandé de conserver l'option par défaut.

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.

Autoriser les mises à jour des modules à partir des supports amovibles – Permet d'effectuer une mise à jour à partir de périphériques amovibles s'ils contiennent un miroir créé. Lorsque l'option **Automatique** est sélectionnée, la mise à jour s'exécute en arrière-plan. Si vous souhaitez afficher les boîtes de dialogue de mise à jour, sélectionnez l'option **Toujours demander**.

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

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

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

> **HTTP numÃ©ro de port du serveur**
> Le numÃ©ro de port du serveur HTTP spÃ©cifiÃ© dans les exemples ci-dessus dÃ©pend du port Ã©coutÃ© par votre serveur HTTP/HTTPS.

Mise Ã jour des composants du programme

Voir Mise Ã jour des composants du programme.

Miroir de mise Ã jour

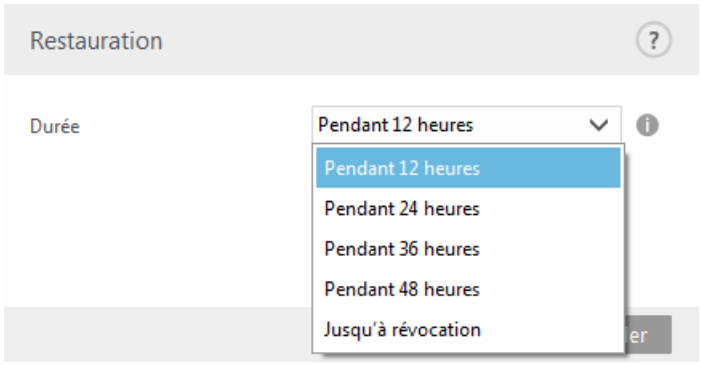
Voir Miroir de mise Ã jour.

Paramètres avancés de mises à jour

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

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

Si vous cliquez sur **Restauration** (**Configuration avancée** (F5) > **Mise à jour** > **Général** > **Restauration du module**), 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 interrompues.



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

Le 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.

> **Remarque**
> Admettons que le numéro 19959 correspond au moteur de détection le plus récent. Les moteurs de détection 19958 et 19956 sont stockés sous forme d'instantanés. Notez que la base numéro 19957 n'est pas disponible parce que l'ordinateur était éteint et qu'une mise à jour plus récente a été mise à disposition avant que 19957 ait été téléchargée, par exemple. 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 19956. Ce processus peut prendre un certain temps. Vérifiez si le moteur de détection est bien retourné à une version antérieure dans la fenêtre principale de ESET Endpoint Antivirus dans la section Mise à jour.

Mise à jour des composants du programme

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

Les mises à jour des composants du programme offrent de nouvelles fonctionnalités ou modifient les versions précédentes. Cette mise à jour peut s'effectuer sans intervention de l'utilisateur ou après sa notification. Le redémarrage de l'ordinateur peut être nécessaire après la mise à jour des composants du programme.

Le menu déroulant **Mode de mise à jour** contient trois options :

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

Par défaut, les mises à jour des composants du programme sont téléchargées à partir des serveurs de répertoire

ESET. Dans les environnements de grande taille ou hors ligne, le trafic peut être distribué pour permettre la mise en cache interne des fichiers de composants du programme.

Définition d'un serveur personnalisé pour les mises à jour des composants du programme

1.Définissez le chemin d'accès à la mise à jour des composants du programme dans le champ **Serveur personnalisé**.
Il peut s'agit d'un lien HTTP(S), d'un chemin d'accès à un partage réseau SMB, un lecteur de disque local ou un chemin d'accès à des périphériques amovibles. Pour les lecteurs réseau, utilisez le chemin UNC au lieu de la lettre de lecteur mappée.

2.Laissez les champs **Nom d'utilisateur** et **Mot de passe** vides s'ils ne sont pas obligatoires.
Si nécessaire, définissez les informations d'identification appropriées à cet emplacement pour l'authentification HTTP sur le serveur web personnalisé.

3.Confirmez les modifications et testez la présence d'une mise à jour des composants du programme à l'aide d'une mise à jour ESET Endpoint Antivirus.

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

Options de connexion

Pour accéder aux options de configuration du serveur proxy pour un profil de mise à jour donné, cliquez sur **Mise à jour** dans l'arborescence **Configuration avancée** (F5), puis sur **Profils** > **Mises à jour** > **Options de connexion**.

Serveur proxy

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 les options de configuration de serveur proxy déjà indiquées dans la branche **Outils** > **Serveur proxy** de la configuration avancée complète.

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

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

- Un autre serveur proxy que celui défini dans **Outils** > **Serveur proxy** est utilisé pour mettre à jour ESET Endpoint 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 Endpoint 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.

Partages Windows

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

Pour configurer un compte de ce type, sélectionnez **Se connecter au réseau local en tant que** dans le menu déroulant :

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

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

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

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

Les paramètres **Nom d'utilisateur** et **Mot de passe** sont facultatifs.

Avertissement

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

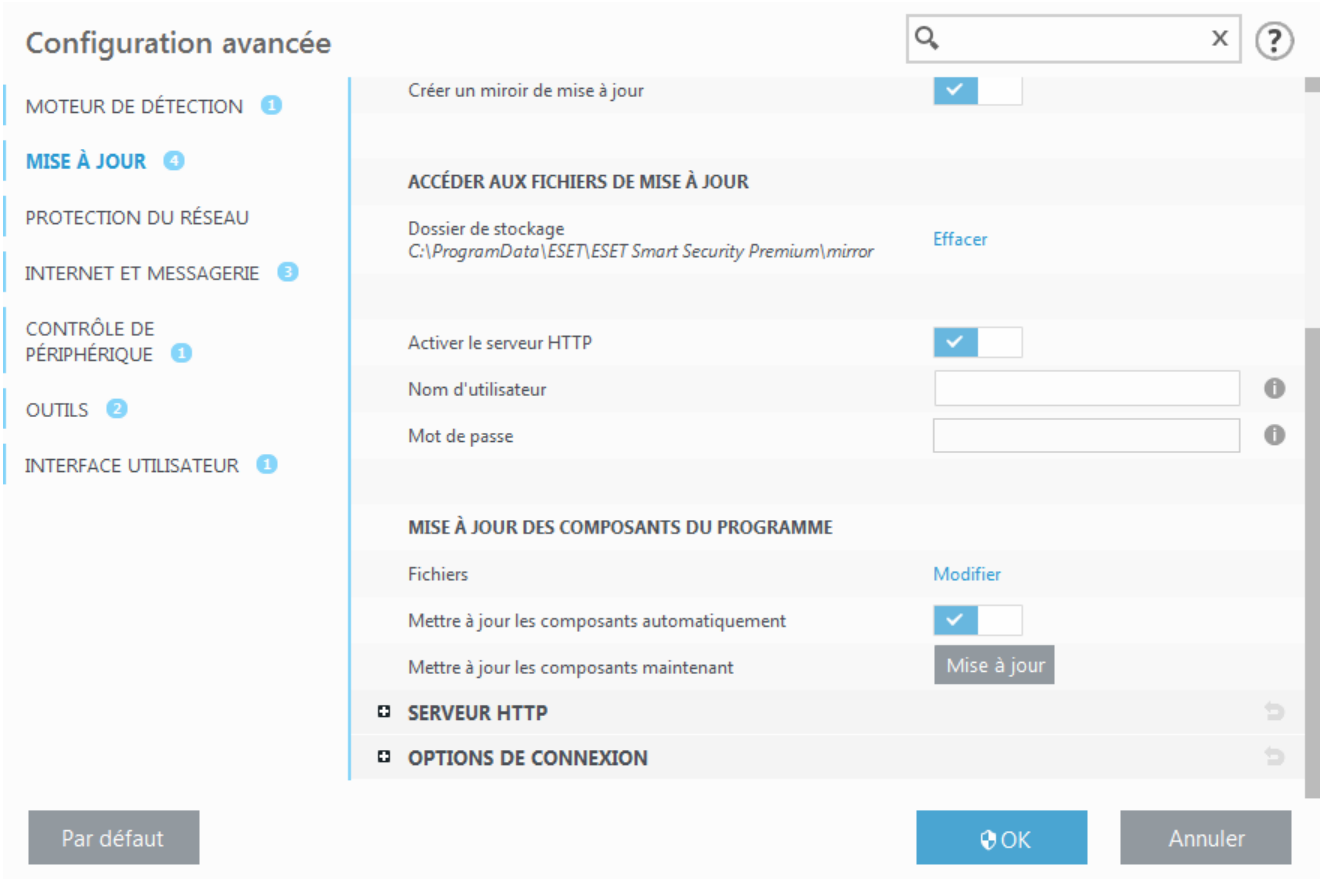
Sélectionnez **Déconnecter du serveur après la mise à jour pour forcer une déconnexion si la** connexion au

serveur reste active, même après le téléchargement des mises à jour.

Miroir de mise à jour

ESET Endpoint Antivirus permet de créer des copies des fichiers de mises à jour afin de les utiliser pour la mise à jour d'autres postes de travail du réseau. L'utilisation d'un miroir, copie des fichiers de mise à jour dans l'environnement du réseau local, s'avère pratique puisque les fichiers de mise à jour doivent être téléchargés du serveur de mise à jour du fournisseur de manière répétée, pour toutes les stations de travail. Les mises à jour sont téléchargées sur le serveur miroir local puis distribuées à toutes les stations de travail pour éviter tout risque de surcharge du réseau. La mise à jour de postes de travail à partir d'un miroir optimise l'équilibre de la charge réseau et libère les bandes passantes des connexions Internet.

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



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

Accéder aux fichiers de mise à jour

Activer le serveur HTTP – Si cette option est activée, les fichiers de mise à jour sont accessibles via un serveur HTTP. Aucune information d'identification n'est requise.

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

dossier réseau partagé ou les clients peuvent accéder au miroir situé sur un serveur HTTP.

Le dossier dédié aux fichiers de mise à jour du miroir peut être défini sous **Dossier de stockage des fichiers miroir**. Pour sélectionner un autre dossier, cliquez sur **Effacer** pour supprimer le dossier *C:\ProgramData\ESET\ESET Endpoint Antivirus\mirror* prédéfini, puis cliquez sur **Modifier** pour accéder à un dossier sur l'ordinateur local ou un dossier réseau partagé. Si une autorisation pour le dossier spécifié est requise, les données d'authentification doivent être entrées dans les champs **Nom d'utilisateur** et **Mot de passe**. Si le dossier destination sélectionné se trouve sur un disque réseau exécutant le système d'exploitation Windows NT/2000/XP, le nom d'utilisateur et le mot de passe spécifiés doivent disposer du droit d'écriture sur ce dossier. Le nom d'utilisateur et le mot de passe doivent être entrés sous le format *Domaine/Utilisateur* ou *Workgroup/Utilisateur*. N'oubliez pas de fournir les mots de passe correspondants.

Mise à jour des composants du programme

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

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

Mettre à jour les composants maintenant – Met à jour les composants du programme avec la nouvelle version.

Serveur HTTP

Port du serveur – Par défaut, le port su serveur est défini sur 2221.

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

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

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

Mise à jour à partir du miroir

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

Accès au miroir au moyen d'un serveur HTTP interne

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

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

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

SSL pour serveur HTTP

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

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

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

- **Accédez à Configuration avancée** (F5), puis cliquez sur **Mise à jour** > **Profils** > **Général**.

- Désactivez l'option **Choisir automatiquement**, puis ajoutez un nouveau serveur dans le champ **Serveur de mise à jour** dans l'un des formats suivants :
http://adresse_IP_de_votre_serveur:2221
https://adresse_IP_de_votre_serveur:2221 (si vous utilisez SSL)

Accès au miroir via le partage des systèmes

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

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

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

Pour accéder au dossier miroir, vous devez effectuer cette procédure sous le même compte que celui utilisé pour se connecter à l'ordinateur sur lequel le miroir est créé. Dans le cas où l'ordinateur se trouve dans un domaine, le nom d'utilisateur « domaine\utilisateur » devrait être utilisé. Dans le cas contraire, « adresse_IP_de_votre_serveur\utilisateur » ou « nom_d'hôte\utilisateur » devrait être utilisé.

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

1. Ouvrez la **Configuration avancée** de ESET Endpoint Antivirus et cliquez sur **Mise à jour** > **Profils** > **Mises à jour**.

2. Désactivez l'option **Choisir automatiquement** en regard de **Mises à jour du module**, puis ajoutez un nouveau serveur dans le champ **Serveur de mise à jour** à l'aide du format *UNC**CHEMIN*.

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

Création du miroir à l'aide de l'outil Miroir

L'outil Miroir crée une structure de dossiers différente de celle du miroir Endpoint. Chaque dossier contient des fichiers de mise à jour pour un groupe de produits. Vous devez spécifier le chemin d'accès complet au dossier adéquat dans les configurations de mise à jour du produit à l'aide du miroir.

Par exemple, pour mettre à jour ESMC 7 à partir du miroir, définissez le serveur de mise à jour sur (en fonction de l'emplacement de la racine de votre serveur HTTP) :

```
http://your_server_address/mirror/eset_upd/era6
```

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

Dépannage des problèmes de miroir de mise à jour

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

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

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

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

ESET Endpoint Antivirus signale une erreur lors du téléchargement des fichiers de mise à jour, probablement causée par une spécification incorrecte du serveur de mise à jour (chemin réseau du dossier miroir) à partir duquel les postes de travail locaux téléchargent les mises à jour.

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 suivantes sont activées dans ESET Endpoint Antivirus :

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

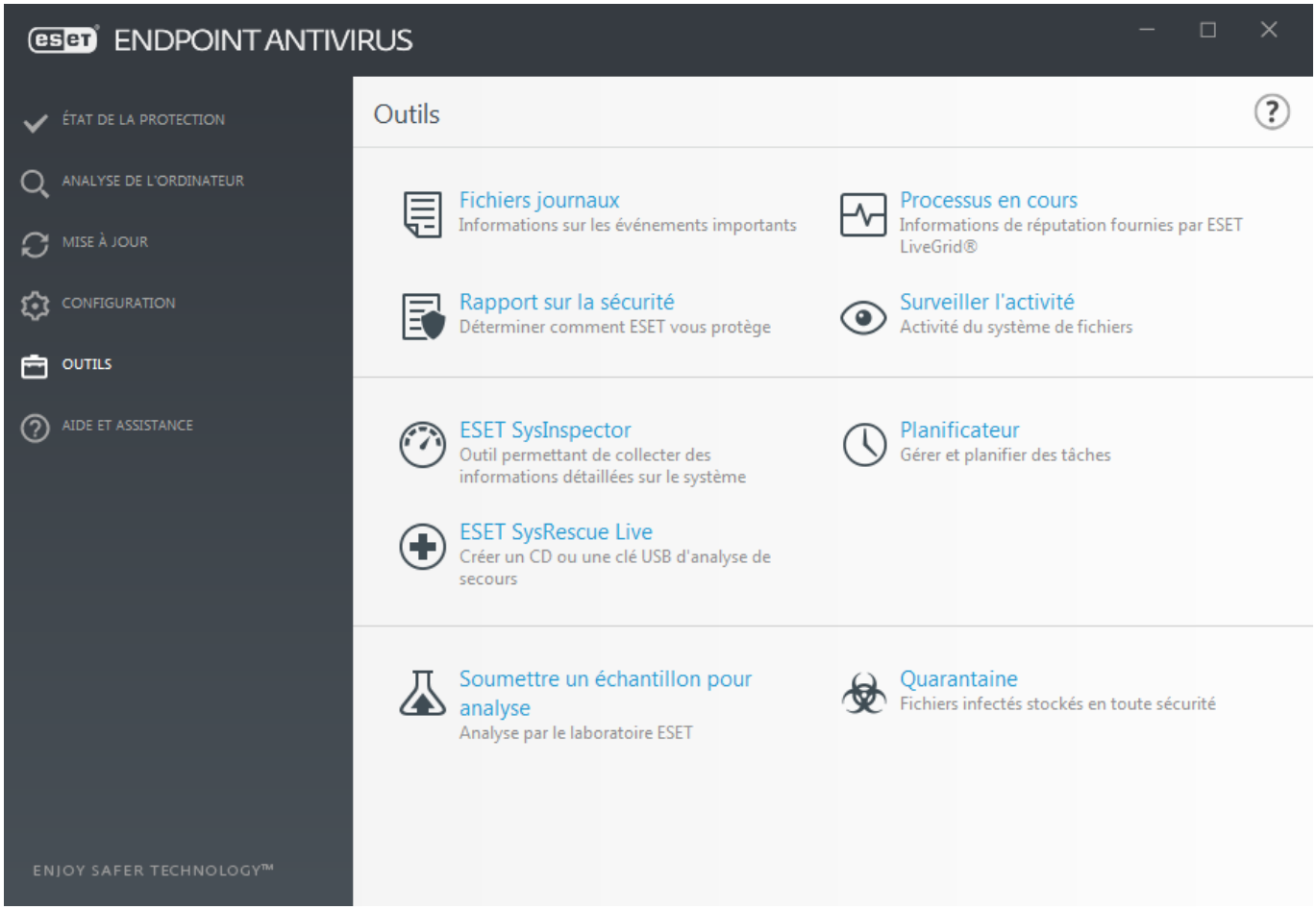
Chaque tâche de mise à jour peut être modifiée selon les besoins de l'utilisateur. Outre les tâches de mise à jour par défaut, vous pouvez en créer des nouvelles avec vos propres paramètres. Pour plus d'informations sur la création et la configuration des tâches de mise à jour, reportez-vous à Planificateur.

Outils

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

Ce menu comprend les éléments suivants :

- Fichiers journaux
- Rapport sur la sécurité
- Processus en cours (si ESET LiveGrid® est activé dans ESET Endpoint Antivirus)
- Surveiller l'activité
- Planificateur
- ESET SysInspector
- ESET SysRescue Live – Vous redirige vers le site Web ESET SysRescue Live à partir duquel vous pouvez télécharger l'image du CD/DVD .iso ESET SysRescue Live.
- Quarantaine
- Soumettre un échantillon pour analyse – Permet de soumettre un fichier suspect pour analyse au laboratoire d'ESET. La boîte de dialogue qui s'affiche lorsque vous cliquez sur cette option est décrite dans la section.



Fichiers journaux

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

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

- **Détections** – Ce journal contient des informations sur les détections et infiltrations détectées par les modules de ESET Endpoint Antivirus. Ces informations comprennent l'heure de détection, le nom de la détection, l'emplacement, l'action exécutée et le nom de l'utilisateur connecté au moment où l'infiltration a été détectée. Double-cliquez sur une entrée du journal pour afficher son contenu dans une fenêtre distincte. 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 Endpoint 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** – Tous les résultats des analyses sont affichés dans cette fenêtre. Chaque ligne correspond à un seul contrôle d'ordinateur. Double-cliquez sur une entrée pour afficher les détails de l'analyse correspondante.

- **Fichiers bloqués** – Contient des enregistrements des fichiers qui ont été bloqués et n'étaient pas accessibles. Le protocole montre la raison et le module source qui a bloqué le fichier, ainsi que l'application et l'utilisateur qui ont exécuté le fichier.

- **Fichiers envoyés** – Contient les entrées des fichiers qui ont été envoyés à ESET LiveGrid® ou ESET Dynamic Threat Defense pour analyse.

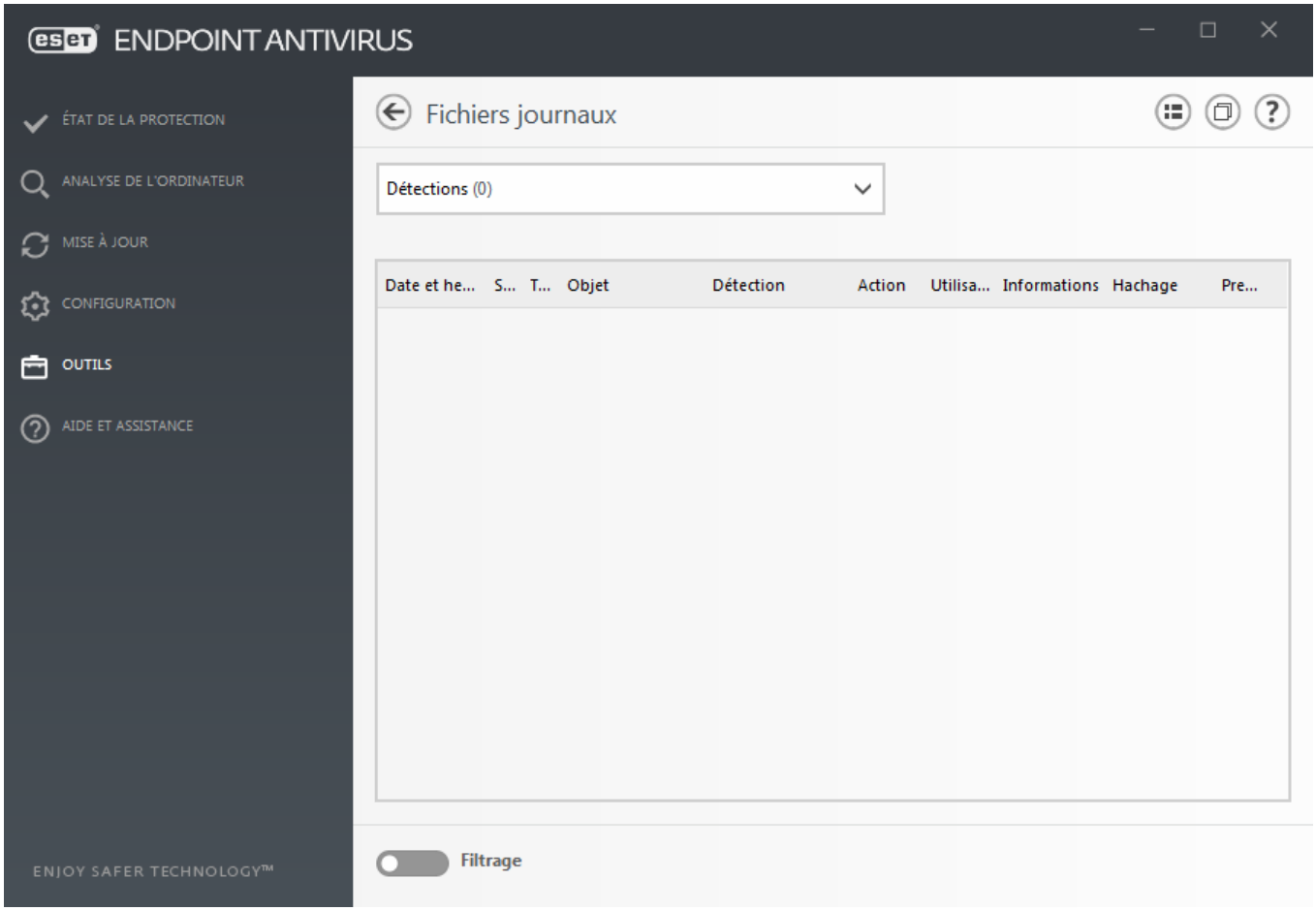
- **Journaux d'audit** – Chaque journal contient des informations sur la date et l'heure de la modification, le type de modification, la description, la source et l'utilisateur. Pour plus d'informations, consultez Journaux d'audit.

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

- **Protection du réseau** – Le journal du pare-feu affiche toutes les attaques distantes détectées par la protection contre les attaques réseau. Le journal du pare-feu contient toutes les attaques distantes détectées par le pare-feu. Il comprend des renseignements sur les attaques subies par votre ordinateur. La colonne Événement répertorie les attaques détectées. La colonne Source fournit des informations sur l'attaquant. La colonne Protocole indique le protocole de communication utilisé pour l'attaque. L'analyse du journal de pare-feu permet de détecter à temps les tentatives d'infiltration du système et d'éviter tout accès non autorisé à votre système. Pour plus de détails sur des attaques réseau spécifiques, voir Options IDS avancées.

- **Sites Web filtrés** – Cette liste est utile pour afficher la liste des sites Web bloqués par la Protection de l'accès Web. Ces journaux permettent de voir l'heure, l'URL, l'utilisateur et l'application ayant ouvert une connexion au site Web en question.

- **Contrôle de périphérique** : contient des enregistrements des supports amovibles ou périphériques qui ont été connectés à l'ordinateur. Seuls les périphériques auxquels correspond une règle de contrôle de périphérique seront enregistrés dans le fichier journal. Si la règle ne correspond pas à un périphérique connecté, aucune entrée de journal ne sera créée pour un périphérique connecté. Des détails figurent également tels que le type de périphérique, le numéro de série, le nom du fabricant 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 + 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.../Rechercher...** – 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 des informations sur toutes les entrées de la fenêtre.
- **Supprimer/Supprimer tout** – Supprime les entrées sélectionnées ou toutes les entrées affichées. Vous devez disposer des privilèges d'administrateur pour effectuer cette action.
- **Exporter...** – Exporte les informations sur les entrées au format XML.

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

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

- **Créer une exclusion** – Permet de créer une exclusion de détection à l'aide d'un assistant (non disponible pour les détections de logiciel malveillant).

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.

Configuration de la consignation

La configuration de la consignation d'ESET Endpoint Antivirus est accessible à partir de la fenêtre principale du programme. Cliquez sur **Configuration** > **Configuration avancée** > **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** – Consigne uniquement les erreurs critiques (erreur de démarrage de la protection antivirus, etc...).

Remarque
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 de fragmentation 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. Toutes les entrées vides des journaux sont supprimées pour améliorer les performances et accélérer 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** – Sélectionnez le répertoire dans lequel les fichiers journaux sont stockés (s'applique uniquement aux formats texte/CSV). Vous pouvez copier le chemin d'accès ou sélectionner un répertoire en cliquant sur **Effacer**. Chaque section de journal dispose de son propre fichier avec un nom de fichier prédéfini (par exemple *virlog.txt* pour la section **Menaces détectées** 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.

Activer le suivi des modifications de configuration dans le journal de vérification – Vous informe de chaque modification de configuration. Pour plus d'informations, consultez les journaux d'audit.

> **ESET Log Collector**
> 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.

Journal de vérification

Un environnement d'entreprise comprend généralement plusieurs utilisateurs avec des droits d'accès définis pour la configuration des endpoints. Comme la modification de la configuration du produit peut avoir une incidence considérable sur le fonctionnement de celui-ci, il est essentiel que les administrateurs suivent les modifications apportées par les utilisateurs pour qu'ils puissent identifier et résoudre rapidement les problèmes et éviter qu'ils se reproduisent.

Le journal d'audit est un nouveau type de journalisation depuis ESET Endpoint Antivirus version 7.1 qui offre une solution pour identifier l'origine d'un problème. Il suit les modifications de la configuration et de l'état de la protection et enregistre des instantanés pour des références ultérieures.

Pour consulter le **journal d'audit**, cliquez sur **Outils** dans le menu principal, sur **Fichiers journaux**, puis sélectionnez **Journaux d'audit** dans le menu déroulant.

Le journal d'audit contient les informations suivantes :

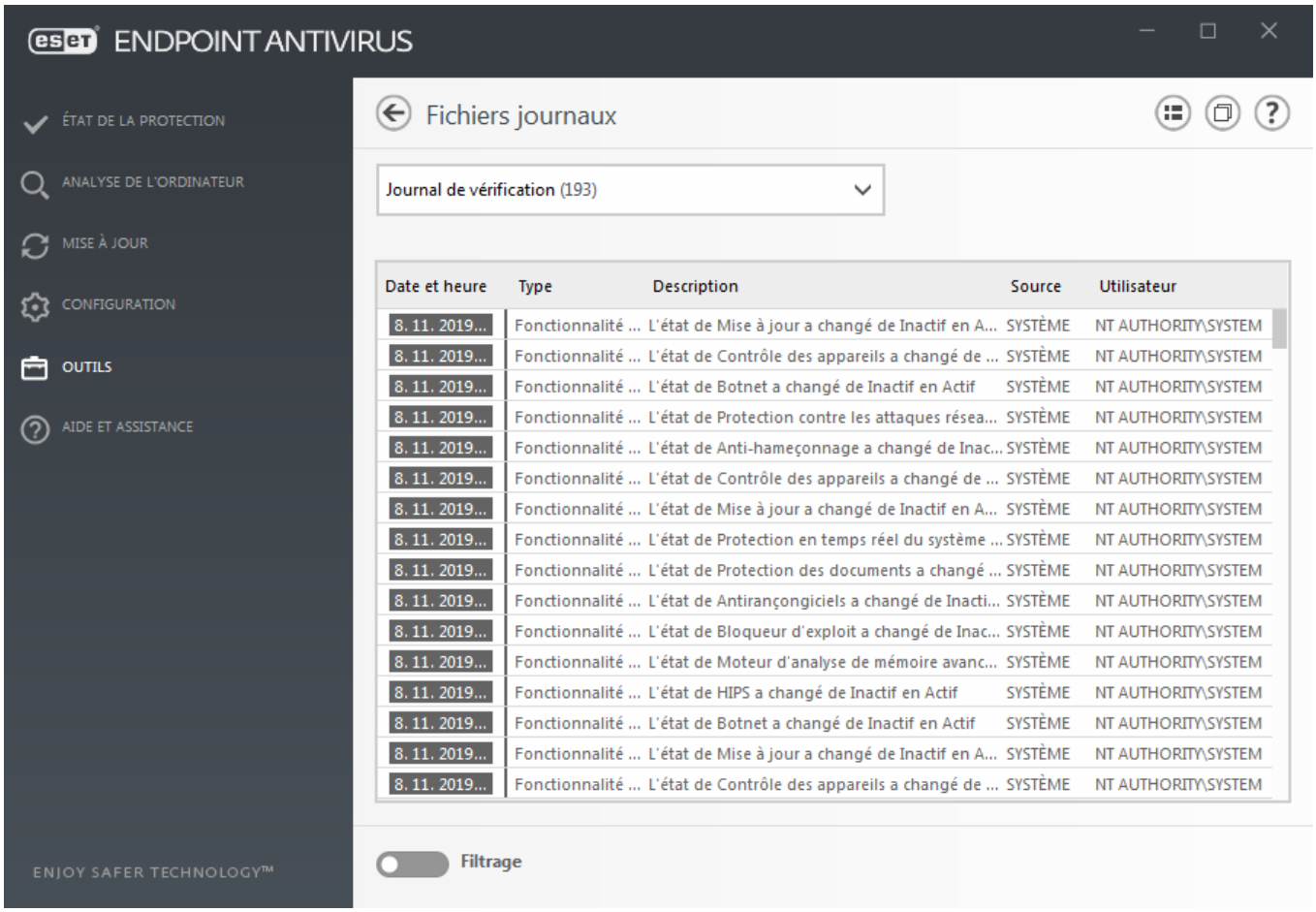
• Heure : quand la modification a été apportée.

