ESET Endpoint Security

Guide de l'utilisateur

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

ESET Endpoint Security 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 Security

ESET Endpoint Security représente une nouvelle approche de sécurité informatique véritablement intégrée. La dernière version du moteur d'analyse ESET LiveGrid®, associée à notre pare-feu personnalisé et notre module antispam des clients de messagerie, 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 Security est une solution complète de sécurité qui résulte de notre engagement à long terme d'offrir à la fois une protection maximale et un impact minimal sur le système. 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 Security est principalement destiné à être utilisé sur des postes de travail dans un environnement de petite entreprise.

Dans la section Installation, 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 Security avec ESET PROTECT On-Prem 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 Security et propose automatiquement des contenus de support mis à jour.
Mode sombre	Extension qui permet de passer rapidement l'écran dans un thème sombre. Vous pouvez choisir votre modèle de couleurs préféré dans les éléments de l'interface utilisateur.
Antivirus et antispyware	Détecte et supprime de manière proactive un grand nombre de virus, vers, chevaux de Troie et rootkits, connus et inconnus. La technologie d'heuristique avancée reconnaît même les logiciels malveillants jamais rencontrés auparavant ; elle vous protège des menaces inconnues et les neutralise avant qu'elles ne puissent causer le moindre dommage à votre ordinateur. La protection de l'accès Web et l'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 Security.
Gestion à distance	ESET PROTECT On-Prem 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. À l'aide de la console web ESET PROTECT On-Prem Web Console (ESET PROTECT On-Prem Web Console), vous pouvez 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.
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 filtrage web permet de bloquer les pages web dont le contenu est susceptible d'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

Nouveautés d'ESET Endpoint Security version 11

Nouvel éditeur de règles de pare-feu

L'éditeur de règles de pare-feu a été repensé pour vous permettre de définir plus facilement des règles de pare-feu avec des options de configuration supplémentaires.

Gestion des vulnérabilités et des correctifs

Fonctionnalité disponible dans ESET PROTECT qui analyse régulièrement un poste de travail pour détecter tout logiciel installé vulnérable aux risques de sécurité. La gestion des correctifs vérifie si l'espace disponible correspond avant de commencer le téléchargement (la valeur par défaut et minimale est de 2 Go) et permet de limiter ces risques grâce à des mises à jour logicielles automatisées, ce qui renforce la sécurité des appareils.

États de produit en fin de vie

ESET Endpoint Security dans cette version peut afficher divers états de prise en charge de l'application. Vous pouvez configurer les communications de l'état de la prise en charge de l'application dans Notifications.

Corrections de bogue diverses et améliorations des performances

Configuration système requise

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

Processeurs pris en charge

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

processeur ARM64, 1 GHz ou vitesse supérieure

Systèmes d’exploitation

Microsoft® Windows® 11

Microsoft® Windows® 10

Pour obtenir la liste détaillée des versions de Microsoft® Windows® 10 et Microsoft® Windows® 11 prises en charge, consultez la politique de prise en charge des systèmes d’exploitation Windows.

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

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

Configuration requise pour les fonctionnalités ESET Endpoint Security

Consultez la configuration requise pour des fonctionnalités ESET Endpoint Security spécifiques dans le tableau suivant :

Fonctionnalité	Configuration requise
Intel® Threat Detection Technology	Consultez les processeurs pris en charge.
Navigateur sécurisé	Consultez les navigateurs web pris en charge.
Outil de nettoyage spécialisé	Processeur autre que ARM64.
Bloqueur d'exploit	Processeur autre que ARM64.
Inspection comportementale approfondie	Processeur autre que ARM64.

Le programme d'installation ESET Endpoint Security créé dans ESET PROTECT On-Prem prend en charge Windows 10 Entreprise pour les bureaux virtuels et le mode multisession de Windows 10.

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

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

(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) L'espace disque est nécessaire pour télécharger le programme d'installation, installer le produit, conserver une copie du package d'installation dans les données du programme et enregistrer 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). Nous recommandons de conserver suffisamment d'espace disque pour prendre en charge les mises à jour du système d'exploitation et des produits ESET.
(3) Bien que ce type de mise à jour ne soit pas recommandé, vous pouvez mettre à jour manuellement le produit à partir d'un support amovible.

Langues prises en charge

ESET Endpoint Security 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
Nederlands	nl-NL	1043
Norvégien	nb-NO	1044
Polonais	pl-PL	1045

Langue	Code de langue	LCID
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
Ukrainien (Ukraine)	uk-UA	1058
*Vietnamien	vi-VN	1066

* ESET Endpoint Security 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).

Journal des modifications

Prévention

Lorsque vous utilisez votre ordinateur et particulièrement lorsque vous surfez sur Internet, n'oubliez pas qu'aucun antivirus ne peut complètement éliminer le risque de détections et d'attaques distantes. Pour bénéficier d'une protection maximale, vous devez utiliser votre solution antivirus correctement et 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 les niveaux de protection des utilisateurs. Pour une efficacité maximale, les mises à jour doivent être configurées correctement sur votre système. Pour plus d'informations sur la procédure de configuration des mises à jour, reportez-vous au Configuration des mises à jour.

Télécharger les patchs de sécurité

Les auteurs de programmes malveillants exploitent souvent des 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 Microsoft Edge, 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 de données. Il est essentiel de sauvegarder régulièrement vos données 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 en temps réel du système de fichiers. 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

La règle la plus utile et la plus efficace est d'être 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.

État de fin de vie

ESET Endpoint Security peut afficher des notifications ou des avertissements automatisés pour vous informer d'état de fin de vie à venir à plusieurs endroits dans la fenêtre principale du programme.

En savoir plus sur :
- Politique de fin de vie (produits pour les entreprises)
- Mises à jour du produit
- Mises à jour de la sécurité et de la stabilité

Pour plus d'informations sur les modifications d'ESET Endpoint Security, consultez cet article de la base de connaissances ESET.

Le tableau ci-dessous présente quelques exemples d'états de produit et de notifications avec des actions basées sur des catégories :

Catégorie	Fenêtre de notification ou d'alerte	Page de mise à jour	Page d'aide et d'assistance
Nouvelle fonctionnalité ou mise à jour disponible	Nouvelle version de disponible Une mise à jour contenant des correctifs importants requis par ESET Endpoint Security est disponible. Effectuez maintenant la mise à jour pour bénéficier de la protection la plus récente. **Action** : En savoir plus	Nouvelle version de ESET Endpoint Security disponible. Nouvelle version de ESET Endpoint Security disponible. **Actions** : Mettre à jour maintenant/Activer les mises à jour automatiques	Nouvelle version de ESET Endpoint Security disponible. Effectuez maintenant une mise à jour pour obtenir la dernière version avec de nouvelles fonctionnalités et améliorations. Prise en charge jusqu'au : jj/mm/aaaa
	Une mise à jour est disponible Nouvelle version de ESET Endpoint Security disponible. Effectuez maintenant une mise à jour pour obtenir la dernière version avec de nouvelles fonctionnalités et améliorations. **Action** : En savoir plus	Une mise à jour pour ESET Endpoint Security est disponible Numéro de version installée Prise en charge jusqu'au : jj/mm/aaaa **Action** : En savoir plus	Une mise à jour contenant des correctifs importants requis par ESET Endpoint Security est disponible. Effectuez maintenant la mise à jour pour bénéficier de la protection la plus récente. Prise en charge jusqu'au : jj/mm/aaaa
	Un redémarrage de l'appareil est recommandé Une mise à jour contenant des correctifs importants requis par ESET Endpoint Security est disponible. Effectuez maintenant la mise à jour pour bénéficier de la protection la plus récente. **Action** : En savoir plus		Prise en charge jusqu'au : jj/mm/aaaa
	Une mise à jour critique est disponible Une mise à jour contenant des correctifs critiques requis par ESET Endpoint Security est disponible. Effectuez maintenant la mise à jour pour bénéficier de la protection la plus récente. **Action** : En savoir plus	Une mise à jour critique pour ESET Endpoint Security est disponible Numéro de version installée Prise en charge jusqu'au : jj/mm/aaaa **Action** : En savoir plus	Une mise à jour contenant des correctifs critiques requis par ESET Endpoint Security est disponible. Effectuez maintenant la mise à jour pour bénéficier de la protection la plus récente. Prise en charge jusqu'au : jj/mm/aaaa
	Un redémarrage de l'appareil est nécessaire Une mise à jour de numéro de version a été téléchargée. Elle contient des correctifs de maintenance et de stabilité importants requis par ESET Endpoint Security. Effectuez maintenant la mise à jour pour bénéficier de la protection la plus récente. **Action** : En savoir plus		Prise en charge jusqu'au : jj/mm/aaaa

Catégorie	Fenêtre de notification ou d'alerte	Page de mise à jour	Page d'aide et d'assistance
Expiration de la prise en charge de l'application	La prise en charge de la version de l'application installée se termine le jj/mm/aaaa. Votre appareil ne sera bientôt plus protégé. Effectuez maintenant une mise à jour pour rester protégé. **Action** : Mettre à jour maintenant	Numéro de version installée/Prise en charge jusqu'au : jj/mm/aaaa **Actions** : Mettre à jour maintenant/Activer les mises à jour automatiques	La prise en charge de la version installée d'ESET Endpoint Security se termine bientôt. Votre ordinateur ne sera alors plus protégé. Effectuez maintenant une mise à jour pour rester protégé. Prise en charge jusqu'au : jj/mm/aaaa
	La prise en charge étendue ESET pour la version de l'application installée se termine le jj/mm/aaaa. Votre appareil ne sera bientôt plus protégé. Effectuez maintenant une mise à jour pour rester protégé. **Action** : Mettre à jour maintenant	Numéro de version installée/Prise en charge jusqu'au : jj/mm/aaaa **Actions** : Mettre à jour maintenant/Activer les mises à jour automatiques	La prise en charge étendue ESET pour la version installée d'ESET Endpoint Security se termine bientôt. Votre appareil ne sera alors plus protégé. Effectuez maintenant une mise à jour pour rester protégé. Prise en charge jusqu'au : jj/mm/aaaa
	Le système d'exploitation installé est obsolète et la prise en charge de la version de l'application installée se termine le jj/mm/aaaa. Mettez votre système d'exploitation à niveau pour obtenir la dernière mise à jour de l'application et rester protégé. **Actions** : En savoir plus	Numéro de version installée Prise en charge jusqu'au : jj/mm/aaaa **Action** : En savoir plus	La prise en charge de la version installée d'ESET Endpoint Security se termine bientôt. Votre ordinateur ne sera alors plus protégé. Effectuez maintenant une mise à jour pour rester protégé. Prise en charge jusqu'au : jj/mm/aaaa
	La prise en charge étendue ESET pour la version de l'application installée se termine bientôt Le système d'exploitation installé est obsolète et la prise en charge de la version de l'application installée se termine le jj/mm/aaaa. Mettez votre système d'exploitation à niveau pour obtenir la dernière mise à jour de l'application et rester protégé. **Action** : En savoir plus	La prise en charge étendue ESET pour la version installée d'ESET Endpoint Security se termine bientôt Numéro de version installée Prise en charge jusqu'au : jj/mm/aaaa **Actions** : En savoir plus	La prise en charge étendue ESET pour la version installée d'ESET Endpoint Security se termine bientôt. Votre appareil ne sera alors plus protégé. Effectuez maintenant une mise à jour pour rester protégé. Prise en charge jusqu'au : jj/mm/aaaa

Catégorie	Fenêtre de notification ou d'alerte	Page de mise à jour	Page d'aide et d'assistance
La version de l'application n'est plus prise en charge	⚠ La version de l'application installée n'est plus prise en charge La prise en charge de la version de l'application installée a pris fin. Votre appareil n'est peut-être plus protégé. Effectuez maintenant une mise à jour pour obtenir une protection. **Action** : Mettre à jour maintenant	⚠ La version installée d'ESET Endpoint Security n'est plus prise en charge Numéro de la version installée/Prise en charge jusqu'au : jj/mm/aaaa **Actions** : Mettre à jour maintenant/Activer les mises à jour automatiques	⚠ Prise en charge jusqu'au : jj/mm/aaaa
	⚠ La version de l'application installée n'est plus prise en charge Le système d'exploitation installé est obsolète et la prise en charge de la version de l'application installée a pris fin. Votre ordinateur n'est pas protégé. Mettez votre système d'exploitation à niveau pour recevoir la dernière mise à jour de l'application et bénéficier d'une protection. **Action** : En savoir plus	⚠ La version installée d'ESET Endpoint Security n'est plus prise en charge Numéro de version installée Prise en charge jusqu'au : jj/mm/aaaa **Action** : En savoir plus	⚠ La prise en charge de la version installée d'ESET Endpoint Security a pris fin. Votre ordinateur n'est plus protégé. Effectuez maintenant une mise à jour pour obtenir une protection. Prise en charge jusqu'au : jj/mm/aaaa
Mise à jour du système d'exploitation requise	Le système d'exploitation installé est obsolète Le système d'exploitation installé est obsolète. Mettez votre système d'exploitation à niveau pour obtenir la dernière mise à jour de l'application et rester protégé. **Action** : En savoir plus	✓ ESET Endpoint Security Numéro de version installée	Prise en charge jusqu'au : jj/mm/aaaa

Pages d'aide

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

Mise en route

Avant de commencer à utiliser ESET Endpoint Security, notez que le produit peut être géré à distance à l'aide d'ESET PROTECT On-Prem. 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 Security. Nous avons également préparé un guide qui vous aidera à configurer et à personnaliser les paramètres de base ESET Endpoint Security.

Utilisation des pages d'aide ESET Endpoint Security

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 Security. Un ensemble uniforme de symboles est également utilisé pour souligner des informations importantes.

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

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

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

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

Convention	Signification
Gras	Noms des éléments de l'interface (boutons d'option ou boîtes de dialogue, par exemple).
Italique	Espaces réservés 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 Security 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 Security peut être géré à distance par ESET PROTECT On-Prem ou ESET PROTECT.

- Présentation de ESET PROTECT On-Prem
- Présentation de ESET PROTECT

- ESET PROTECT HUB : passerelle centrale vers la plate-forme de sécurité unifiée ESET PROTECT On-Prem. Cette passerelle permet une gestion centralisée des identités, des abonnements et des utilisateurs pour tous les modules de la plate-forme ESET. Pour obtenir des instructions pour activer votre produit, consultez Gestion des licences ESET PROTECT On-Prem. ESET PROTECT HUB remplacera entièrement ESET Business Account et ESET MSP Administrator.

- ESET Business Account : portail de gestion des licences pour les produits ESET pour les entreprises. Consultez Gestion des licences ESET PROTECT On-Prem pour obtenir des instructions afin d'activer votre produit ou consultez l'aide en ligne ESET Business Account pour obtenir des informations supplémentaires sur l'utilisation d'ESET Business Account. Si vous possédez déjà un nom d'utilisateur et un mot de passe fournis par ESET et si vous voulez les convertir en clé de licence, consultez la section Convertir les informations d'identification de licence héritée.

Autres produits de sécurité

- ESET Inspect : il s'agit d'un système complet de détection et de réponse des terminaux comprenant les fonctionnalités suivantes : détection d'incidents, gestion des incidents et réponse, collecte de données, indicateurs de détection de corruptions, détection d'anomalies, détection de comportements et violations de politiques.
- ESET Endpoint Encryption : application de sécurité complète conçue pour protéger vos données au repos et en transit. Avec ESET Endpoint Encryption, vous pouvez chiffrer des fichiers, des dossiers et des e-mails ou créer des disques virtuels chiffrés, compresser des archives et inclure un outil de destruction de fichiers de bureau pour une suppression sécurisée des fichiers.

Outils de gestion à distance tiers

- Surveillance et administration à distance (RMM)

Bonnes pratiques

- Connectez tous les endpoints avec ESET Endpoint Security à ESET PROTECT On-Prem
- 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 Security

Guides de procédure

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

Présentation de ESET PROTECT On-Prem

ESET PROTECT On-Prem 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.

À l'aide de la console web ESET PROTECT On-Prem 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. Consultez également les rubriques suivantes : Présentation des éléments d'architecture et d'infrastructure ESET PROTECT On-Prem, Mise en route de la console web ESET PROTECT On-Prem Web Console et Environnements de configuration des postes de travail pris en charge.