• Type : type de configuration ou de fonctionnalité ayant été modifié.

• Description : élément changé et partie de la configuration qui a été modifiée ainsi que le nombre de configurations modifiées.

• Source : source de la modification.

• Utilisateur : personne ayant effectué la modification.



Cliquez avec le bouton droit sur un des **Paramètres modifiés** du journal d'audit dans la fenêtre Fichiers journaux, puis sélectionnez **Afficher les modifications** dans le menu contextuel pour afficher des informations détaillées sur la modification apportée. Vous pouvez en outre restaurer la modification de la configuration en cliquant sur **Restaurer** dans le menu contextuel (non disponible pour un produit géré par ESMC). Si vous sélectionnez **Effacer tout** dans le menu contextuel, un journal contenant les informations relatives à cette action est créé.

Si l'option **Optimiser automatiquement les fichiers journaux** est activée dans **Configurations avancées** > **Outils** > **Fichiers journaux**, les journaux d'audit seront automatiquement défragmentés comme les autres journaux.

Si l'option **Supprimer automatiquement les entrées plus anciennes que (jours)** est activée dans **Configurations avancées** > **Outils** > **Fichiers journaux**, les entrées des journaux plus anciennes que le nombre de jours spécifiés seront automatiquement supprimées.

Planificateur

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

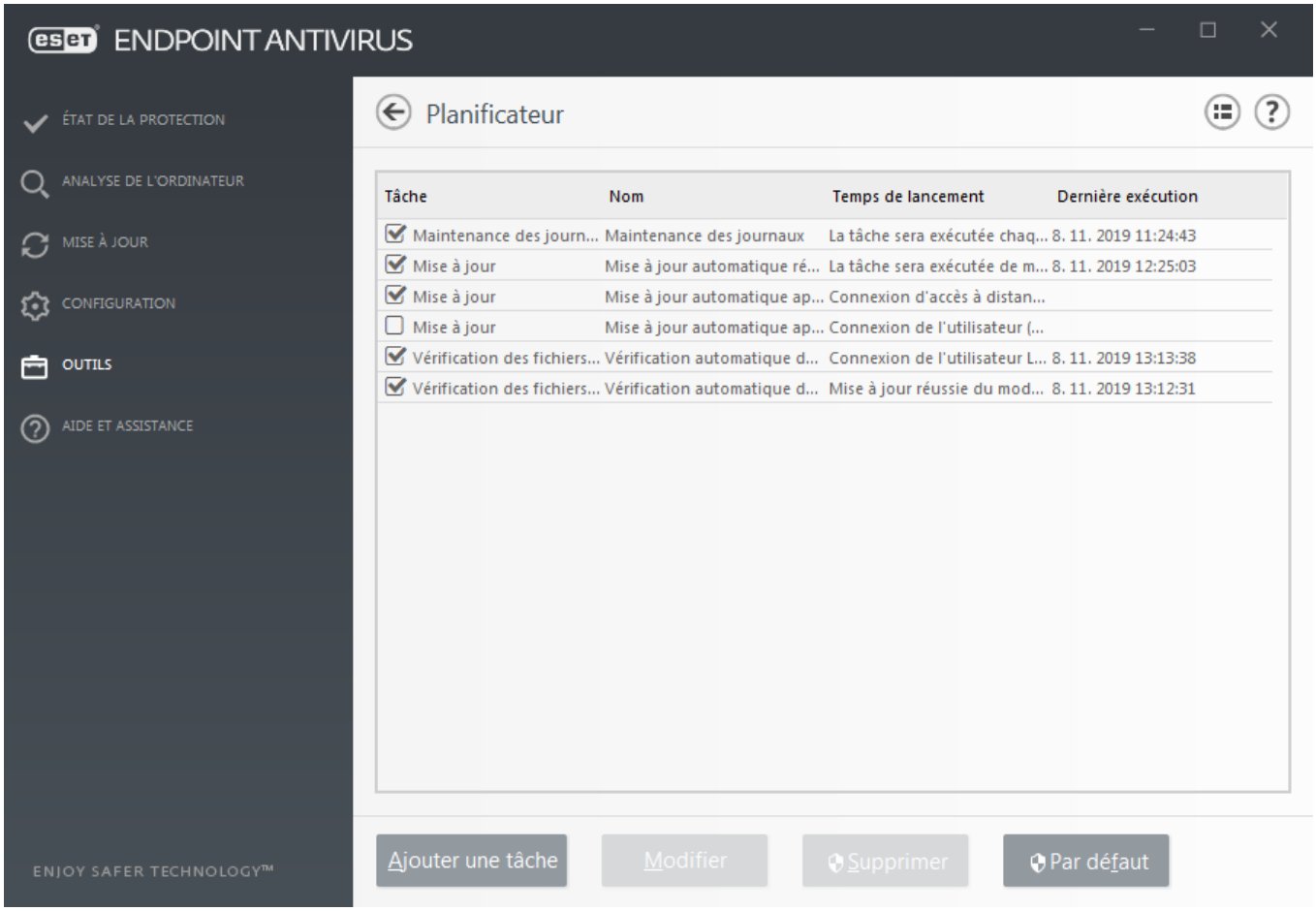
Le planificateur est accessible depuis la fenêtre principale de ESET Endpoint Antivirus, dans **Outils** > **Planificateur**. Le **planificateur** contient la liste de toutes les tâches planifiées, des propriétés de configuration telles que la date et l'heure prédéfinies, ainsi que le profil d'analyse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

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

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

- **Maintenance des journaux**
- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion commutée**
- **Mise à jour automatique après ouverture de session utilisateur**
- **Vérification des fichiers de démarrage** (après l'ouverture de session de l'utilisateur)
- **Vérification des fichiers de démarrage** (après la mise à jour réussie des modules)

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



Ajout d'une nouvelle tâche

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

2. Entrez le nom de la tâche.

3. Sélectionnez la tâche souhaitée dans le menu déroulant :

• **Exécuter une application externe** – Permet de programmer l'exécution d'une application externe.
• **Maintenance des journaux** – Les fichiers journaux contiennent également des éléments provenant d'enregistrements supprimés. Cette tâche optimise régulièrement les entrées des fichiers journaux pour garantir leur efficacité.
• **Contrôle des fichiers de démarrage du système** – Vérifie les fichiers autorisés à s'exécuter au démarrage du système ou lors de l'ouverture de session de l'utilisateur.
• **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 le moteur de détection et les modules de l'application.

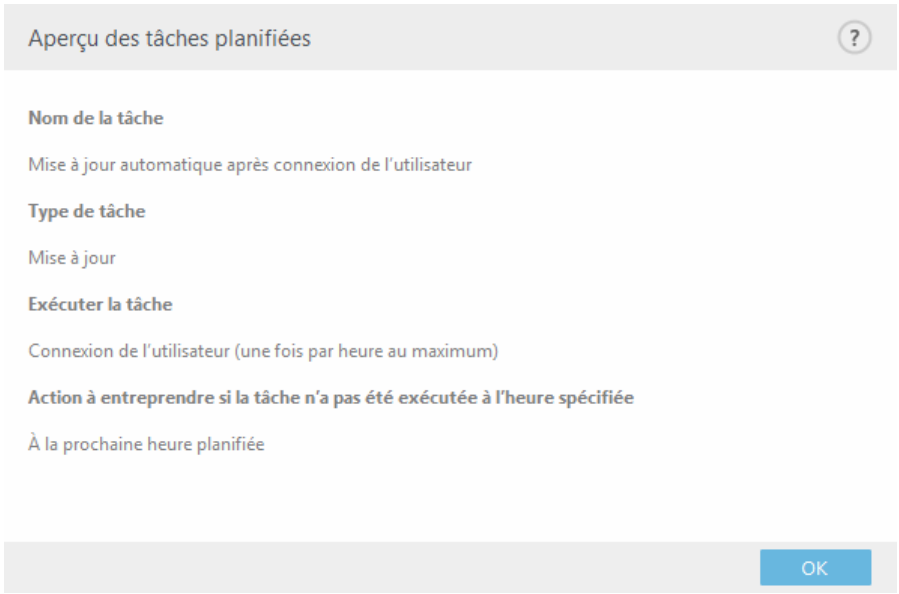
4. Activez le bouton bascule **Activé** si vous souhaitez activer la tâche (vous pouvez le faire ultérieurement en activant/désactivant la case à cocher correspondante dans la liste des tâches planifiées). Cliquez ensuite sur **Suivant** et sélectionnez une des options de planification :

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

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

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

Pour examiner une tâche planifiée, cliquez sur **Afficher les détails des tâches**.



Statistiques de protection

Pour afficher un graphique des données statistiques relatives aux modules de protection d'ESET Endpoint Antivirus, cliquez sur **Outils** > **Statistiques**. Dans le menu déroulant **Statistiques**, sélectionnez le module de protection applicable pour afficher le graphique et la légende correspondants. Si vous faites glisser le pointeur de la souris sur un élément de la légende, seules les données correspondant à cet élément sont représentées dans le graphique.

Un nouveau type de rapport a été introduit dans ESET Endpoint Antivirus version 7.1. Il s'agit du rapport sur la sécurité. La section Statistiques de protection ne sera plus disponible.

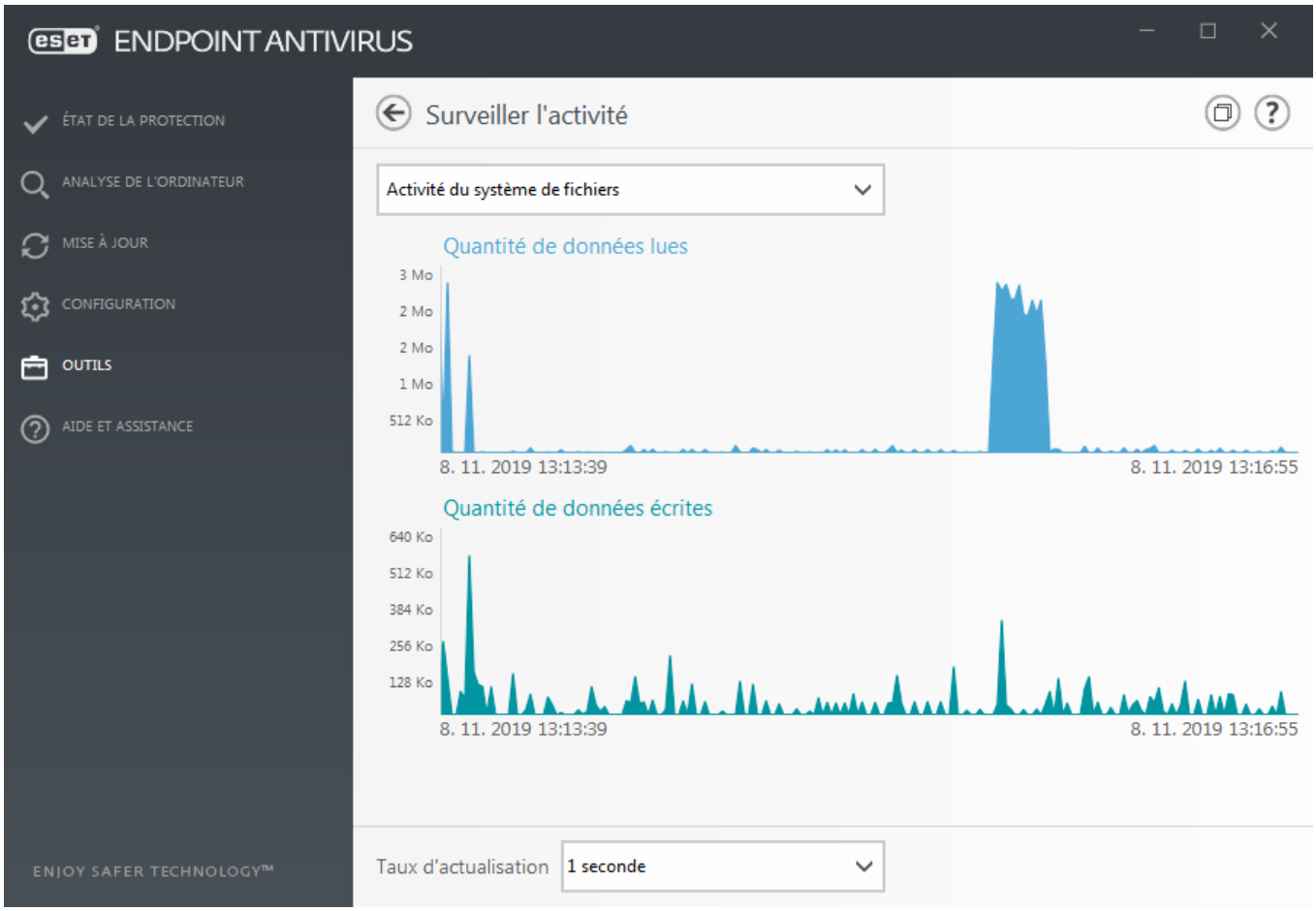
Les graphiques statistiques suivants sont disponibles :

- **Protection antivirus et antispyware** – Affiche le nombre d'objets infectés et nettoyés.
- **Protection du système de fichiers** – Affiche uniquement les objets lus ou écrits dans le système de fichiers.
- **Protection du client de messagerie** – Affiche uniquement les objets envoyés ou reçus par les clients de messagerie.
- **Protection de l'accès Web et antihameçonnage** – Affiche uniquement les objets téléchargés par des navigateurs Web.

À côté des graphiques statistiques, vous pouvez voir le nombre total d'objets analysés, le nombre d'objets infectés, le nombre d'objets nettoyés et le nombre d'objets propres. Cliquez sur **Réinitialiser** pour effacer les informations de statistiques. Pour effacer et supprimer toutes les données existantes, cliquez sur **Tout réinitialiser**.

Surveiller l'activité

Pour voir l'**activité actuelle du système de fichiers** sous forme graphique, cliquez sur **Outils** > **Surveiller l'activité**. Au bas du graphique figure une chronologie qui enregistre en temps réel l'activité du système de fichiers sur la base de l'intervalle sélectionné. Pour modifier l'intervalle, effectuez une sélection dans le menu déroulant **Taux d'actualisation**.



Les options disponibles sont les suivantes :

- **Pas : 1 seconde** – Le graphique est actualisé toutes les secondes et la chronologie couvre les 10 dernières minutes.
- **Pas : 1 minute (24 dernières heures)** – Le graphique est actualisé toutes les minutes et la chronologie couvre les 24 dernières heures.
- **Pas : 1 heure (dernier mois)** – Le graphique est actualisé toutes les heures et la chronologie couvre le dernier mois.
- **Pas : 1 heure (mois sélectionné)** – Le graphique est actualisé toutes les heures et la chronologie couvre les X mois sélectionnés.

L'axe vertical du **Graphique d'activité du système de fichiers** représente les données lues (en bleu) et les données écrites (en bleu turquoise). Les deux valeurs sont exprimées en Ko (kilo-octets)/Mo/Go. Si vous faites glisser le curseur de la souris sur les données lues ou écrites dans la légende sous le graphique, celui-ci n'affiche que les données relatives à ce type d'activité.

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. Consultez aussi le guide de l'utilisateur en ligne d'ESET SysInspector.

La fenêtre SysInspector affiche les informations suivantes relatives aux journaux créés :

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

Les actions disponibles sont les suivantes :

- **Afficher** – Ouvre le journal créé. Vous pouvez également cliquer avec le bouton droit sur un fichier journal, puis sélectionner **Afficher** dans le menu contextuel.
- **Comparer** – Compare deux journaux existants.
- **Créer...** – Crée un journal. Patientez jusqu'à ce qu'ESET SysInspector ait terminé (l'état du journal s'affiche en tant que créé) avant d'accéder au journal.
- **Supprimer** – Supprime les journaux sélectionnés de la liste.

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

- **Afficher** – Ouvre le journal sélectionné dans ESET SysInspector (équivaut à double-cliquer sur un journal).
- **Comparer** – Compare deux journaux existants.
- **Créer...** – Crée un journal. Patientez jusqu'à ce qu'ESET SysInspector ait terminé (l'état du journal s'affiche en tant que créé) avant d'accéder au journal.
- **Supprimer** – Supprime le journal sélectionné.
- **Supprimer tout** – Supprime tous les journaux.
- **Exporter...** – Exporte le journal dans un fichier .xml ou un fichier .xml compressé.

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.

Il existe trois possibilités :

Option 1 : activer le système de réputation ESET LiveGrid®

Le système de réputation ESET LiveGrid® permet la mise en liste blanche et en liste noire dans 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®.

Option 2 : activer le 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 un échantillon ou une copie du fichier dans lequel la menace est apparue, le chemin et le nom du fichier, la date et l'heure, le processus par lequel la menace est apparue sur votre ordinateur et des informations sur le système d'exploitation de votre ordinateur.

Par défaut, ESET Endpoint 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.

Option 3 : choisir de ne pas activer ESET LiveGrid®

Vous ne perdez rien de la fonctionnalité du logiciel, mais ESET Endpoint Antivirus peut répondre dans certains cas plus rapidement aux nouvelles menaces que la mise à jour du moteur de détection lorsque l'option ESET LiveGrid® est activée.

Informations connexes

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

Configuration de la protection dans le cloud dans les configurations avancées

Pour accéder aux configurations d'ESET LiveGrid®, appuyez sur **F5** pour accéder aux Configurations avancées, puis développez **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.

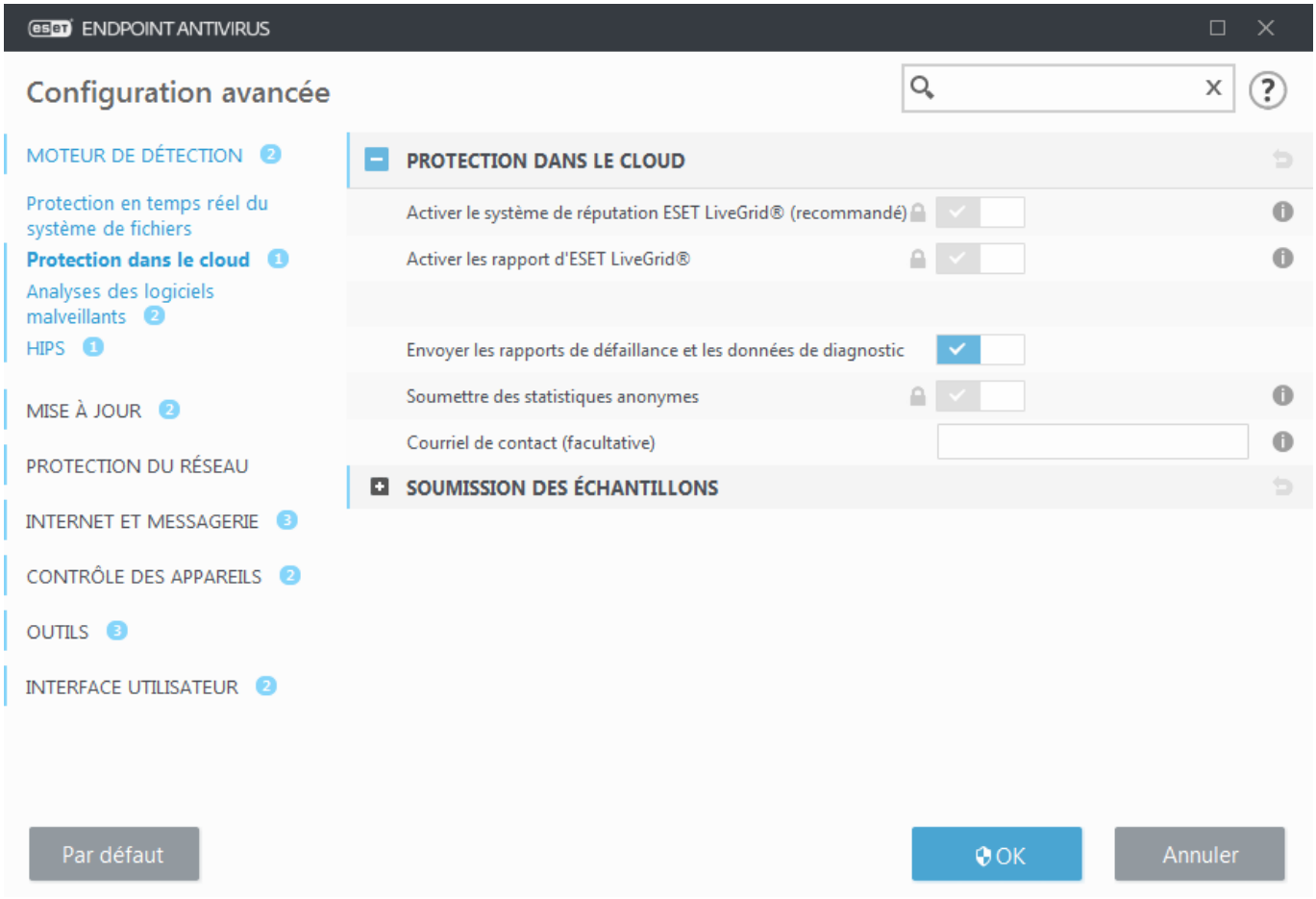
Activer le système de réputation ESET LiveGrid® – Envoie les données pertinentes de soumission (décrites dans la section **Soumission des échantillons** ci-dessous) ainsi que les rapports de défaillance et les statistiques au laboratoire de recherche ESET pour une analyse plus approfondie.

Activer ESET Dynamic Threat Defense (non visible dans ESET Endpoint Antivirus) – ESET Dynamic Threat Defense est un service payant fourni par ESET. Il est destiné à ajouter une couche de protection spécifiquement conçue pour limiter les nouvelles menaces. Les fichiers suspects sont automatiquement soumis au cloud ESET. Dans le cloud, ils sont analysés par nos moteurs avancés de détection des logiciels malveillants. L'utilisateur qui a fourni l'échantillon reçoit un rapport de comportement qui offre une synthèse du comportement de l'échantillon observé.

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 automatique des échantillons infectés

Sélectionnez quels échantillons seront soumis à ESET pour analyse afin d'améliorer les prochaines détections. Les options suivantes sont disponibles :

- **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 au cas où le moteur de détection ne les aurait 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 ESET Endpoint Antivirus modules de protection.

- **Exécutables** – Comprend les fichiers suivants : .exe, .dll, .sys etc.
- **Archives** – Comprend les fichiers suivants : .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Scripts** – Comprend les fichiers 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 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 certains fichiers/dossiers de la soumission (par exemple, il peut être utile d'exclure des fichiers qui peuvent comporter des informations confidentielles, telles que des documents ou des feuilles de calcul). Les fichiers de la liste ne seront jamais envoyés aux laboratoires d'ESET pour analyse, même s'ils contiennent un code suspect. Les fichiers les plus ordinaires sont exclus par défaut (.doc, etc.). Vous pouvez ajouter des fichiers à la liste des fichiers exclus si vous le souhaitez.

ESET Dynamic Threat Defense

Pour activer le service ESET Dynamic Threat Defense sur un ordinateur client à l'aide de la console web ESMC Web Console, consultez la configuration EDTD pour ESET Endpoint Antivirus.

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.

Filtre d'exclusion pour la protection dans le cloud

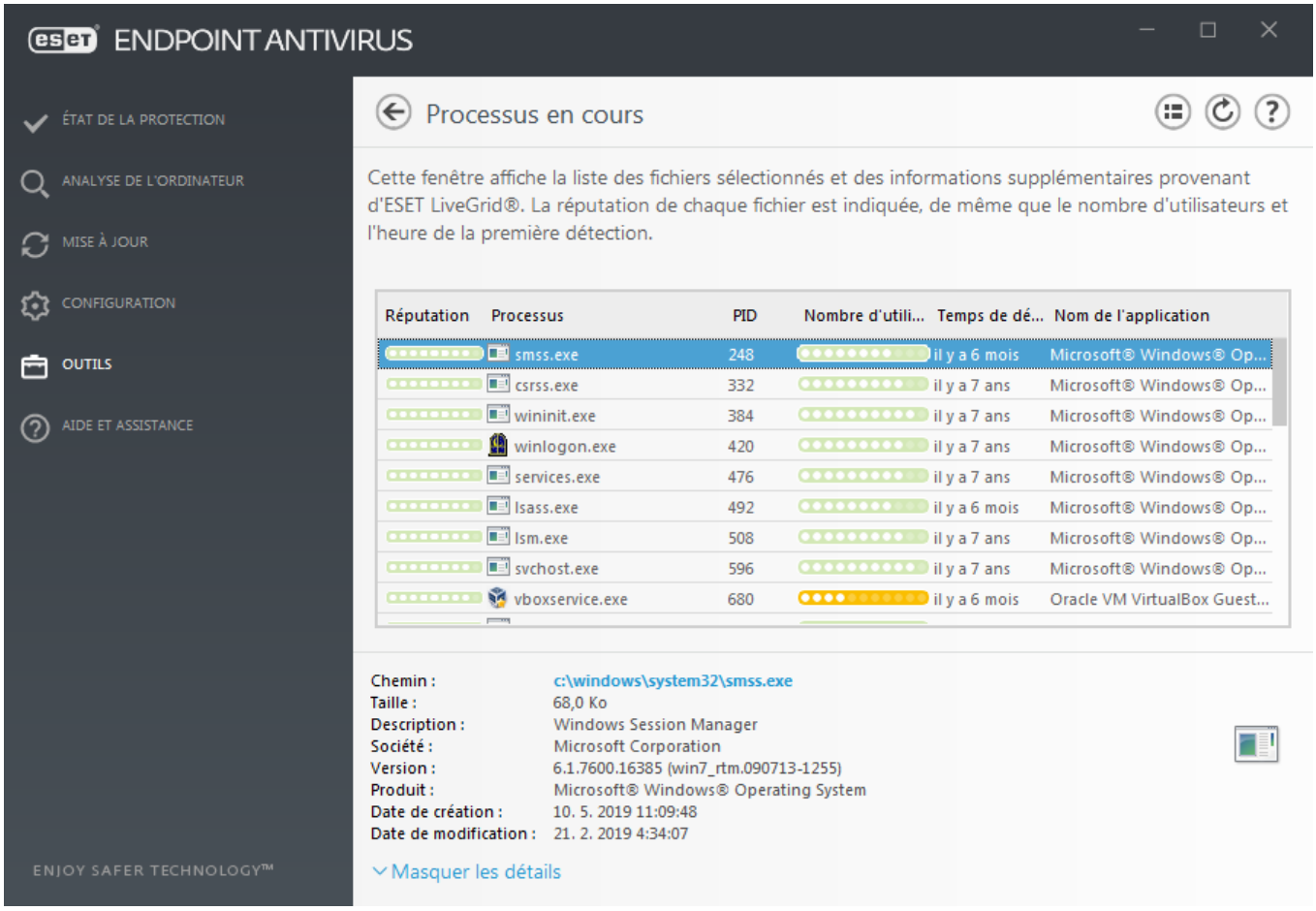
Le filtre d'exclusion permet d'exclure certains fichiers ou dossiers de la soumission d'échantillons. Les fichiers de la liste ne seront jamais envoyés aux laboratoires d'ESET pour analyse, même s'ils contiennent un code suspect. Les types de fichiers courants (tels que .doc, etc.) sont exclus par défaut.

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

Processus en cours

Les processus en cours affichent les programmes ou processus en cours d'exécution sur votre ordinateur et informe ESET immédiatement et en permanence de l'existence de nouvelles infiltrations. ESET Endpoint 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 Endpoint 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 9 – OK (vert) à 0 – Risqué (rouge).

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

PID – ID des processus en cours d'exécution dans les systèmes d'exploitation Windows.

> **Remarque**
> Les applications connues marquées en vert sont saines (répertoriées dans la liste blanche) et sont exclues de l'analyse, ce qui améliore la vitesse de l'analyse d'ordinateur à la demande ou de la protection en temps réel du système de fichiers de votre ordinateur.

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®.

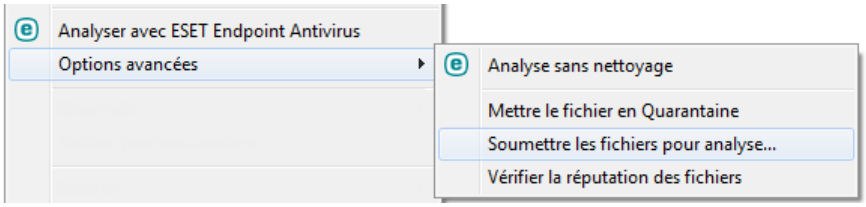
> **Remarque**
> Une application marquée avec le niveau de sécurité Inconnu (orange) n'est pas nécessairement un logiciel malveillant. Il s'agit généralement d'une nouvelle application. Vous pouvez soumettre un fichier pour analyse au laboratoire ESET si ce fichier vous semble suspect. Si le fichier s'avère être une application malveillante, sa détection sera ajoutée à l'une des prochaines mises à jour du moteur de détection.

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

Lorsque vous cliquez sur une application située au bas de la fenêtre, les informations suivantes apparaissent dans la partie inférieure de la fenêtre :

- **Chemin** – Emplacement de l'application sur l'ordinateur.
- **Taille** – Taille du fichier en Ko (kilo-octets) ou Mo (méga-octets).
- **Description** – Caractéristiques du fichier basées sur sa description du système d'exploitation.
- **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 et heure de création d'une application.
- **Date de modification** – Date et heure de dernière modification d'une application.