ESET PROTECT On-Prem est constitué des composants suivants :

- ESET PROTECT On-Prem serveur : Il gère les communications avec les Agents, collecte les données d'application et les stocke dans la base de données. ESET PROTECT On-Prem Server peut être installé sur des serveurs Windows et Linux.
- ESET PROTECT On-Prem Web Console : Web Console constitue l'interface principale qui permet d'administrer les ordinateurs clients de votre environnement. Elle affiche une vue d'ensemble de l'état des clients sur le réseau et peut être utilisée pour déployer à distance les solutions ESET sur des ordinateurs non gérés. Une fois ESET PROTECT On-Prem Server (Server) installé, vous pouvez accéder à la console Web à l'aide de votre navigateur Web. Si vous décidez de rendre le serveur Web accessible à partir d'Internet, vous pouvez utiliser ESET PROTECT On-Prem à partir de presque n'importe quel emplacement et/ou appareil disposant d'une connexion Internet.
- ESET Management Agent : facilite la communication entre ESET PROTECT On-Prem Server et les ordinateurs clients. L'Agent doit être installé sur l'ordinateur client pour établir une communication entre ce dernier et ESET PROTECT On-Prem Server. Dans la mesure où ESET Management Agent est situé sur l'ordinateur client et peut stocker plusieurs scénarios de sécurité, son utilisation réduit considérablement le délai de réaction face aux nouvelles détections. À l'aide de la console web ESET PROTECT On-Prem Web Console, vous pouvez déployer ESET Management Agent sur des ordinateurs non administrés identifiés par Active Directory ou ESET RD Sensor. Vous pouvez également installer manuellement ESET Management Agent sur les ordinateurs clients, si nécessaire.
- ESET Rogue Detection Sensor : détecte les ordinateurs non administrés présents sur le réseau et envoie leurs informations à ESET PROTECT On-Prem Server. Vous pouvez ainsi gérer les nouveaux ordinateurs clients dans ESET PROTECT On-Prem sans avoir à les rechercher et à les ajouter manuellement. Rogue Detection Sensor mémorise les ordinateurs qui ont été détectés et n'envoie pas deux fois les mêmes informations.
- ESET Bridge : service qui peut être utilisé conjointement avec ESET PROTECT On-Prem pour :
    - Distribuer des mises à jour aux ordinateurs client et des packages d'installation à ESET Management Agent ;
    - Transférer les communications des ESET Management Agents vers ESET PROTECT On-Prem Server.
- Connecteur de périphérique mobile : composant qui permet de gérer les périphériques mobiles avec ESET PROTECT On-Prem, ce qui vous permet de gérer les périphériques mobiles (Android et iOS) et de gérer ESET Endpoint Security pour Android.
- Appliance virtuelle ESET PROTECT On-Prem : est destinée aux utilisateurs qui souhaitent exécuter ESET PROTECT On-Prem dans un environnement virtualisé.
- ESET PROTECT On-Prem Virtual Agent Host : un composant d'ESET PROTECT On-Prem qui virtualise les entités de l'agent pour gérer les machines virtuelles sans agent. Cette solution active l'automatisation, l'utilisation des groupes dynamiques et le même niveau de gestion des tâches qu'ESET Management Agent sur les ordinateurs physiques. L'Agent virtuel collecte les informations des machines virtuelles et les envoie

à ESET PROTECT On-Prem Server.

- Outil Miroir : est nécessaire pour les mises à jour des modules hors ligne. Si vos ordinateurs clients ne disposent pas d'une connexion Internet, vous pouvez utiliser l'outil Miroir pour télécharger les fichiers de mise à jour depuis les serveurs de mise à jour ESET et les stocker localement.
- ESET Remote Deployment Tool : déploie les packages tout-en-un qui ont été créés dans la console web <%PRODUCT%> Web Console. Il permet de distribuer de manière efficace ESET Management Agent avec un produit ESET sur les ordinateurs via un réseau.

Pour plus d'informations, reportez-vous à l'aide en ligne d'ESET PROTECT On-Prem.

Présentation de ESET PROTECT

ESET PROTECT 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 ESET PROTECT On-Prem ou . À l'aide de la console Web ESET PROTECT, 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.

ESET PROTECT est constitué des composants suivants :

- ESET PROTECT Instance : Il gère les communications avec les Agents, collecte les données d'application et les stocke dans la base de données.
- ESET PROTECT Web Console : Web Console constitue l'interface principale qui permet d'administrer les ordinateurs clients de votre environnement. Elle affiche une vue d'ensemble de l'état des clients sur le réseau et peut être utilisée pour déployer à distance les solutions ESET sur des ordinateurs non gérés. Vous pouvez utiliser ESET PROTECT à partir de n'importe quel endroit ou appareil doté d'une connexion internet.
- ESET Management Agent : facilite la communication entre ESET PROTECT et les ordinateurs clients. L'Agent doit être installé sur l'ordinateur client pour établir une communication entre ce dernier et ESET PROTECT. Dans la mesure où ESET Management Agent est situé sur l'ordinateur client et peut stocker plusieurs scénarios de sécurité, son utilisation réduit considérablement le délai de réaction face aux nouvelles détections. À l'aide de la console web ESET PROTECT Web Console, vous pouvez déployer ESET Management Agent sur des ordinateurs non administrés. Vous pouvez également installer manuellement ESET Management Agent sur les ordinateurs clients, si nécessaire.
- ESET Bridge : service qui peut être utilisé conjointement avec ESET PROTECT pour :
    - Distribuer des mises à jour aux ordinateurs client et des packages d'installation à ESET Management Agent ;
    - Transférer les communications des ESET Management Agents vers ESET PROTECT.
- Gestion des appareils mobiles : composant qui permet de gérer les périphériques mobiles avec ESET PROTECT, ce qui vous permet de gérer les périphériques mobiles (Android et iOS) et de gérer ESET Endpoint Security pour Android.
- Gestion des vulnérabilités et des correctifs : fonctionnalité disponible dans ESET PROTECT qui analyse régulièrement un poste de travail pour détecter tout logiciel installé susceptible d'être vulnérable aux risques de sécurité. La gestion des correctifs permet de corriger ces risques par le biais de mises à jour logicielles automatisées, ce qui renforce la sécurité des appareils.

Pour plus d'informations, reportez-vous à l'aide en ligne d'ESET PROTECT.

Paramètres protégés par mot de passe

Afin de procurer une sécurité maximale à votre système, ESET Endpoint Security 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 Security par mot de passe sur les ordinateurs clients connectés. Pour créer une politique :

1. Dans la console web ESET PROTECT On-Prem Web Console, cliquez sur **Politiques** dans le menu principal sur la 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 d'ESET Endpoint Security, cliquez sur le bouton bascule afin d'activer **Mot de passe pour protéger les paramètres**. Notez que la version 7 et les versions ultérieures d'ESET Endpoint offrent une protection améliorée. Si vous disposez des versions 7 et ultérieures et de la version 6 des produits Endpoint sur le réseau, il est recommandé de créer deux politiques distinctes avec un mot de passe différent pour chacune des versions.
7. Dans la fenêtre de notification, 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'ESET PROTECT On-Prem Web Console. Une politique 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 politiques sont appliquées dans l'ordre des groupes statiques. Pour les groupes dynamiques, les groupes dynamiques enfants sont d'abord parcourus. Vous pouvez ainsi appliquer des politiques avec un plus grand impact au niveau supérieur de l'arborescence des groupes et des politiques plus spécifiques pour les sous-groupes. À l'aide des indicateurs, un utilisateur ESET Endpoint Security 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'ESET PROTECT On-Prem.

Il est recommandé d'affecter des politiques plus génériques (la politique 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 Security 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 ESET PROTECT On-Prem 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.

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**.

Installation

Vous pouvez utiliser plusieurs méthodes d'installation de ESET Endpoint Security sur un poste de travail client, sauf si vous déployez ESET Endpoint Security à distance sur des postes de travail clients via ESET PROTECT On-Prem ou ESET PROTECT.

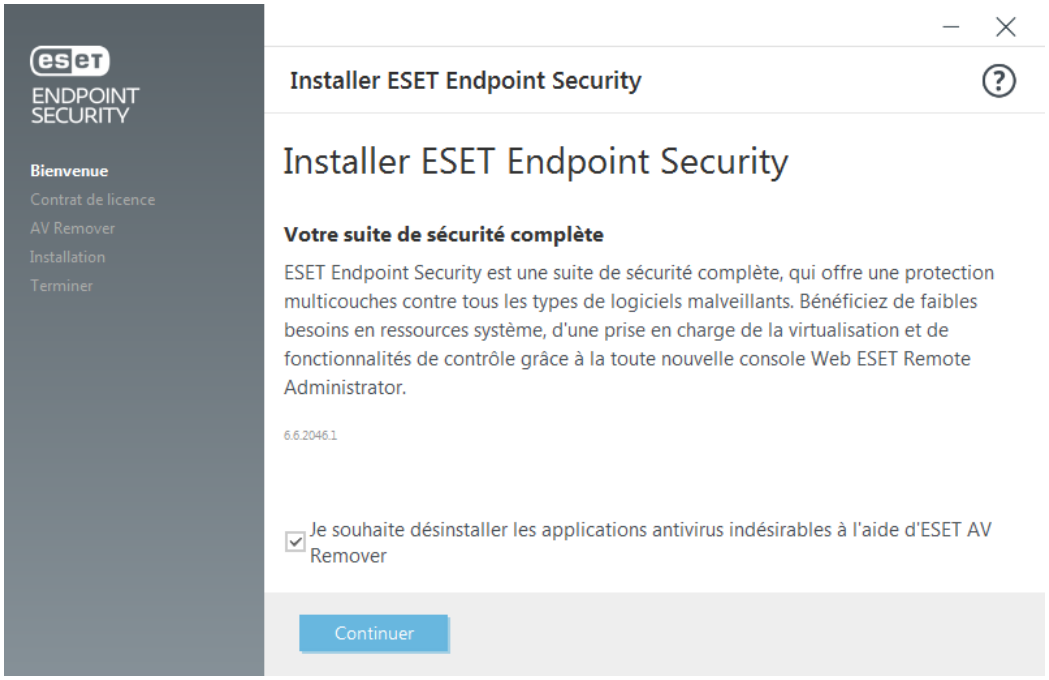
Vous pouvez passer de ESET Endpoint Security à ESET Endpoint Antivirus en exécutant le programme d'installation d'ESET Endpoint Antivirus avec ESET Endpoint Security déjà installé. Vous devez toutefois installer la même version ou une version ultérieure.

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 (version 64 bits) Télécharger (version 32 bits)
*** Installation (.exe)	Installation sans ESET AV Remover.	Télécharger (version 64 bits) Télécharger (version 32 bits)
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 PROTECT On-Prem.	Télécharger (version 64 bits) Télécharger (version 32 bits)
Installation à l'aide d'une ligne de commande	ESET Endpoint Security peut être installé localement à l'aide d'une ligne de commande ou à distance à l'aide d'une tâche client d'ESET PROTECT On-Prem.	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 Security 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 Security sur des postes de travail clients.	N/A

ESET Endpoint Security est disponible dans plus de 30 langues.

Installation à l'aide d'ESET AV Remover

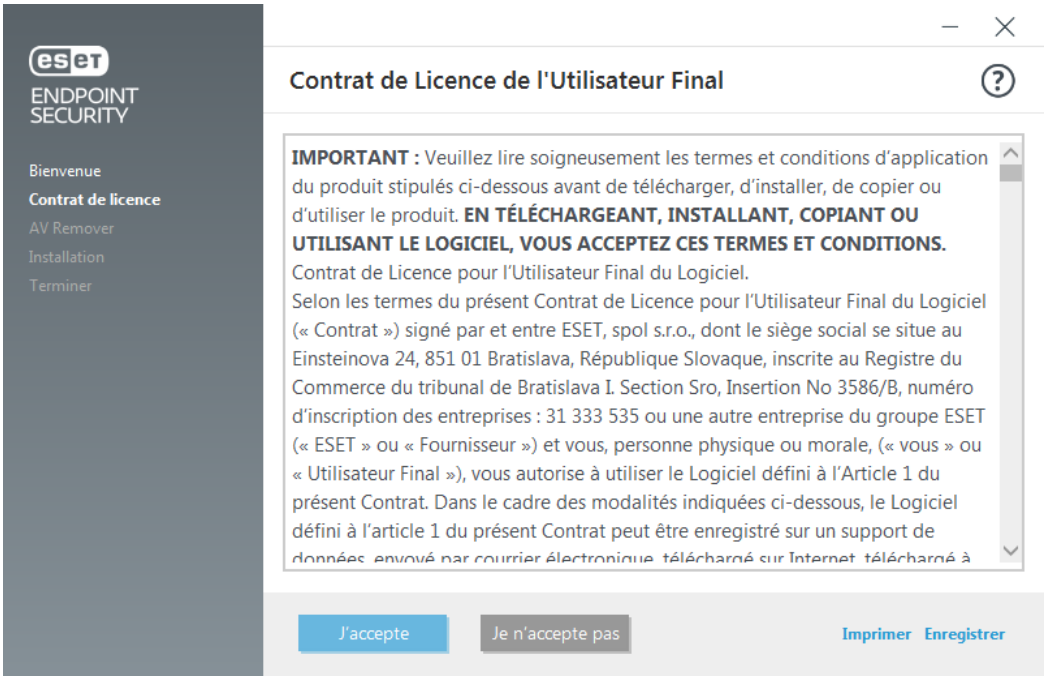
Avant de continuer la procédure d'installation, il est important de désinstaller toutes les applications de sécurité de l'ordinateur. Cochez la case en regard de l'option **Je souhaite désinstaller les applications antivirus indésirables à l'aide d'ESET AV Remover** pour qu'ESET AV Remover recherche 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 Security sans exécuter ESET AV Remover.



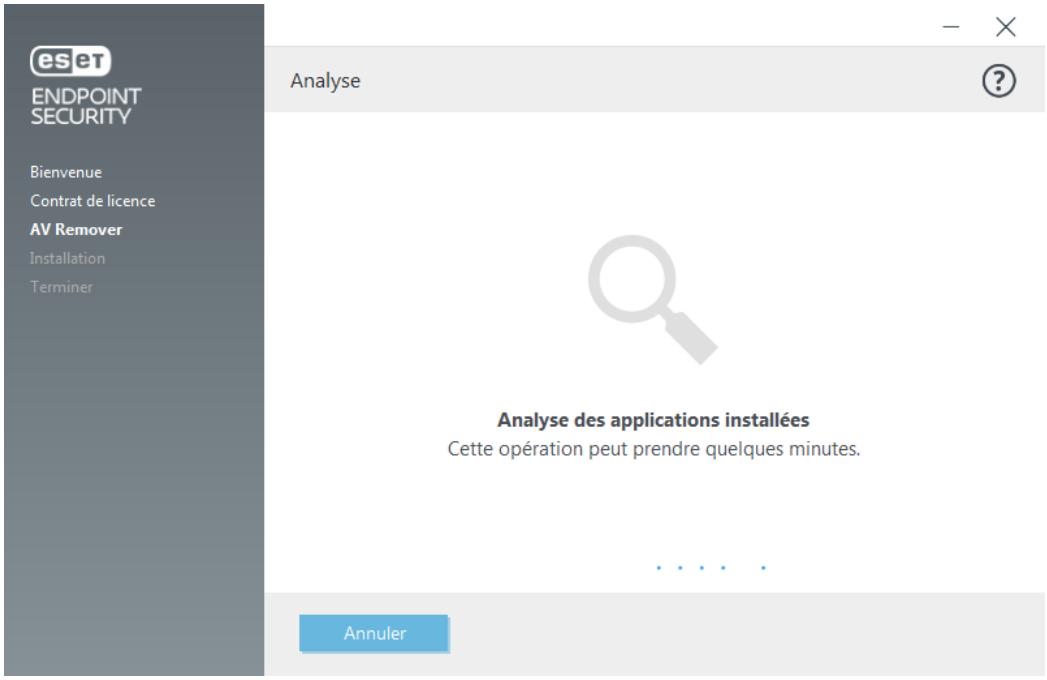
ESET AV Remover

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.

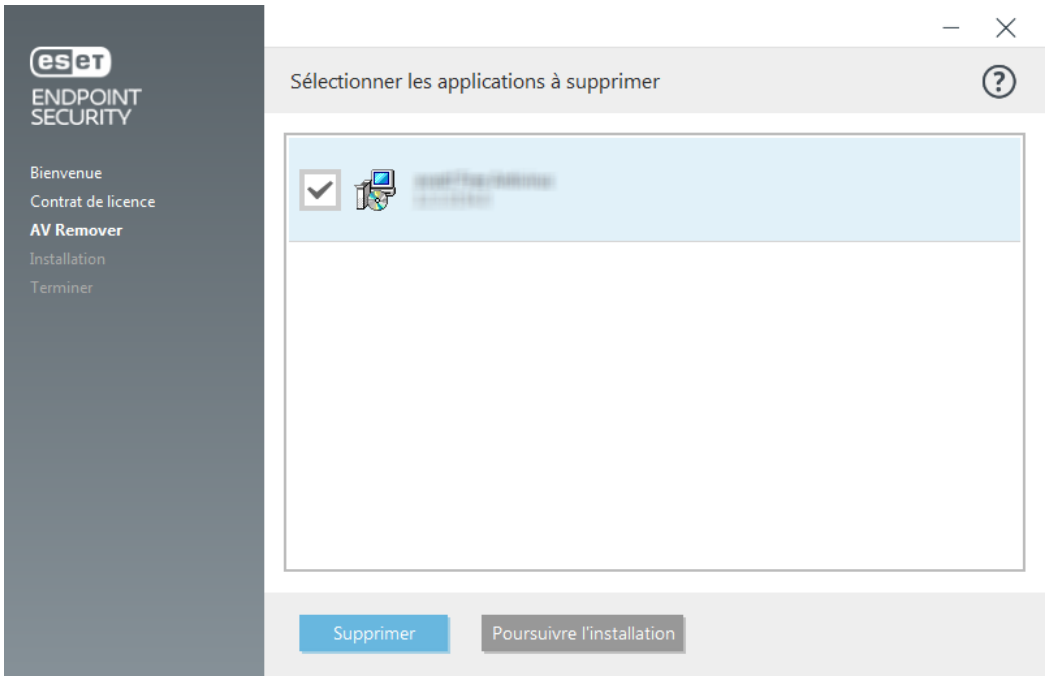
1. Pour afficher la liste des logiciels antivirus qu'ESET AV Remover peut supprimer, consultez l'article de la base de connaissances ESET.
2. Lisez les termes du contrat de licence de l'utilisateur final, puis cliquez sur **Accepter** pour confirmer que vous les acceptez. Si vous cliquez sur **Refuser**, l'installation de ESET Endpoint Security continue sans la suppression des applications de sécurité existantes sur l'ordinateur.