> **Remarque**
> La réputation peut également être vérifiée sur des fichiers qui n'agissent pas en tant que programmes/processus en cours - Marquez les fichiers que vous souhaitez vérifier, cliquez dessus avec le bouton droit et, dans le menu contextuel, sélectionnez **Options avancées** > **Évaluer la réputation des fichiers à l'aide de ESET LiveGrid®**.



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 vérifiés – 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.

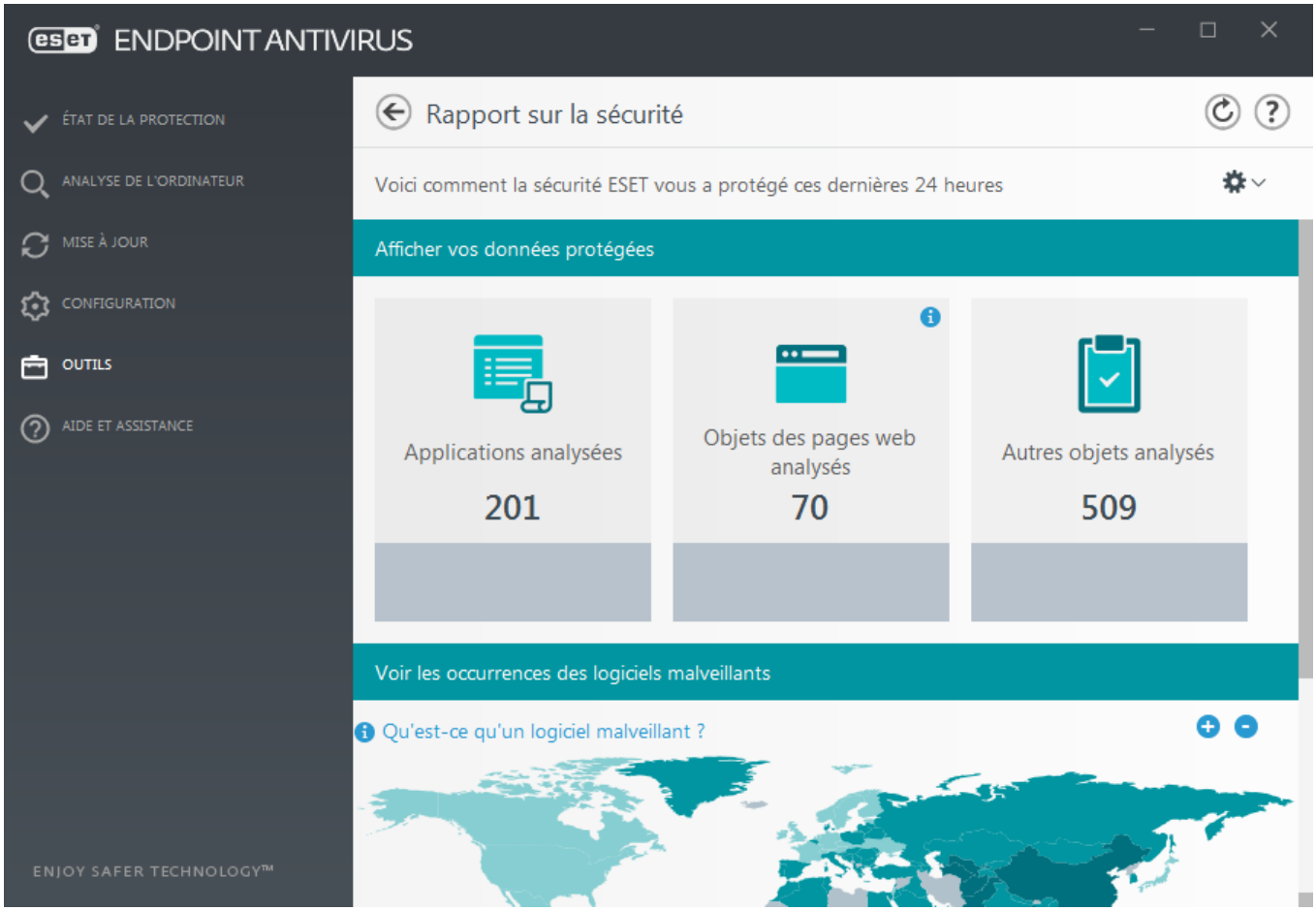
Objets des pages Web analysés – Indique le nombre d'objets de pages Web analysés.

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.

En dessous des catégories, vous pouvez consulter la situation virale actuelle sur la carte du monde. La présence de virus dans chaque pays est indiquée par une couleur (plus la couleur est foncée, plus le nombre de virus est élevé). Les pays sans données sont grisés. Placez la souris sur un pays pour afficher les données de celui-ci. Vous pouvez sélectionner un continent spécifique pour qu'un zoom soit automatiquement effectué.

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 Endpoint 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** > **Interface utilisateur** > **Alertes et boîtes de message** > **Messages de confirmation**.

ESET SysRescue Live

ESET SysRescue Live est un utilitaire gratuit qui permet de créer un CD/DVD ou un lecteur USB de secours amorçable. Vous pouvez démarrer un ordinateur infecté à partir de votre support de secours pour rechercher des logiciels malveillants et nettoyer les fichiers infectés.

Le principal avantage d'ESET SysRescue Live réside dans le fait que la solution est exécutée indépendamment du système d'exploitation hôte, tout en ayant un accès direct au disque et au système de fichiers. Il est par conséquent possible de supprimer les menaces qui ne pourraient normalement pas être supprimées, (par exemple lorsque le système d'exploitation est en cours d'exécution, etc.).

- Aide en ligne d'ESET SysRescue Live

Soumission d'échantillons pour analyse

Si vous trouvez un fichier au comportement suspect sur votre ordinateur ou un site suspect sur Internet, vous pouvez le soumettre au laboratoire de recherche d'ESET pour analyse.

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).

La soumission d'échantillon permet d'envoyer un fichier ou un site à ESET pour analyse à l'aide de l'une des méthodes suivantes :

1. La boîte de dialogue de soumission d'échantillon se trouve dans **Outils** > **Soumettre un échantillon pour analyse**.

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

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

Lorsque la boîte de dialogue **Sélectionner un échantillon pour analyse** est ouverte, sélectionnez dans le menu déroulant **Motif de soumission de l'échantillon** la description correspondant le mieux à votre message :

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

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

Adresse de contact : l'adresse de contact est envoyée à ESET avec les fichiers suspects. Elle pourra servir à vous contacter si des informations complémentaires sont nécessaires à l'analyse. La spécification d'une adresse de contact est facultative. 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 processus d'identification du fichier suspect.

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

- **Hameçonnage** : 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 site d'escroquerie ou 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 : saisissez éventuellement 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.

> **Remarque**
> 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 fichier 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.

Notifications

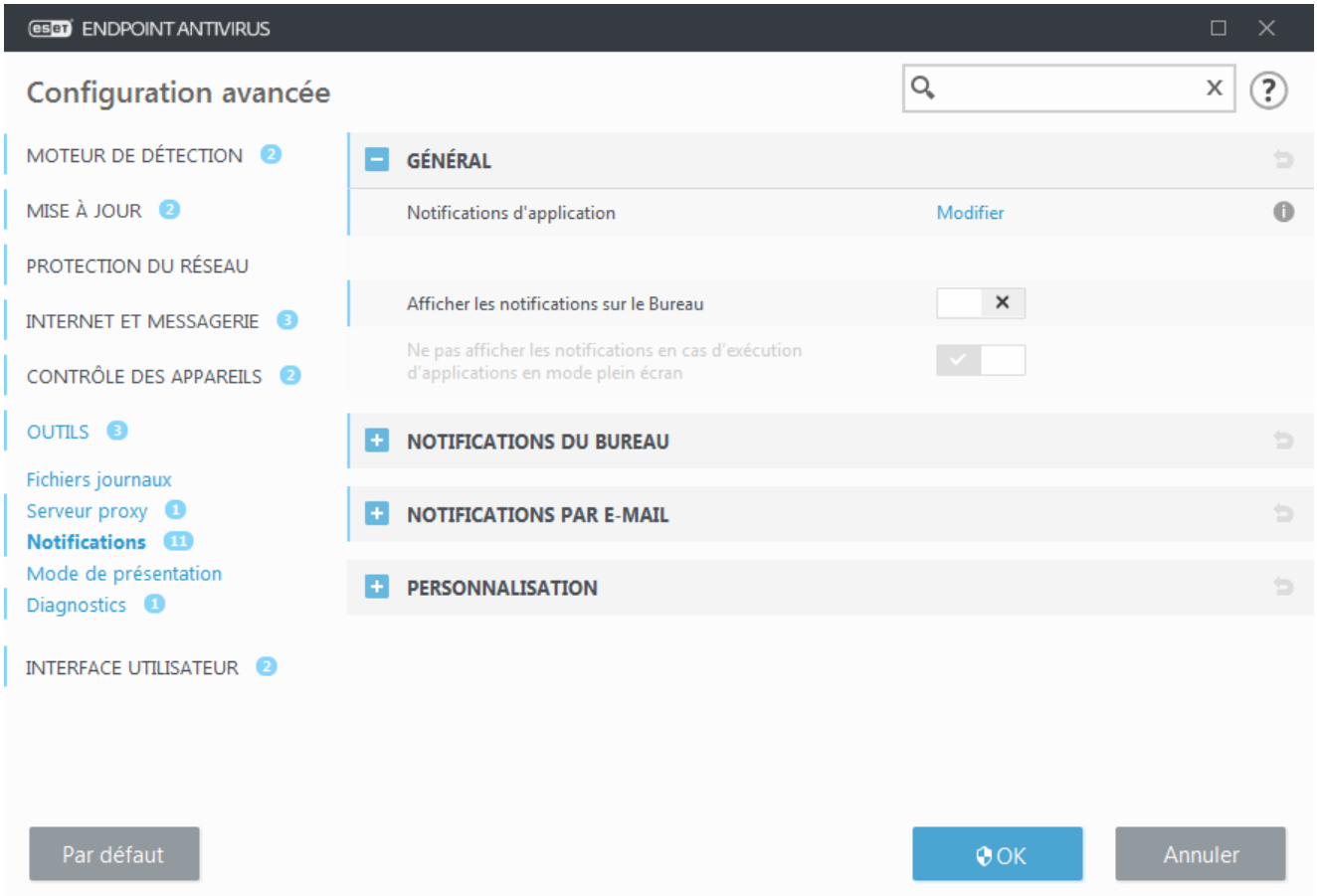
Pour gérer la manière dont ESET Endpoint Antivirus communique les événements aux utilisateurs, accédez à **Configurations avancées (F5)** > **Outils** > **Notifications**. Cette fenêtre de configuration permet de définir les types de notifications suivants :

- Notifications d'application : s'affichent directement dans la fenêtre principale du programme.
- Notifications du Bureau : s'affichent sous la forme d'une petite fenêtre contextuelle en regard de la barre des tâches système.
- Notifications par e-mail : sont envoyées à l'adresse e-mail indiquée.
- Personnalisation des notifications : permet d'ajouter un message personnalisé à une notification du bureau, par exemple.

Dans la section **Général**, utilisez les boutons bascule correspondants pour régler les options suivantes :

Bouton bascule	Par défaut	Description
Afficher les notifications sur le Bureau	✓	Désactivez cette option pour masquer les notifications contextuelles en regard de la barre des tâches système. Il est recommandé de laisser cette option activée afin que le produit puisse vous informer lorsqu'un nouvel événement se produit.
Ne pas afficher les notifications en cas...	✓	Conservez l'option **Ne pas afficher les notifications en cas d'exécution d'applications en mode plein écran** activée pour supprimer toutes les notifications qui ne sont pas interactives.
Afficher les notifications des rapports de sécurité	×	Activez cette option pour recevoir une notification lorsqu'une nouvelle version durapport de sécurité est générée.
Afficher la notification de réussite de la mise à jour	×	Activez cette option pour recevoir une notification lorsque le produit met à jour ses composants et les modules du moteur de détection.
Envoyer des notifications d'événement par e-mail	×	Activez cette option pour recevoir des notifications par e-mail.

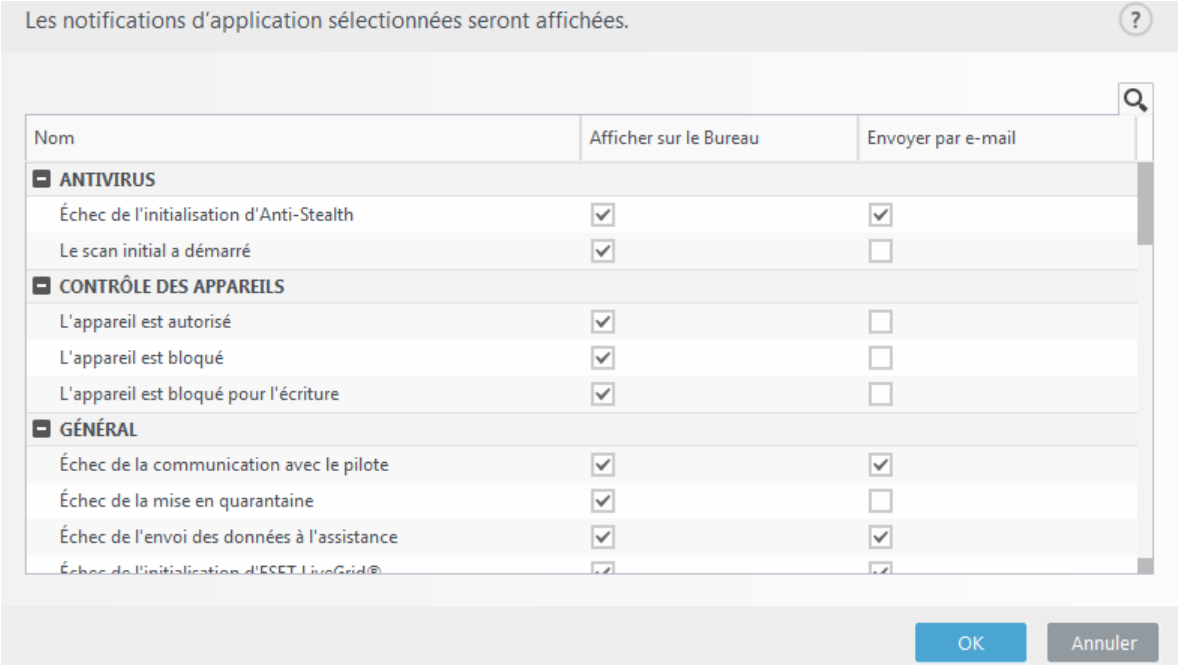
Pour activer ou désactiver des notifications d'application spécifiques, cliquez sur **Modifier** en regard de l'option **Notifications d'application**.



Notifications d'application

Pour régler la visibilité des notifications d'application (affichées en bas à droite de l'écran), accédez à **Outils** > **Notifications** > **Général** > **Notifications d'application** dans l'arborescence Configurations avancées d'ESET Endpoint Antivirus.

La liste des notifications est divisée en trois colonnes. Les noms des notifications sont triés par catégories dans la première colonne. Pour modifier la façon dont le produit informe des nouveaux événements d'application, cochez les cases correspondantes dans les colonnes **Afficher sur le bureau** et **Envoyer par e-mail**.



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** > **Outils** > **Notifications**.

Pour définir le format des e-mails et configurer les paramètres du serveur SMTP, accédez à Notifications par e-mail dans **Configuration avancée** > **Outils** > **Notifications**.

Notifications du Bureau

Une notification du bureau est une petite fenêtre contextuelle située à côté de la barre des tâches système. Par défaut, elle est configurée pour s'afficher pendant 10 secondes et disparaître lentement. C'est la méthode principale utilisée par ESET Endpoint Antivirus pour communiquer avec l'utilisateur, en l'avertissant des mises à jour réussies du produit, des nouveaux appareils connectés, de l'achèvement des analyses antivirus ou de la découverte de nouvelles menaces.

La section **Notifications du Bureau** permet de personnaliser le comportement des notifications contextuelles. Les attributs suivants peuvent être définis :

Durée – Définit la durée pendant laquelle le message de notification est visible. La valeur doit être comprise entre 3 et 30 secondes.

Transparence – Définit la transparence du message de notification en pourcentage. La plage prise en charge est comprise entre 0 (pas de transparence) et 80 (transparence très élevée).

Verbosité minimale des événements à afficher – Dans le menu déroulant, vous pouvez sélectionner le niveau de gravité de départ des notifications à afficher :

- **Diagnostic** – Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** – Enregistre tous les messages d'information (les événements réseau non standard, par exemple), y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.

• **Avertissements** – Enregistre les erreurs critiques et les messages d'avertissement (Anti-Stealth ne s'exécute pas correctement ou une mise à jour a échoué).

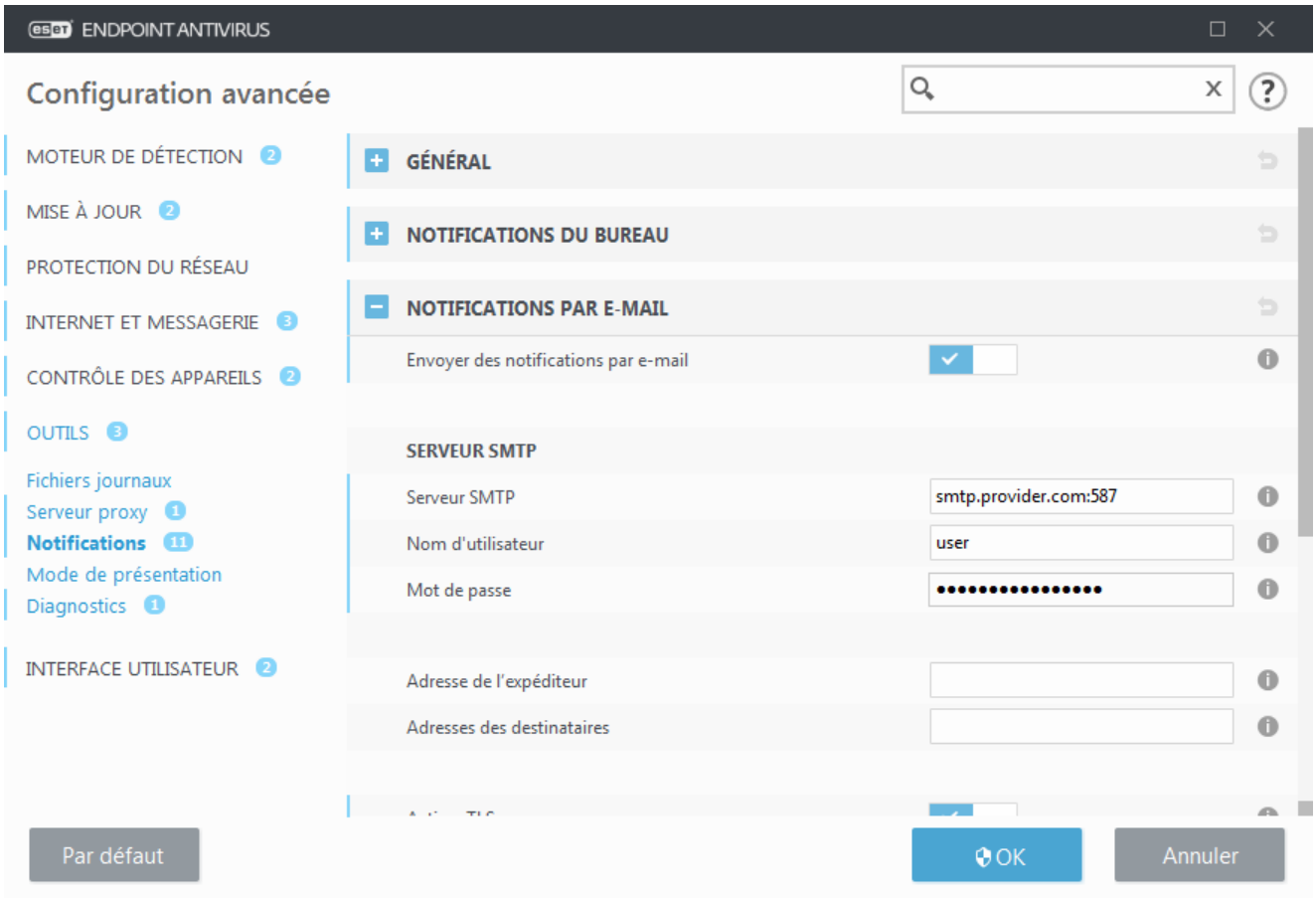
• **Erreurs** – Enregistre les erreurs (la protection des documents n'a pas démarré) et les erreurs critiques.

• **Critique** – Consigne uniquement les erreurs critiques (erreur de démarrage de la protection antivirus ou système infecté.).

Sur les systèmes multi-utilisateurs, afficher les notifications sur l'écran de l'utilisateur suivant – Saisissez les noms complets des comptes des utilisateurs autorisés à recevoir des notifications sur le bureau (lorsque vous utilisez votre ordinateur avec un autre compte que le compte administrateur et que vous souhaitez continuer à être informé des nouveaux événements du produit, par exemple).

Notifications par e-mail

ESET Endpoint Antivirus peut automatiquement envoyer des e-mails de notification si un événement avec le niveau de verbosité sélectionné se produit. Dans la section **Général**, activez l'option **Envoyer des notifications d'événement par e-mail** pour activer les notifications par e-mail.



Serveur SMTP

Serveur SMTP – Serveur SMTP utilisé pour envoyer des notifications (*smtp.fournisseur.com:587*, le port prédéfini est le port 25).

> **Remarque**
> Les serveurs SMTP avec chiffrement TLS sont pris en charge par ESET Endpoint 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.

Adresse de l'expéditeur – Ce champ spécifie l'adresse de l'expéditeur qui apparaît dans l'en-tête des notifications.

Adresses du destinataire – Ce champ spécifie les adresses du destinataire qui apparaissent dans l'en-tête des notifications. Utilisez un point-virgule (« ; ») pour séparer plusieurs adresses électroniques.

Activer TLS – Permet d'activer l'envoi de messages d'alerte et de notification pris en charge par le chiffrement TLS.

Configurations des e-mails

Dans le menu déroulant **Verbosité minimale des notifications**, vous pouvez sélectionner le niveau de gravité de départ des notifications à envoyer.

- **Diagnostic** – Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** – Enregistre tous les messages d'information (les événements réseau non standard, par exemple), y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissements** – Enregistre les erreurs critiques et les messages d'avertissement (Anti-Stealth ne s'exécute pas correctement ou une mise à jour a échoué).
- **Erreurs** – Enregistre les erreurs (la protection des documents n'a pas démarré) et les erreurs critiques.
- **Critique** – Consigne uniquement les erreurs critiques (erreur de démarrage de la protection antivirus ou système infecté.).

Envoyer chaque notification dans un e-mail séparé – Lorsque cette option est activée, le destinataire recevra un nouvel e-mail pour chaque notification spécifique. Cela peut se traduire par la réception d'un nombre important d'e-mails dans une courte période de temps.

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.

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. Il est déconseillé de modifier ce format. Toutefois, dans certaines circonstances (par exemple, si vous avez un système automatisé de traitement des messages), vous serez peut-être amené à modifier le format des messages.

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).

Les mots-clés (chaînes entourées de signes %) sont remplacés dans le message par les informations réelles spécifiées. Les mots-clés suivants sont disponibles :

- **%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.

Personnalisation des notifications

Cette fenêtre vous permet de personnaliser les messages utilisés dans les notifications.

Message de notification par défaut : message par défaut à afficher dans le pied de page de la notification.

Menaces

Activez l'option **Ne pas fermer automatiquement les notifications de logiciels malveillants** pour que ces notifications restent affichées à l'écran jusqu'à ce qu'elles soient fermées manuellement.

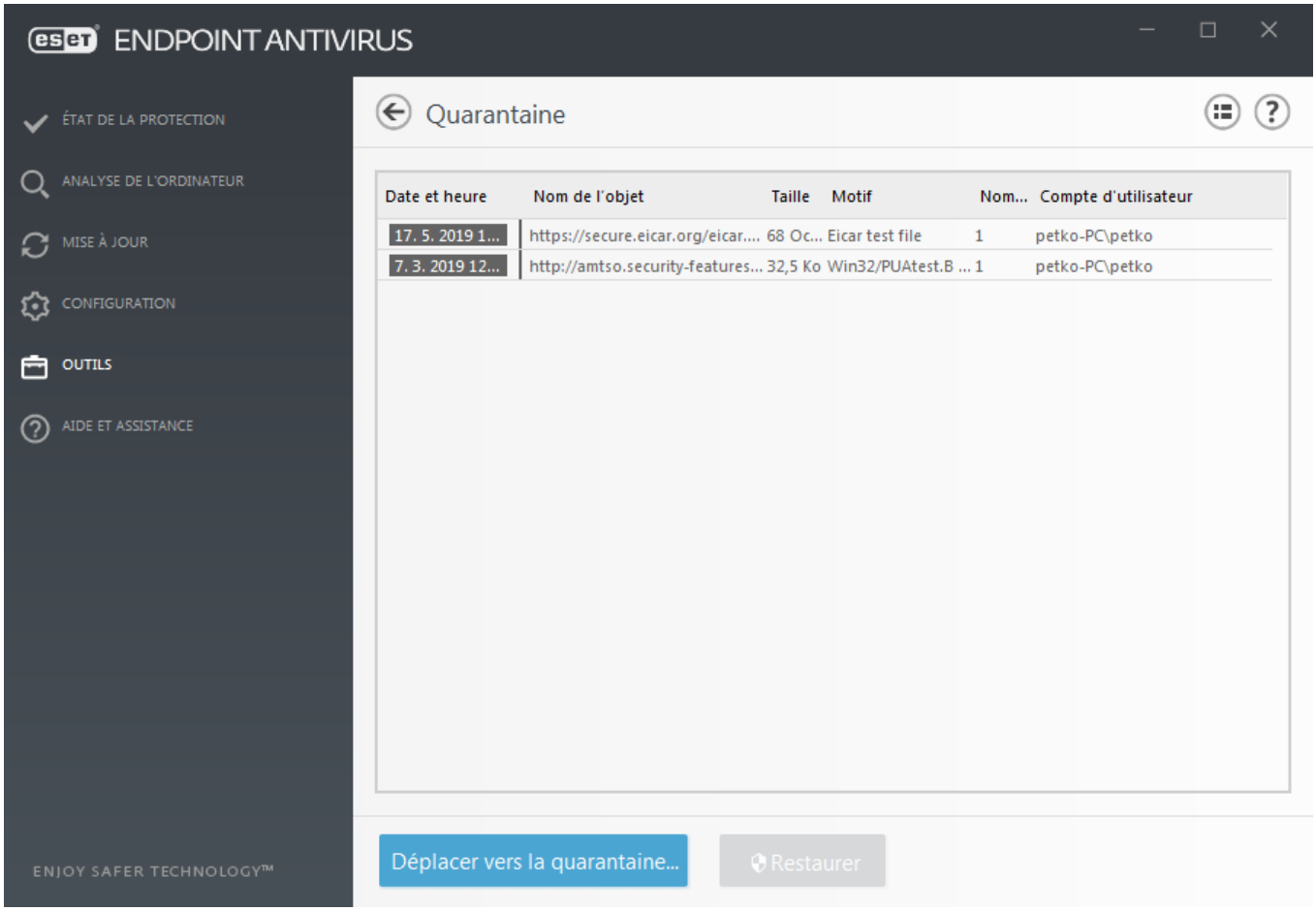
Désactivez l'option **Utiliser le message par défaut** et saisissez votre message dans le champ **Message de notification de menace** pour utiliser des messages de notification personnalisés.

Quarantaine

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

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

Vous pouvez choisir de mettre n'importe quel fichier en quarantaine ou vous pouvez utiliser la fonctionnalité de mise en quarantaine par glisser-déposer pour mettre manuellement en quarantaine un fichier 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. Cette action est conseillée si un fichier se comporte de façon suspecte, mais n'a pas été détecté par le scanner antivirus. Les fichiers en quarantaine peuvent être soumis pour analyse au laboratoire de recherche d'ESET.



Les fichiers du dossier de quarantaine peuvent être visualisés dans un tableau qui affiche la date et l'heure de mise en quarantaine, le chemin d'accès à l'emplacement d'origine du fichier infecté, sa taille en octets, la raison (par exemple, objet ajouté par l'utilisateur) et le nombre de détections.

Mise en quarantaine de fichiers

ESET Endpoint Antivirus met automatiquement les fichiers supprimés en quarantaine (si vous n'avez pas désactivé cette option dans la fenêtre d'alerte). Au besoin, vous pouvez mettre manuellement en quarantaine tout fichier suspect en cliquant sur **Déplacer vers la quarantaine.** Le fichier d'origine est supprimé de son emplacement initial. Il est également possible d'utiliser le menu contextuel à cette fin : cliquez avec le bouton droit dans la fenêtre **Quarantaine** et sélectionnez l'option **Mettre le fichier en quarantaine**.

Restoring from Quarantine

Les fichiers mis en quarantaine peuvent aussi être restaurés à leur emplacement d'origine. Pour restaurer un fichier en quarantaine, cliquez avec le bouton droit dessus dans la fenêtre Quarantaine, puis sélectionnez **Restaurer** dans le menu contextuel. Si un fichier est marqué comme étant une application potentiellement indésirable, l'option **Restaurer et exclure de l'analyse est également disponible**. Le menu contextuel contient également l'option **Restaurer vers...** qui permet de restaurer des fichiers vers un emplacement autre que celui

d'origine dont ils ont été supprimés.

Suppression d'un élément en quarantaine – Cliquez avec le bouton droit sur un élément donné, puis sélectionnez **Supprimer l'élément en quarantaine.** Vous pouvez également sélectionner l'élément à supprimer, puis appuyer sur **Suppr** sur votre clavier. Vous pouvez aussi sélectionner plusieurs éléments et les supprimer simultanément.

Remarque
Si le programme met en quarantaine, par erreur, un fichier inoffensif, il convient de le restaurer, de l'exclure de l'analyse et de l'envoyer au support technique ESET.

Soumission de fichiers mis en quarantaine

Si vous avez mis en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été détecté par erreur comme une menace et placé en quarantaine, envoyez ce fichier au laboratoire d'ESET. Pour soumettre un fichier mis en quarantaine, cliquez avec le bouton droit sur le fichier et sélectionnez l'option **Soumettre le fichier pour analyse** dans le menu contextuel.

Configuration du serveur proxy

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

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

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

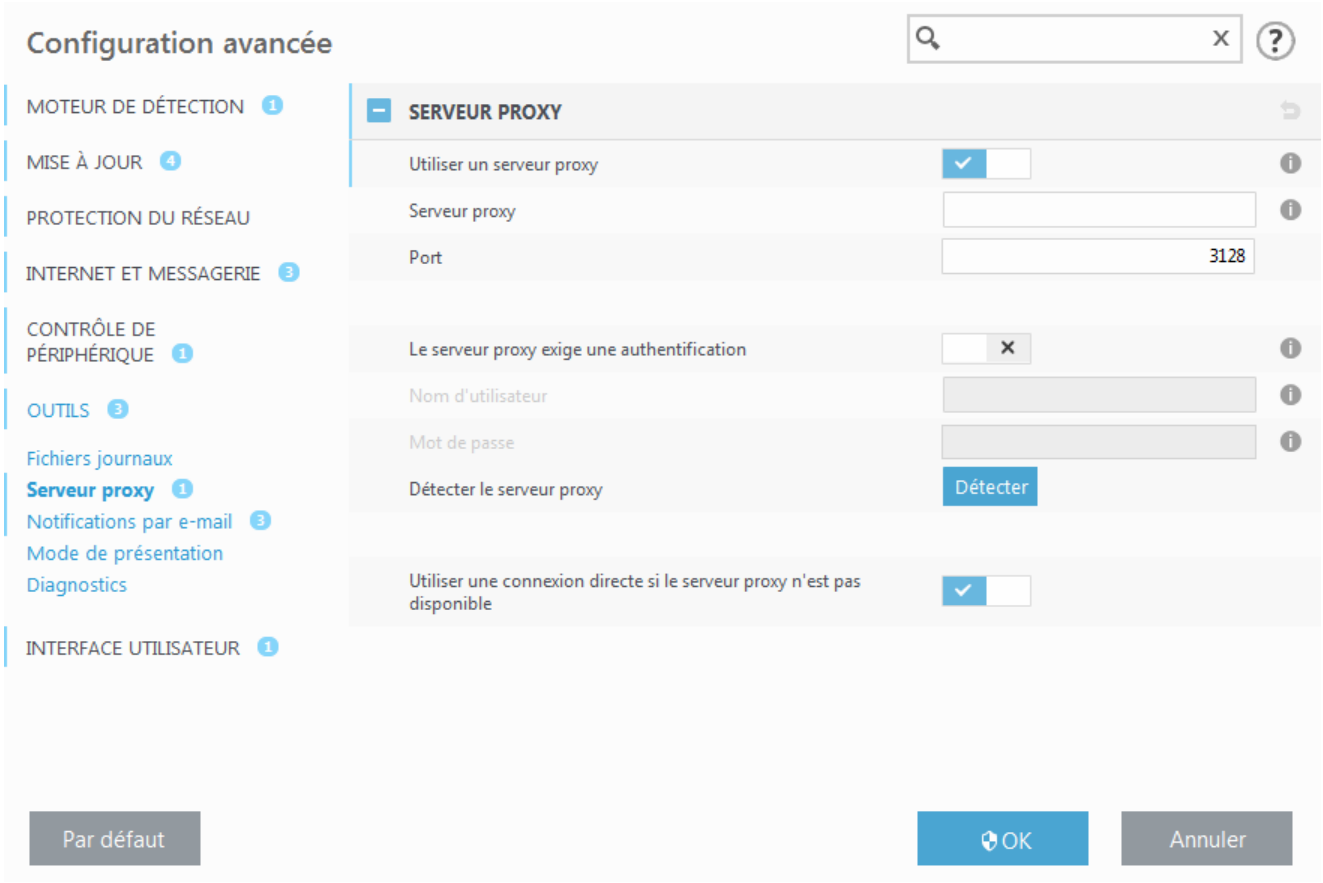
Si les communications avec le serveur proxy exigent une authentification, sélectionnez **Le serveur proxy nécessite une authentification** et entrez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants. Cliquez sur **Détecter** pour détecter et renseigner automatiquement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

Remarque
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 Endpoint Antivirus est configuré pour se connecter via le proxy et que ce dernier est injoignable, ESET Endpoint Antivirus ignore le proxy et communique directement avec les serveurs ESET.

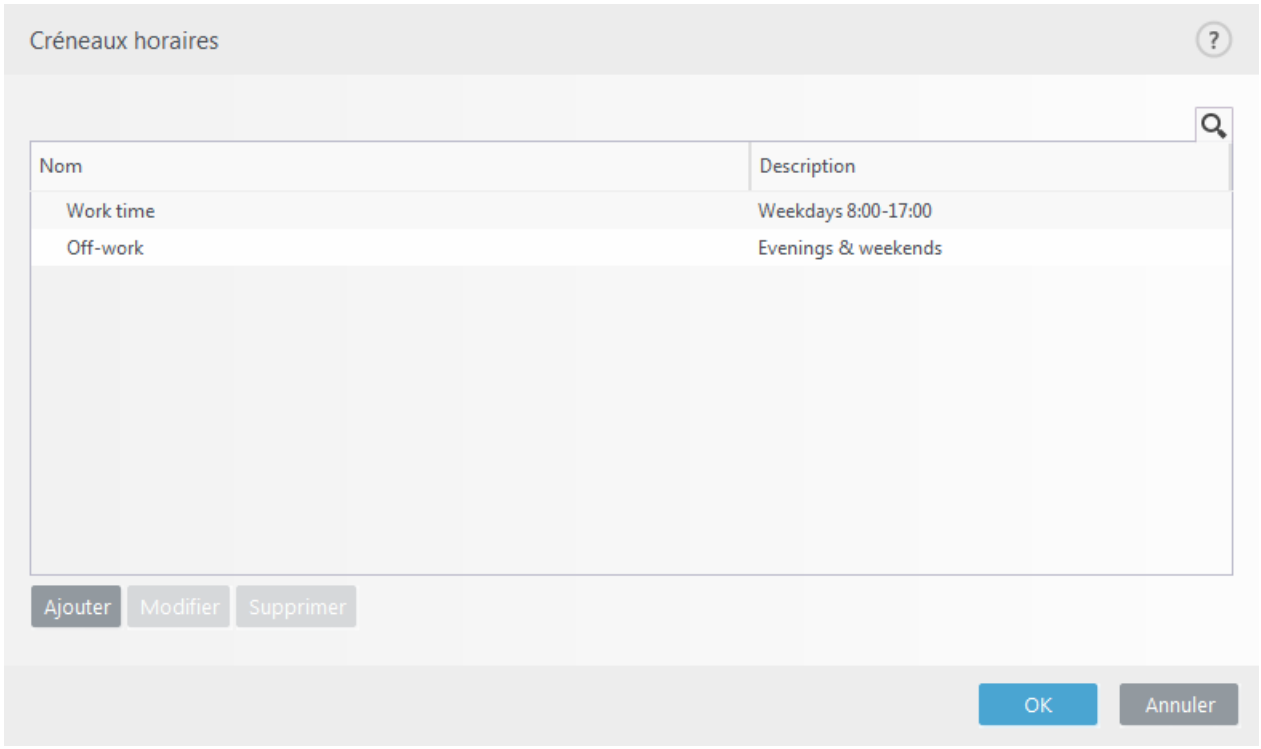
Les paramètres de serveur proxy peuvent également définis dans la configuration avancée des mises à jour (**Configuration avancée** > **Mise à jour** > **Profils** > **Mises à jour** > **Options de connexion** en sélectionnant

Connexion via un serveur proxy dans le menu déroulant **Mode proxy**). Ce paramètre s'applique au profil de mise à jour donné et est recommandé pour les ordinateurs portables, car il permet de recevoir les mises à jour du moteur de détection depuis des emplacements distants. Pour plus d'informations sur ce paramètre, consultez Configuration avancée des mises à jour.



Créneaux horaires

Les créneaux horaires peuvent être créés et ensuite affectés aux règles pour **Contrôle des appareils**. Le paramètre **Créneaux horaires** se trouve dans **Configurations avancées** > **Outils**. Il vous permet de définir les créneaux horaires fréquemment utilisés (par exemple, heures de bureau, week-end, etc.) et les réutiliser sans redéfinir les périodes pour chacune des règles. Les créneaux horaires peuvent s'appliquer à tout type de règle pertinent prenant en charge le contrôle temporel.



Pour créer un créneau horaire, procédez comme suit :

1. Cliquez sur **Modifier** > **Ajouter.**
2. Saisissez le nom et la **description** du créneau horaire et cliquez sur **Ajouter**.
3. Indiquez le jour et l'heure de début/fin du créneau horaire ou sélectionnez **Toute la journée**.
4. Cliquez sur **OK** pour confirmer.

Un créneau horaire peut être défini avec une ou plusieurs périodes basées sur des jours et des heures. Une fois créé, le créneau horaire apparaît dans le menu déroulant **Appliquer durant** dans la fenêtre de l'éditeur de règles de contrôle des appareils.

Microsoft Windows Update

La fonctionnalité Windows Update est un élément important de la protection des utilisateurs contre les logiciels malveillants. C'est pourquoi il est essentiel d'installer les mises à jour de Microsoft Windows dès qu'elles sont disponibles. ESET Endpoint Antivirus vous informe des mises à jour manquantes en fonction du niveau que vous spécifiez. Les niveaux suivants sont disponibles :

- **Pas de mise à jour** – Aucune mise à jour système n'est proposée au téléchargement.
- **Mises à jour optionnelles** – Les mises à jour marquées comme étant faiblement prioritaires et au-dessus sont proposées au téléchargement.
- **Mises à jour recommandées** – Les mises à jour marquées comme étant courantes et au-dessus sont proposées au téléchargement.
- **Mises à jour importantes** – Les mises à jour marquées comme étant importantes et au-dessus sont proposées au téléchargement.

- **Mises à jour critiques** – Seules les mises à jour critiques sont proposées pour le téléchargement.

Cliquez sur **OK** pour enregistrer les modifications. La fenêtre Mises à jour système s'affiche après la vérification de l'état à l'aide du serveur de mise à jour. C'est pourquoi les informations de mise à jour système ne sont peut-être pas immédiatement disponibles après l'enregistrement des modifications.

Intervalle de vérification des licences

ESET Endpoint Antivirus doit se connecter automatiquement aux serveurs ESET. Pour modifier cette configuration, accédez à **Configurations avancées (F5)** > **Outils** > **Licence**. Par défaut, l'option **Vérification de l'intervalle** est définie sur **Automatique** et le serveur de licences ESET vérifie plusieurs fois le produit par heure. En cas d'augmentation du trafic réseau, définissez les configurations sur **Limité** pour réduire la surcharge. Lorsque l'option **Limité** est sélectionnée, ESET Endpoint Antivirus ne vérifie le serveur de licences qu'une fois par jour ou au redémarrage de l'ordinateur.

Important
Si la configuration **Vérification de l'intervalle** est définie sur **Limité**, toutes les modifications associées aux licences effectuées via ESET Business Account/ESET MSP Administrator peuvent prendre jusqu'à un jour pour s'appliquer aux configurations d'ESET Endpoint Antivirus.

Interface utilisateur

La section **Interface utilisateur** permet de configurer le comportement de l'interface utilisateur graphique du programme (GUI).

Grâce à l'outil Éléments de l'interface utilisateur, vous pouvez ajuster l'apparence du programme et l'utilisation des effets.

Pour bénéficier de la sécurité maximum de votre logiciel de sécurité, vous pouvez empêcher toute modification non autorisée à l'aide de l'outil Configuration de l’accès.

En configurant Alertes et boîtes de message et Notifications, vous pouvez modifier le comportement des alertes concernant les détections et les notifications système. Ces alertes peuvent être personnalisées en fonction de vos besoins.

Si vous choisissez de ne pas afficher certaines notifications, ces dernières apparaissent dans **Éléments de l'interface utilisateur** > **États d'application**. Vous pouvez vérifier dans cette section leur état ou empêcher leur affichage.

L'intégration dans le menu contextuel s'affiche lorsque vous cliquez avec le bouton sur l'objet sélectionné. Utilisez cet outil pour intégrer les options ESET Endpoint Antivirus dans le menu contextuel.

Le mode de présentation est utile pour les utilisateurs qui souhaitent travailler dans une application sans être interrompus par des fenêtres contextuelles, des tâches planifiées et tout autre composant qui pourrait augmenter la charge du processeur et de la mémoire RAM.

Consultez également Comment limiter l'interface utilisateur d'ESET Endpoint Antivirus (utilise pour les environnements administrés).

Éléments de l'interface utilisateur

La configuration de l'interface utilisateur d'ESET Endpoint Antivirus peut être modifiée de manière à adapter l'environnement de travail à vos besoins. Ces options de configuration sont accessibles depuis la branche **Interface utilisateur** > **Éléments de l'interface utilisateur** de l'arborescence de la configuration avancée ESET Endpoint Antivirus.

Dans la section **Éléments de l'interface utilisateur**, vous pouvez ajuster l'environnement de travail. Utilisez le menu déroulant **Mode de démarrage** pour sélectionner un mode de démarrage de l'interface utilisateur graphique parmi les suivants :

Complet – L'intégralité de l'interface utilisateur graphique est affichée.

Minimal – L'interface utilisateur graphique est en cours d'exécution, mais seules les notifications sont affichées pour l'utilisateur.

Manuel – L'interface utilisateur graphique n'est pas démarrée automatiquement à la connexion. N'importe quel utilisateur peut la démarrer manuellement.

Silencieux – Les notifications et les alertes ne sont pas affichées. L'interface utilisateur graphique ne peut être démarrée que par l'administrateur. Dans les environnements administrés, ce mode peut s'avérer utilise lorsque vous devez préserver les ressources système.

> **Remarque**
> une fois le mode de démarrage Minimal sélectionné et l'ordinateur redémarré, les notifications s'affichent, mais pas l'interface graphique. Pour rétablir le mode complet, exécutez l'interface utilisateur graphique dans le menu Démarrer, **Tous les programmes** > **ESET** > ESET Endpoint Antivirus (en tant qu'administrateur). Vous pouvez également effectuer cette opération via ESET Security Management Center à l'aide d'une stratégie.

Pour désactiver l'écran de démarrage de ESET Endpoint Antivirus, désactivez **Afficher l'écran de démarrage**.

Pour qu'ESET Endpoint Antivirus émette un signal sonore en cas d'événement important lors d'une analyse, par exemple lorsqu'une menace est découverte ou lorsque l'analyse est terminée, sélectionnez **Utiliser un signal sonore**.

Intégrer dans le menu contextuel – Intègre les options ESET Endpoint Antivirus dans le menu contextuel.

États

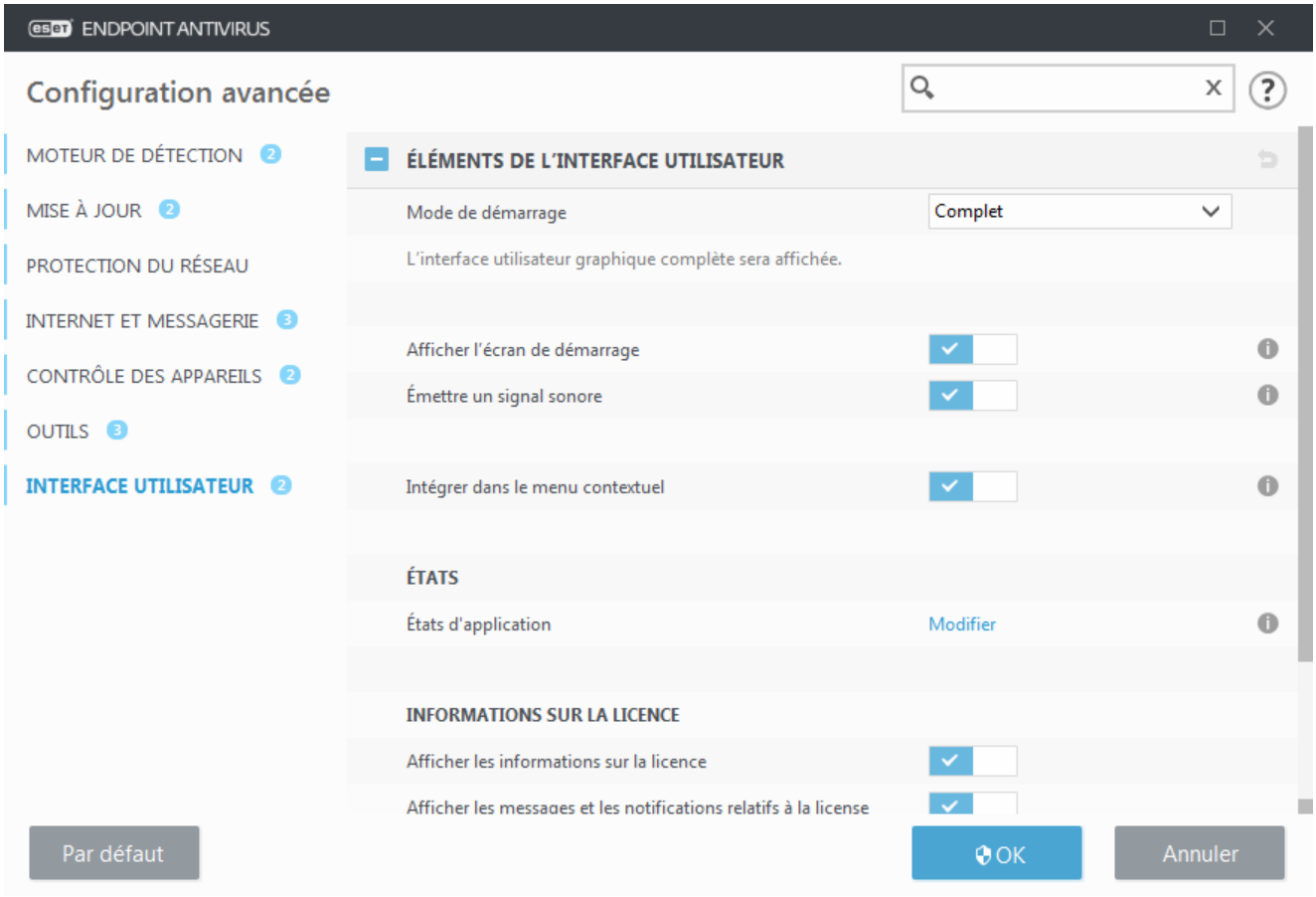
États d'application – Cliquez sur le bouton **Modifier** pour gérer (désactiver) les états affichés dans le volet **État de la protection** du menu principal.

Informations sur la licence

Afficher les informations sur la licence – Lorsque cette option est activée, la date d'expiration de la licence ne s'affiche pas dans les écrans **État de la protection** et **Aide et assistance**.

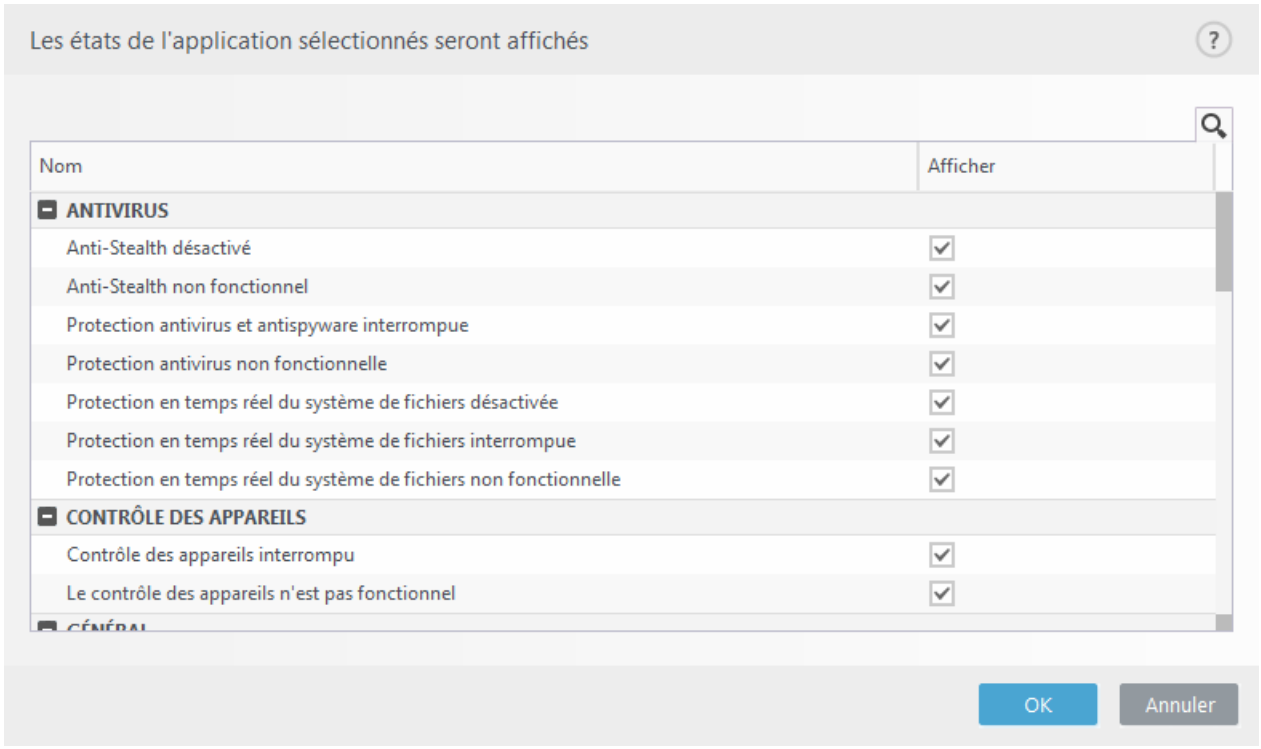
Afficher les messages et les notifications relatifs à la licence – Lorsque cette option est désactivée, les notifications et messages ne s'affichent que quand la licence arrive à expiration.

> **Remarque**
> Les paramètres d'informations sur la licence sont appliqués mais ne sont pas accessibles pour ESET Endpoint Antivirus activé à l'aide d'une licence MSP.



États d'application

Pour ajuster les états dans le produit dans le premier volet d'ESET Endpoint Antivirus, accédez à **Interface utilisateur** > **Éléments de l'interface utilisateur** > **États d'application** dans l'arborescence Configurations avancées d'ESET Endpoint Antivirus.



Activez ou désactivez les états d'application qui seront affichés ou non (par exemple, lorsque vous interrompez la protection antivirus et antispyware ou lorsque vous activez le mode de présentation). Un état d'application est également affiché si votre produit n'est pas activé ou si la licence est arrivée à expiration. Cette configuration peut être modifiée par le biais des politiques d'ESET Security Management Center.

Configuration de l'accès

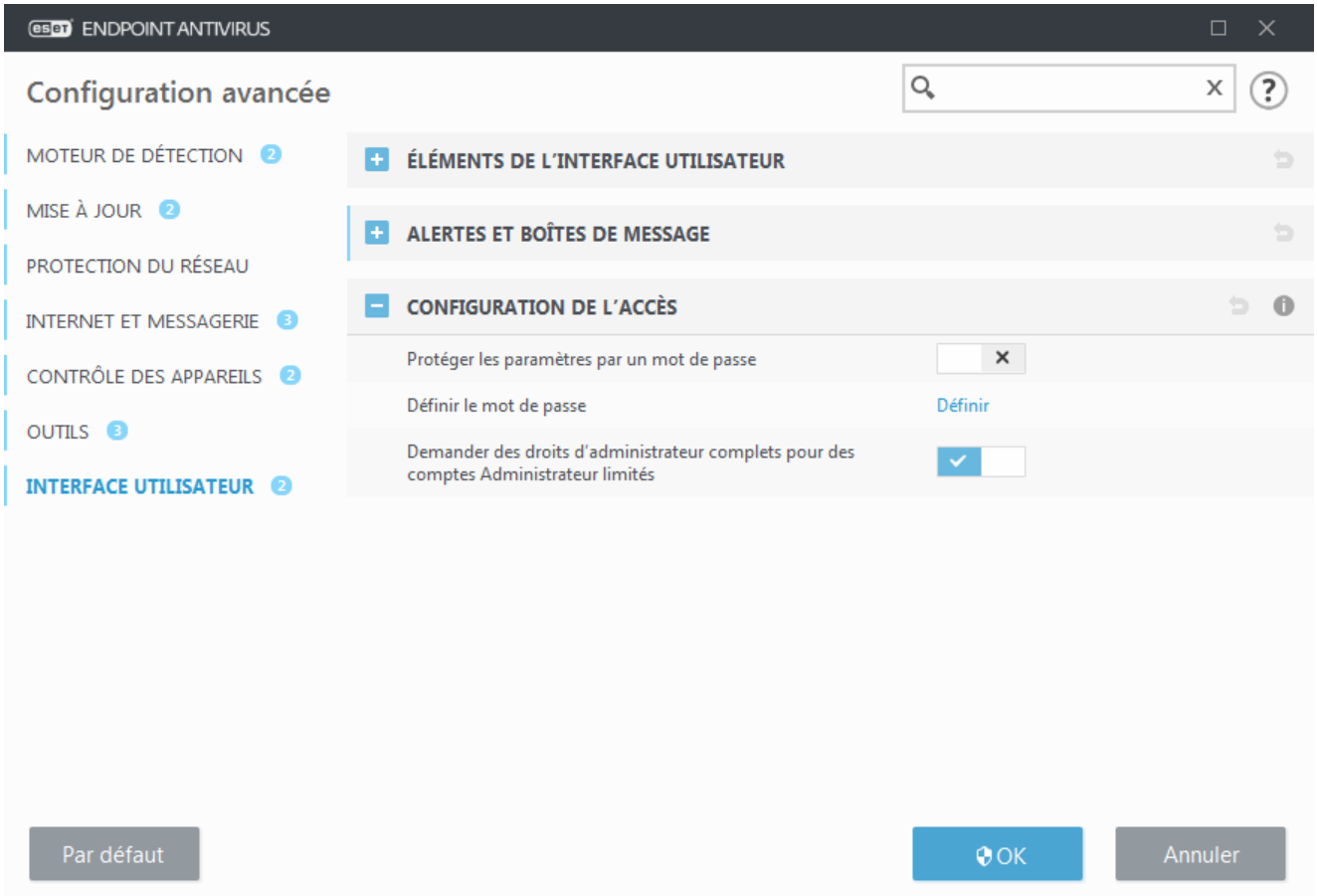
Il est essentiel que ESET Endpoint Antivirus soit correctement configuré pour garantir la sécurité maximale du système. Tout changement inapproprié peut entraîner la perte de données importantes. Pour éviter des modifications non autorisées, les paramètres de la configuration d'ESET Endpoint Antivirus peuvent être protégés par mot de passe.

Environnements gérés

L'administrateur peut créer une politique de façon à protéger les configurations de ESET Endpoint Antivirus par mot de passe sur les ordinateurs clients connectés. Pour créer une politique, consultez Configurations protégées par mot de passe.

Non géré

Les paramètres de configuration pour la protection par mot de passe sont situés dans **Configurations avancées** (F5) sous **Interface utilisateur** > **Configuration de l'accès**.



Protéger les paramètres par un mot de passe : indiquez les paramètres du mot de passe. Cliquez sur cette option pour ouvrir la fenêtre Configuration du mot de passe.

Pour définir ou modifier un mot de passe visant à protéger les paramètres de configuration, cliquez sur **Définir**.

Demander des droits d'administrateur complets pour des comptes Administrateur limités : conservez cette option active pour inviter l'utilisateur actuel (s'il ne possède pas les autorisations d'administrateur) à saisir le nom d'utilisateur et le mot de passe d'administrateur lors de la modification de certains paramètres du système (semblable au contrôle UAC dans Windows Vista). Elles portent également sur la désactivation des modules de protection.

Pour Windows XP uniquement :

Demander des droits d'administrateur (système sans prise en charge UAC) : activez cette option pour qu'ESET Endpoint Antivirus demande des informations d'identification d'administrateur.

Mot de passe des configurations avancées

Pour protéger les paramètres de configuration d'ESET Endpoint Antivirus afin d'éviter toute modification non autorisée, vous devez définir un nouveau mot de passe.

Environnements gérés

L'administrateur peut créer une politique de façon à protéger les configurations de ESET Endpoint Antivirus par mot de passe sur les ordinateurs clients connectés. Pour créer une politique, consultez Configurations protégées par mot de passe.

Non géré

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 sera nécessaire pour toute modification future de ESET Endpoint Antivirus.

Si vous oubliez votre mot de passe, l'accès aux configurations avancées peut être restauré.