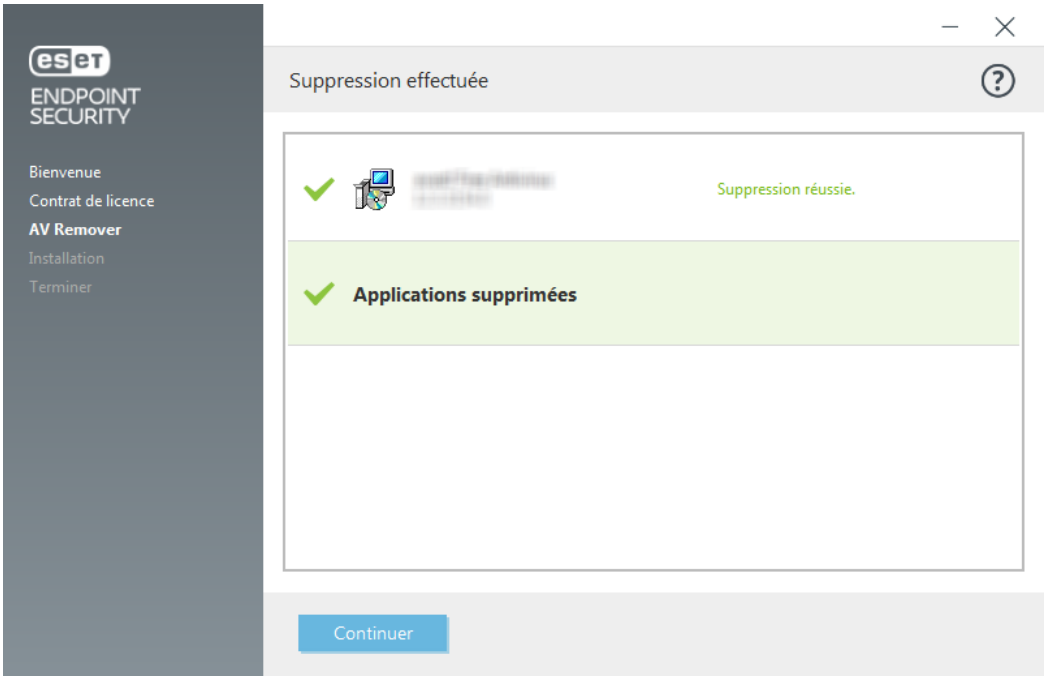
2. ESET AV Remover commence à rechercher les logiciels antivirus sur votre système.



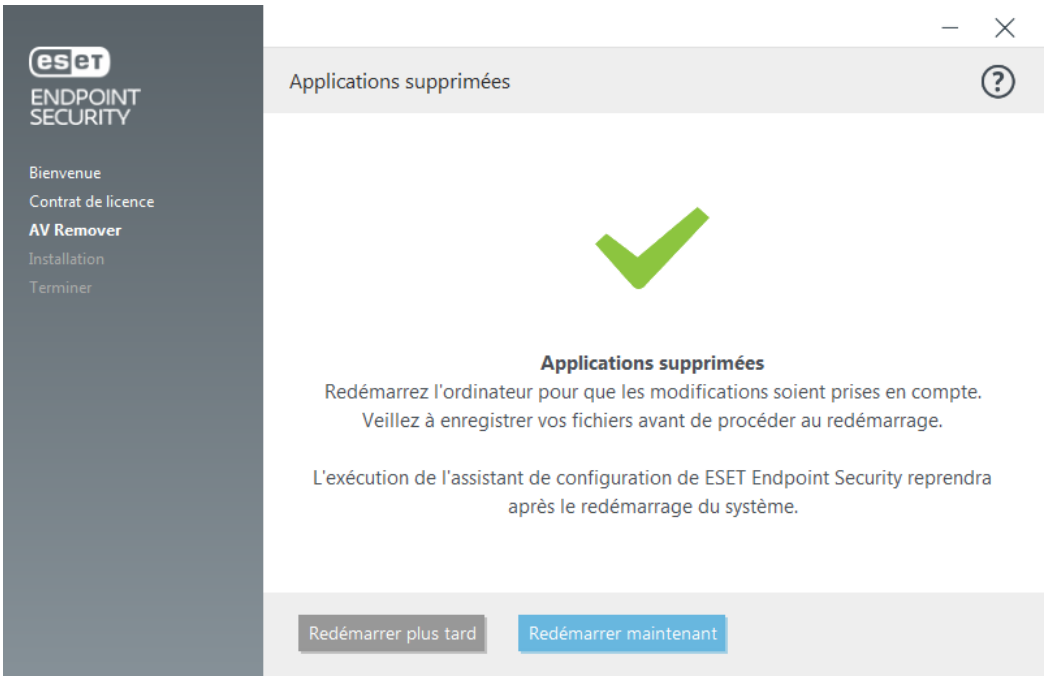
2. Sélectionnez les applications antivirus répertoriées, puis cliquez sur **Supprimer**. La suppression peut prendre quelques instants.



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



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



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.

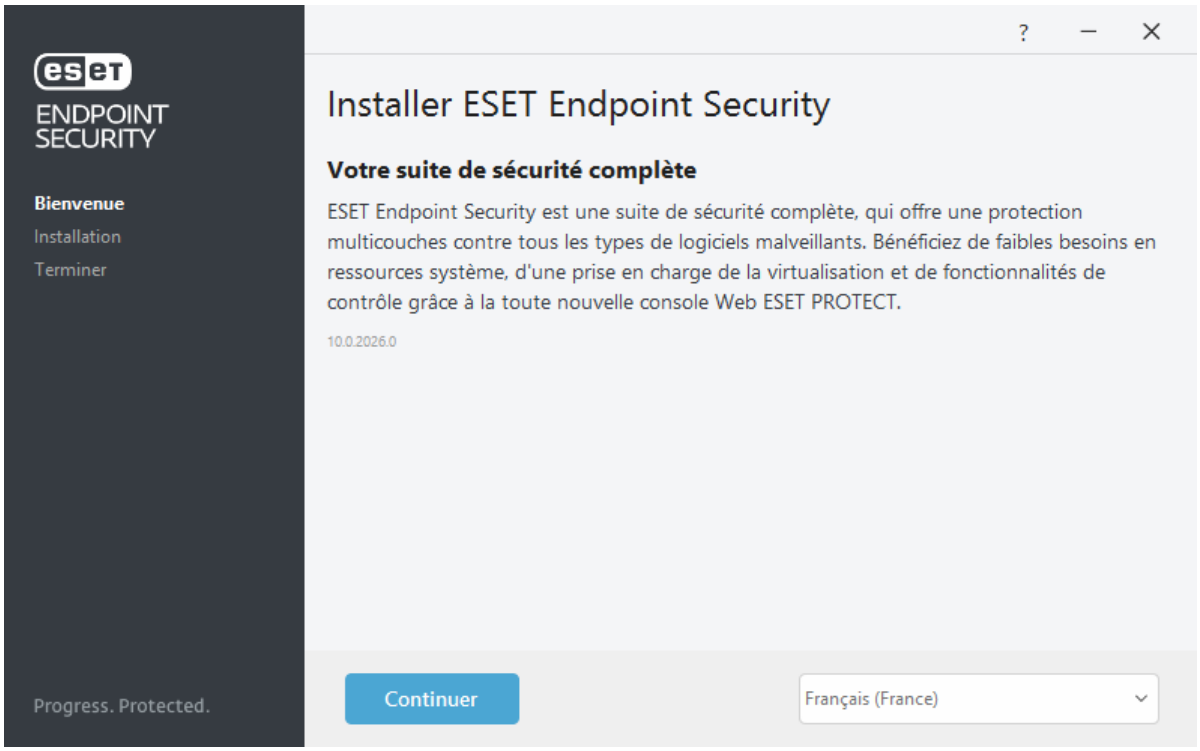
En cas d'échec de la désinstallation d'un produit de sécurité ou d'une désinstallation partielle de certains de ses composants, vous êtes invité à **redémarrer et relancer une analyse** de l'ordinateur. Confirmez le Contrôle de compte d'utilisateur (UAC) après le démarrage et continuez la procédure d'analyse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

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

- Système de commentaire ESET LiveGrid®
- Détection d'applications potentiellement indésirables

En cliquant sur **Continuer** ou **Tout autoriser et continuer**, vous acceptez les termes du contrat de licence de l'utilisateur final et reconnaissez avoir pris connaissance de la politique de confidentialité. Vous pouvez installer ESET Endpoint Security dans un dossier spécifique en cliquant sur Modifier le dossier d'installation.

2. Une fois l'installation terminée, vous êtes invité à activer ESET Endpoint Security.

Modification du dossier d'installation (.exe)

Vous pouvez **modifier le dossier d'installation** pendant l'installation. Sélectionnez un emplacement d'installation pour ESET Endpoint Security. 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 **Précédent**, puis continuez 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.

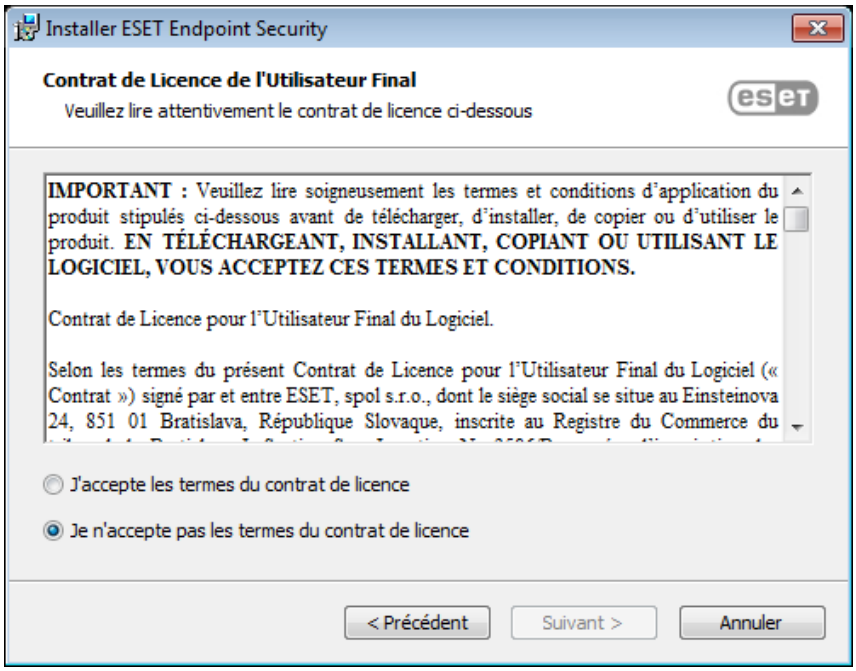
✓ Dans les environnements d'entreprise, le programme d'installation .msi est le package d'installation préféré. Principalement en raison des déploiements hors ligne et distants qui utilisent différents outils tels que ESET PROTECT On-Prem.

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

Le programme d'installation ESET Endpoint Security créé dans ESET PROTECT On-Prem prend en charge Windows 10 Entreprise pour les bureaux virtuels et le mode multisession de Windows 10.

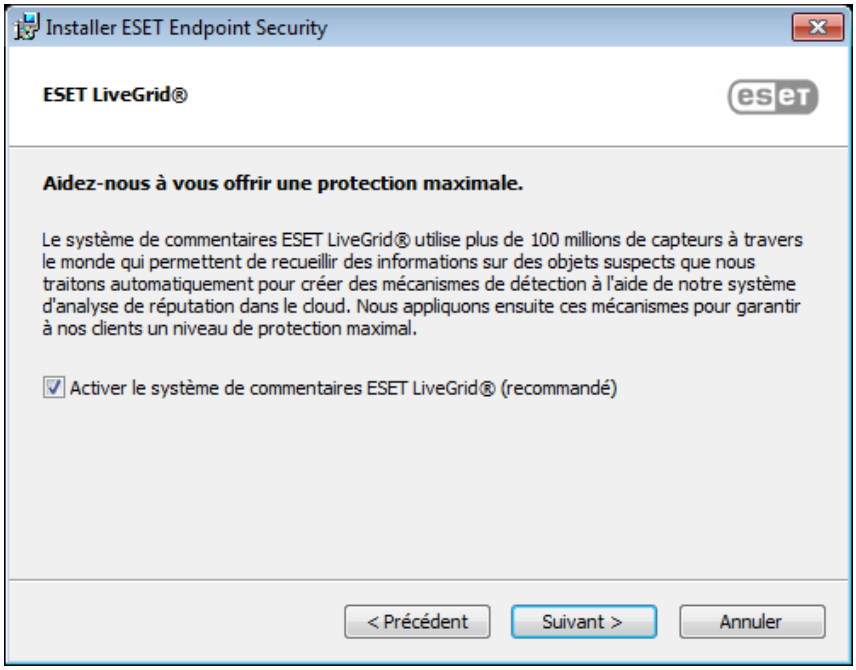
1. Sélectionnez la langue souhaitée, puis cliquez sur **Suivant**.

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. Cliquez sur **Paramètres avancés** pour configurer d'autres paramètres d'installation.



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

Installation avancée (.msi)

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

1. Vous pouvez **modifier le dossier d'installation** pendant l'installation. Sélectionnez un emplacement d'installation pour ESET Endpoint Security. 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).

2. Sélectionnez quels composants du produit à installer. Vous pouvez sélectionner vos préférences pour l'analyse de l'ordinateur et toutes les protections disponibles. Le composant Miroir de mise à jour peut être utilisé pour mettre à jour les autres ordinateurs du réseau. La surveillance et l'administration à distance (RMM) 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.

3. Cliquez sur **Installer** pour lancer le processus d'installation.

Installation minimale de modules

Pour réduire le trafic réseau lié à la taille du programme d'installation et économiser des ressources, ESET propose un programme d'installation minimale de modules. Le programme d'installation ne contient que les modules essentiels. Tous les autres modules sont téléchargés lors de la mise à jour initiale des modules après l'activation du produit. Le principal avantage est un programme d'installation dont la taille est nettement plus petite. ESET Endpoint Security télécharge uniquement les derniers modules d'application lorsque vous activez le produit.

Le programme d'installation minimale de modules contient toujours les modules suivants :

- Chargeurs
- Communication Direct Cloud
- Traduction
- Configuration
- SSL

Une fois le produit activé, l'état **Initialisation de la protection** s'affiche pour vous informer de l'initialisation des fonctionnalités.

En cas de problème lié au téléchargement des modules (paramètres du proxy, pas de réseau, etc.), un état d'application d'avertissement **Attention requise** s'affiche. Dans la fenêtre principale du programme, cliquez sur **Mis à jour** > **Rechercher des mises à jour** pour recommencer le processus.

Après plusieurs tentatives infructueuses, un état d'application rouge **Échec de la configuration de la protection** s'affiche. Cliquez sur Réessayer pour redémarrer la configuration de la protection. Si le processus d'initialisation échoue et que vous ne parvenez toujours pas à télécharger les modules, téléchargez les programmes d'installation MSI complets.

Si vos ordinateurs clients ne disposent pas d'une connexion Internet ou sont en mode hors connexion et nécessitent des mises à jour, utilisez les méthodes suivantes pour télécharger les fichiers de mise à jour depuis les serveurs de mise à jour ESET :
- Mise à jour à partir du miroir
- Utilisation de l'outil Miroir

Installation à l'aide d'une ligne de commande

Vous pouvez installer ESET Endpoint Security localement à l'aide de la ligne de commande ou à distance en utilisant une tâche client d'ESET PROTECT On-Prem.

Paramètres pris en charge

APPDIR=<path>

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

APPDATADIR=<path>

- Chemin : chemin d'accès valide au répertoire

- Répertoire d'installation des données de l'application.

MODULEDIR=<path>

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

ADDLOCAL=<list>

- 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=<list>

- 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`

> **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

> 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 Security 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
Navigateur sécurisé	OnlinePaymentProtection	WebAndEmail	Facultative
Internet et messagerie	WebAndEmail		Espace réservé
Internet et messagerie / Filtrage des protocoles	ProtocolFiltering	WebAndEmail	Invisible
Internet et messagerie/Protection de l'accès web	WebAccessProtection	WebAndEmail	Facultative
Internet et messagerie/Protection du client de messagerie	EmailClientProtection	WebAndEmail	Facultative
Internet et messagerie/Protection du client de messagerie/Clients de messagerie	MailPlugins	EmailClientProtection	Invisible
Internet et messagerie/Protection du client de messagerie/Antipourriel du client de messagerie	Antispam	EmailClientProtection	Facultative
Internet et messagerie/Filtrage Web	WebControl	WebAndEmail	Facultative
Outils/ESET RMM	Rmm		Facultative
Mise à jour/Profils/Miroir de mise à jour	UpdateMirror		Facultative
Module d'extension ESET Inspect	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=	<username>	Nom d'utilisateur pour l'authentification
CFG_PROXY_PASSWORD=	<password>	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=	<path>	Chemin d'accès à la configuration XML exportée (valeur par défaut *cfg.xml*)

Propriétés de configuration uniquement dans ESET Endpoint Security

CFG_EPFW_MODE=	0 - Automatique (par défaut) 1 - Interactif 2 - Basé sur la politique 3 - Apprentissage	Mode de filtrage du Pare-feu
CFG_EPFW_LEARNINGMODE_ENDTIME=	<timestamp>	Date de fin du mode d'apprentissage en tant qu'horodatage Unix

Propriété LiveGrid®

Lors de l'installation d'ESET Endpoint Security avecCFG_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 Security (vous devez spécifier les deux propriétés).

Propriété	Valeur
`PRODUCT_LANG=`	Décimal LCID (ID de paramètres régionaux), par exemple 1033 pour l'anglais (États-Unis). Consultez 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. Consultez la liste des codes de langue.

Propriétés de redémarrage

Spécifiez les paramètres suivants pour redémarrer l'ordinateur après une installation :

Propriété	Valeur	Fonctionnalité
`REBOOT_WHEN_NEEDED=`	0 - Désactivé 1 - Activé	Si ce paramètre est activé, l'ordinateur redémarrera après l'installation.
`REBOOT_CANCELABLE=`	0 - Désactivé 1 - Activé	Si ce paramètre est activé, l'utilisateur peut annuler le redémarrage de l'ordinateur.
`REBOOT_POSTPONE=`	valeur en secondes	Durée maximale en secondes pendant laquelle l'utilisateur peut reporter le redémarrage de l'ordinateur.