- Restauration à l'aide de la méthode Restaurer le mot de passe (version 7.1 et versions ultérieures)
- Restauration à l'aide de l'outil ESET Unlock Tool (version 7.0 et versions antérieures)

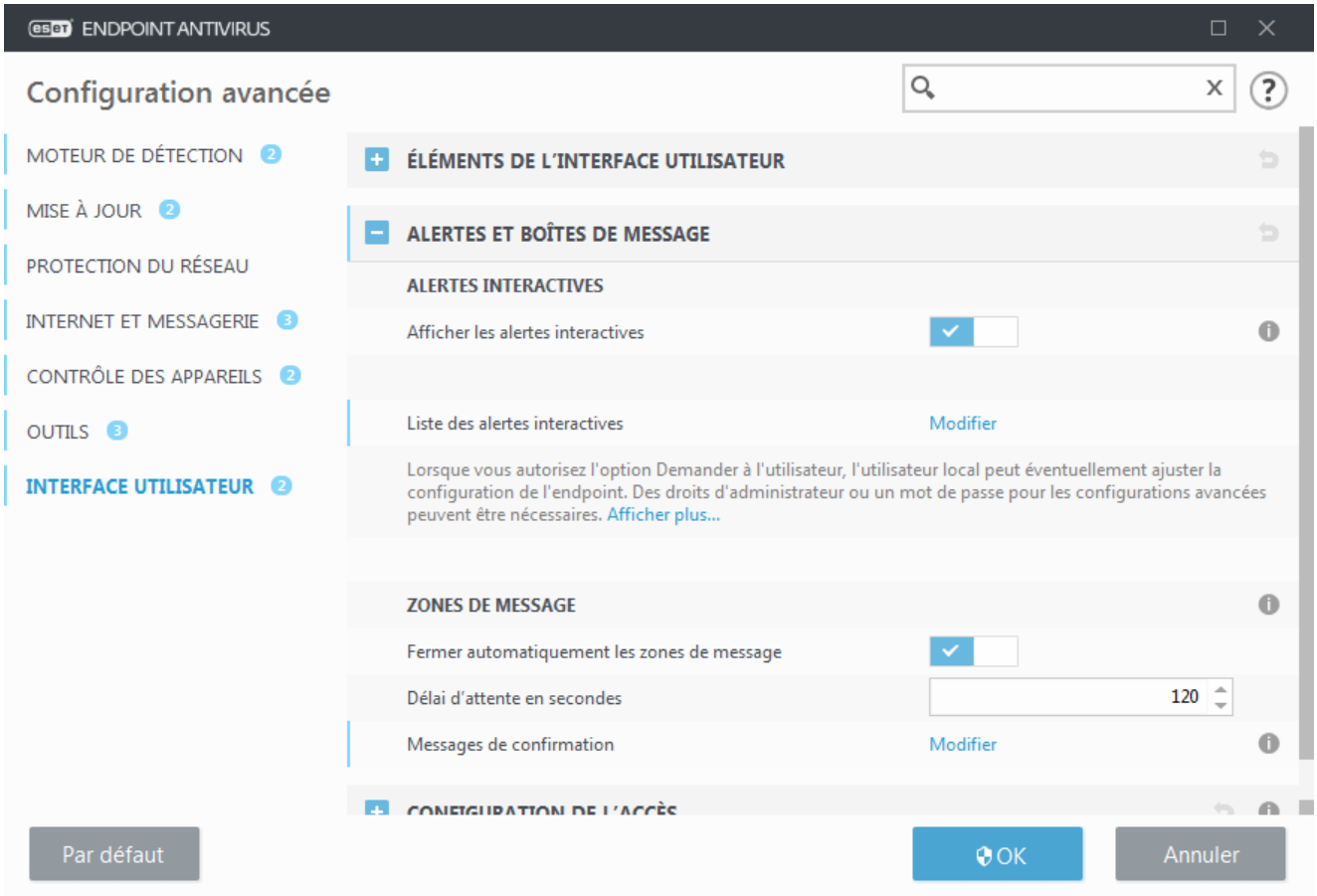
Cliquez ici si vous avez oublié votre clé de licence émise par ESET, la date d'expiration de votre licence ou d'autres informations relatives à la licence d'ESET Endpoint Antivirus.

Alertes et boîtes de message

Vous recherchez des informations sur les alertes et les notifications courantes ?

- Menace détectée
- L'adresse a été bloquée.
- Produit non activé
- 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 »
- « Fichier endommagé » ou « Impossible de renommer le fichier »
- Certificat du site Web révoqué
- Menace réseau bloquée

La section **Alertes et boîtes de message** (anciennement **Alertes et notifications**) sous **Interface utilisateur** vous permet de configurer la manière dont ESET Endpoint Antivirus traite les détections pour lesquelles une décision doit être prise par un utilisateur (par exemple, des sites web d'hameçonnage potentiels).



Alertes interactives

Les fenêtres des alertes interactives s'affichent si une détection a été effectuée ou si une intervention de l'utilisateur est nécessaire.

Afficher les alertes interactives

ESET Endpoint Antivirus version 7.2 et versions ultérieures :

- Pour les utilisateurs non gérés, il est recommandé de conserver le paramètre par défaut de cette option (activé).
- Pour les utilisateurs gérés, gardez ce paramètre activé et sélectionnez une action prédéfinie pour les utilisateurs dans la liste des alertes interactives.

La désactivation de l'option **Afficher les alertes interactives** entraîne le masquage des fenêtres d'alerte et des boîtes de dialogue dans le navigateur. Une action prédéfinie par défaut sera automatiquement sélectionnée (par exemple, « site web d'hameçonnage potentiel » sera bloqué).

ESET Endpoint Antivirus version 7.1 et versions antérieures :

Le nom de ce paramètre est **Afficher les alertes**. Il n'est pas possible de personnaliser des actions prédéfinies pour des fenêtres d'alerte interactives spécifiques.

Notifications du Bureau

Les notifications sur le bureau et les info-bulles sont fournies à titre d'information uniquement et n'exigent aucune interaction avec l'utilisateur. La section **Notifications du Bureau** a été déplacée sous **Outils** > **Notifications**

dans Configurations avancées (version 7.1 et ultérieure).

Zones de message

Pour fermer automatiquement les fenêtres d'alerte après un certain délai, sélectionnez **Fermer automatiquement les zones de message**. Si les fenêtres d'alerte ne sont pas fermées manuellement, le système les ferme automatiquement une fois le laps de temps écoulé.

Messages de confirmation – Affiche une liste de messages de confirmation que vous pouvez choisir d'afficher ou non.

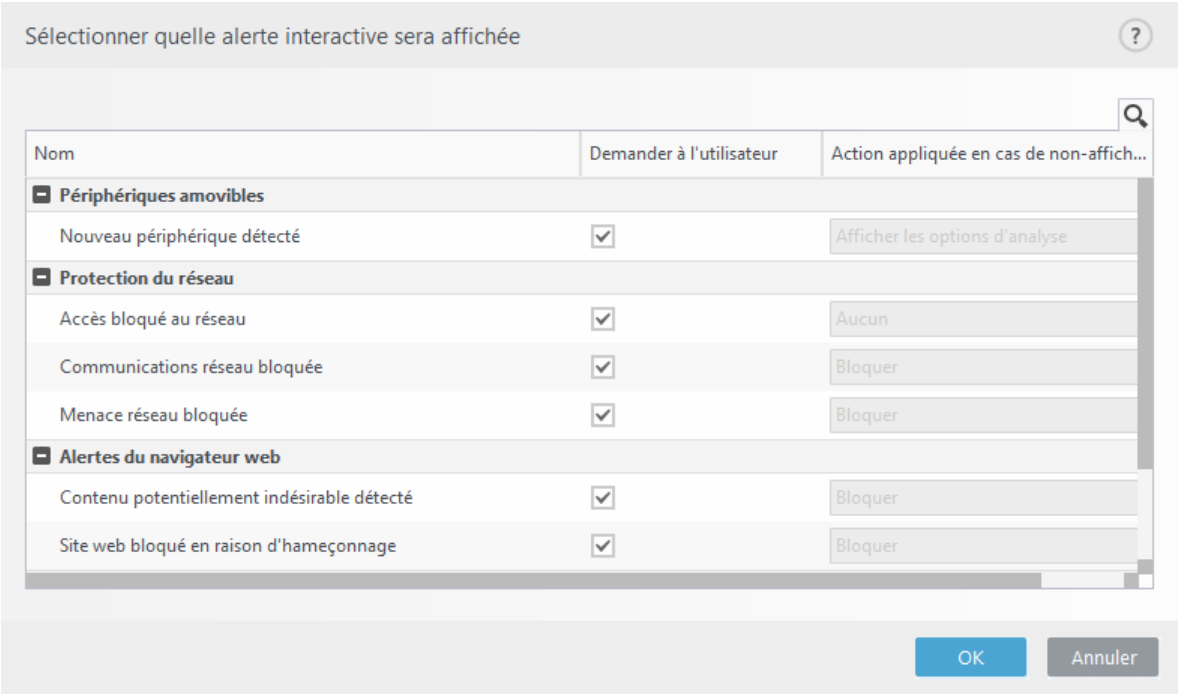
Alertes interactives

Cette section décrit plusieurs fenêtres d'alerte interactives qu'ESET Endpoint Antivirus affichera avant toute action.

Pour ajuster le comportement des alertes interactives configurables, accédez à **Interface utilisateur** > **Alertes et boîtes de message** > **Liste des alertes interactives** dans l'arborescence Configurations avancées d'ESET Endpoint Antivirus, puis cliquez sur **Modifier**.

Objectif

Utiles pour les environnements gérés où l'administrateur peut désélectionner **Demander à l'utilisateur** partout et sélectionner une action prédéfinie à appliquer lorsque des fenêtres d'alerte interactives sont affichées.
Consultez également les états d'application dans le produit.



Recherchez dans les autres sections de l'aide une fenêtre d'alerte interactive spécifique :

Supports amovibles

- Nouvel appareil détecté

Protection du réseau

- Le message Accès bloqué au réseau s'affiche lorsque la tâche client **Isoler l'ordinateur du réseau** de ce poste de travail est déclenchée depuis ESMC.
- Communications réseau bloquées
- Menace réseau bloquée

Alertes du navigateur web

- Contenu potentiellement indésirable détecté
- Site web bloqué en raison d'hameçonnage

Ordinateur

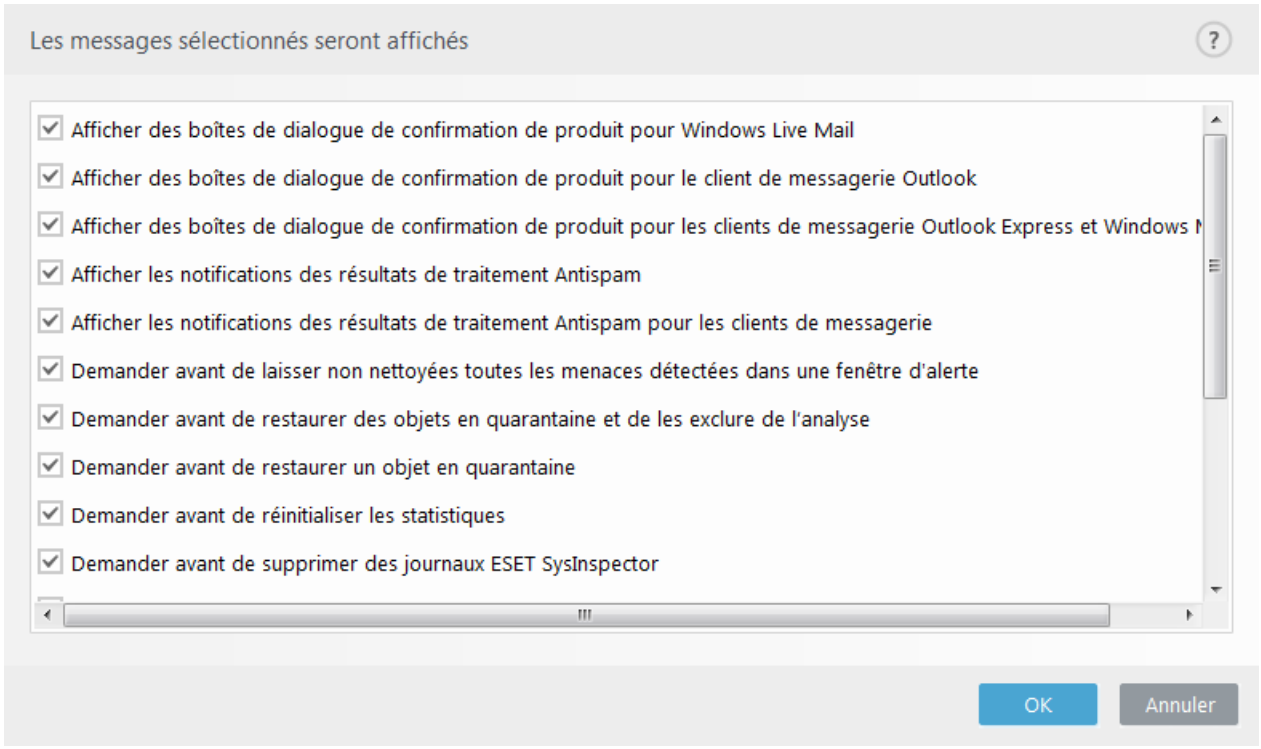
La présence de ces alertes mettra l'interface utilisateur en orange :

- Redémarrer l'ordinateur (requis)
- Redémarrer l'ordinateur (recommandé)

> **Limites**
> Les alertes interactives ne contiennent pas de fenêtres interactives Moteur de détection, HIPS ou Pare-feu, car leur comportement peut être configuré séparément dans la fonctionnalité spécifique.

Messages de confirmation

Pour régler les messages de confirmation, accédez à **Interface utilisateur** > **Alertes et boîtes de message** > **Messages de confirmation** dans l'arborescence de configurations avancées ESET Endpoint Antivirus, puis cliquez sur **Modifier**.



Cette boîte de dialogue contient les messages de confirmation qu'ESET Endpoint 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.

Erreur de conflit de paramètres avancés

Cette erreur peut se produire si un composant (par exemple le système HIPS) et un utilisateur créent simultanément les règles en mode interactif ou d'apprentissage.

Important
Il est recommandé de changer le mode de filtrage en **mode automatique** par défaut si vous souhaitez créer vos propres règles. En savoir plus sur le système HIPS et les modes de filtrage HIPS.

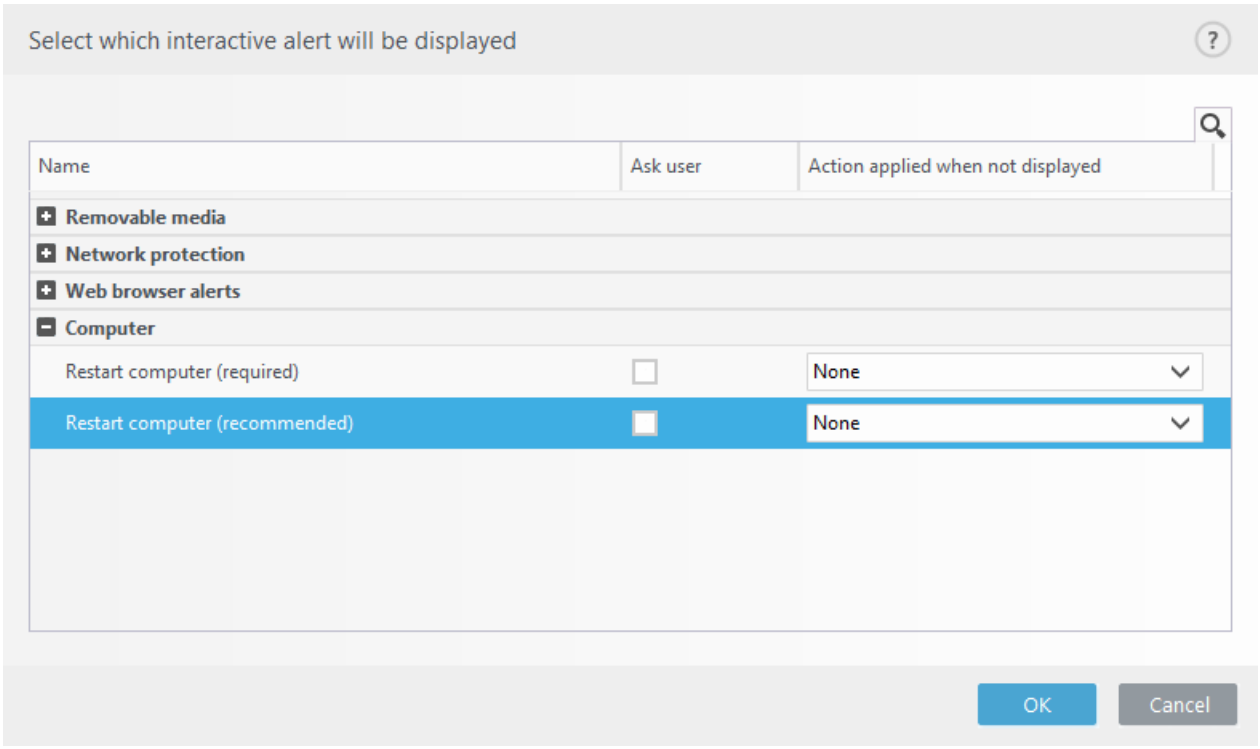
Redémarrage nécessaire

Si l'alerte rouge « Redémarrage requis » s'affiche sur les ordinateurs endpoint, vous pouvez désactiver son affichage.

Pour désactiver les alertes « Redémarrage requis » ou « Redémarrage recommandé », procédez comme suit :

1. Appuyez sur la touche **F5** pour accéder à Configurations avancées, puis développez la section **Alertes et boîtes de message**.

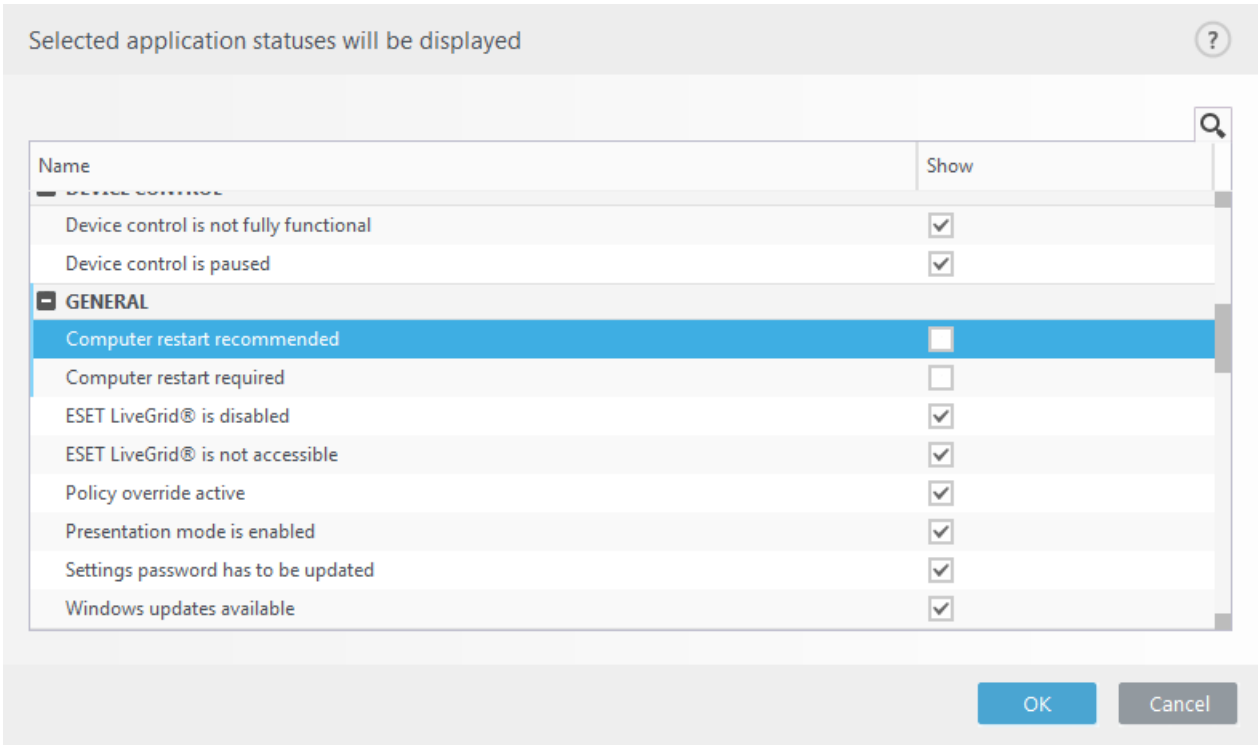
2. Cliquez sur **Modifier** en regard de l'option **Liste des alertes interactives**. Dans la section **Ordinateur**, décochez les cases en regard des options **Redémarrer l'ordinateur (requis)** et **Redémarrer l'ordinateur (recommandé)**.



3.Cliquez sur **OK** pour enregistrer les modifications dans les deux fenêtres ouvertes.

4.Les alertes ne s'afficheront plus sur l'ordinateur endpoint.

5.(Facultatif) Pour désactiver l'état de l'application dans la fenêtre principale du programme d'ESET Endpoint Antivirus, dans la fenêtre États d'application, décochez les cases situées en regard des options **Un redémarrage de l'ordinateur est nécessaire** et **Un redémarrage de l'ordinateur est recommandé**.



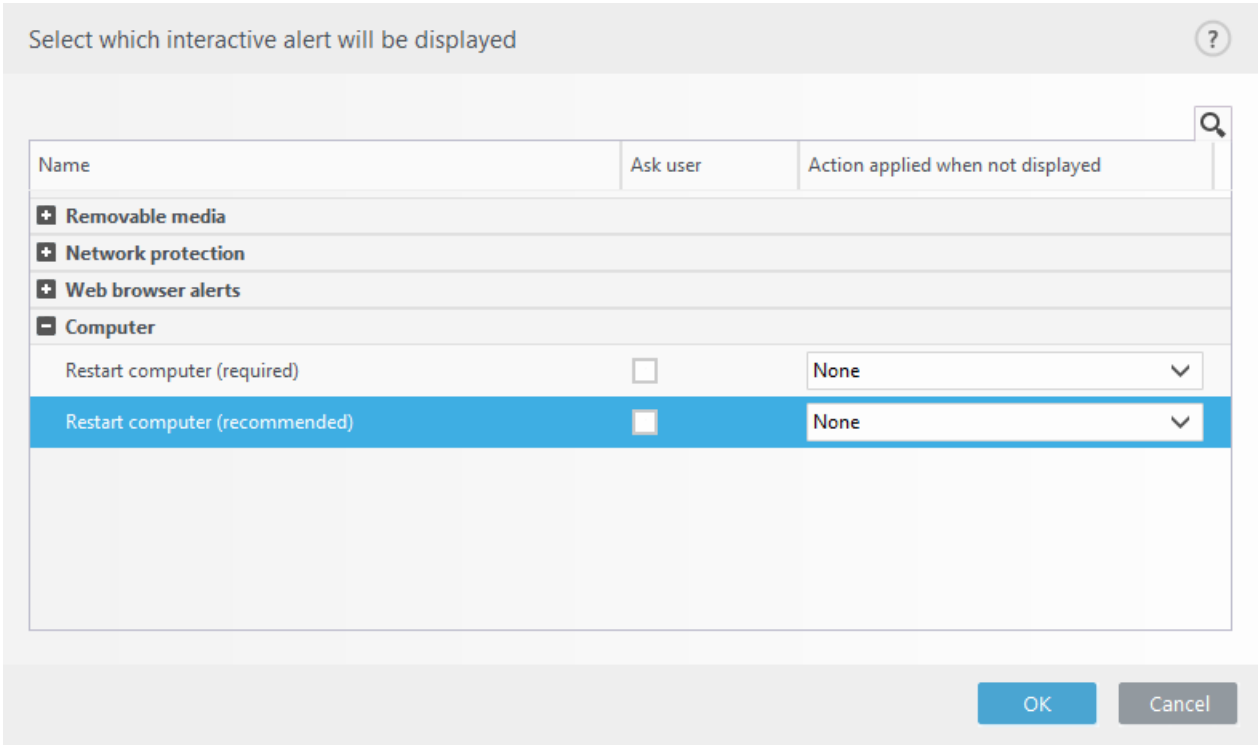
Redémarrage recommandé

Si l'alerte jaune « Redémarrage recommandé » s'affiche sur les ordinateurs endpoint, vous pouvez désactiver son affichage.

Pour désactiver les alertes « Redémarrage requis » ou « Redémarrage recommandé », procédez comme suit :

1.Appuyez sur la touche **F5** pour accéder à Configurations avancées, puis développez la section **Alertes et boîtes de message**.

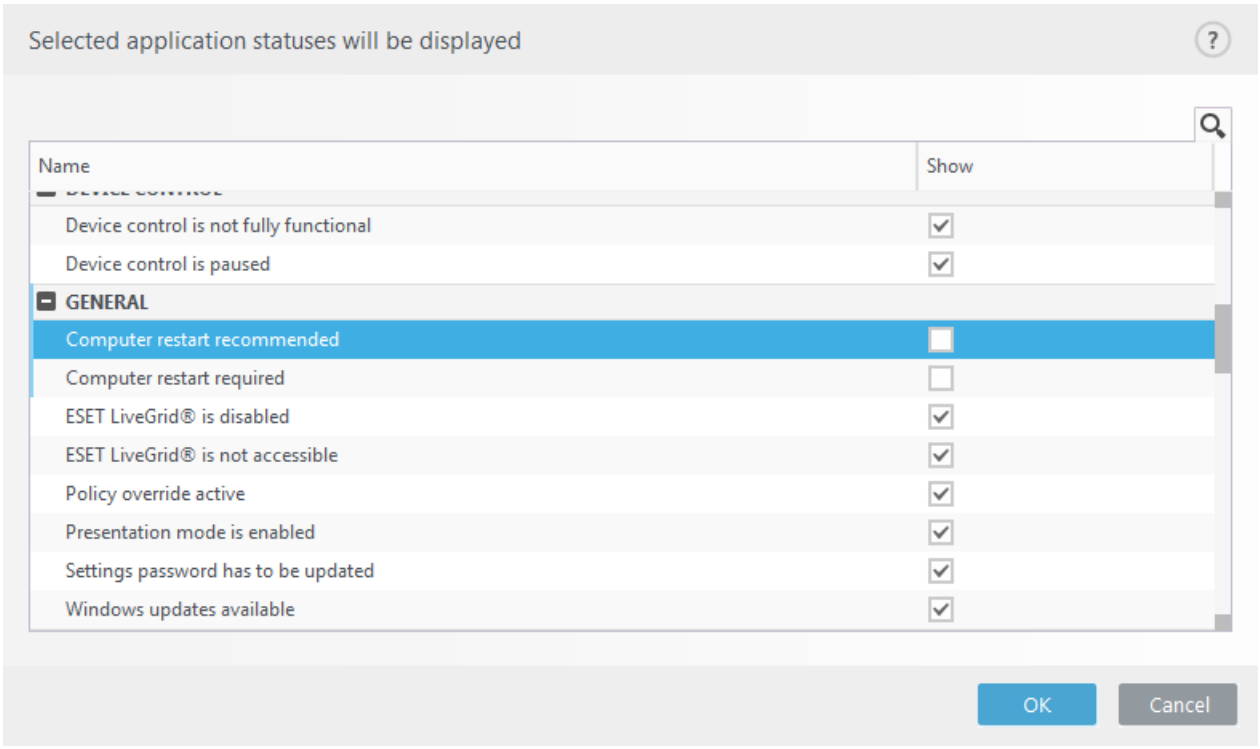
2.Cliquez sur **Modifier** en regard de l'option **Liste des alertes interactives**. Dans la section **Ordinateur**, décochez les cases en regard des options **Redémarrer l'ordinateur (requis)** et **Redémarrer l'ordinateur (recommandé)**.



3.Cliquez sur **OK** pour enregistrer les modifications dans les deux fenêtres ouvertes.

4.Les alertes ne s'afficheront plus sur l'ordinateur endpoint.

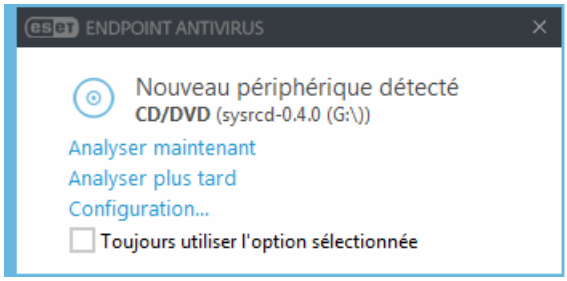
5.(Facultatif) Pour désactiver l'état de l'application dans la fenêtre principale du programme d'ESET Endpoint Antivirus, dans la fenêtre États d'application, décochez les cases situées en regard des options **Un redémarrage de l'ordinateur est nécessaire** et **Un redémarrage de l'ordinateur est recommandé**.



Supports amovibles

ESET Endpoint Antivirus permet d'analyser automatiquement les appareils 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 appareil amovible est inséré et que l'option **Afficher les options d'analyse** est définie dans ESET Endpoint Antivirus, la boîte de dialogue suivante s'affiche :



Options de cette boîte de dialogue :

- **Analyser maintenant** – Cette option déclenche l'analyse du support amovible.
- **Analyser ultérieurement** – L'analyse du support amovible est reportée.
- **Configuration** – Ouvre la section **Configurations avancées**.
- **Toujours utiliser l'option sélectionnée** – Lorsque cette option est sélectionnée, la même action sera exécutée lorsqu'un support amovible sera inséré plus tard.

En outre, ESET Endpoint 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.

ESET Endpoint Antivirus 7.2 et versions ultérieures

Pour accéder aux paramètres de l’analyse de supports amovibles, ouvrez Configuration avancée (**F5**) > **Interface utilisateur** > **Alertes et boîtes de message** > **Alertes interactives** > **Liste des alertes interactives** > **Modifier** > **Nouvel appareil détecté**.

Si l'option **Demander à l'utilisateur** n’est pas sélectionnée, sélectionnez 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 **Alertes interactives**.

ESET Endpoint Antivirus version 7.1 et version antérieure

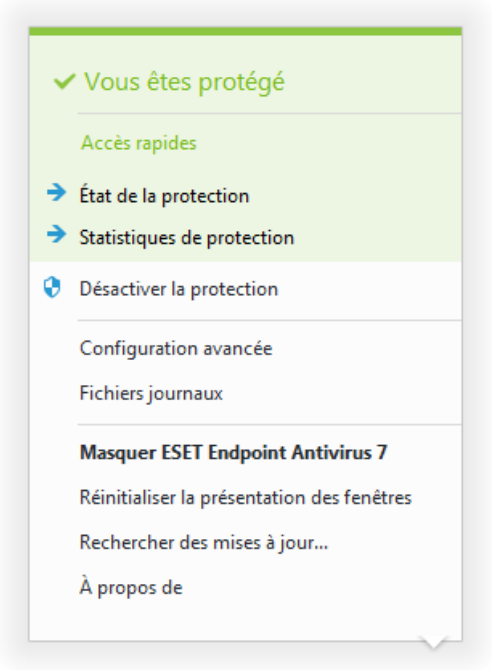
Pour accéder aux paramètres de l'analyse de supports amovibles, ouvrez Configurations avancées (**F5**) > **Moteur de détection** > **Analyses des logiciels malveillants** > **Appareils amovibles**.

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**.

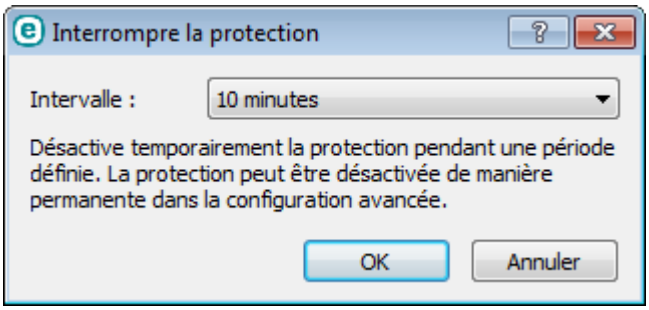
Icône dans la partie système de la barre des tâches

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 des attaques malveillantes en contrôlant les fichiers et les communications par e-mail et Internet.

Le menu déroulant **Intervalle** indique la durée pendant laquelle la protection est désactivée.



Configuration avancée – Sélectionnez cette option pour afficher l'arborescence **Configuration avancée**. Vous pouvez également accéder à Configuration avancée en appuyant sur la touche F5 ou en accédant à **Configuration** > **Configuration avancée**.

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

Ouvrir ESET Endpoint Antivirus – Ouvre la fenêtre principale du programme ESET Endpoint Antivirus depuis l'icône de la barre d'état.

Réinitialiser la disposition des fenêtres – Rétablit la taille et la position par défaut de la fenêtre ESET Endpoint Antivirus.

Rechercher des mises à jour... – Commence la mise à jour des modules du programme afin de garantir un niveau optimal de protection contre les codes malveillants.

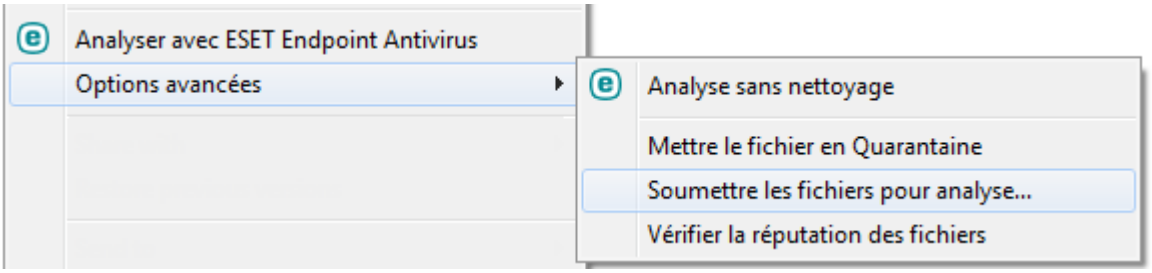
À propos – Les informations système fournissent des détails sur la version installée d'ESET Endpoint Antivirus, sur les modules installés et sur la date d'expiration de votre licence. Des informations sur votre système d'exploitation et les ressources système figurent dans la partie inférieure de la page.

Menu contextuel

Le menu contextuel est le menu qui s'affiche lorsque vous cliquez avec le bouton sur un objet (fichier). Il répertorie toutes les actions que vous pouvez effectuer sur un objet.

Il est possible d'intégrer les options ESET Endpoint Antivirus dans le menu contextuel. Les options de configuration de cette fonctionnalité figurent dans l'arborescence de la configuration avancée, sous **Interface utilisateur** > **Éléments de l'interface utilisateur**.

Intégrer dans le menu contextuel – Intègre les options ESET Endpoint Antivirus dans le menu contextuel.



Aide et assistance

ESET Endpoint Antivirus contient des outils de dépannage et des informations d'assistance qui vous aideront à résoudre les problèmes que vous pouvez rencontrer.

Aide

Rechercher dans la base de connaissances ESET – 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.

Ouvrir l'aide – Cliquez sur ce lien pour lancer les pages d'aide ESET Endpoint Antivirus.

Trouver une solution rapide – Cliquez sur ce lien pour trouver les solutions aux problèmes les plus fréquents. Nous vous recommandons de lire cette section avant de contacter le support technique.

Assistance technique

Envoyer une demande d'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 notre support technique.

Informations détaillées pour le support technique – Lorsque le système vous y invite, vous pouvez copier et envoyer des informations au support technique ESET (nom et version du produit, système d'exploitation et type de processeur).

Outils d'assistance

Encyclopédie des menaces – Conduit à l'encyclopédie des menaces ESET, qui contient des informations sur les

dangers et les symptômes de différents types d'infiltration.

Historique du moteur de détection – Mène à ESET Virus radar, qui contient des informations sur chaque version de la base de détection ESET(précédemment appelée « base de signatures des virus »).

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 le guide de l'utilisateur en ligne ESET Log Collector.

ESET Specialized Cleaner – Outils de suppression des infections courantes par logiciels malveillants. Pour obtenir plus d'informations, consultez cet article de la base de connaissances ESET.

Informations sur le produit et la licence

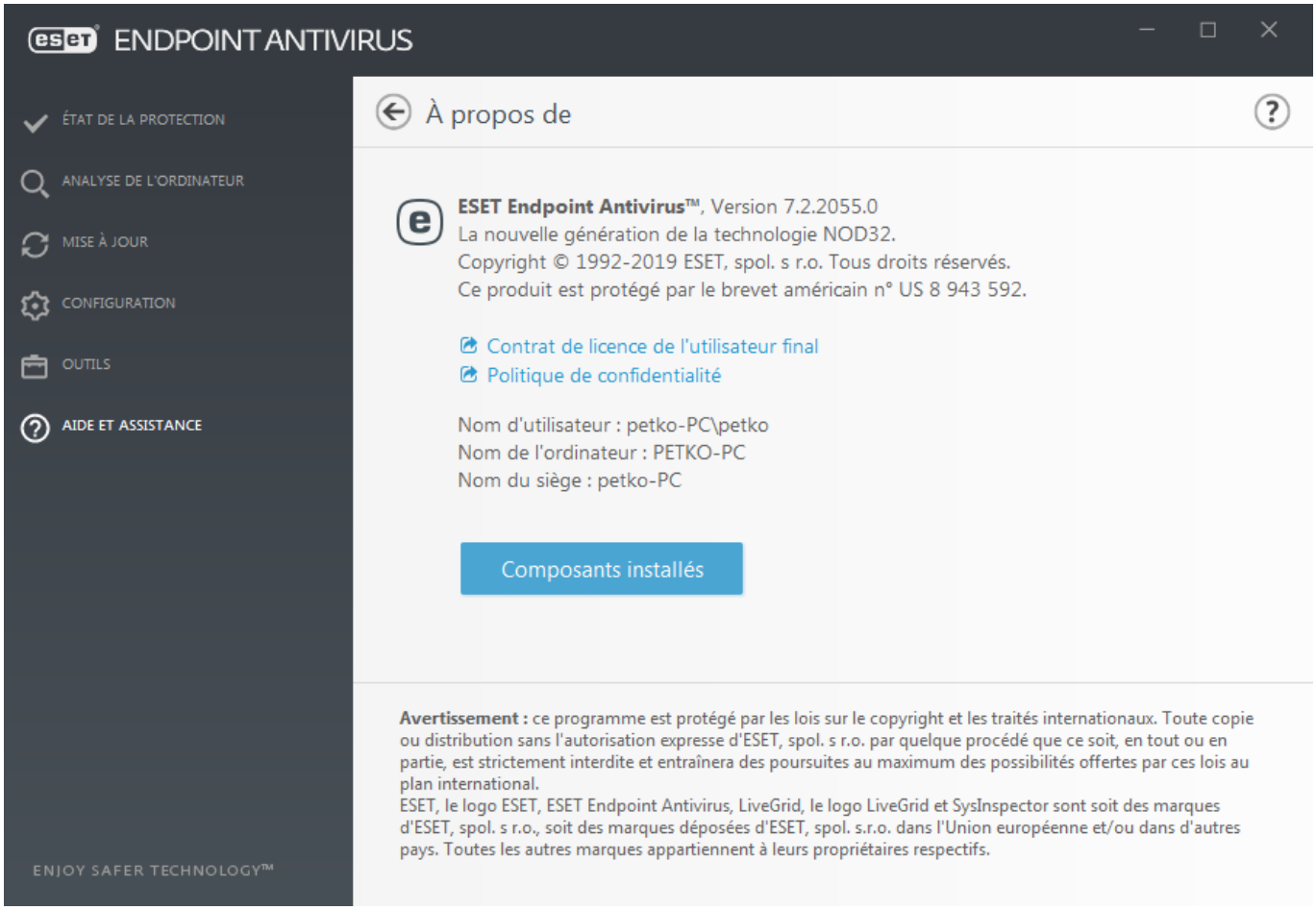
À propos de ESET Endpoint Antivirus – Affiche des informations sur votre copie de ESET Endpoint Antivirus.

Activer le produit/Modifier la licence – Cliquez sur cette option pour ouvrir la fenêtre d'activation et activer votre produit.

À propos d'ESET Endpoint Antivirus

Cette fenêtre fournit des informations détaillées sur la version de ESET Endpoint Antivirus installée, le système d'exploitation et les ressources système.

Cliquez sur **Composants installés** pour afficher des informations sur la liste des modules installés. 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.



Soumettre les données de configuration système

Pour offrir une assistance adéquate le plus rapidement possible, ESET requiert des informations sur la configuration de ESET Endpoint 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.

Lorsque vous envoyez 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 sans envoyer de données, cliquez sur **Ne pas envoyer les données**. Vous pouvez ainsi contacter le support technique ESET à l'aide du formulaire d'assistance en ligne.

Ce paramètre peut être également configuré dans **Configuration avancée** > **Outils** > **Diagnostics** > **Support technique**.

Remarque
si vous avez décidé d'envoyer les données système, vous devez remplir le formulaire Web et l'envoyer. Sinon, votre ticket n'est pas créé et vos données système sont perdues.

Gestionnaire de profils

Le gestionnaire de profil est utilisé à deux endroits dans ESET Endpoint Antivirus – dans les sections **Analyse de l'ordinateur à la demande** et **Mise à jour**.

Analyse de l'ordinateur à la demande

Vos paramètres d'analyse préférés peuvent être enregistrés pour les prochaines analyses. Il est recommandé de créer autant de profils (avec différentes cibles et méthodes, et d'autres paramètres d'analyse) que d'analyses utilisées régulièrement.

Pour créer un profil, ouvrez la fenêtre Configuration avancée (F5) et cliquez sur **Antivirus** > **Analyse de l'ordinateur à la demande**. Cliquez ensuite sur **Modifier** en regard de **Liste des profils**. Le menu déroulant **Profil de mise à jour** répertorie les profils d'analyse existants. Pour plus d'informations sur la création d'un profil d'analyse correspondant à vos besoins, reportez-vous à la section ThreatSenseConfiguration du moteur ; vous y trouverez une description de chaque paramètre de configuration de l'analyse.

> **Remarque**
> 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 **nettoyage strict**. Entrez le nom du nouveau profil dans la fenêtre **Gestionnaire de profils**, puis cliquez sur **Ajouter**. Sélectionnez le nouveau profil dans le menu déroulant **Profil sélectionné** et réglez les paramètres restants selon vos besoin. Cliquez sur **OK** pour enregistrer le nouveau profil.

Mettre à jour

L'éditeur de profils de la section de configuration des mises à jour permet aux utilisateurs de créer de nouveaux profils de mise à jour. Il est 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.

Raccourcis clavier

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

Raccourcis clavier	Action exécutée
F1	ouvre les pages d'aide
F5	ouvre la boîte de dialogue Configuration avancée
Up/Down	navigation dans les différents composants du produit
TAB	déplace le curseur dans une fenêtre
Esc	ferme la boîte de dialogue active

Ctrl+U	affiche des informations sur la licence ESET et votre ordinateur (détails pour le support technique)
Ctrl+R	réinitialise la taille et la position par défaut de la fenêtre du produit à l'écran

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 Endpoint 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 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 du noyau – Enregistrez tous les événements qui se produisent dans le service du noyau ESET (ekrn) pour permettre le diagnostic et la résolution des problèmes (disponible dans la version 7.2 et les versions ultérieures).

Activer la journalisation avancée des licences – Enregistrez toutes les communications du produit avec les serveurs d'activation ESET et ESET Business Account.

Activer la journalisation avancée de la protection du réseau – Enregistrez toutes les données réseau qui passent par le pare-feu au format PCAP. Les développeurs peuvent ainsi diagnostiquer et résoudre les problèmes liés au pare-feu.

Activer la journalisation avancée du système d'exploitation – Des informations supplémentaires sur le système d'exploitation telles que les processus en cours, l'activité de l'UC et les opérations du disque sont recueillies. 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 du filtrage des protocoles – Enregistrez toutes les données qui passent par le moteur de filtrage des protocoles au format PCAP. Les développeurs peuvent ainsi diagnostiquer et résoudre les problèmes liés au filtrage des protocoles.

Activer la journalisation avancée du scanner – Enregistrez les problèmes qui se produisent lors de l'analyse des fichiers et des dossiers par l'analyse de l'ordinateur ou la protection en temps réel du système de fichiers (disponible dans la version 7.2 et les versions ultérieures).

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.

Activer la journalisation avancée du filtrage Internet – Enregistrez tous les événements qui se produisent dans le contrôle parental. Les développeurs peuvent ainsi diagnostiquer et résoudre les problèmes liés au contrôle parental.

Emplacement des fichiers journaux

Système d'exploitation	Répertoire des fichiers journaux
Windows Vista et versions ultérieures	C:\ProgramData\ESET\ESET Endpoint Antivirus\Diagnostics\
Versions antérieures de Windows	C:\Documents and Settings\All Users\...

Analyseur de ligne de commande

Le module antivirus d'ESET Endpoint Antivirus peut être lancé depuis la ligne de commande, manuellement (avec la commande « ecls ») ou au moyen d'un fichier de commandes (« bat »). Module d'interface à ligne de commande ESET :

```
ecls [OPTIONS..] FILES..
```

Les paramètres suivants peuvent être utilisés lors de l'exécution de l'analyseur à la demande, à partir de la ligne de commande :

Options

/base-dir=FOLDER	charger les modules depuis le DOSSIER
/quar-dir=FOLDER	DOSSIER de quarantaine
/exclude=MASK	exclure les fichiers correspondant à MASQUE de l'analyse
/subdir	analyser les sous-dossiers (valeur par défaut)
/no-subdir	ne pas analyser les sous-dossiers
/max-subdir-level=LEVEL	sous-niveau maximal de sous-dossiers dans les dossiers à analyser
/symlink	suivre les liens symboliques (valeur par défaut)
/no-symlink	ignorer les liens symboliques

/ads	analyser ADS (valeur par défaut)
/no-ads	ne pas analyser ADS
/log-file=FILE	journaliser les résultats dans un FICHIER
/log-rewrite	écraser le fichier de résultats (valeur par défaut – 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=SIZE	analyser uniquement les fichiers plus petits que TAILLE Mo (valeur par défaut 0 = illimité)
/max-arch-level=LEVEL	sous-niveau maximal d'archives à analyser dans les archives (archives imbriquées)
/scan-timeout=LIMIT	analyser les archives pendant un maximum de LIMITE secondes
/max-arch-size=SIZE	n'analyser les fichiers contenus dans une archive que s'ils sont plus petits que TAILLE (valeur par défaut 0 = illimité)
/max-sfx-size=SIZE	n'analyser les fichiers d'une archive auto-extractible que s'ils sont plus petits que TAILLE Mo (valeur par défaut 0 = illimité)
/mail	analyser les fichiers des courriers électroniques (valeur par défaut)
/no-mail	ne pas analyser les fichiers des courriers électroniques
/mailbox	analyser les boîtes aux lettres (valeur par défaut)
/no-mailbox	ne pas analyser les boîtes aux lettres
/sfx	analyser les archives auto-extractibles (valeur par défaut)
/no-sfx	ne pas analyser les archives auto-extractibles
/rtp	analyser les fichiers exécutables compressés par un compresseur d'exécutables (valeur par défaut)
/no-rtp	ne pas analyser les fichiers exécutables compressés
/unsafe	rechercher les applications potentiellement dangereuses
/no-unsafe	ne pas rechercher les applications potentiellement dangereuses (valeur par défaut)
/unwanted	rechercher les applications potentiellement indésirables
/no-unwanted	ne pas rechercher les applications potentiellement indésirables (valeur par défaut)
/suspicious	rechercher les applications suspectes (valeur par défaut)

/no-suspicious	ne pas rechercher les applications suspectes
/pattern	utiliser les signatures (valeur par défaut)
/no-pattern	ne pas utiliser les signatures
/heur	activer l'heuristique (valeur par défaut)
/no-heur	désactiver l'heuristique
/adv-heur	activer l'heuristique avancée (valeur par défaut)
/no-adv-heur	désactiver l'heuristique avancée
/ext-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 : • aucun nettoyage – Aucun nettoyage automatique ne se produit. • nettoyage standard (valeur par défaut) – ecls.exe tente automatiquement de nettoyer ou de supprimer les fichiers infectés. • nettoyage strict – ecls.exe tente automatiquement de nettoyer ou de supprimer les fichiers infectés sans intervention de l'utilisateur (vous ne recevez pas d'invite avant la suppression des fichiers). • nettoyage rigoureux – ecls.exe supprime les fichiers sans tenter de les nettoyer, quel que soit leur type. • suppression – ecls.exe supprime les fichiers sans tenter de les nettoyer, mais s'abstient de supprimer les fichiers sensibles tels que les fichiers système de Windows.
/quarantine	copier les fichiers infectés (si nettoyés) vers Quarantaine (complète l'action effectuée lors du nettoyage)
/no-quarantine	ne pas copier les fichiers infectés vers Quarantaine

Options générales

/help	afficher l'aide et quitter
/version	afficher les informations de version et quitter
/preserve-time	conserver la date et l'heure du dernier accès

Codes de sortie

0	aucune menace détectée
1	menace détectée et nettoyée
10	certains fichiers n'ont pas pu être analysés (peuvent être des menaces)
50	menace détectée
100	erreur

Remarque

Un code sortie supérieur à 100 signale un fichier non analysé qui est potentiellement infecté.

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 Endpoint Antivirus peut être exportée dans un fichier .xml.*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 Endpoint Antivirus. Vous pouvez le faire manuellement ou créer un script pour l'automatisation.

Important
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.

Remarque
Les commandes ecmd ne peuvent être exécutées que localement. L'exécution d'une tâche client **Exécuter une commande** à l'aide d'ESMC ne fonctionnera pas.

Exemple
Commande d'exportation des paramètres :
```
ecmd /getcfg c:\config\settings.xml
```

Commande d'importation des paramètres :
```
ecmd /setcfg c:\config\settings.xml
```

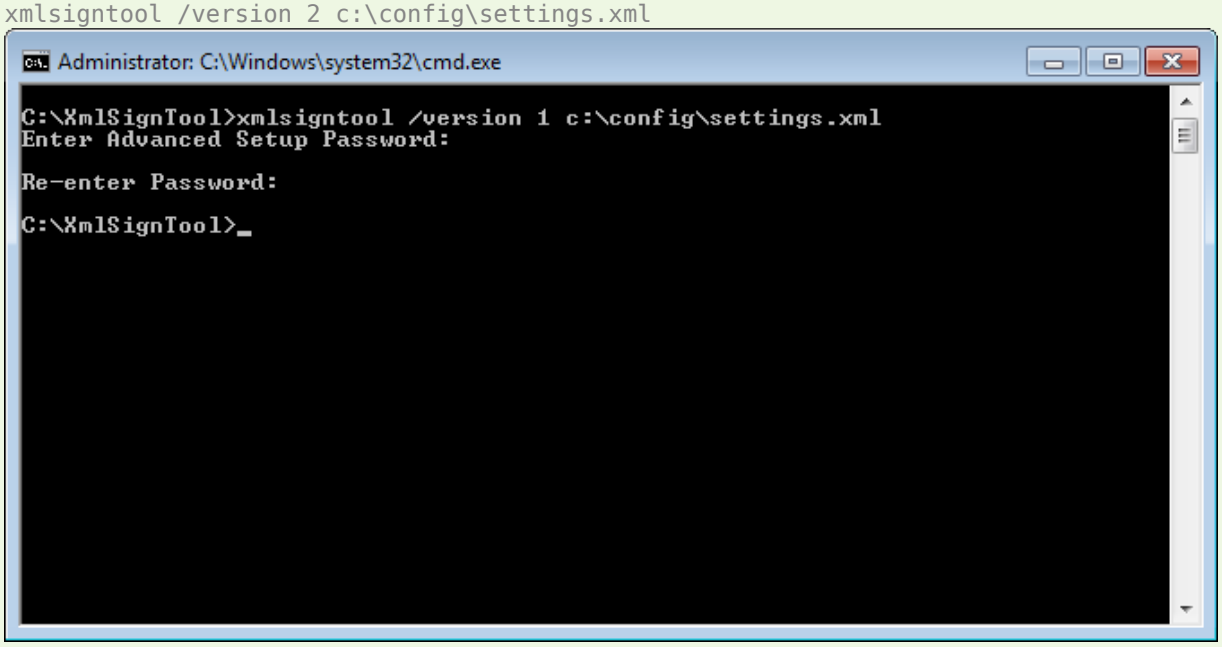
Signature d'un fichier de configuration *.xml* :

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>`

Important
La valeur du paramètre `/version` dépend de la version d'ESET Endpoint Antivirus. Utilisez `/version 2` pour la version 7 et les versions ultérieures.

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 Endpoint Antivirus avec ESET CMD à l'aide de la méthode d'autorisation du mot de passe.

Exemple
Commande de signature du fichier de configuration exporté :
`xmlsigntool /version 2 c:\config\settings.xml`



REMARQUE
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 Endpoint Antivirus avant l'importation.

Avertissement
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.

Liste des commandes ecmd

Des fonctionnalités de sécurité distinctes peuvent être activées et temporairement désactivées à l'aide de la commande d'exécution de tâche client ESMC. Les commandes ne remplacent pas les paramètres de politique et tous les paramètres suspendus retourneront dans leur état d'origine après l'exécution de la commande ou le redémarrage d'un appareil. Pour utiliser cette fonctionnalité, indiquez la ligne de commande à exécuter dans le

champ du même nom.

Consultez la liste des commandes pour chaque fonctionnalité de sécurité suivante :

Fonctionnalité de protection	Commande d'interruption temporaire	Commande d'activation
Protection en temps réel du système de fichiers	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
Protection des documents	ecmd /setfeature document pause	ecmd /setfeature document enable
Contrôle de périphérique	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
Mode de présentation	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
Technologie Anti-Stealth	ecmd /setfeature antistealth pause	ecmd /setfeature antistealth enable
Pare-feu personnel	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
Protection contre les attaques réseau (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
Protection anti-botnet	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Contrôle Web	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
Protection de l'accès Web	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
Protection du client de messagerie	ecmd /setfeature email pause	ecmd /setfeature email enable
Protection antipourriel	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Protection antihameçonnage	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

Détection en cas d’inactivité

Les paramètres de détection en cas d'inactivité peuvent être configurés dans **Configuration avancée**, sous **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, quand :

- l'économiseur d'écran est en cours d'exécution,
- l'ordinateur est verrouillé,
- un utilisateur se déconnecte de sa session.

Utilisez les boutons bascules pour chaque état respectif, afin d'activer ou désactiver les différents déclencheurs de détection d'état inactif.

Importer et exporter les paramètres

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

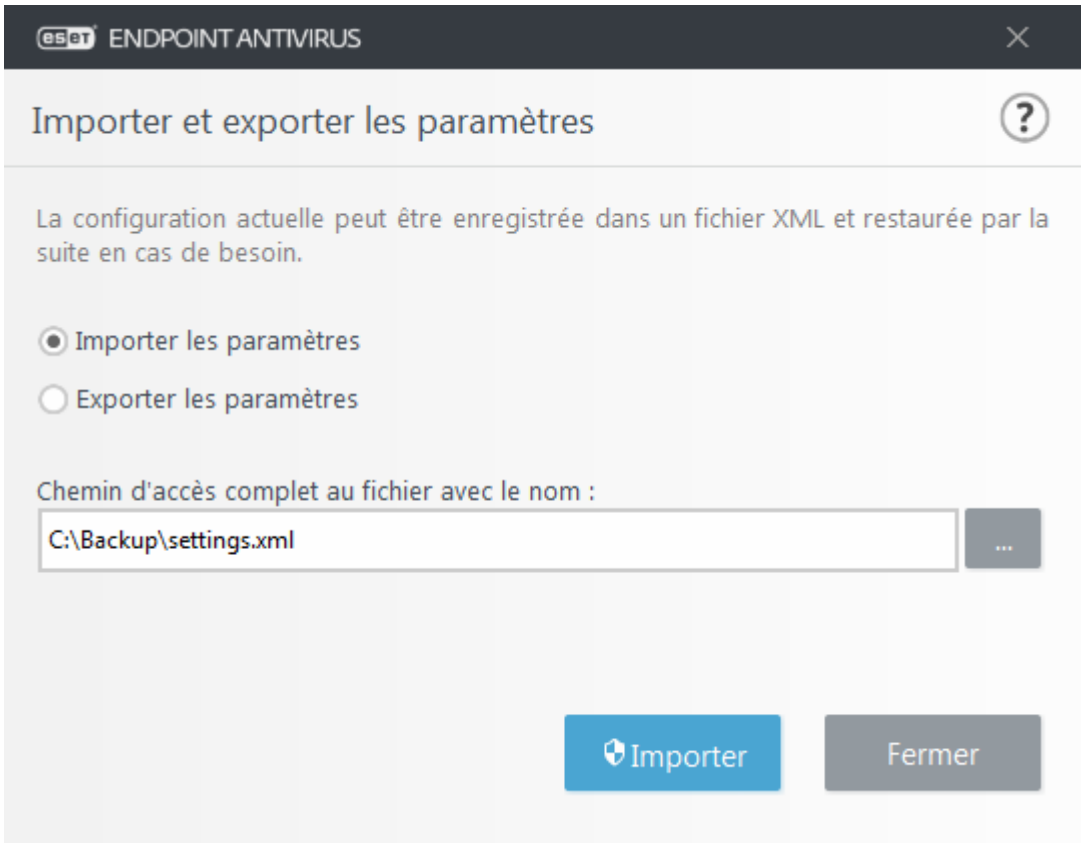
Ces opérations sont utiles si vous devez sauvegarder la configuration actuelle de ESET Endpoint Antivirus pour

l'utiliser ultérieurement. L'option Exporter les paramètres est également pratique pour les utilisateurs qui souhaitent utiliser leur configuration préférée sur plusieurs systèmes. Il leur suffit d'importer un fichier .xml pour transférer ces paramètres.

L'importation d'une configuration est très facile. Dans la fenêtre principale du programme, cliquez sur **Configuration** > **Importer/exporter les paramètres**, puis sélectionnez **Importer les paramètres**. Saisissez le nom du fichier de configuration ou cliquez sur le bouton **...** pour accéder au fichier de configuration à importer.

La procédure d'exportation d'une configuration est très semblable. Dans la fenêtre principale du programme, cliquez sur **Configuration** > **Importer/exporter les paramètres**. Sélectionnez **Exporter les paramètres** et saisissez le nom de fichier du fichier de configuration (par exemple, *export.xml*). Utilisez le navigateur pour sélectionner un emplacement de votre ordinateur pour enregistrer le fichier de configuration.

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



Rétablir tous les paramètres par défaut

Pour rétablir tous les paramètres du programme, pour tous les modules, cliquez sur **Par défaut** dans les Configurations avancées (F5). 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.

Surveillance et administration à distance

La surveillance et l'administration à distance (RMM, Remote Monitoring and Management) est le processus qui consiste à surveiller et contrôler les systèmes logiciels à l'aide d'un agent installé localement qui est accessible par un fournisseur de services d'administration.

ERMM - Module d'extension ESET pour RMM

- L'installation par défaut d'ESET Endpoint Antivirus contient le fichier `ermm.exe` situé dans l'application Endpoint au sein du répertoire :
  C:\Program Files\ESET\ESET Security\ermm.exe

- `ermm.exe` est un utilitaire de ligne de commande qui a été conçu pour faciliter la gestion des produits endpoint et les communications avec n'importe quel module d'extension RMM.

- `ermm.exe` échange des données avec le module d'extension RMM, qui communique avec le RMM Agent lié à un serveur RMM Server. Par défaut, l'outil ESET RMM est désactivé.