Les paramètres REBOOT_CANCELABLE et REBOOT_POSTPONE ne sont disponibles que si le paramètre REBOOT_WHEN_NEEDED est activé.

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

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

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
```

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

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\
```

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

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`

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 Security directement sur un poste de travail client, 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 Security via ESET PROTECT On-Prem. ESET PROTECT On-Prem 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 ESET PROTECT On-Prem.
5. Déployez et activez ESET Endpoint Security sur vos ordinateurs clients.

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

Non géré

Pour les ordinateurs non administrés, vous pouvez déployer ESET Endpoint Security directement sur les postes de travail clients. Cette méthode n'est toutefois pas recommandée, car vous ne pourrez pas surveiller et appliquer les politiques pour tous vos produits Endpoint ESET sur les postes de travail.

Par défaut, ESET Endpoint Security n'est pas activé après l'installation et n'est donc pas fonctionnel.

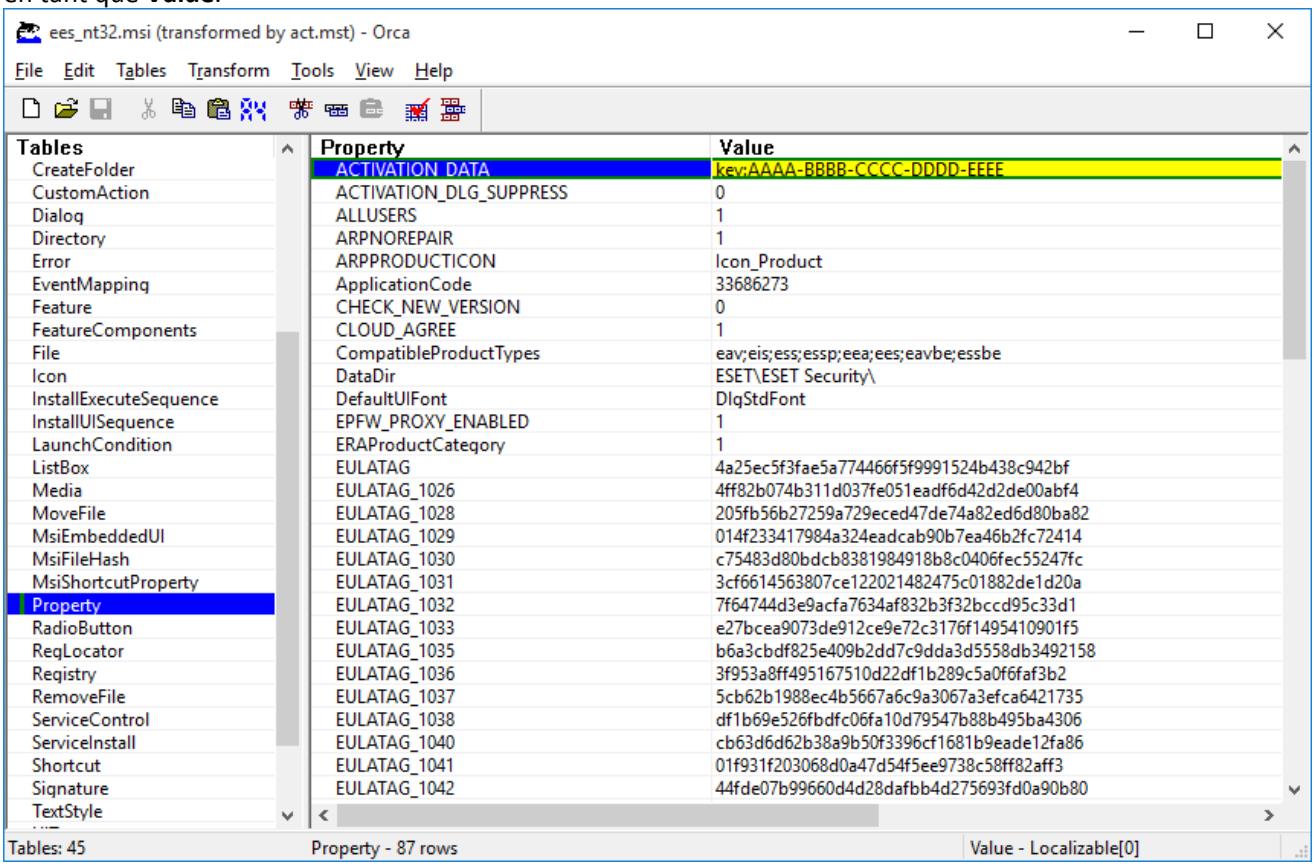
Option 1 (installation de logiciel)

1. Téléchargez le programme d'installation .msi pour ESET Endpoint Security.
2. Créez un package de transformation .mst à partir du fichier .msi (en utilisant par exemple l'éditeur .msi Orca) pour inclure la propriété d'activation du produit (voir `ACTIVATION_DATA` dans Installation à l'aide

d'une ligne de commande).

Afficher la procédure pour créer un fichier .mst dans Orca

1. Ouvrir Orca.
2. Chargez le programme d'installation .msi en cliquant sur **File** > **Open**.
3. Cliquez sur **Transform** > **New Transform**.
4. Cliquez sur **Property** dans la section **Tables**, puis dans le menu **Tables** > **Add row**.
5. Dans les fenêtres **Add Row**, saisissez ACTIVATION_DATA en tant que **Property** et les informations de licence en tant que **Value**.



6. Cliquez sur **Transform** > **Generate Transform** pour enregistrer le fichier .mst.

1. Facultatif : pour importer le fichier de configuration .xml personnalisé d'ESET Endpoint Security (par exemple, pour activer RMM ou configurer les paramètres du serveur proxy, placez le fichier cfg.xml au même emplacement que le programme d'installation .msi.
2. Déployez le programme d'installation .msi avec le fichier .mst à distance à l'aide de GPO (via l'installation de logiciel) ou SCCM.

Option 2 (utilisation d'une tâche planifiée)

1. Téléchargez le programme d'installation .msi pour ESET Endpoint Security.
2. Préparez un script d'installation à l'aide d'une ligne de commande pour inclure la propriété d'activation du produit (voir `ACTIVATION_DATA`).
3. Rendez le programme d'installation .msi et le script .cmd accessibles dans le réseau pour tous les postes de travail.
4. Facultatif : pour importer le fichier de configuration .xml personnalisé d'ESET Endpoint Security (par exemple, pour activer RMM ou configurer les paramètres du serveur proxy, placez le fichier cfg.xml au même emplacement que le programme d'installation .msi.
5. Appliquez un script préparé d'installation à l'aide d'une ligne de commande en utilisant GPO ou SCCM.

- Pour GPO, utilisez Préférences de politique de groupe > Tâches de planification d'une politique de groupe > Tâche immédiate

> Si vous ne souhaitez pas utiliser ESET PROTECT On-Prem our gérer à distance vos produits ESET Endpoint, ESET Endpoint Security contient le module d'extension ESET pour RMM qui permet de superviser et de contrôler les systèmes logiciels à l'aide d'un agent installé localement auquel un prestataire de services de gestion peut accéder. Trouver des informations supplémentaires

Mise à niveau vers une nouvelle version

Les nouvelles versions d'ESET Endpoint Security offrent des améliorations ou apportent des solutions aux problèmes que les mises à jour automatiques des modules de programme ne peuvent pas résoudre.

La mise à niveau vers une nouvelle version peut s'effectuer de différentes manières :

1. Automatiquement, en utilisant ESET PROTECT On-Prem, ou ESET PROTECT.
2. Automatiquement, à l'aide de GPO ou SCCM.
3. Automatiquement, à l'aide d'une mise à jour du programme.
   Les mises à niveau du programme sont distribuées à tous les utilisateurs et peuvent avoir un impact sur certaines configurations système. Elles sont par conséquent mises à disposition après de longues périodes de test afin que leur fonctionnement soit correct sur toutes les configurations système. Pour effectuer la mise à niveau vers une nouvelle version dès que celle-ci est disponible, utilisez l'une des méthodes ci-dessous.
   Vérifiez que vous avez activé l'option **Mode de mise à jour** dans Configuration avancée > **Mise à jour** > **Profils** > **Mises à jour du produit**.
4. Manuellement, en téléchargeant la nouvelle version et en l'installant sur l'installation précédente.

Scénarios de mise à niveau recommandés

Je gère ou je souhaite gérer mes produits ESET à distance

Si vous gérez plus de 10 produits ESET Endpoint, envisagez de gérer les mises à niveau à l'aide d'ESET PROTECT On-Prem ou ESET PROTECT. Consultez la documentation suivante :

- ESET PROTECT On-Prem | Mise à niveau d'un logiciel ESET par le biais d'une tâche client
- ESET PROTECT On-Prem | Guide pour les petites et moyennes entreprises gérant jusqu'à 250 produits Endpoint ESET pour Windows
- Présentation de ESET PROTECT

Mise à niveau manuelle sur un poste de travail client

Pour mettre à niveau manuellement ESET Endpoint Security sur chaque poste de travail client :

1. Vérifiez que la version actuellement installée est prise en charge.
2. Vérifiez que votre système d'exploitation est pris en charge.

2. Téléchargez et installez la dernière version sur la version précédente.

Une installation de la dernière version sur une précédente n'est pas garantie pour les versions dont le niveau de prise en charge est « Fin de vie ». Consultez la politique de fin de vie pour examiner le niveau de prise en charge d'ESET Endpoint Security.
Pour effectuer une mise à niveau à partir de versions non prises en compte, désinstallez d'abord ESET Endpoint Security. Pour plus d'informations sur la mise à niveau d'ESET Endpoint Security sur un poste de travail client, consultez cet article de la base de connaissances ESET.

Mise à niveau automatique des anciens produits

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

Problèmes d'installation courants

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

Pour terminer l'installation :

1. Cliquez sur **Accepter et continuer** pour accepter les termes du Contrat de licence de l'utilisateur final et reconnaître avoir pris connaissance de la Politique de confidentialité. Si vous n'êtes pas d'accord avec les termes du Contrat de licence de l'utilisateur final, cliquez sur **Désinstaller**. Vous ne pouvez pas revenir à la version précédente.
2. Cliquez sur **Tout autoriser et continuer** pour autoriser le système de commentaires ESET LiveGrid® ou cliquez sur **Continuer** si vous ne souhaitez pas participer à ce programme.
3. Une fois le nouveau produit ESET activé avec votre clé de licence, la page d'accueil s'affiche. Si aucune information de licence n'est trouvée, continuez avec une nouvelle licence d'essai. Si la licence utilisée pour le produit précédent n'est pas valide, activez votre produit ESET.
4. Un redémarrage de l'appareil est nécessaire pour terminer l'installation.

Mises à jour de la sécurité et de la stabilité

La mise à jour d'ESET Endpoint Security est un élément essentiel de la protection totale contre les codes malveillants. Chaque nouvelle version d'ESET Endpoint Security propose de nombreuses améliorations et de nombreux correctifs. Il est vivement recommandé d'effectuer régulièrement des mises à jour d'ESET Endpoint Security pour vous protéger des menaces et des failles de sécurité. ESET Endpoint Security s'inscrit dans une étape spécifique du cycle de vie du produit comme tout autre produit ESET.

En savoir plus sur :
Politique de fin de vie (produits pour les entreprises)
Mises à jour du produit
Mises à jour de la sécurité et de la stabilité
Pour plus d'informations sur les modifications d'ESET Endpoint Security, consultez cet article de la base de connaissances ESET.

Les mises à jour automatiques garantissent une sécurité et une stabilité maximales de votre produit. Vous ne pouvez pas les désactiver.

Activation du produit

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.).

Vous pouvez activer ESET Endpoint Security dans la fenêtre principale du programme > **Aide et assistance** > **Activer le produit** ou **État de la protection** > **Activer la licence**.

Vous pouvez utiliser l'une ou l'autre des méthodes ci-après pour activer ESET Endpoint Security :

- **Utiliser une clé de licence achetée** – Chaîne unique au format XXXX-XXXX-XXXX-XXXX-XXXX qui sert à identifier le propriétaire de la licence et à activer la licence.
- **ESET PROTECT HUB** – Un compte ESET PROTECT HUB que vous devez créer. ESET PROTECT HUB est une passerelle centrale vers la plate-forme de sécurité unifiée ESET PROTECT On-Prem. Cette passerelle permet une gestion centralisée des identités, des abonnements et des utilisateurs pour tous les modules de la plate-forme ESET. Vous pouvez utiliser cette option pour activer ESET Endpoint Security également avec des outils de gestion de licences plus anciens : ESET Business Account ou ESET MSP Administrator.
- **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 PROTECT On-Prem. 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, convertissez vos identifiants hérités en clé de licence.

Vous pouvez modifier la licence de votre produit à tout moment dans la fenêtre principale du programme > **Aide et assistance** > **Changer de licence**. L'ID de licence publique s'affiche ; il sert à identifier votre licence auprès de l'assistance ESET.

ESET PROTECT On-Prem peut activer des ordinateurs clients en silence à l'aide des licences fournies par l'administrateur. Pour obtenir des instructions, consultez l'aide en ligne ESET PROTECT On-Prem.

En cas d'échec de l'activation du produit

Saisie de la clé de licence pendant l'activation

Les mises à jour automatiques sont importantes pour votre sécurité. ESET Endpoint Security ne recevra des mises à jour que lorsque le programme aura été activé à l'aide de votre **clé de licence**.

Si vous n'avez pas saisi votre clé de licence après l'installation, votre produit n'est pas activé. Vous pouvez modifier votre licence dans la fenêtre principale du programme. Pour ce faire, cliquez sur **Aide et assistance** > **Activer la licence**, puis saisissez dans la fenêtre d'activation du produit les informations de la licence que vous

avez reçue avec votre produit de sécurité ESET.

Lors de la saisie de votre **clé de licence**, il est important de respecter scrupuleusement leur forme :

- Votre clé de licence est une chaîne unique au format XXXX-XXXX-XXXX-XXXX-XXXX qui sert à identifier le propriétaire de la licence et à activer la licence.

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

Compte ESET PROTECT HUB

ESET PROTECT HUB est une passerelle centrale vers la plate-forme de sécurité unifiée ESET PROTECT On-Prem. Cette passerelle permet une gestion centralisée des identités, des abonnements et des utilisateurs pour tous les modules de la plate-forme ESET. Avec ESET PROTECT HUB, vous pouvez :

- Obtenir une vue d'ensemble des abonnements de sécurité
- Vérifier l'utilisation et l'état des services abonnés
- Allouer et contrôler l’accès granulaire à chaque plateforme ESET
- Authentification unique pour toutes les plateformes ESET liées et accessibles

Vous pouvez utiliser cette option d'activation pour activer ESET Endpoint Security également avec des outils de gestion de licences plus anciens : ESET Business Account ou ESET MSP Administrator.

Vous pouvez créer un compte ESET PROTECT HUB et vous connecter avec votre **adresse e-mail** et votre **mot de passe**.

Si vous avez oublié votre mot de passe, cliquez sur **J'ai oublié mon mot de passe** pour être redirigé vers l’ESET PROTECT HUB. 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 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.

Échec de l'activation

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

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

Vérifiez que vous avez saisi la clé 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

Enregistrement

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

Progression de l'activation

ESET Endpoint Security procède maintenant à l'activation. Cette opération peut prendre quelques minutes.

Activation réussie

L'activation a été effectuée, et ESET Endpoint Security est désormais activé. À partir de maintenant, ESET Endpoint Security recevra des mises à jour régulières pour identifier les menaces les plus récentes et protéger votre ordinateur. Cliquez sur **Terminé** pour terminer l'activation du produit.

Problèmes d'installation courants

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

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

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

Guide du débutant

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

Icône dans la partie système de la barre des tâches

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

> Pour accéder au menu de l'icône de la barre d'état système (zone de notification Windows), vérifiez que le mode de démarrage des éléments de l'interface utilisateur est défini sur complet.

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** permet d'indiquer la durée pendant laquelle la protection est désactivée.

Interrompre le pare-feu (autoriser l'intégralité du trafic) – Le pare-feu passe en mode inactif. Pour plus d'informations, reportez-vous à la section Réseau.

Bloquer tout le trafic réseau – Bloque l'intégralité du trafic réseau. Vous pouvez le réactiver en cliquant sur **Arrêter le blocage de l'intégralité du trafic**.

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

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

Ouvrir ESET Endpoint Security – Ouvre la fenêtre principale du programme ESET Endpoint Security depuis l'icône de la barre d'état (zone de notification Windows).

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

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

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

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

Raccourcis clavier

Pour simplifier la navigation dans ESET Endpoint Security, vous pouvez utiliser les raccourcis clavier suivants :

Raccourcis clavier	Action
F1	ouvre les pages d'aide
F5	ouvre la boîte de dialogue Configuration avancée
Flèche haut/Flèche bas	permet de naviguer parmi les éléments d'un menu déroulant
TAB	permet de passer à l'élément d'interface utilisateur suivant dans une fenêtre
Shift+TAB	permet de passer à l'élément d'interface utilisateur précédent dans une fenêtre
ESC	ferme la boîte de dialogue active
Ctrl+U	affiche des informations sur 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
ALT + Flèche gauche	permet de naviguer vers l'arrière
ALT + Flèche droite	permet de naviguer vers l'avant

Raccourcis clavier	Action
ALT+Home	permet de naviguer dans la page d'accueil

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

Profils

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

Analyse de l'ordinateur

Il existe quatre profils d'analyse prédéfinis dans ESET Endpoint Security :

- **Analyse intelligente** : il s'agit du profil d'analyse avancée par défaut. Le profil d'analyse intelligente utilise la technologie d'optimisation intelligente qui exclut les fichiers qui ont été détectés comme étant non infectés lors d'une analyse précédente et qui n'ont pas été modifiés depuis. La durée d'analyse est ainsi réduite avec un impact minimal sur la sécurité du système.
- **Analyse par le menu contextuel** : vous pouvez lancer une analyse à la demande de n'importe quel fichier à partir du menu contextuel. Le profil d'analyse par le menu contextuel permet de définir une configuration d'analyse qui sera utilisée lorsque vous déclencherez l'analyse de cette manière.
- **Analyse approfondie** : Le profil d'analyse approfondie n'utilise pas l'optimisation intelligente par défaut. Par conséquent, aucun fichier n'est exclu de l'analyse à l'aide de ce profil.
- **Analyse de l'ordinateur** : il s'agit du profil par défaut utilisé dans l'analyse standard de l'ordinateur.