Ressources supplémentaires

- Ligne de commande ERMM

- Liste des commandes ERMM JSON

  - Activation de la surveillance et de l'administration à distanceESET Endpoint Antivirus

Modules d'extension ESET Direct Endpoint Management pour des solutions RMM tierces

RMM Server s'exécute en tant que service sur un serveur tiers. Pour plus d'informations, consultez les guides de l'utilisateur en ligne ESET Direct Endpoint Management suivants :

- Module d'extension ESET Direct Endpoint Management pour ConnectWise Automate
- Module d'extension ESET Direct Endpoint Management pour DattoRMM
- ESET Direct Endpoint Management pour Solarwinds N-Central
- ESET Direct Endpoint Management pour NinjaRMM

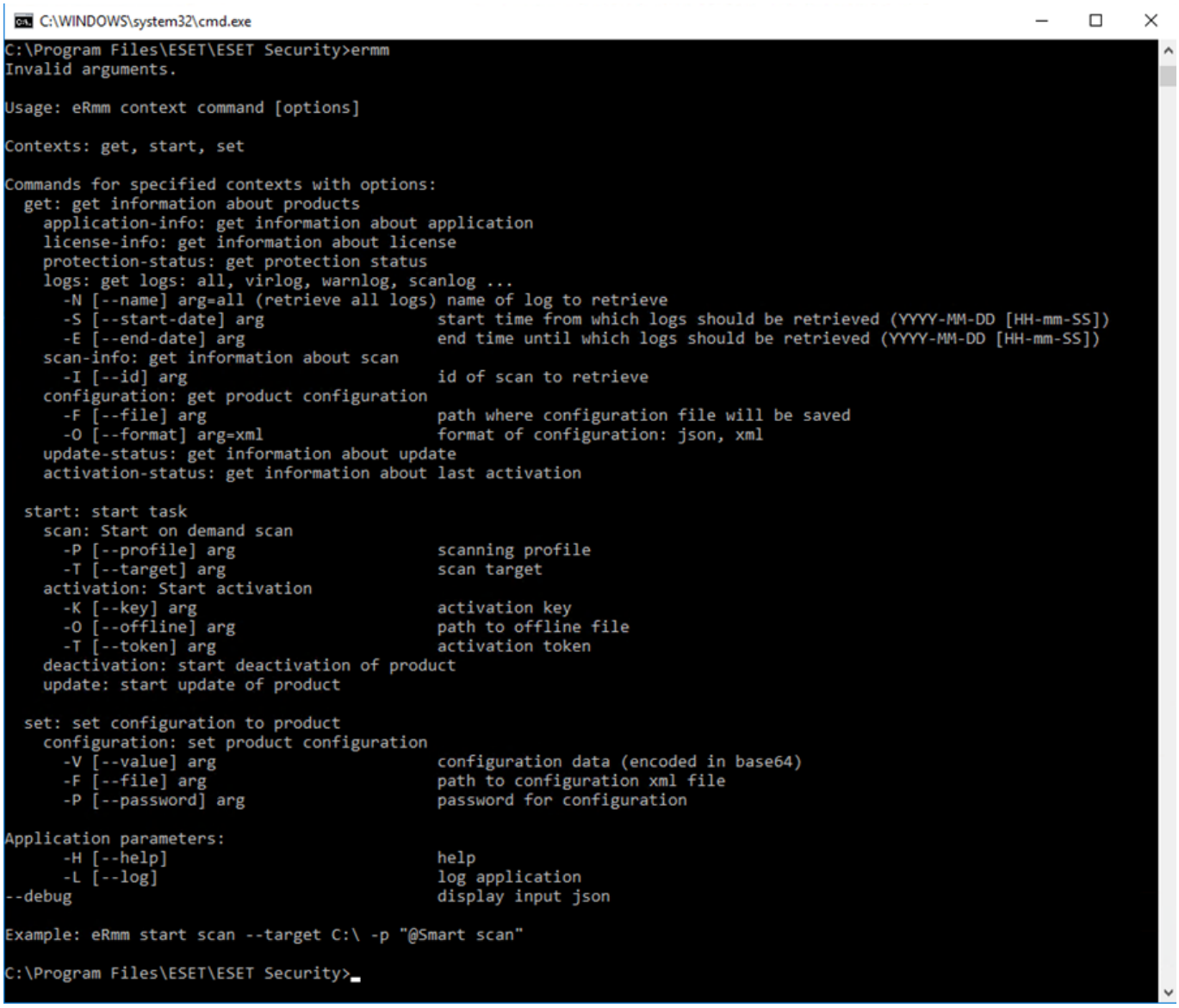
Ligne de commande ERMM

Remote monitoring management is run using the command line interface. The default ESET Endpoint Antivirus installation contains the file ermm.exe located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security*.

Run the Command Prompt (cmd.exe) as an Administrator and navigate to the mentioned path. (To open Command Prompt, press Windows button + R on your keyboard, type a cmd.exe into the Run window and press Enter.)

The command syntax is: `ermm context command [options]`

Also note that the log parameters are case sensitive.



ermm.exe uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter `--debug` at the of the command.

Context	Command	Description
get		**Get information about products**
	application-info	Get information about product
	license-info	Get information about license
	protection-status	Get protection status
	logs	Get logs
	scan-info	Get information about running scan
	configuration	Get product configuration
	update-status	Get information about update

Context	Command	Description
	activation-status	Get information about last activation
start		**Start task**
	scan	Start on demand scan
	activation	Start activation of product
	deactivation	Start deactivation of product
	update	Start update of product
set		**Set options for product**
	configuration	Set configuration to product

In the output result of every command, the first information displayed is result ID. To understand better the result information, check the table of IDs below.

Error ID	Error	Description
0	Success	
1	Command node not present	"Command" node not present in input json
2	Command not supported	Particular command is not supported
3	General error executing the command	Error during execution of command
4	Task already running	Requested task is already running and has not been started
5	Invalid parameter for command	Bad user input
6	Command not executed because it's disabled	RMM isn't enabled in advanced settings or isn't started as an administrator

Liste des commandes ERMM JSON

- get protection-status
- get application-info
- get license-info
- get logs
- get activation-status
- get scan-info
- get configuration
- get update-status
- start scan
- start activation

- start deactivation
- start update
- set configuration

get protection-status

Get the list of application statuses and the global application status

Command line

```
ermm.exe get protection-status
```

Parameters

None

Example

call

```
{
 "command":"get_protection_status",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
  "statuses":[{
    "id":"EkrnNotActivated",
    "status":2,
    "priority":768,
    "description":"Product not activated"
   }],
  "status":2,
  "description":"Security alert"
 },
 "error":null
}
```

get application-info

Get information about the installed application

Command line

```
ermm.exe get application-info
```

Parameters

None

Example

call

```
{
 "command":"get_application_info",
 "id":1,
 "version":"1"
}
```

result

```
{
  "id":1,
  "result":{
   "description":"ESET Endpoint Antivirus",
   "version":"6.6.2018.0",
   "product":"eea",
   "lang_id":1033,
   "modules":[{
    "id":"SCANNER32",
    "description":"Detection engine",
    "version":"15117",
    "date":"2017-03-20"
   },{
    "id":"PEGASUS32",
    "description":"Rapid Response module",
    "version":"9734",
    "date":"2017-03-20"
   },{
    "id":"LOADER32",
    "description":"Update module",
    "version":"1009",
    "date":"2016-12-05"
   },{
    "id":"PERSEUS32",
    "description":"Antivirus and antispyware scanner module",
    "version":"1513",
    "date":"2017-03-06"
   },{
    "id":"ADVHEUR32",
    "description":"Advanced heuristics module",
    "version":"1176",
    "date":"2017-01-16"
   },{
    "id":"ARCHIVER32",
    "description":"Archive support module",
    "version":"1261",
    "date":"2017-02-22"
   },{
    "id":"CLEANER32",
    "description":"Cleaner module",
    "version":"1132",
    "date":"2017-03-15"
   },{
    "id":"ANTISTEALTH32",
    "description":"Anti-Stealth support module",
    "version":"1106",
    "date":"2016-10-17"
   },{
    "id":"SYSTEMSTATUS32",
    "description":"ESET SysInspector module",
    "version":"1266",
    "date":"2016-12-22"
   },{
    "id":"TRANSLATOR32",
    "description":"Translation support module",
    "version":"1588B",
    "date":"2017-03-01"
   },{
    "id":"HIPS32",
    "description":"HIPS support module",
    "version":"1267",
    "date":"2017-02-16"
   },{
    "id":"PROTOSCAN32",
    "description":"Internet protection module",
    "version":"1300",
    "date":"2017-03-03"
   },{
    "id":"DBLITE32",
    "description":"Database module",
    "version":"1088",
    "date":"2017-01-05"
   },{
    "id":"CONFENG32",
    "description":"Configuration module (33)",
    "version":"1496B",
    "date":"2017-03-17"
   },{
    "id":"IRIS32",
    "description":"LiveGrid communication module",
    "version":"1022",
    "date":"2016-04-01"
   },{
    "id":"SAURON32",
    "description":"Rootkit detection and cleaning module",
    "version":"1006",
    "date":"2016-07-15"
   },{
    "id":"SSL32",
    "description":"Cryptographic protocol support module",
    "version":"1009",
    "date":"2016-12-02"
   }
  },
  "error":null
 }
}
```

get license-info

Get information about the license of the product

Command line

```
ermm.exe get license-info
```

Parameters

None

Example

call

```
{
 "command":"get_license_info",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
  "type":"NFR",
  "expiration_date":"2020-12-31",
  "expiration_state":"ok",
  "public_id":"3XX-7ED-7XF",
  "seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
  "seat_name":"M"
 },
 "error":null
}
```

get logs

Get logs of the product

Command line

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-
date "2017-04-04 12-00-00"
```

Parameters

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

Example

call


```
{
 "command":"get_logs",
 "id":1,
 "version":"1",
 "params":{
  "name":"warnlog",
  "start_date":"2017-04-04 06-00-00",
  "end_date":"2017-04-04 12-00-00"
 }
}
```


result


```
{
 "id":1,
 "result":{
  "warnlog":{
   "display_name":"Events",
   "logs":[{
    "Time":"2017-04-04 06-05-59",
    "Severity":"Info",
    "PluginId":"ESET Kernel",
    "Code":"Malware database was successfully updated to version 15198 (20170404).",
    "UserData":""
   },{
    "Time":"2017-04-04 11-12-59",
    "Severity":"Info",
    "PluginId":"ESET Kernel",
    "Code":"Malware database was successfully updated to version 15199 (20170404).",
    "UserData":""
   }]
  }
 },
 "error":null
}
```

get activation-status

Get information about the last activation. Result of status can be { success, error }

Command line

```
ermm.exe get activation-status
```

Parameters

None

Example

call

```
{
 "command":"get_activation_status",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
  "status":"success"
 },
 "error":null
}
```

get scan-info

Get information about running scan.

Command line

```
ermm.exe get scan-info
```

Parameters

None

Example

call

```
{
 "command":"get_scan_info",
 "id":1,
 "version":"1"
}
```

result


```
{
 "id":1,
 "result":{
  "scan-info":{
 "scans":[{
  "scan_id":65536,
  "timestamp":272,
  "state":"finished",
  "pause_scheduled_allowed":false,
  "pause_time_remain":0,
  "start_time":"2017-06-20T12:20:33Z",
  "elapsed_tickcount":328,
  "exit_code":0,
  "progress_filename":"Operating memory",
  "progress_arch_filename":"",
  "total_object_count":268,
  "infected_object_count":0,
  "cleaned_object_count":0,
  "log_timestamp":268,
  "log_count":0,
  "log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
  "username":"test-PC\\test",
  "process_id":3616,
  "thread_id":3992,
  "task_type":2
 }],
 "pause_scheduled_active":false
}
 },
 "error":null
}
```


get configuration

Get the product configuration. Result of status may be { success, error }

Command line

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

Parameters

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Example

call

```
{
 "command":"get_configuration",
 "id":1,
 "version":"1",
 "params":{
  "format":"xml",
  "file":"C:\\tmp\\conf.xml"
 }
}
```

result

```
{
 "id":1,
 "result":{
  "configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
 },
 "error":null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

Command line

```
ermm.exe get update-status
```

Parameters

None

Example

call

```
{
 "command":"get_update_status",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
  "last_update_time":"2017-06-20 13-21-37",
  "last_update_result":"error",
  "last_successful_update_time":"2017-06-20 11-21-45"
 },
 "error":null
}
```

start scan

Start scan with the product

Command line

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parameters

Name	Value

profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Example

call

```
{
 "command":"start_scan",
 "id":1,
 "version":"1",
 "params":{
  "profile":"Smart scan",
  "target":"c:\\"
 }
}
```

result

```
{
 "id":1,
 "result":{
  "task_id":458752
 },
 "error":null
}
```

start activation

Start activation of product

Command line

```
ermm.exe start activation --key "activation key" | --
offline "path to offline file" | --token "activation token"
```

Parameters

Name	Value
key	Activation key
offline	Path to offline file
token	Activation token

Example

call

```
{
 "command":"start_activation",
 "id":1,
 "version":"1",
 "params":{
  "key":"XXXX-XXXX-XXXX-XXXX-XXXX"
 }
}
```

result

```
{
 "id":1,
 "result":{
 },
 "error":null
}
```

start deactivation

Start deactivation of the product

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

call

```
{
 "command":"start_deactivation",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
 },
 "error":null
}
```

start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

Command line

```
ermm.exe start update
```

Parameters

None

Example

call

```
{
 "command":"start_update",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
 },
  "error":{
   "id":4,
   "text":"Task already running."
  }
}
```

set configuration

Set configuration to the product. Result of status may be { success, error }

Command line

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parameters

Name	Value
file	the path where the configuration file will be saved
password	password for configuration
value	configuration data from the argument (encoded in base64)

Example

call

```
{
 "command":"set_configuration",
 "id":1,
 "version":"1",
 "params":{
  "format":"xml",
  "file":"C:\\tmp\\conf.xml",
  "password": "pass"
 }
}
```

result

```
{
 "id":1,
 "result":{
 },
 "error":null
}
```

Questions fréquentes

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

- Comment mise à jour ESET Endpoint Antivirus
- Comment activer ESET Endpoint Antivirus
- Comment utiliser les informations d'identification actuelles pour activer un nouveau produit
- Comment éliminer un virus de mon PC
- Comment créer une tâche dans le Planificateur
- Comment programmer une analyse hebdomadaire de l'ordinateur
- Comment connecter mon produit à ESET Security Management Center

- Utilisation du mode de remplacement
- Comment appliquer une politique recommandée pour ESET Endpoint Antivirus

- Comment configurer un miroir
- Comment effectuer une mise à niveau vers Windows 10 avec ESET Endpoint Antivirus
- Activation de la surveillance et de l'administration à distance
- Blocage du téléchargement de types de fichiers spécifiques depuis Internet
- Comment limiter l'interface utilisateur d'ESET Endpoint Antivirus

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

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

- Meilleures pratiques pour se protéger contre les logiciels malveillants Filecoder (ransomwares)
- FAQ sur ESET Endpoint Security et ESET Endpoint Antivirus 7
- Quels ports et adresses dois-je ouvrir sur mon pare-feu tiers pour autoriser les fonctionnalités complètes du produit ESET ?

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

Comment mettre à jour ESET Endpoint Antivirus

La mise à jour de ESET Endpoint 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** (pour plus d'informations sur le Planificateur, cliquez ici).

Comment activer ESET Endpoint Antivirus

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

Plusieurs méthodes permettent d'activer le produit. Certains scénarios d'activation proposés dans la fenêtre d'activation peuvent varier en fonction du pays et selon le mode de distribution (page Web ESET, type de programme d'installation .msi ou .exe, etc.).

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

Vous pouvez utiliser l'une ou l'autre des méthodes ci-après pour activer ESET Endpoint Antivirus :

- **Clé de licence** – Chaîne unique au format XXXX-XXXX-XXXX-XXXX-XXXX qui sert à identifier le propriétaire de la licence et à activer la licence.

- **ESET Business Account** – Compte créé sur le portail ESET Business Account à l'aide d'informations d'identification (adresse e-mail + mot de passe). Cette méthode permet de gérer plusieurs licences à partir d'un seul emplacement.

- **Licence hors ligne** – Fichier généré automatiquement qui est transféré au produit ESET afin de fournir des informations de licence. Si une licence vous permet de télécharger un fichier de licence hors ligne (.lf), ce dernier peut être utilisé pour effectuer une activation hors ligne. Le nombre de licences hors ligne sera soustrait du nombre total de licences disponibles. Pour plus d'informations sur la génération d'un fichier hors ligne, reportez-vous au guide de l'utilisateur en ligne d'ESET Business Account.

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

Si vous disposez d'un nom d'utilisateur et d'un mot de passe que vous avez utilisés pour activer d'anciens produits ESET et si vous ne savez pas comment activer ESET Endpoint Antivirus, convertissez vos informations d'identification héritées en clé de licence.

En cas d'échec de l'activation du produit

Vous pouvez modifier la licence de votre produit à tout moment. Pour ce faire, cliquez sur **Aide et assistance** > **Modifier la licence** dans la fenêtre principale du programme. L'ID de licence publique s'affiche ; il sert à identifier votre licence auprès d'ESET. Le nom d'utilisateur sous lequel l'ordinateur est enregistré auprès du système de gestion des licences est stocké dans la section **À propos**. Il est visible lorsque vous cliquez avec le bouton droit sur l'icône dans la partie système de la barre des tâches.

> **Remarque**
> ESET Security Management Center peut activer des ordinateurs clients en silence à l'aide des licences fournies par l'administrateur. Pour plus d'informations, reportez-vous à l'aide en ligne d'ESET Security Management Center.

Connexion à ESET Business Account

Le compte Security Admin est un compte créé sur le portail ESET Business Account à l'aide de vos **adresse e-mail** et **mot de passe**. Il peut voir toutes les autorisations des sièges. Un compte Security Admin permet de gérer plusieurs licences. Si vous n'en disposez pas d'un, cliquez sur **Créer un compte** pour être redirigé vers le portail ESET Business Account dans lequel vous pouvez vous enregistrer à l'aide de vos informations d'identification.

Si vous avez oublié votre mot de passe, cliquez sur **J'ai oublié mon mot de passe** pour être redirigé vers le portail ESET Business Account. Saisissez votre adresse e-mail et cliquez sur **Se connecter**. Vous recevrez ensuite un message contenant des instructions pour réinitialiser votre mot de passe.

Utilisation de la clé de licence existante pour activer un nouveau produit ESET Endpoint

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

Comment éliminer un virus de mon PC

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

1. Dans la fenêtre principale du programme, cliquez sur **Analyse de l'ordinateur**.

2. Cliquez sur **Analyse intelligente** pour démarrer l'analyse de votre système.

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

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

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

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 de liste déroulante **Durée écoulée depuis la dernière exécution**)

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

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

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. Sélectionnez **Analyse de l'ordinateur à la demande** dans le menu déroulant.

3. Saisissez un nom pour la tâche et sélectionnez **Chaque semaine pour la 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 connecter ESET Endpoint Antivirus à ESET Security Management Center

Lorsque ESET Endpoint Antivirus est installé sur votre ordinateur et que vous souhaitez vous connecter via ESET Security Management Center, vérifiez qu'ESET Management Agent est également installé sur votre poste de travail client. Il s'agit d'un élément essentiel pour chaque solution client communiquant avec ESMC Server.

- Installer ou déployer ESET Management Agent sur les postes de travail clients

Voir aussi :

- Documentation pour les endpoints administrés à distance
- Utilisation du mode de remplacement
- Comment appliquer une politique recommandée pour ESET Endpoint Antivirus

Utilisation du mode de remplacement

Les utilisateurs qui disposent des produits ESET Endpoint (version 6.5 et ultérieure) pour Windows peuvent utiliser la fonctionnalité de remplacement. Le mode de remplacement permet aux utilisateurs au niveau des ordinateurs client de modifier les paramètres du produit ESET installé, même si une stratégie est appliquée sur ces derniers. Il peut être activé pour certains utilisateurs d'Active Directory ou être protégé par mot de passe. Cette fonction ne peut pas être activée pendant plus de quatre heures d'affilée.

Avertissement

- Le mode de remplacement ne peut pas être arrêté à partir de la console web ESMC Web Console une fois qu'il est activé. Il sera désactivé automatiquement à l'expiration du délai de remplacement. Il peut également être désactivé sur la machine cliente.
- L'utilisateur qui a recours au mode de remplacement doit également disposer des droits d'administrateur Windows. Sinon, il ne peut pas enregistrer les modifications apportées aux paramètres d'ESET Endpoint Antivirus.
- L'authentification de groupe Active Directory est prise en charge pour ESET Endpoint Antivirus version 7.0.2100.4 et les versions ultérieures.

Pour définir le **mode de remplacement** :

1. Accédez à **Politiques** > **Nouvelle politique**.

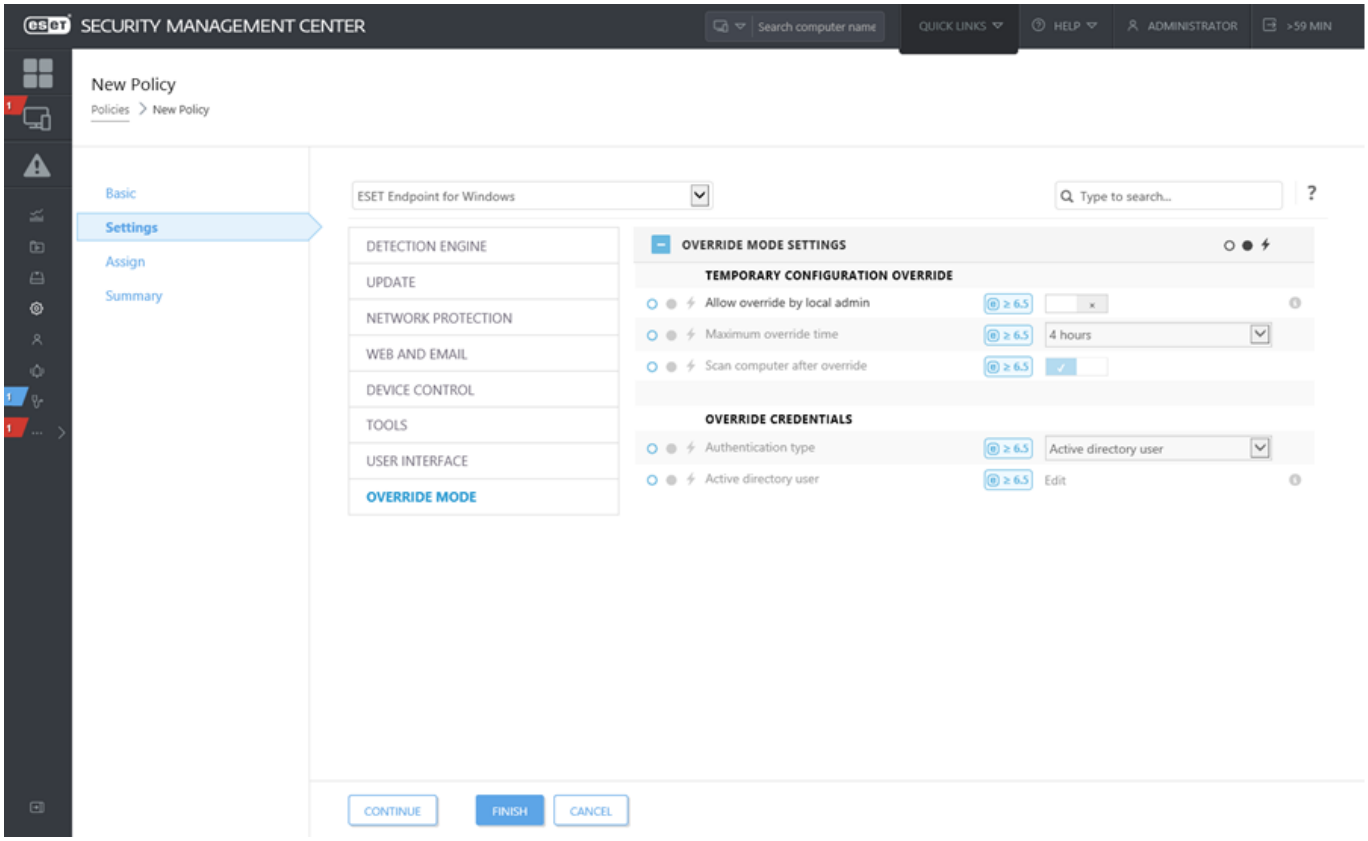
2. Dans la section **Général** , saisissez un **nom** et une **description** pour cette stratégie.

3. Dans la section **Paramètres** , sélectionnez **ESET Endpoint pour Windows**.

4. Cliquez sur **Mode de remplacement**, puis configurez les règles du mode de remplacement.

5. Dans la section **Attribuer** , sélectionnez l'ordinateur ou le groupe d'ordinateurs auquel celle stratégie doit être appliquée.

6. Passez en revue les paramètres dans la section **Synthèse** et cliquez sur **Terminer** pour appliquer la stratégie.



Exemple

Si *John* rencontre un problème parce que ses paramètres Endpoint bloquent une fonctionnalité importante ou l'accès à Internet sur son ordinateur, l'administrateur peut autoriser *John* à remplacer sa stratégie Endpoint existante et modifier manuellement les paramètres sur cet ordinateur. Ces nouveaux paramètres peuvent être ensuite demandés par ESMC pour que l'administrateur puisse créer une stratégie à partir de ces derniers.
Pour ce faire, procédez comme suit :
1. Accédez à **Politiques** > **Nouvelle politique**.
2. Renseignez les champs **Nom** et **Description**. Dans la section **Paramètres**, sélectionnez **ESET Endpoint pour Windows**.
3. Cliquez sur **Mode de remplacement**, activez le mode pour une heure et sélectionnez *Jean* en tant qu'utilisateur Active Directory.
4. Attribuez la stratégie à l'*ordinateur de Jean*, puis cliquez sur **Terminer** pour enregistrer la stratégie.
5. *Jean* doit activer le **mode de remplacement** dans ESET Endpoint et modifier manuellement les paramètres sur son ordinateur.
6. Dans ESMC Web Console, accédez à **Ordinateurs**, sélectionnez l'*ordinateur de Jean*, puis cliquez sur **Afficher les détails**.
7. Dans la section **Configuration**, cliquez sur **Demander la configuration** pour planifier une tâche client afin d'obtenir dès que possible la configuration du client.
8. Peu de temps après, la nouvelle configuration apparaît. Cliquez sur le produit pour lequel vous souhaitez enregistrer les paramètres, puis cliquez sur **Ouvrir la configuration**.
9. Vous pouvez passer en revue les paramètres et cliquer sur **Convertir en stratégie**.
10. Renseignez les champs **Nom** et **Description**.
11. Dans la section **Paramètres**, vous pouvez modifier les paramètres en cas de besoin.
12. Dans la section **Attribuer**, vous pouvez attribuer la stratégie à l'*ordinateur de Jean* (ou à d'autres).
13. Cliquez sur **Terminer** pour enregistrer les paramètres.
14. N'oubliez pas de supprimer la stratégie de remplacement lorsqu'elle n'est plus utile.

Comment appliquer une politique recommandée pour ESET Endpoint Antivirus

Après avoir connecté ESET Endpoint Antivirus à ESET Security Management Center, il est conseillé d'appliquer une politique recommandée ou personnalisée.

Il existe plusieurs politiques intégrées pour ESET Endpoint Antivirus :

Politique	Description
Antivirus - Équilibré	Configuration de la sécurité recommandée pour la plupart des configurations.
Antivirus - Sécurité maximale	Permet de tirer parti de l'apprentissage machine, de l'inspection comportementale profonde et du filtrage de protocole SSL. La détection des applications potentiellement dangereuses, indésirables et suspectes n'est pas affectée.
Système de réputation et de commentaires dans le cloud	Active le système de réputation et de commentaires dans le cloud ESET LiveGrid® pour améliorer la détection des dernières menaces et permettre le partage de menaces potentielles malveillantes ou inconnues pour analyse.
Contrôle des appareils - Sécurité maximale	Tous les appareils sont bloqués. Lorsqu'un appareil doit être connecté, un administrateur doit autoriser la connexion.

Contrôle des appareils - Lecture seule	Tous les périphériques ne sont accessibles qu'en lecture. Aucun accès en écriture n'est autorisé.
Pare-feu - Bloquer tout le trafic, à l'exception des connexions à ESMC et EEI	Bloquez l'ensemble du trafic, à l'exception des connexions à ESET Security Management Center et ESET Enterprise Inspector Server (ESET Endpoint Security uniquement).
Consignation - Consignation des diagnostics complets	Ce modèle permet à l'administrateur de disposer de tous les journaux lorsqu'il en a besoin. Tous les événements sont consignés à partir d'une verbosité minimale, notamment les paramètres Threatsense, HIPS et le pare-feu. Les journaux sont automatiquement supprimés après 90 jours.
Consignation - Consigner uniquement les événements importants	La stratégie permet de s'assurer que les avertissement, erreurs et événements critiques sont consignés. Les journaux sont automatiquement supprimés après 90 jours.
Visibilité - Équilibré	Paramètre de visibilité par défaut. Les états et notifications sont activés.
Visibilité - Mode invisible	Les notifications, les alertes, l'interface utilisateur graphique et les possibilités d'intégration au menu contextuel sont désactivées. Aucun fichier egui.exe n'est exécuté. Ce mode convient uniquement à la gestion à partir d'ESET PROTECT Cloud.
Visibilité - Interaction limitée avec l'utilisateur	Les états et les notifications sont désactivés. L'interface utilisateur graphique est présentée.