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

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

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

Mettre à jour

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

C'est le cas par exemple d'un ordinateur portable qui se connecte normalement à un serveur local (miroir) sur le

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

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

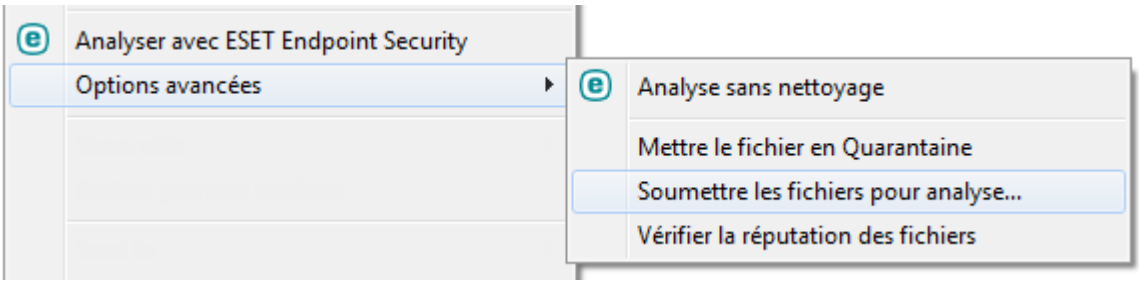
Liste des profils – Permet de créer des profils de mise à jour ou de supprimer ceux existants.

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.

Vous pouvez intégrer les options ESET Endpoint Security dans le menu contextuel. Les options de configuration de cette fonctionnalité sont disponibles dans Configurations avancées > **Interface utilisateur** > **Éléments de l'interface utilisateur**.

Intégrer dans le menu contextuel – Intègre les options ESET Endpoint Security dans le menu contextuel.

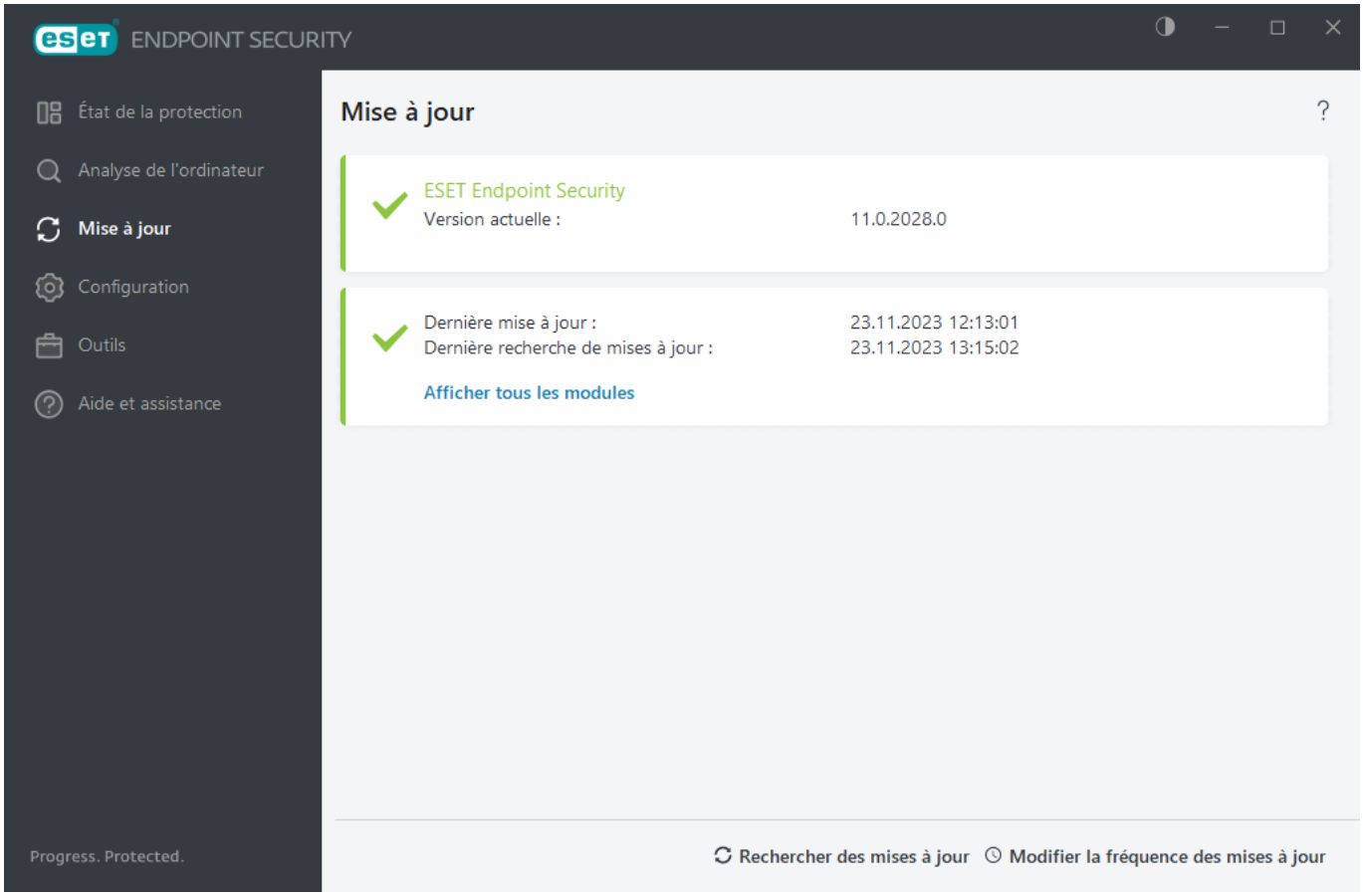


Configuration des mises à jour

La mise à jour régulière d'ESET Endpoint Security est la meilleure méthode pour offrir une sécurité maximale à votre ordinateur. Le module de mise à jour veille à ce que les modules du programme et les composants système soient toujours à jour.

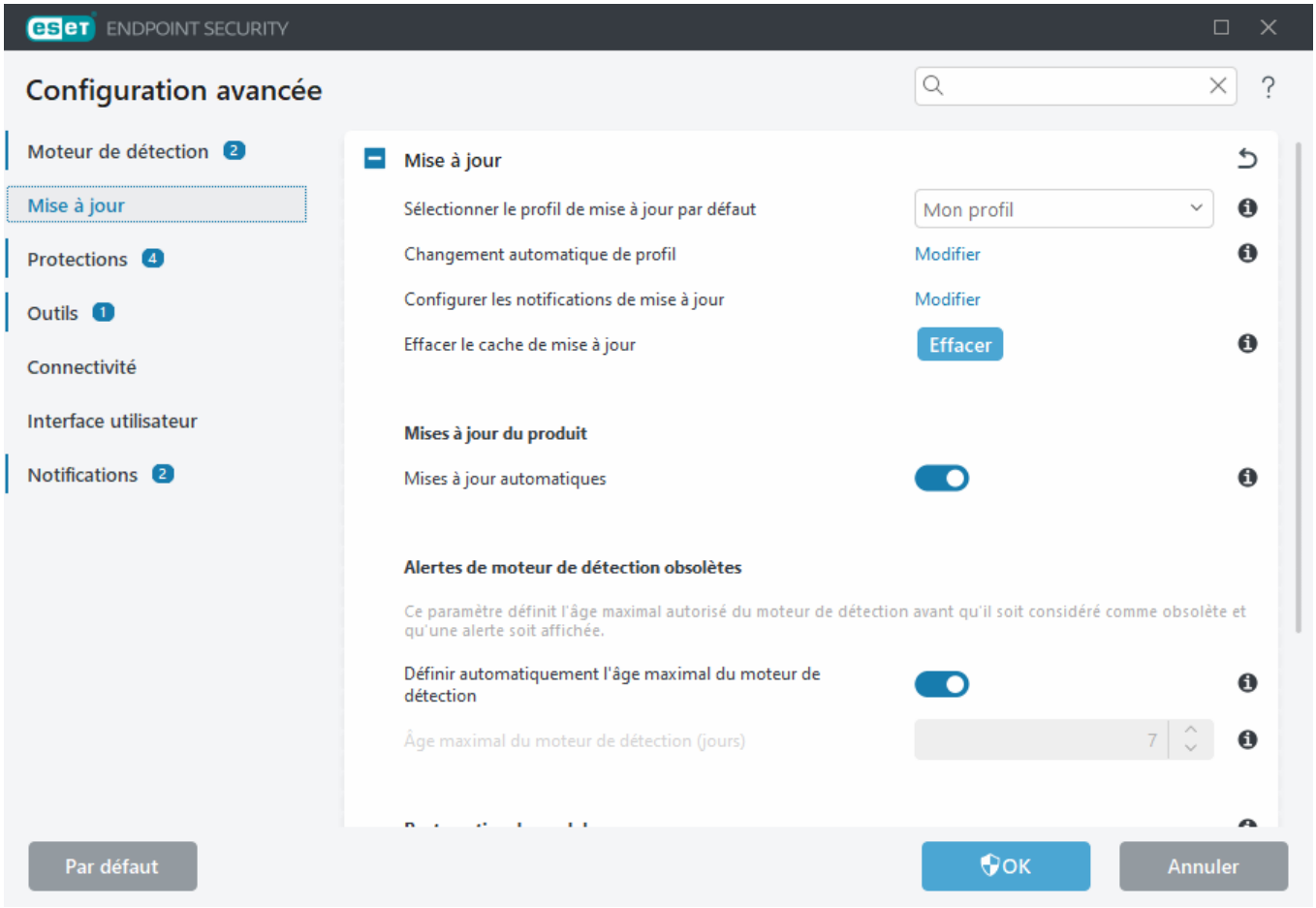
En cliquant sur **Mettre à jour** dans la fenêtre principale du programme, vous pouvez connaître l'état actuel de la mise à jour, notamment la date et l'heure de la dernière mise à jour. Vous pouvez également savoir si une mise à jour est nécessaire.

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



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

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

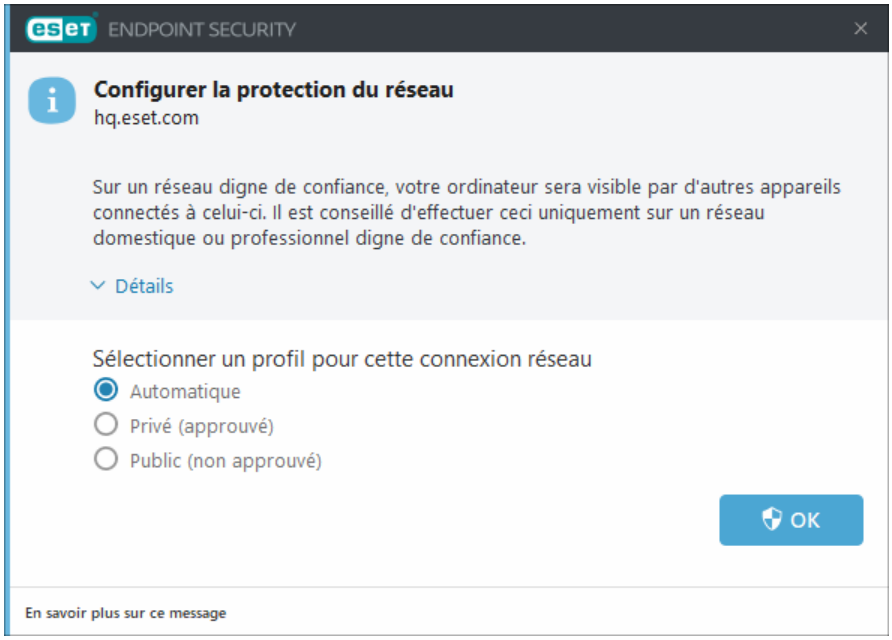


L'option **Choisir automatiquement**, dans Configurations avancées > **Mise à jour** > **Profils** > **Mises à jour** > **Mises à jour du module**, est activée par défaut. Lorsque vous utilisez un serveur de mise à jour ESET pour recevoir des mises à jour, il est recommandé de laisser cette option activée.

Pour un fonctionnement optimal, le programme doit être mis à jour automatiquement. Les mises à jour automatiques ne peuvent s'effectuer 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, consultez Comment activer ESET Endpoint Security.

Configurer la protection du réseau

Par défaut, ESET Endpoint Security utilise les paramètres Windows lorsqu'une nouvelle connexion réseau est détectée. Pour afficher une boîte de dialogue lorsqu'un nouveau réseau est détecté, définissez l'attribution de profil de protection du réseau sur **Demander**. La protection du réseau s'effectue dès que votre ordinateur se connecte à un nouveau réseau.



Vous pouvez effectuer un choix parmi les profils de connexion réseau suivants :

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

Privé : pour des réseaux approuvés (réseau domestique ou professionnel). Votre ordinateur et les fichiers partagés stockés sur votre ordinateur sont visibles par les autres utilisateurs du réseau, et les ressources du système sont accessibles aux autres utilisateurs du réseau (l'accès aux fichiers et imprimantes partagés est activé, la communication RPC entrante est activée et le partage du bureau à distance est disponible). Il est recommandé d'utiliser ce paramètre lors des accès à un réseau local sécurisé. Ce profil est automatiquement attribué à une connexion réseau s'il est configuré en tant que domaine ou réseau privé dans Windows.

Non : pour des réseaux non approuvés (réseau public). les fichiers et les dossiers de votre système ne sont pas partagés ou visibles par les autres utilisateurs du réseau et les partages des ressources système sont désactivés. Il est recommandé d'utiliser ce paramètre lors des accès à des réseaux sans fil. Ce profil est automatiquement attribué à toute connexion réseau qui n'est pas configurée en tant que domaine ou réseau privé dans Windows.

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

⚠ Une configuration incorrecte du réseau peut compromettre la sécurité de votre ordinateur.

Outils du contrôle web

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

Hachages bloqués

L'utilisation d'ESET Inspect dans votre environnement permet aux administrateurs de bloquer l'accès à des exécutables spécifiques en fonction de leur hachage. Si l'administrateur bloque l'accès à un exécutable et que vous tentez d'y accéder, ESET Endpoint Security affiche la notification suivante :

Accès au fichier bloqué : l'application (le nom de l'application est affiché) a essayé d'accéder à un fichier qui n'est pas autorisé par votre administrateur.

Si vous êtes l'administrateur et que vous souhaitez autoriser l'accès à l'application spécifiée dans la notification, consultez Hachages bloqués dans l'aide en ligne d'ESET Inspect. Si vous êtes un utilisateur et que vous souhaitez modifier le comportement de l'application, contactez l'administrateur.

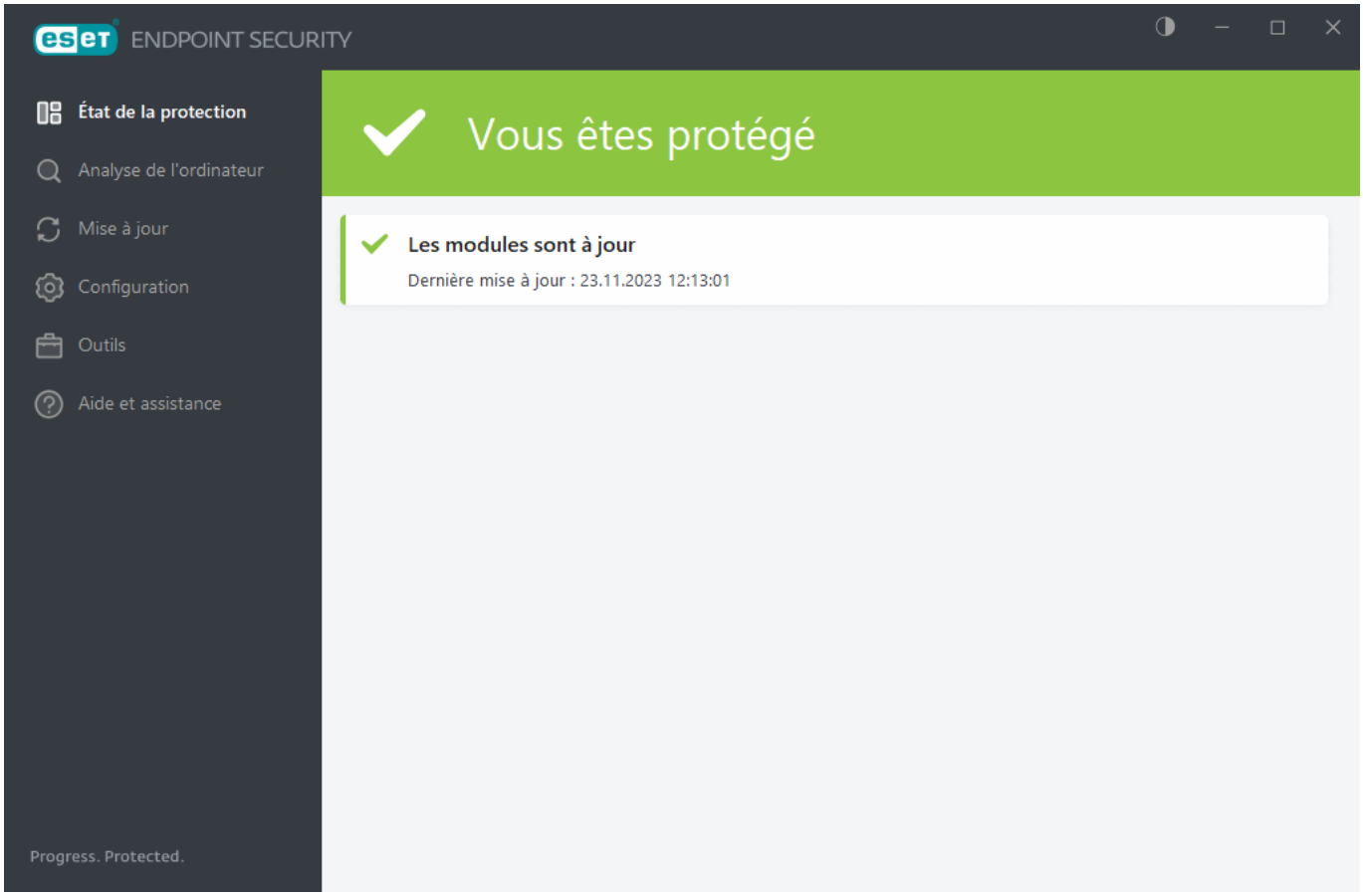
Utilisation d'ESET Endpoint Security

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

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

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

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



Options du menu principal :

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

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

Mise à jour – Affiche des informations sur les mises à jour du module et du moteur de détection.

Outils : Fonctionnalités qui contribuent à simplifier l'administration du programme et offrent des options supplémentaires aux utilisateurs expérimentés.

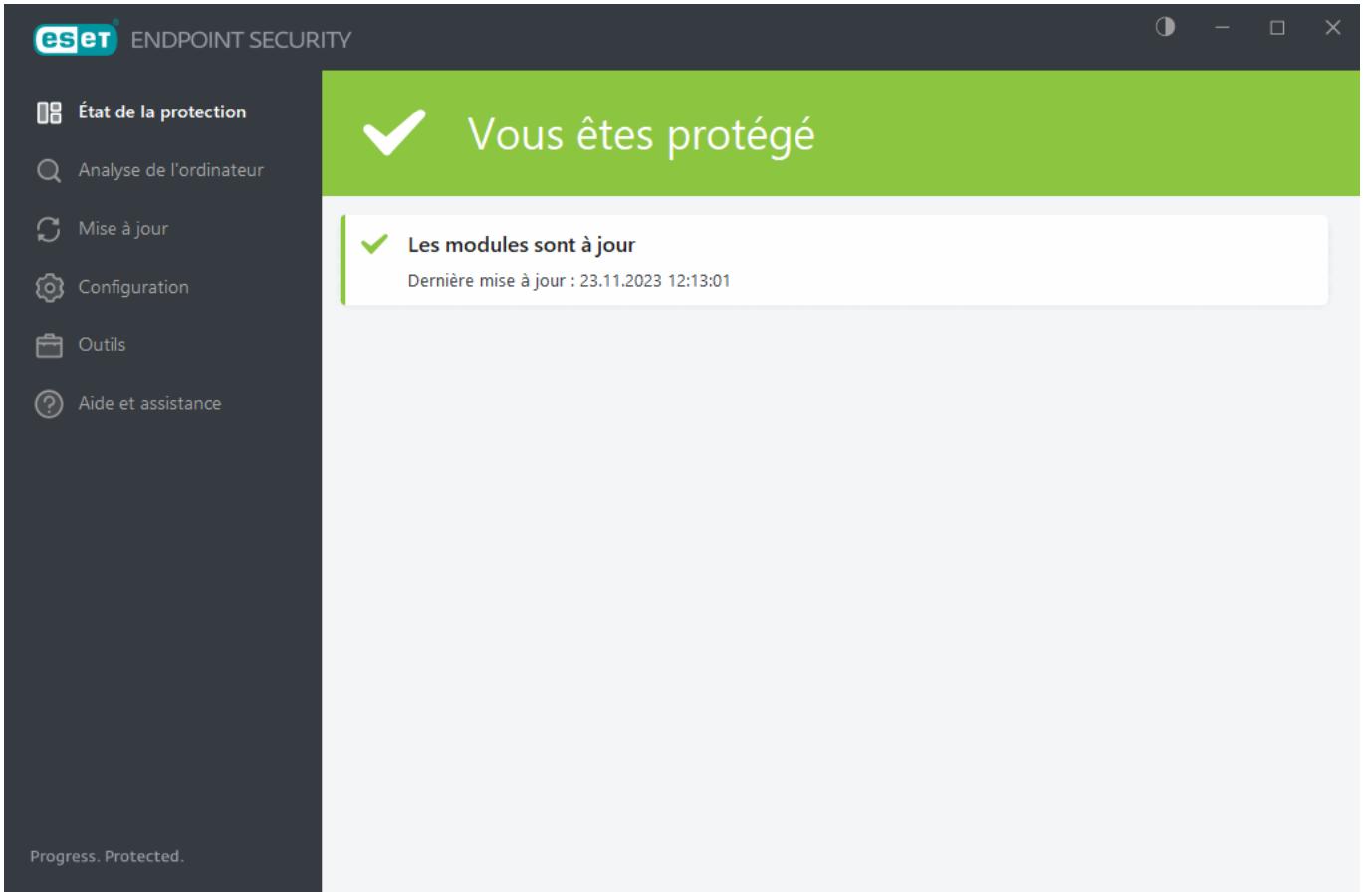
Configuration – Propose des options de configuration pour les fonctionnalités de protection d'ESET Endpoint Security et permet d'accéder aux Configurations avancées.

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

État de la protection

La fenêtre **État de la protection** affiche des informations sur la protection actuelle de votre ordinateur et la dernière mise à jour. L'icône verte d'état **Protection maximale** indique qu'une protection maximale est assurée.

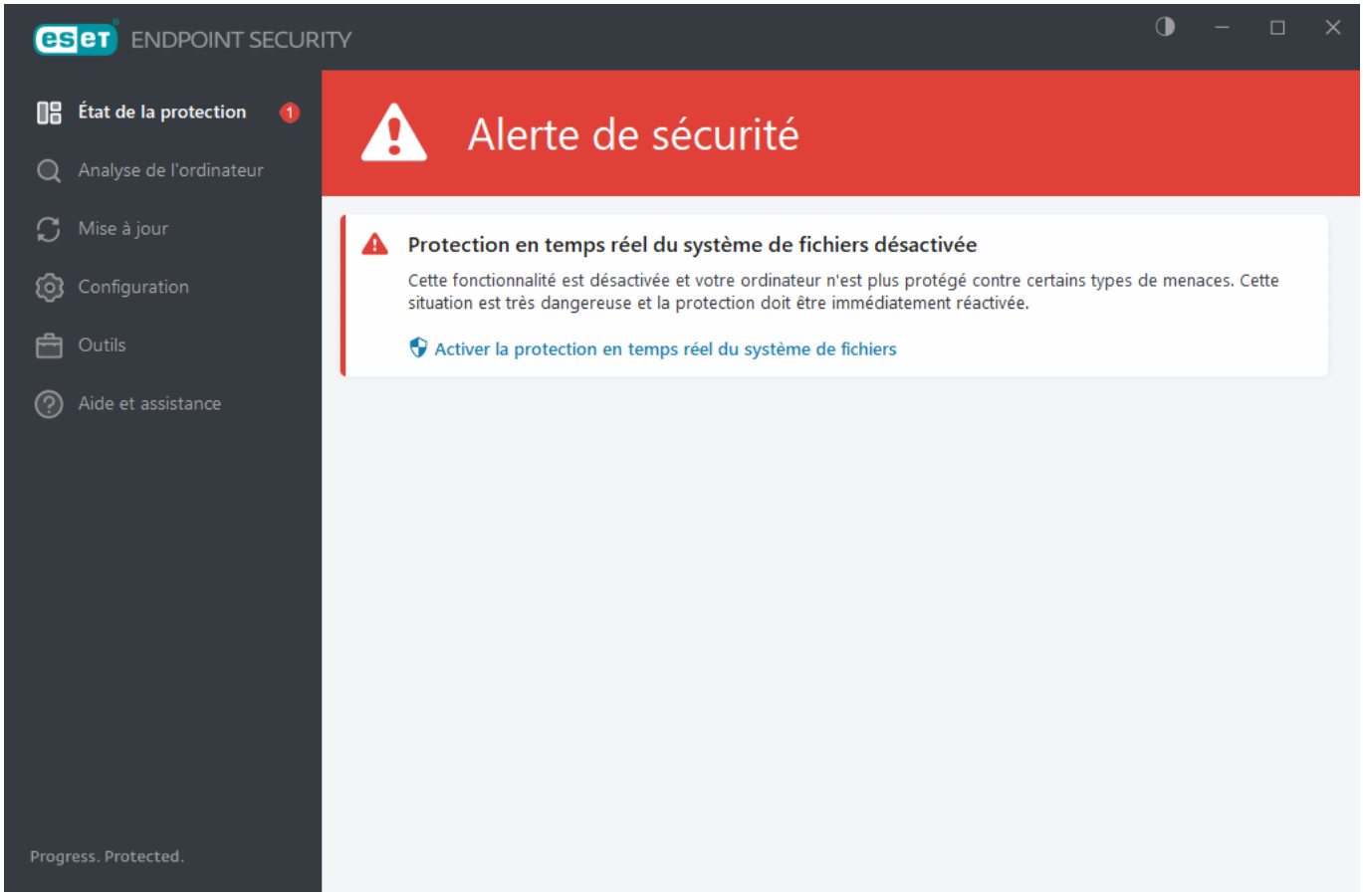
La fenêtre **État de la protection** affiche des notifications avec des informations détaillées et des solutions recommandées pour renforcer la sécurité d'ESET Endpoint Security, activer d'autres fonctionnalités ou assurer une protection maximale.



L'icône verte et l'état vert **Vous êtes protégé** indiquent que la protection maximale est assurée.

Que faire lorsque le programme ne fonctionne pas correctement

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 Security 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 pare-feu est désactivé** – Ce problème est signalé par une icône rouge et une notification de sécurité en regard de l'élément **Réseau**. Cliquez sur **Activer le mode de filtrage** pour réactiver la protection réseau.
- **L'initialisation du pare-feu a échoué** – Le pare-feu est désactivé en raison de problèmes d'intégration système. Redémarrez votre ordinateur dès que possible.
- **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 **Votre licence est 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. Votre ordinateur n'est plus protégé contre certains types de menace et la protection doit être réactivée immédiatement en cliquant sur **Activer HIPS**.
- **Aucune mise à jour régulière planifiée** – ESET Endpoint Security ne recherche pas des mises à jour

importantes ou ne les reçoit pas, sauf si vous planifiez une tâche de mise à jour.

- **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 ESET PROTECT On-Prem. 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 arrive bientôt à expiration/Votre licence arrive à expiration aujourd'hui** – cette information est donnée par l'icône d'état de protection qui affiche un point d'exclamation. Après l'expiration de votre licence, le programme ne peut plus se mise à jour et l'icône d'état de la protection devient rouge.
- **La protection anti-botnet est interrompue** – Cliquez sur **Activer la protection anti-botnet** pour réactiver cette fonctionnalité.
- **La protection contre les attaques réseau (IDS) est interrompue** – Cliquez sur **Activer la protection contre les attaques réseau (IDS)** pour réactiver cette fonctionnalité.
- **Antispam des clients de messagerie interrompu** – Cliquez sur **Activer l'antispam des clients de messagerie** 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 Security, consultez États d'application.

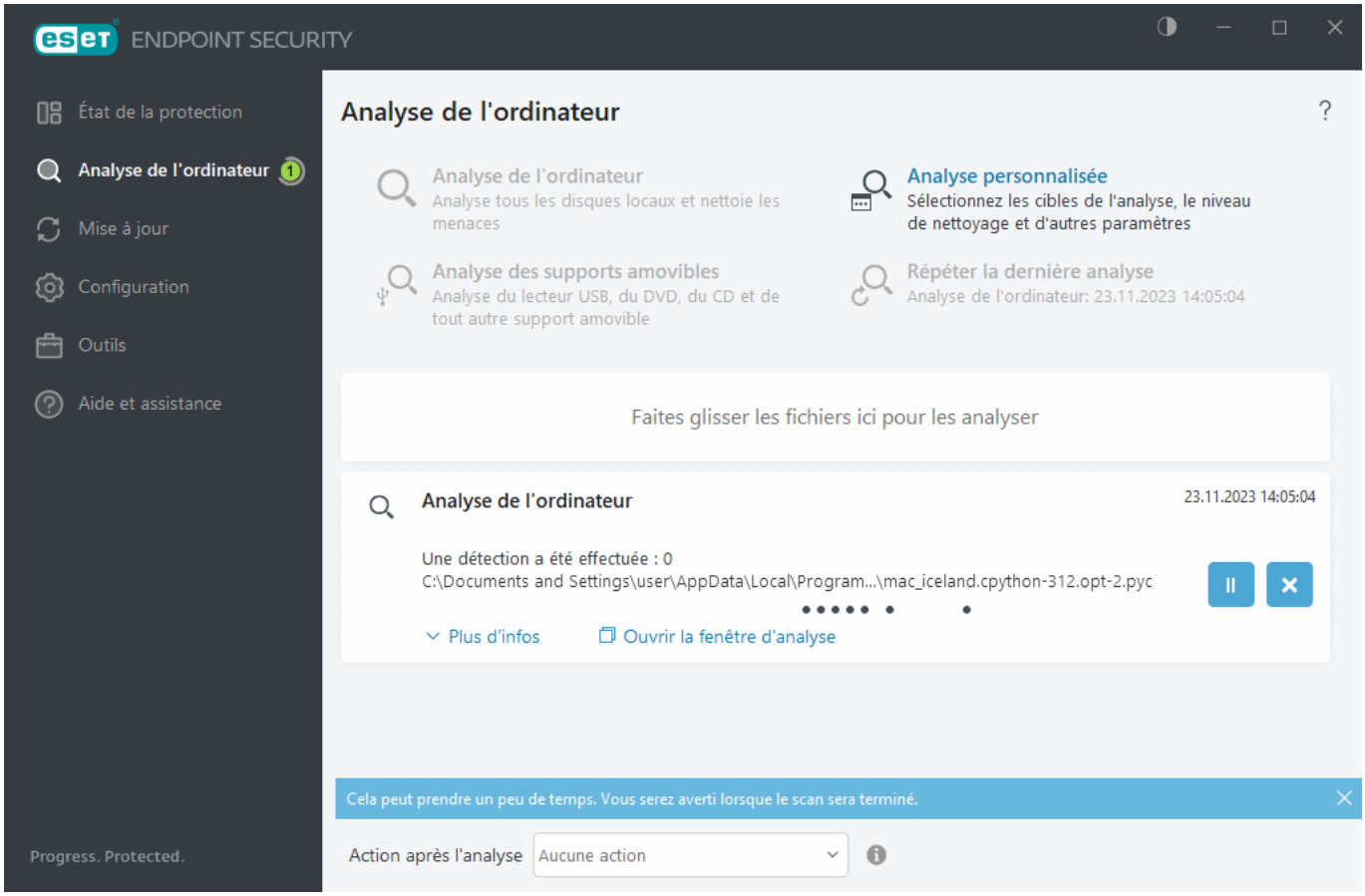
Si vous ne parvenez pas à résoudre le problème à l'aide des solutions suggérées, cliquez sur **Aide et assistance** pour accéder aux fichiers d'aide ou pour effectuer des recherches dans la base de connaissances ESET. Si vous avez encore besoin d'aide, vous pouvez envoyer une demande d'assistance technique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

> Si l'état est associé à une fonctionnalité bloquée par la stratégie d'ESET PROTECT On-Prem, il n'est pas possible de cliquer sur le lien.

Analyse de l'ordinateur

L'analyseur à la demande est un composant important d'ESET Endpoint Security. Il permet d'analyser des fichiers et des répertoires de votre ordinateur. Pour votre sécurité, il est essentiel que l'ordinateur soit analysé non seulement en cas de suspicion d'une infection, mais aussi régulièrement dans le cadre de mesures de sécurité routinières. Nous vous recommandons d'effectuer des analyses en profondeur de votre système de façon régulière (une fois par mois, par exemple) afin de 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'option **Analyse intelligente** permet de lancer rapidement une analyse de l'ordinateur et de nettoyer les fichiers infectés sans intervention de l'utilisateur. **Analyse intelligente** présente l'intérêt d'être facile à utiliser et de ne pas nécessiter de configuration détaillée. Elle vérifie tous les fichiers des disques locaux, et nettoie ou supprime automatiquement les infiltrations détectées. Le niveau de nettoyage est automatiquement réglé sur sa valeur par défaut. Pour plus d'informations sur les types de nettoyage, reportez-vous à la section Nettoyage.

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

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

Analyse personnalisée

L'**analyse personnalisée** vous permet de préciser 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.