Pour définir la politique appelée **Antivirus - Sécurité maximale** qui applique plus de 50 configurations recommandées pour le produit ESET Endpoint Antivirus installé sur vos postes de travail, procédez comme suit :

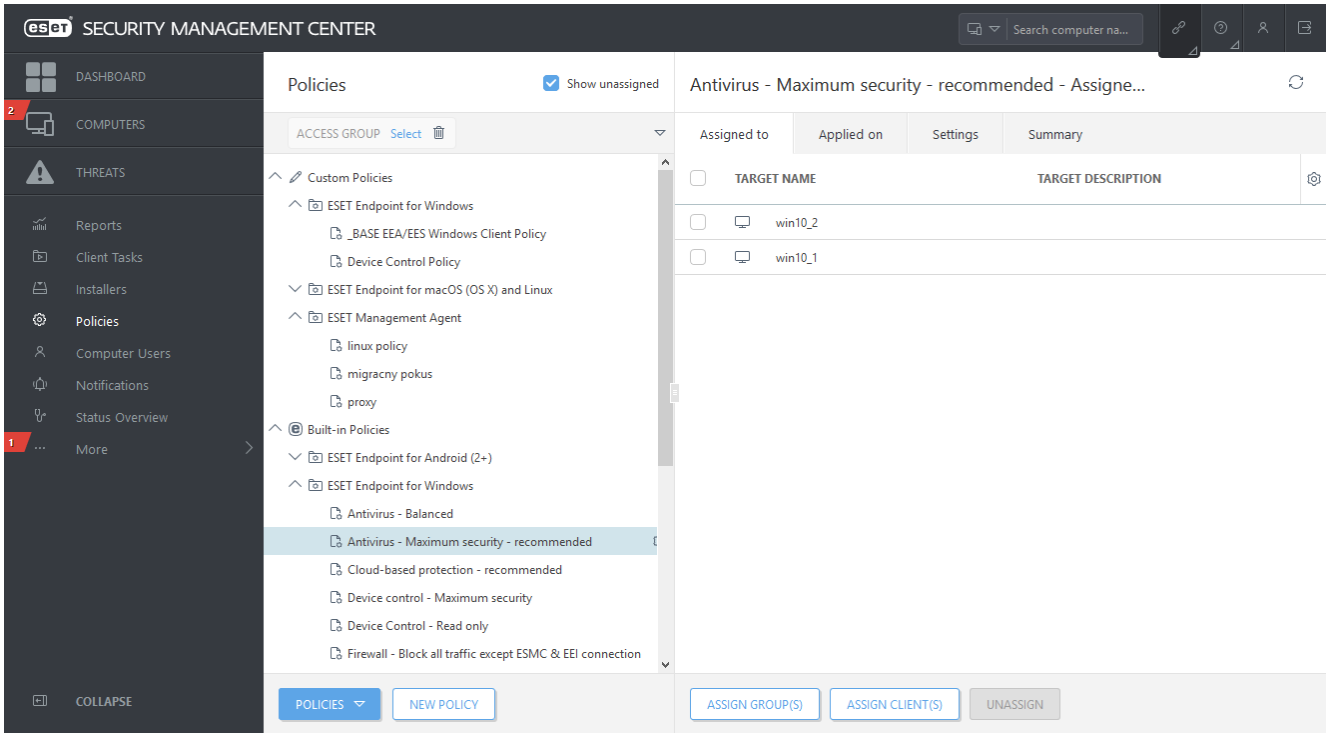
> **Instructions illustrées**
> Les articles suivants de la base de connaissances ESET peuvent être disponibles uniquement en anglais :
> • Appliquer une politique recommandée ou prédéfinie pour ESET Endpoint Antivirus à l'aide d'ESMC

1. Ouvrez la console web ESMC Web Console.

2. Accédez à **Politiques**, puis développez **Politiques prédéfinies** > **ESET Endpoint pour Windows**.

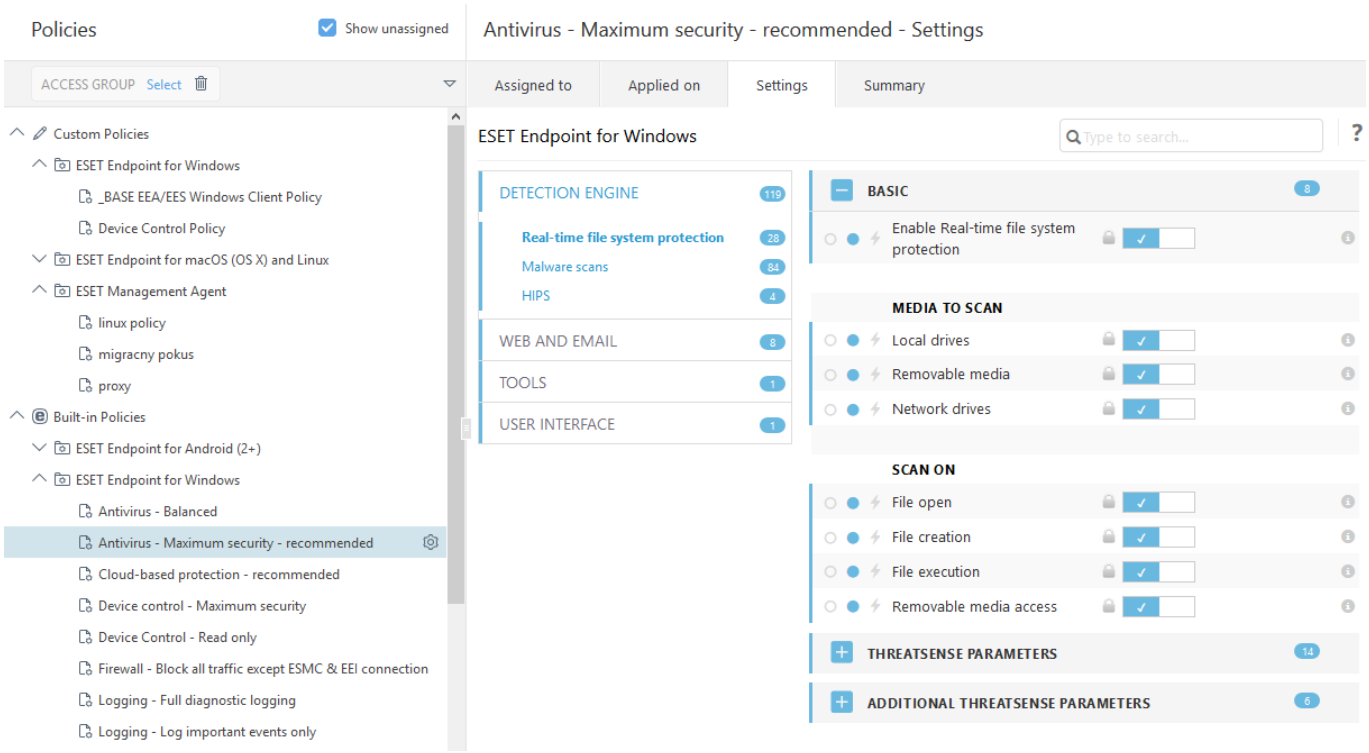
3. Cliquez sur **Antivirus - Sécurité maximale - recommandé**.

4. Dans l'onglet **Affectée à**, cliquez sur **Affecter un ou des clients** ou **Affecter un ou des groupes**, puis sélectionnez les ordinateurs appropriés pour lesquels vous souhaitez appliquer cette politique.



Pour déterminer quelles configurations sont appliquées pour cette politique, cliquez sur l'onglet **Paramètres** et développez l'arborescence Configurations avancées.

- Le point bleu représente une configuration modifiée pour cette politique.
- Le chiffre dans le cadre bleu représente le nombre de configurations modifiées par cette politique.
- En savoir plus sur les politiques ESMC



Comment configurer un miroir

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

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

1. Appuyez sur **F5** pour accéder à la Configuration avancée, puis développez **Mise à jour** > **Profils** > **Miroir de mise à jour**.

2. Développez **Mises à jour** et vérifiez que l'option **Choisir automatiquement** sous **Mises à jour des modules** est activée.

3. Développez **Miroir de mise à jour** et activez **Créer un miroir de mise à jour** et **Activer le serveur HTTP**.

Pour plus d'informations, consultez Miroir de mise à jour.

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

1. Créez un dossier partagé sur un appareil local ou réseau. Ce dossier doit être accessible en lecture par tous les utilisateurs exécutant les solutions de sécurité ESET. Il doit également être accessible en écriture à partir du compte SYSTEM local.

2. Activez **Créer un miroir de mise à jour** sous **Configuration avancée** > **Mise à jour** > **Profils** > **Miroir de mise à jour**.

3. Sélectionnez un **dossier de stockage** adéquat en cliquant sur **Effacer**, puis sur **Modifier**. Accédez au dossier partagé créé, puis sélectionnez-le.

> **Remarque**
> Si vous ne souhaitez pas fournir des mises à jour de module via un serveur HTTP interne, désactivez **Créer un miroir de mise à jour**.

Comment effectuer une mise à niveau vers Windows 10 avec ESET Endpoint Antivirus

> **Avertissement**
> Il est vivement conseillé d'effectuer une mise à niveau vers la dernière version du produit ESET, puis de télécharger les mises à jour les plus récentes des modules avant la mise à niveau vers Windows 10. Cela permet de garantir une protection maximale et de conserver les paramètres du programme et les informations de licence pendant la mise à niveau vers Windows 10.

Version 7.x :

Pour télécharger et installer la version la plus récente afin de préparer la mise à niveau vers Windows 10, cliquez sur le lien adéquat ci-dessous :

Télécharger ESET Endpoint Security 7 32 bits Télécharger ESET Endpoint Antivirus 7 32 bits

Télécharger ESET Endpoint Security 7 64 bits Télécharger ESET Endpoint Antivirus 7 64 bits

Version 5.x :

Important
Les produits ESET Endpoint version 5 font actuellement l'objet d'un support de base. Cela signifie qu'ils ne peuvent plus être téléchargés publiquement. Il est vivement recommandé d'effectuer une mise à niveau vers la dernière version des produits ESET Endpoint. Si vous devez accéder aux programmes d'installation MSI, contactez le support technique ESET pour obtenir de l'aide.

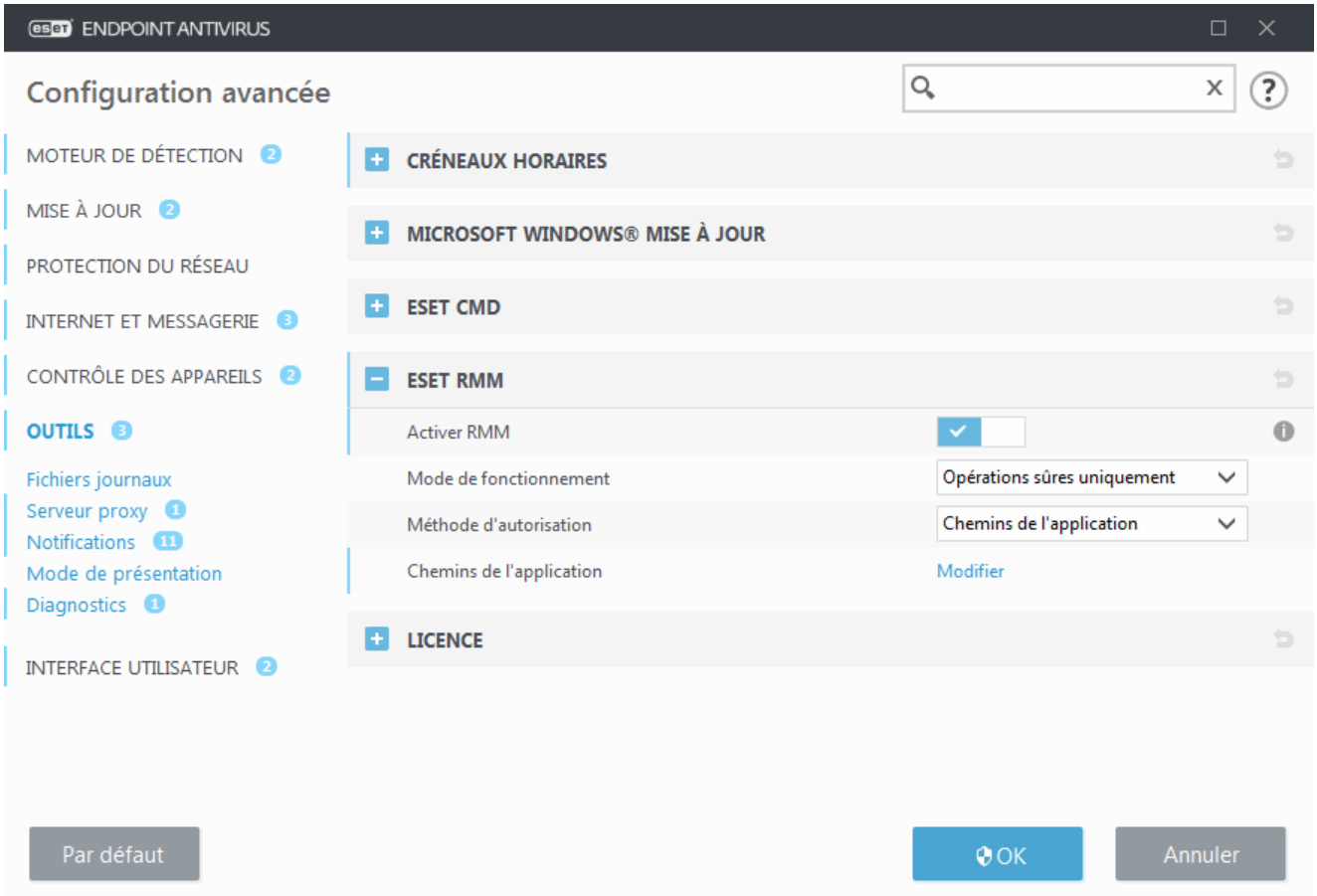
Autres versions linguistiques :

Si vous recherchez une autre version linguistique du produit ESET Endpoint, consultez notre page de téléchargement.

Remarque
Informations supplémentaires sur la compatibilité des produits ESET pour les entreprises avec Windows 10.

Activation de la surveillance et de l'administration à distance

La surveillance et l'administration à distance (RMM, Remote Monitoring and Management) est le processus qui consiste à surveiller et contrôler les systèmes logiciels (comme ceux des postes de travail, serveurs et appareils mobiles) à l'aide d'un agent installé localement qui est accessible par un fournisseur de services d'administration. ESET Endpoint Antivirus peut être géré par RMM à partir de la version 6.6.2028.0.



Par défaut, ESET RMM est désactivé. Pour l'activer, appuyez sur **F5** afin d'accéder à la configuration avancée, cliquez sur **Outils**, développez **ESET RMM** et activez le commutateur situé en regard de l'option **Activer RMM**.

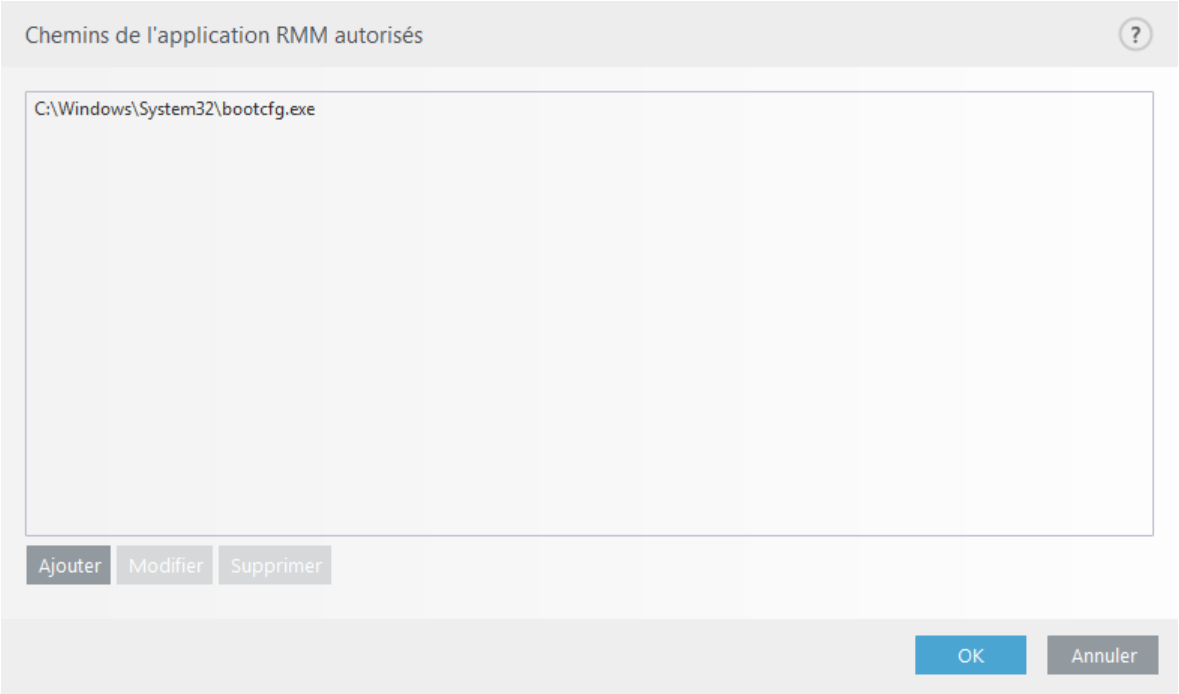
Mode de fonctionnement : sélectionnez **Opérations sûres uniquement** si vous souhaitez activer l'interface RMM pour les opérations sûres et en lecture seule. Sélectionnez **Toutes les opérations** si vous souhaitez activer l'interface RMM pour toutes les opérations.

Opération	Mode Opérations sûres uniquement	Mode Toutes les opérations
Get application-info	✔	✔
Get configuration	✔	✔
Obtenir des informations sur les licences	✔	✔
Get logs	✔	✔
Obtenir l'état de la protection	✔	✔
Obtenir l'état de la mise à jour	✔	✔
Set configuration		✔
Start activation		✔
Start scan	✔	✔
Start update	✔	✔

Méthode d'autorisation – Définissez la méthode d'autorisation RMM. Pour utiliser l'autorisation, sélectionnez **Chemin d'accès à l'application** dans le menu déroulant. Sinon, sélectionnez **Aucune**.

Avertissement
RMM doit toujours utiliser une méthode d'autorisation pour empêcher les logiciels malveillants de désactiver ou de contourner la protection d'ESET Endpoint.

Chemins de l'application : application spécifique autorisée à exécuter RMM. Si vous avez sélectionné **Chemin d'accès à l'application** comme méthode d'autorisation, cliquez sur **Modifier** pour ouvrir la fenêtre de configuration **Chemins de l'application RMM autorisés**.



Ajouter : permet de créer un chemin d'accès autorisé à l'application RMM. Saisissez le chemin d'accès ou cliquez sur le bouton **...** pour sélectionner un exécutable.

Modifier : permet de modifier un chemin d'accès autorisé existant. Utilisez l'option **Modifier** si l'emplacement de l'exécutable a été changé et qu'il se trouve dans un autre dossier.

Supprimer : permet de supprimer un chemin d'accès autorisé existant.

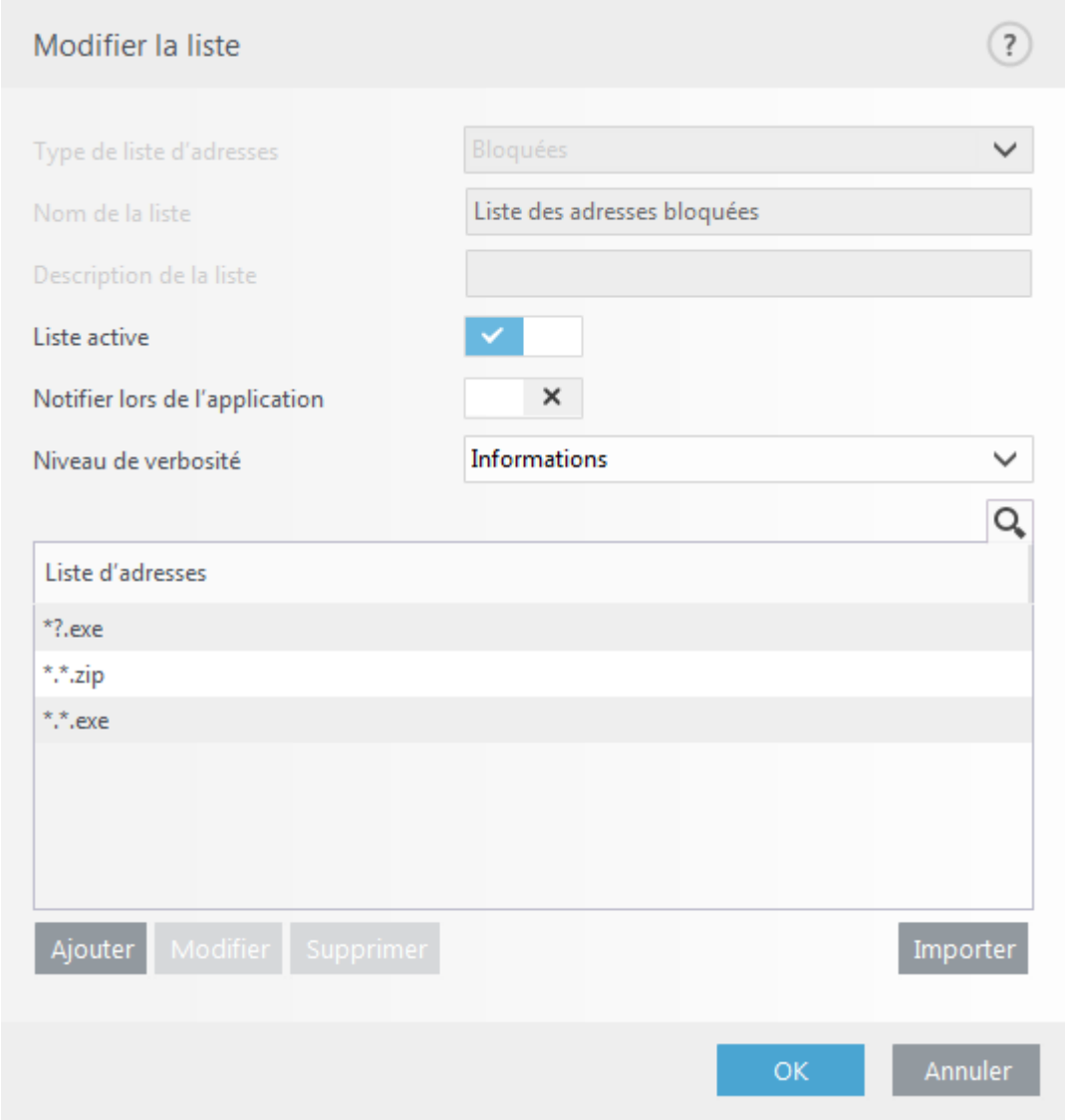
ESET Endpoint Antivirus Par défaut contient le fichier ermm.exe qui figure dans le répertoire de l'application Endpoint (chemin d'accès par défaut : C*:\Program Files\ESET\ESET Security*). ermm.exe échange des données avec RMM Plugin, qui communique avec RMM Agent, associé à un serveur RMM Server.

- ermm.exe : utilitaire de ligne de commande développé par ESET qui permet de gérer les produits Endpoint et les communications avec un RMM Plugin.
- RMM Plugin est une application tierce qui s'exécute localement sur le système Endpoint Windows. Le plugin a été conçu pour communiquer avec un RMM Agent spécifique (Kaseya, par exemple) et ermm.exe.
- RMM Agent est une application tierce (de Kaseya par exemple) qui s'exécute localement sur le système Endpoint Windows. L'Agent communique avec RMM Plugin et RMM Server.

Blocage du téléchargement de types de fichiers spécifiques depuis Internet

Si vous ne souhaitez pas autoriser le téléchargement de types de fichiers spécifiques (par exemple, exe, pdf ou zip) sur Internet, utilisez la Gestion des adresses URL avec une combinaison de caractères génériques. Appuyez sur la touche F5 pour accéder à Configuration avancée. Cliquez sur Internet et messagerie > Protection de l'accès Web et développez Gestion des adresses URL. Cliquez sur Modifier en regard de la liste d'adresses.

Dans la fenêtre Liste d'adresses, sélectionnez Liste des adresses bloquées et cliquez sur Modifier ou cliquez sur Ajouter pour créer une liste. Une nouvelle fenêtre s'ouvre. Si vous créez une liste, sélectionnez Bloqué dans le menu déroulant du type de liste d'adresses et donnez un nom à la liste. Si vous souhaitez être averti lors de l'accès à un type de fichier figurant dans la liste actuelle, activez la barre de curseur Notifier lors de l'application. Sélectionnez le niveau de verbosité dans le menu déroulant. Remote Administrator peut collecter des entrées avec la verbosité Avertissement.



Cliquez sur Ajouter pour entrer un masque qui spécifie les types de fichiers dont vous voulez bloquer le téléchargement. Saisissez l'URL complète si vous souhaitez bloquer le téléchargement d'un fichier spécifique d'un site Web spécifique, par exemple, http://exemple.fr/fichier.exe. Vous pouvez utiliser des caractères génériques pour indiquer un groupe de fichiers. Un point d'interrogation (?) représente un seul caractère variable tandis qu'un astérisque (*) représente une chaîne variable de zéro caractère ou plus. Par exemple, le masque */* bloque

le téléchargement de tous les fichiers ZIP compressés.

Notez que vous ne pouvez bloquer le téléchargement de types de fichiers spécifiques à l'aide de cette méthode que si l'extension du fichier fait partie de l'URL du fichier. Si la page web utilise des URL de téléchargement de fichier, par exemple *www.example.com/download.php?fileid=42*, les fichiers situés à cette adresse seront téléchargés même s'ils sont dotés d'une extension que vous avez bloquée.

Comment limiter l'interface utilisateur d'ESET Endpoint Antivirus

En cas de gestion à distance, vous pouvez appliquer une politique prédéfinie de visibilité.

Sinon, effectuez les étapes manuellement :

1. Appuyez sur **F5** pour accéder aux Configurations avancées, puis développez **Interface utilisateur** > **Éléments de l'interface utilisateur**.
2. Définissez **Mode de démarrage** sur la valeur souhaitée. Plus d'informations sur les modes de démarrage.
3. Désactivez les options **Afficher l'écran de démarrage** et **Émettre un signal sonore**.
4. Configurez les notifications.
5. Configurez les états d'application.
6. Configurez les messages de confirmation.
7. Configurez les alertes et boîtes de message.

Contrat de licence de l'utilisateur final

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, EN INSTALLANT, EN COPIANT OU EN 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, 851 01 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. Si vous n'êtes pas d'accord avec tous les termes et conditions du présent Contrat, 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) **Version Business Edition.** Une version Business Edition du Logiciel est requise pour utiliser le Logiciel sur des serveurs de courrier, relais de courrier, passerelles de courrier 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.** La Licence du Logiciel acheté à un fabricant d'équipement informatique ne s'applique qu'à l'ordinateur avec lequel vous l'avez obtenu. 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 à publier des mises à jour du Logiciel (« Mises à jour ») de temps à autre, mais n'en a pas l'obligation. Cette fonction est activée dans la configuration standard du Logiciel ; les Mises à jour sont donc installées automatiquement, sauf si l'Utilisateur Final a désactivé l'installation automatique des Mises à jour. 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.

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. Vous acceptez de recevoir des notifications et des messages, notamment des informations commerciales.

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. 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. 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 (« Lois sur le contrôle des exportations ») 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 (« Lois sur les sanctions »).

(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, 851 01 Bratislava, Slovak Republic.

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. En cas de discordance entre les versions linguistiques du présent Contrat, seule la version en langue anglaise fait foi. Le présent Contrat ne pourra être modifié que par un avenant écrit et signé par un représentant autorisé du Fournisseur ou une personne expressément autorisée à agir à ce titre en vertu d'un contrat de mandat.

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.

EULA ID: BUS-STANDARD-20-01

Politique de confidentialité

ESET, spol. s r.o., dont le siège social est établi au Einsteinova 24, 851 01 Bratislava, Slovaquie, enregistrée au registre du commerce géré par le Tribunal de district de Bratislava I, Section Sro, Entrée No 3586/B, Numéro d'identification de l'entreprise 31333532, en tant que Contrôleur des données (« ESET » ou « Nous ») souhaite faire preuve de transparence en ce qui concerne le traitement des données personnelles et la confidentialité des clients. Pour cela, Nous publions cette Politique de confidentialité dans le seul but d'informer notre client (« Utilisateur Final » ou « Vous ») sur les sujets suivants :

- traitement des données personelles,
- confidentialité des données,
- droits des personnes concernées.

Traitement des données personelles

Les services ESET qui sont implémentés dans le produit sont fournis selon les termes du Contrat de Licence de l'Utilisateur Final (« 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 produit, tels qu'un service de mise à jour/mise à niveau, ESET LiveGrid®, une protection contre toute utilisation abusive des données, une assistance, etc. Pour que tous ces services soient fonctionnels, Nous devons collecter les informations suivantes :

- Mise à jour et autres statistiques relatives aux informations concernant l'installation et votre ordinateur, notamment la plate-forme sur laquelle notre produit est installé, et 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).
- Hachages unidirectionnels liés aux infiltrations dans le cadre du système de réputation ESET LiveGrid® qui améliore l'efficacité de nos solutions contre les logiciels malveillants en comparant les fichiers analysés à une base de données d'éléments en liste blanche et liste noire dans le cloud.
- 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 sur les appareils du réseau local, telles que le type, le fabricant, le modèle et/ou le nom de

l'appareil ;

- 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.

- Des informations de licence, telles que l'identifiant de la licence, et des données personnelles comme le nom, le prénom, l'adresse, l'adresse e-mail sont nécessaires pour la facturation, la vérification de l'authenticité de la licence et la fourniture de nos services.
- Des coordonnées et des données contenues dans vos demandes d'assistance sont requises pour la fourniture du 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.

Confidentialité des données

ESET est une entreprise présente dans le monde entier par le biais d'entités affiliées et de partenaires du réseau de distribution, de service et d'assistance ESET. Les informations traitées par ESET peuvent être transférées depuis et vers les entités affiliées ou les partenaires pour l'exécution du CLUF (pour la fourniture de services, l'assistance ou la facturation, par exemple). Selon votre position géographique et le service que Vous choisissez d'utiliser, il est possible que Nous devions transférer vos données vers un pays en l'absence de décision d'adéquation de la Commission européenne. Même dans ce cas, chaque transfert d'informations est soumis à la législation en matière de protection des données et n'est effectué que si cela s'avère nécessaire. Des clauses contractuelles standard, des règles d'entreprise contraignantes ou toute autre protection adéquate doivent être mises en place, sans aucune exception.

Nous faisons tout notre possible pour éviter que les données soient stockées plus longtemps que nécessaire, tout en fournissant les services en vertu du Contrat de Licence de l'Utilisateur Final. Notre période de rétention peut être plus longue que la durée de validité de votre licence, pour vous donner le temps d'effectuer votre renouvellement. Des statistiques réduites et rendues anonymes et d'autres données anonymes d'ESET LiveGrid® peuvent être traitées ultérieurement à des fins statistiques.

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 de données entraînant un risque pour vos droits et libertés, Nous sommes prêts à informer l'autorité de contrôle ainsi que les personnes concernées. En tant que personne concernée, Vous avez le droit de déposer une plainte auprès d'une autorité de contrôle.

Droits des personnes concernées

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. Sous réserve des conditions fixées par les lois applicables en matière de protection des données, en tant que personne concernée, les droits suivants Vous sont conférés :

- droit de demander l'accès à vos données personnelles auprès d'ESET,
- droit à la rectification de vos données personnelles si elles sont inexactes (Vous avez également le droit de compléter les données personnelles incomplètes),
- droit de demander l'effacement de vos données personnelles,
- droit de demander de restreindre le traitement de vos données personnelle,
- le droit de s'opposer au traitement des données
- le droit de porter plainte et
- droit à la portabilité des données.

Nous pensons que toutes les informations que nous traitons sont utiles et nécessaires pour fournir les services et produits à nos clients.

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