Analyse de supports amovibles

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

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

Répéter la dernière analyse

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

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

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

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

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

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

Lanceur d'analyses personnalisées

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

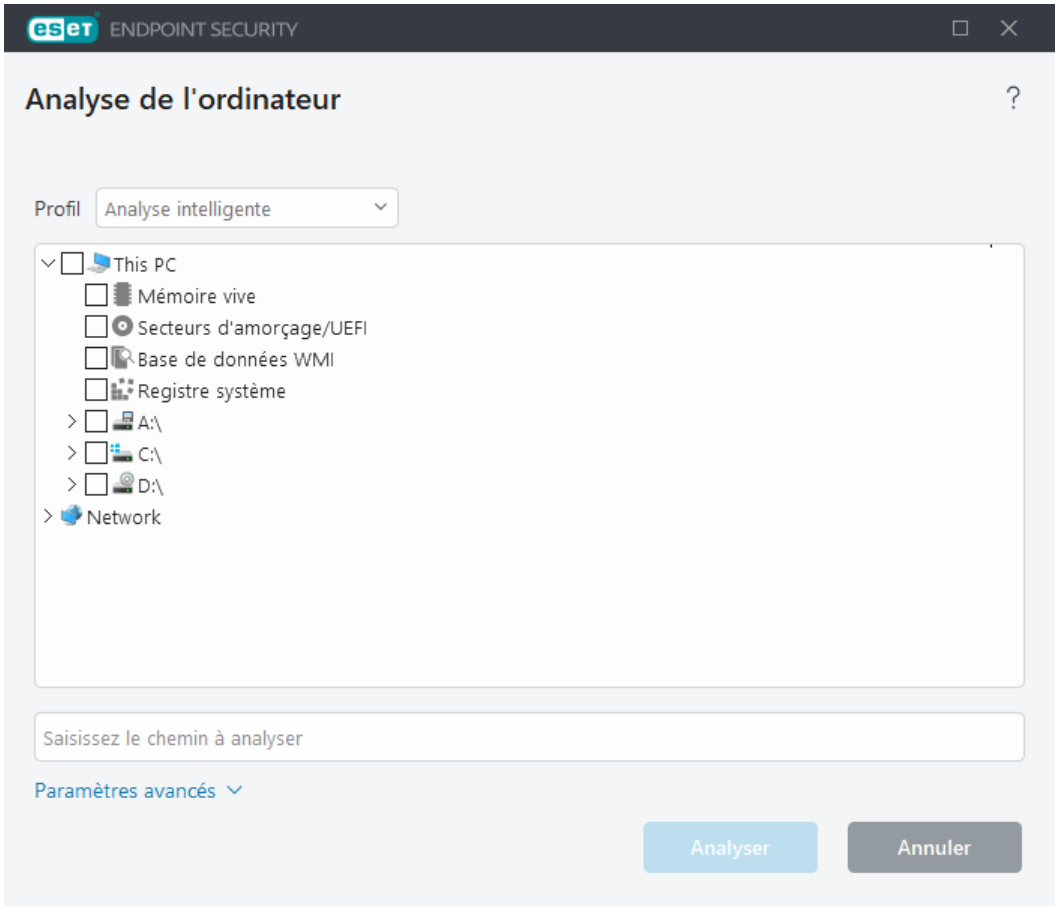
Vous pouvez choisir un profil à utiliser lors de l'analyse de cibles spécifiques dans le menu déroulant **Profil**. Le profil par défaut est **Analyse intelligente**. Il existe trois autres profils d'analyse prédéfinis nommés **Analyse approfondie**, **Analyse par le menu contextuel** et **Analyse de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

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

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

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

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



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

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

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

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

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

Progression de l'analyse

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

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

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

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

Cible – Nom de l'élément analysé et emplacement.

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

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

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

Icône Pause – Suspend une analyse.

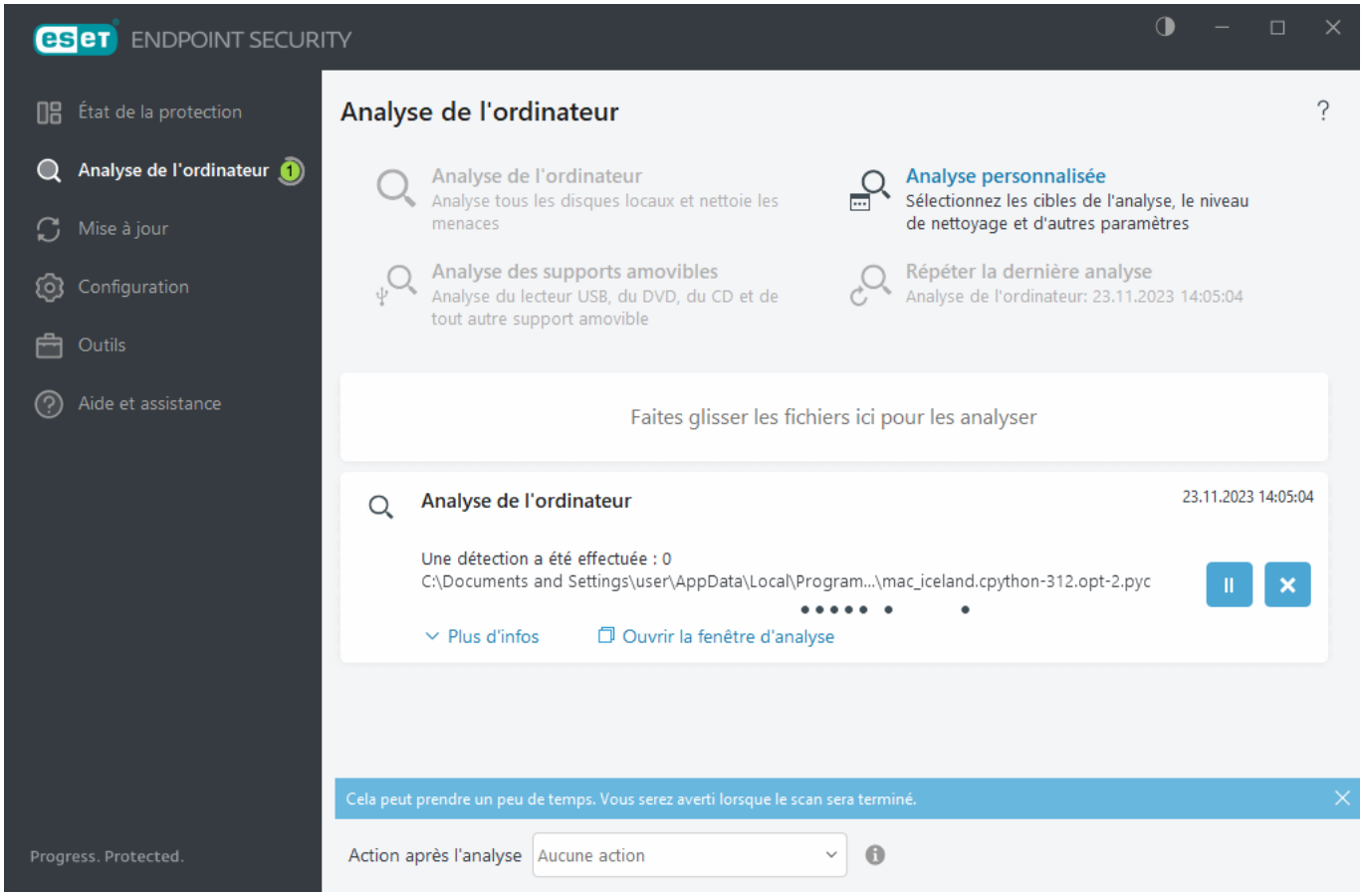
Icône Reprendre – Cette option est visible lorsque l'analyse est suspendue. Cliquez sur l'icône pour poursuivre l'analyse.

Icône Arrêter – Met fin à l'analyse.

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

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

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



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

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

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

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

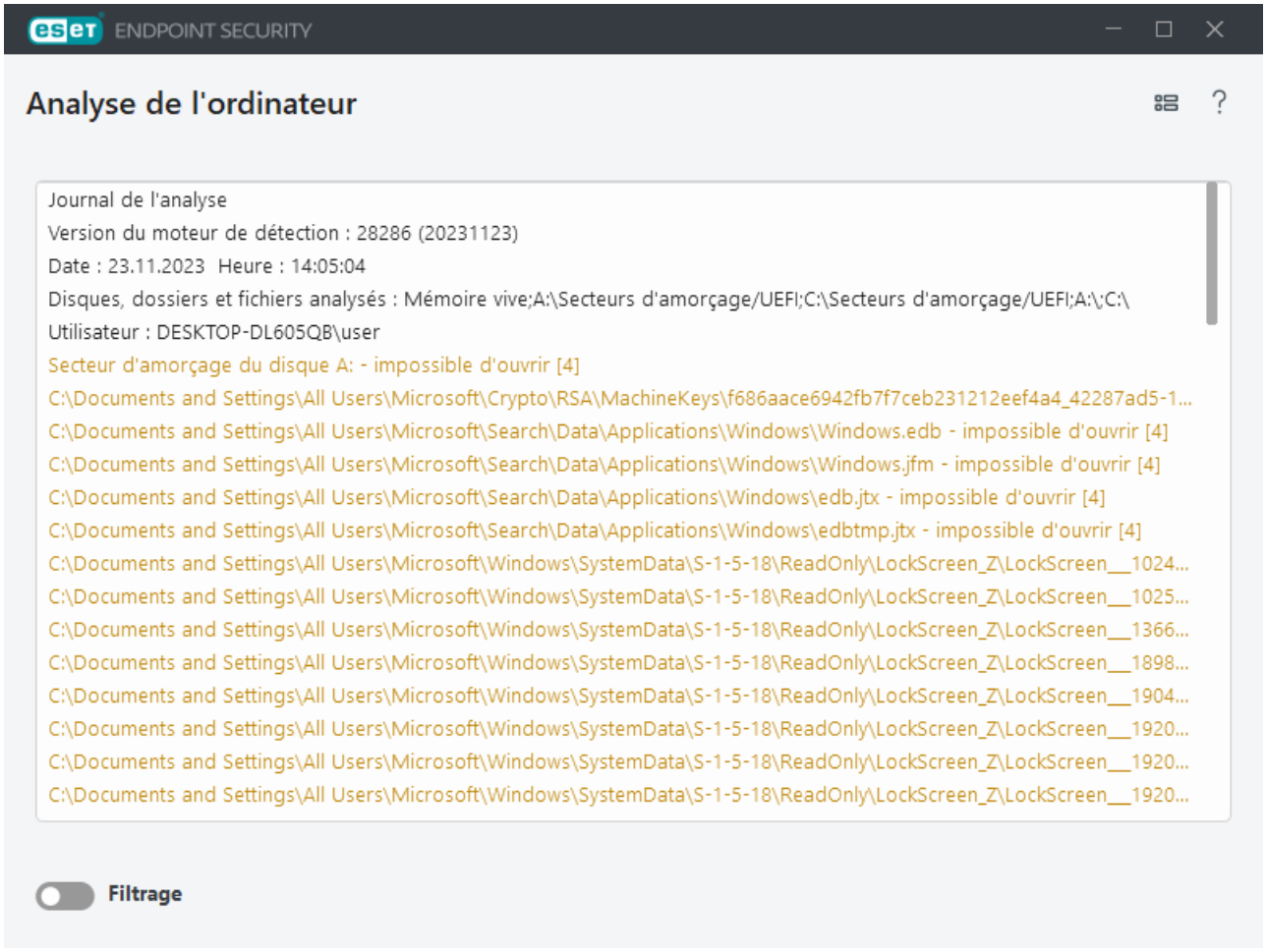
Journal d'analyse de l'ordinateur

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

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

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

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



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

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

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

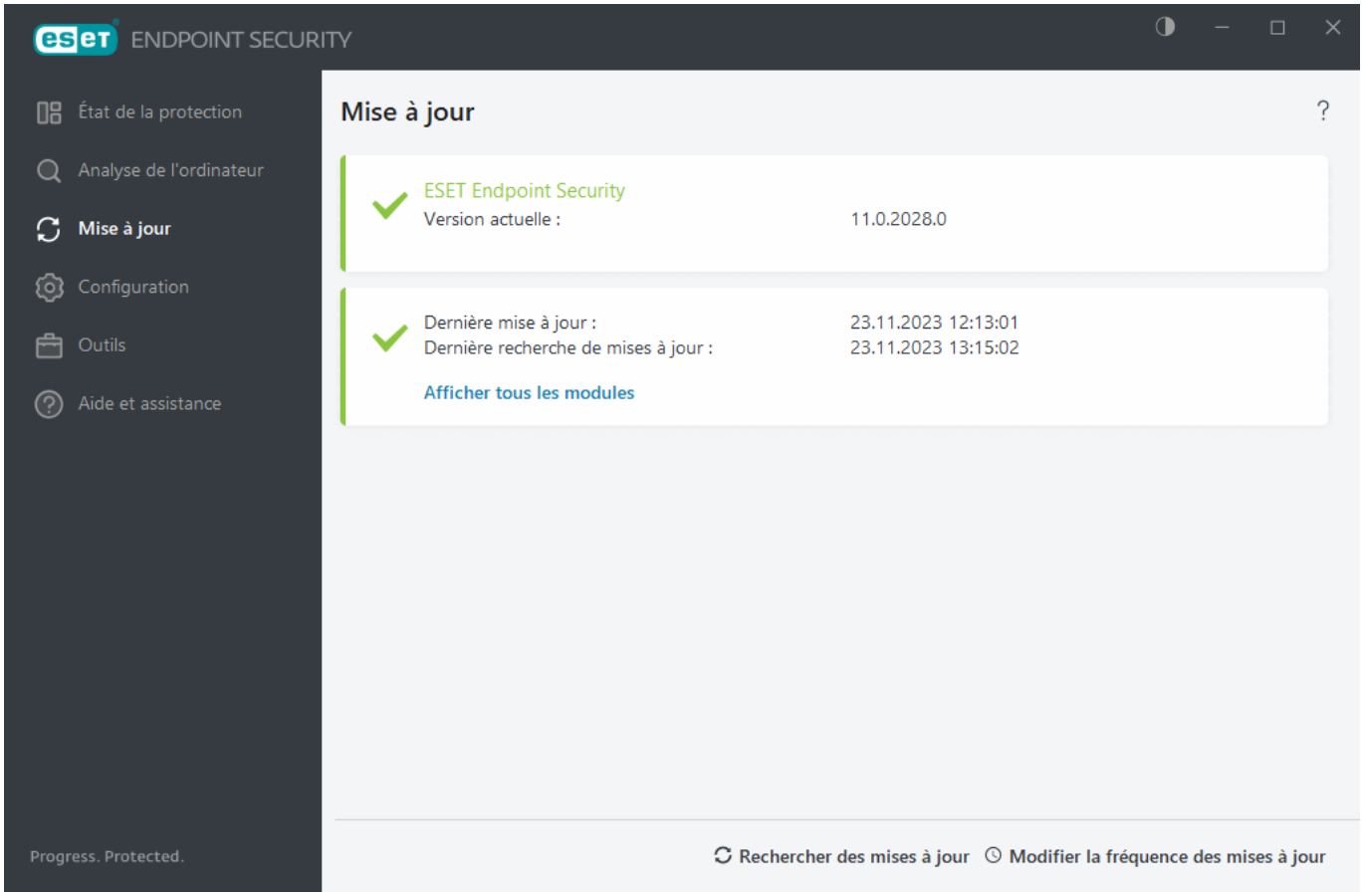
Mettre à jour

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

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

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

Si vous activez ESET Endpoint Security 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.



Version actuelle : numéro de version de ESET Endpoint Security.

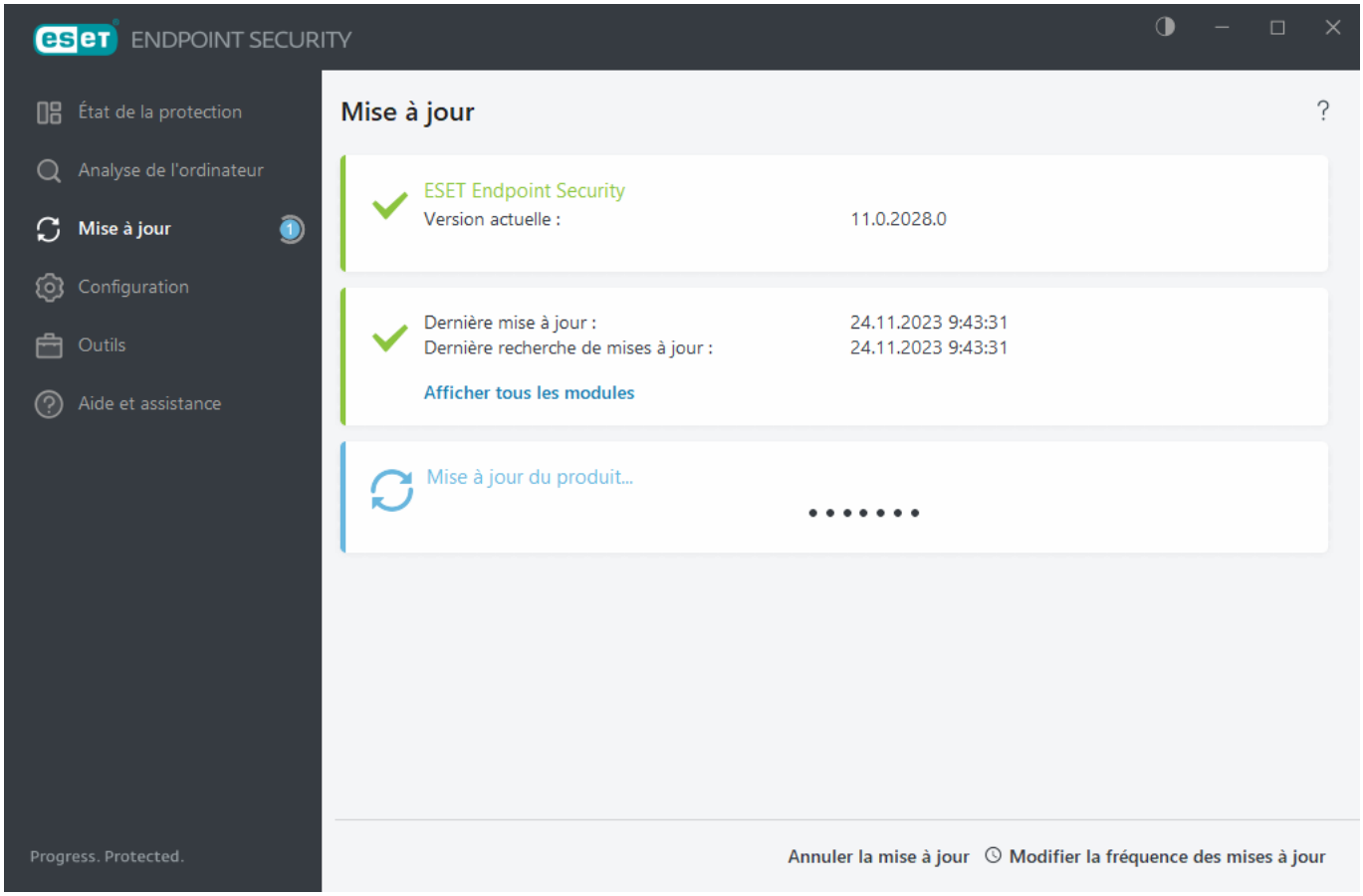
Dernière mise à jour réussie – Date et heure de la dernière mise à jour réussie. Vérifiez qu'il s'agit d'une date récente indiquant que le moteur de détection est à jour.

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**.



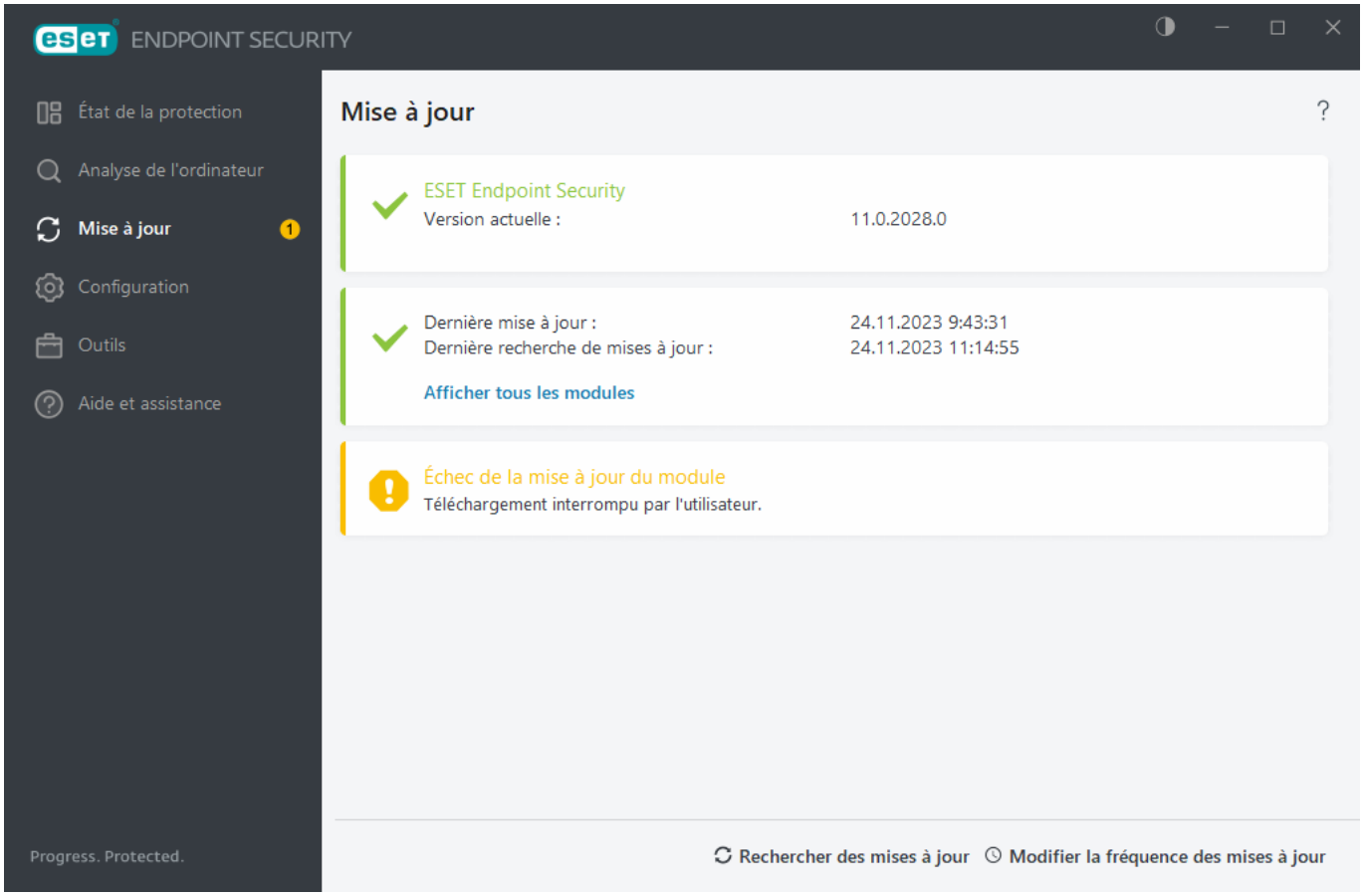
Dans des circonstances normales, une coche verte s'affiche dans la fenêtre **Mise à jour** pour indiquer que le programme est à jour. Si ce n'est pas le cas, le programme n'est pas à jour et le risque d'infection est accru. Veuillez mettre à jour les modules du programme dès que possible.

Échec de la mise à jour

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 paramètres 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** – Votre licence n'est pas active. Nous vous recommandons de vérifier vos données d'authentification. 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. Vérifiez que vous disposez d'une connexion Internet active auprès de votre fournisseur d'accès Internet (FAI).



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

Comment créer des tâches de mise à jour

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

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

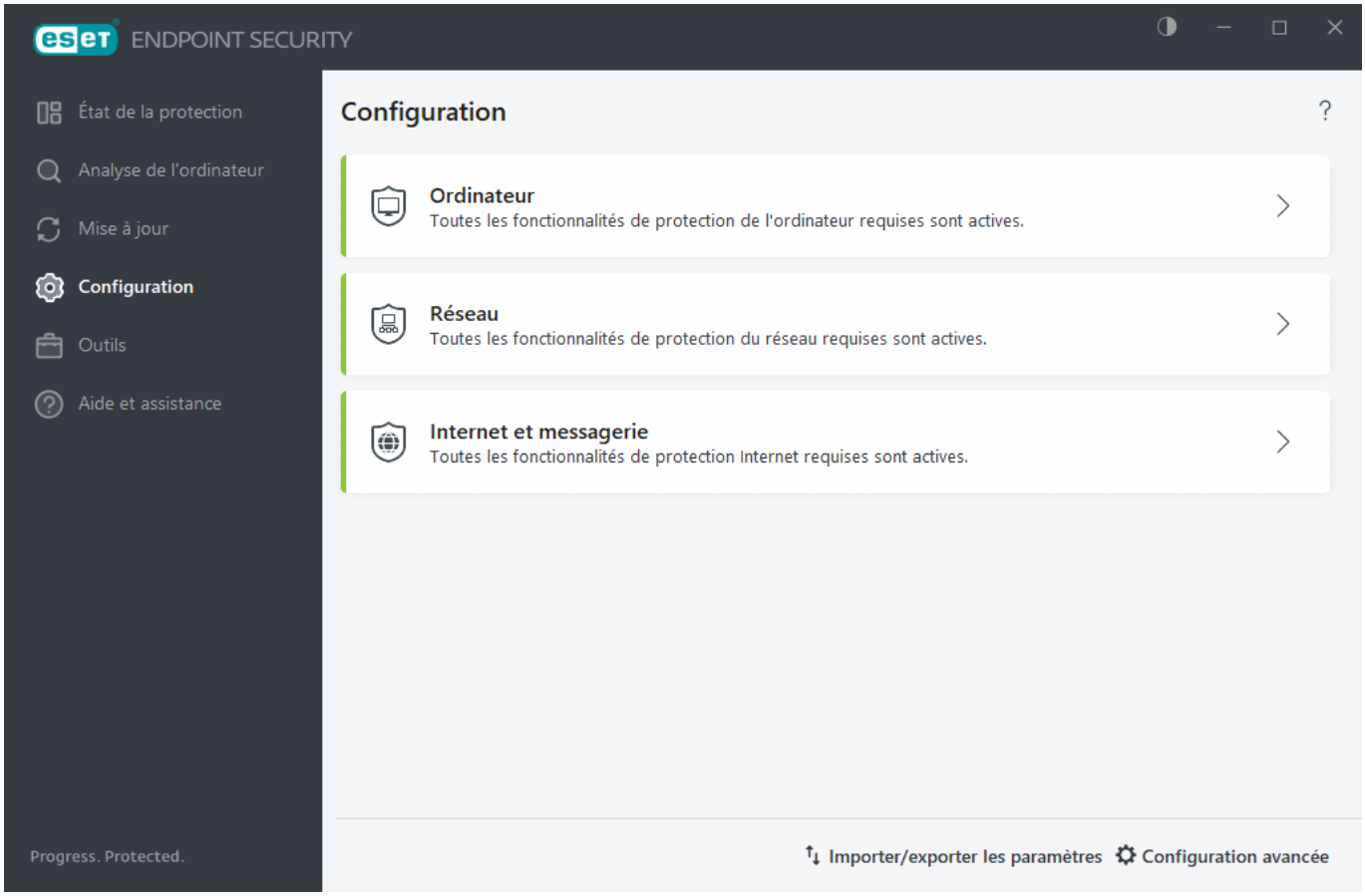
- **Mise à jour automatique régulière**
- **Mise à jour automatique après ouverture de session utilisateur**

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

Param

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

Lors de la création d'une stratégie à partir d'ESET PROTECT On-Prem 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'ESET PROTECT On-Prem.



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

Ordinateur

Réseau

Web et courier électronique

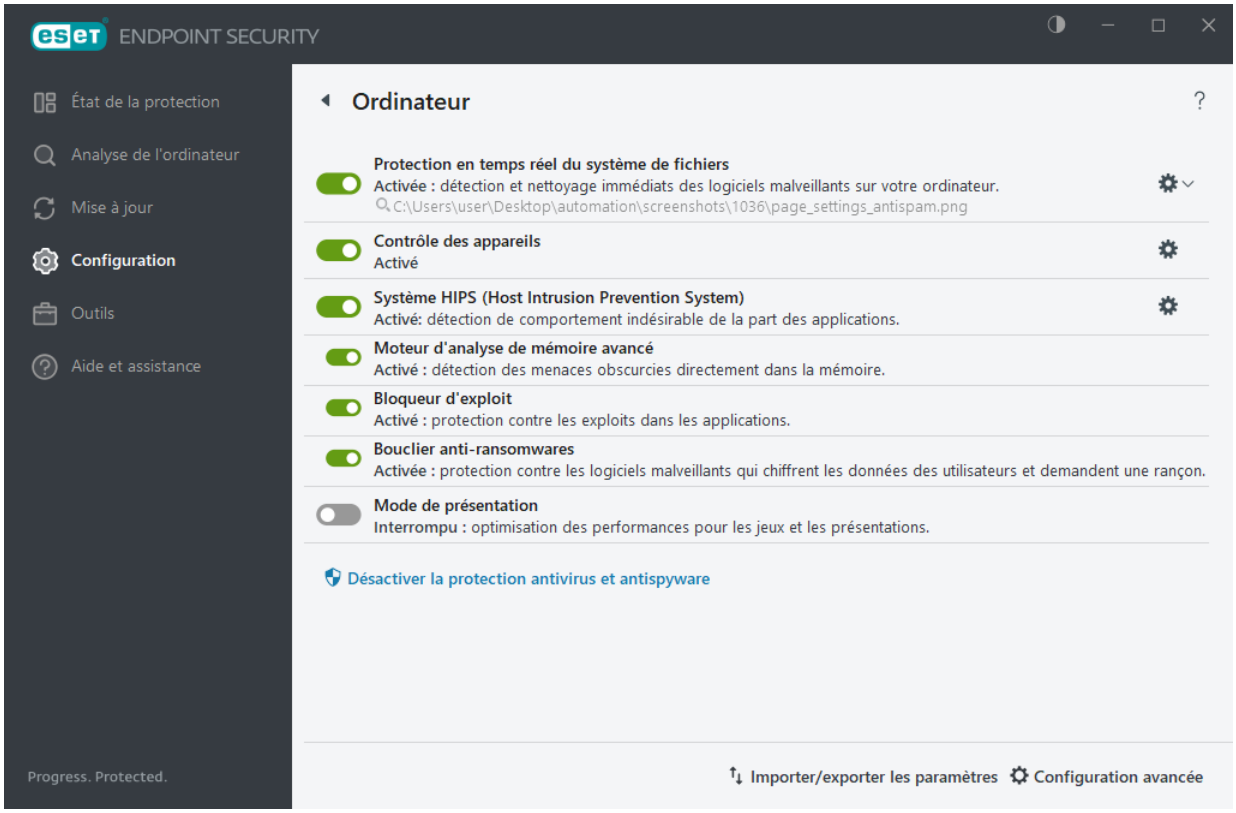
Lorsque la stratégie ESET PROTECT On-Prem est appliquée, l'icône représentant un verrou s'affiche en regard d'un composant spécifique. La stratégie appliquée par ESET PROTECT On-Prem peut être remplacée localement après l'authentification par l'utilisateur connecté (l'administrateur, par exemple). Pour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

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

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

Ordinateur

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



Dans la section **Ordinateur**, vous pouvez activer ou 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. Cliquez sur l'icône d'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. Pour ouvrir les configurations avancées de la protection en temps réel du système de fichiers, cliquez sur Configurer.
- 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 périphérique 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®. Lire des informations supplémentaires 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 notifications 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**.

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

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

Une menace est détectée

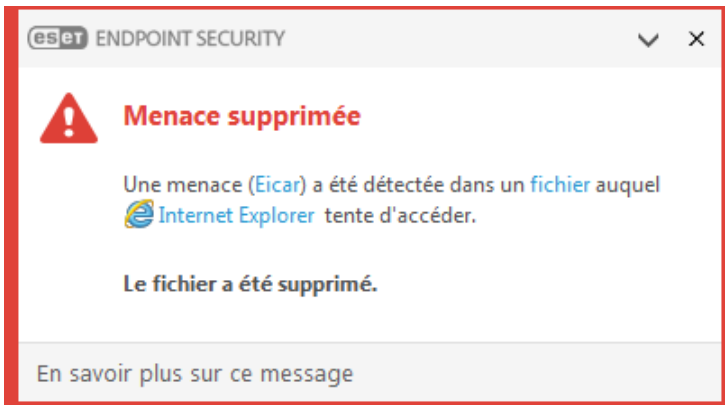
Des infiltrations peuvent atteindre le système à partir de différents points d'entrée : pages Web, dossiers partagés, courrier électronique ou périphériques amovibles (USB, disques externes, CD, DVD, etc.).

Comportement standard

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

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

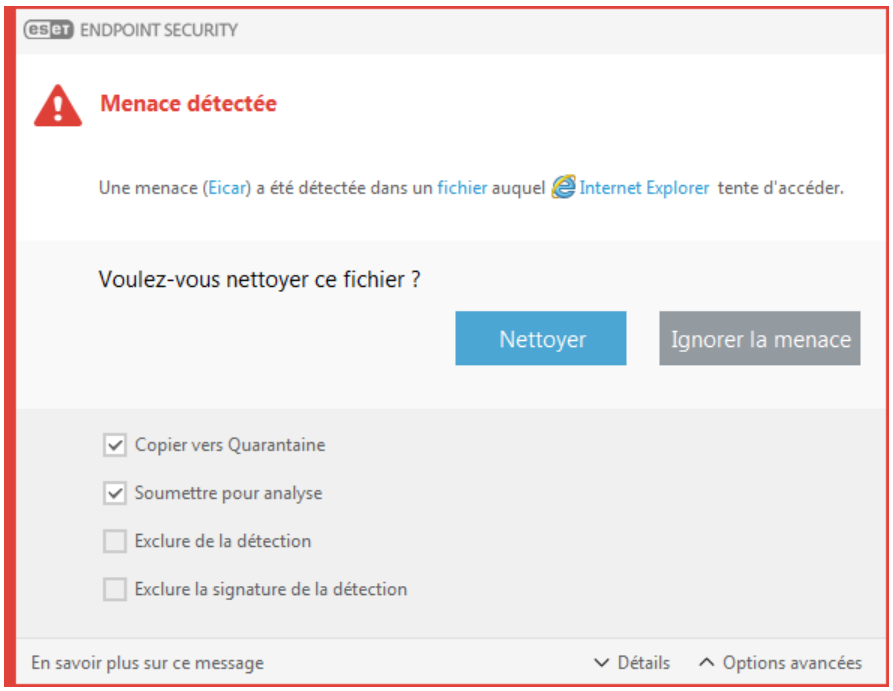
Chaque fonction utilise le niveau de nettoyage standard et tente de nettoyer le fichier et de le déplacer en Quarantaine ou met fin à la connexion. Une fenêtre de notification s'affiche dans la zone de notification, dans l'angle inférieur droit de l'écran. Pour obtenir des informations détaillées sur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

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

Restoring from Quarantine

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

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

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

Menaces multiples

Si des fichiers infectés n'ont pas été nettoyés durant une analyse de l'ordinateur (ou si le niveau de nettoyage a été défini sur **Pas de nettoyage**), une fenêtre d'alerte s'affiche ; elle vous invite à sélectionner 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 Security et cliquez sur Analyse de l'ordinateur
- Cliquez sur **Analyse intelligente** (pour plus d'informations, voir Analyse de l'ordinateur)
- Lorsque l'analyse est terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés

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

Réseau

Ouvrez la fenêtre principale du programme > **Configuration** > **Réseau** pour configurer les paramètres de base de la protection du réseau ou résoudre les problèmes de communication réseau.

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

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

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

Pare-feu – Filtre toutes les communications réseau en fonction de la configuration d'ESET Endpoint Security.

Configurer – Ouvre Configurations avancées du pare-feu où vous pouvez configurer la gestion des communications réseau par le pare-feu.

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

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

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

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

Protection contre les attaques réseau (IDS) – Analyse le contenu du trafic réseau et protège contre les attaques réseau. Tout trafic considéré comme nuisible est bloqué. ESET Endpoint Security vous informe lorsque vous vous

connectez à un réseau sans fil sans protection ou à un réseau avec une faible protection.

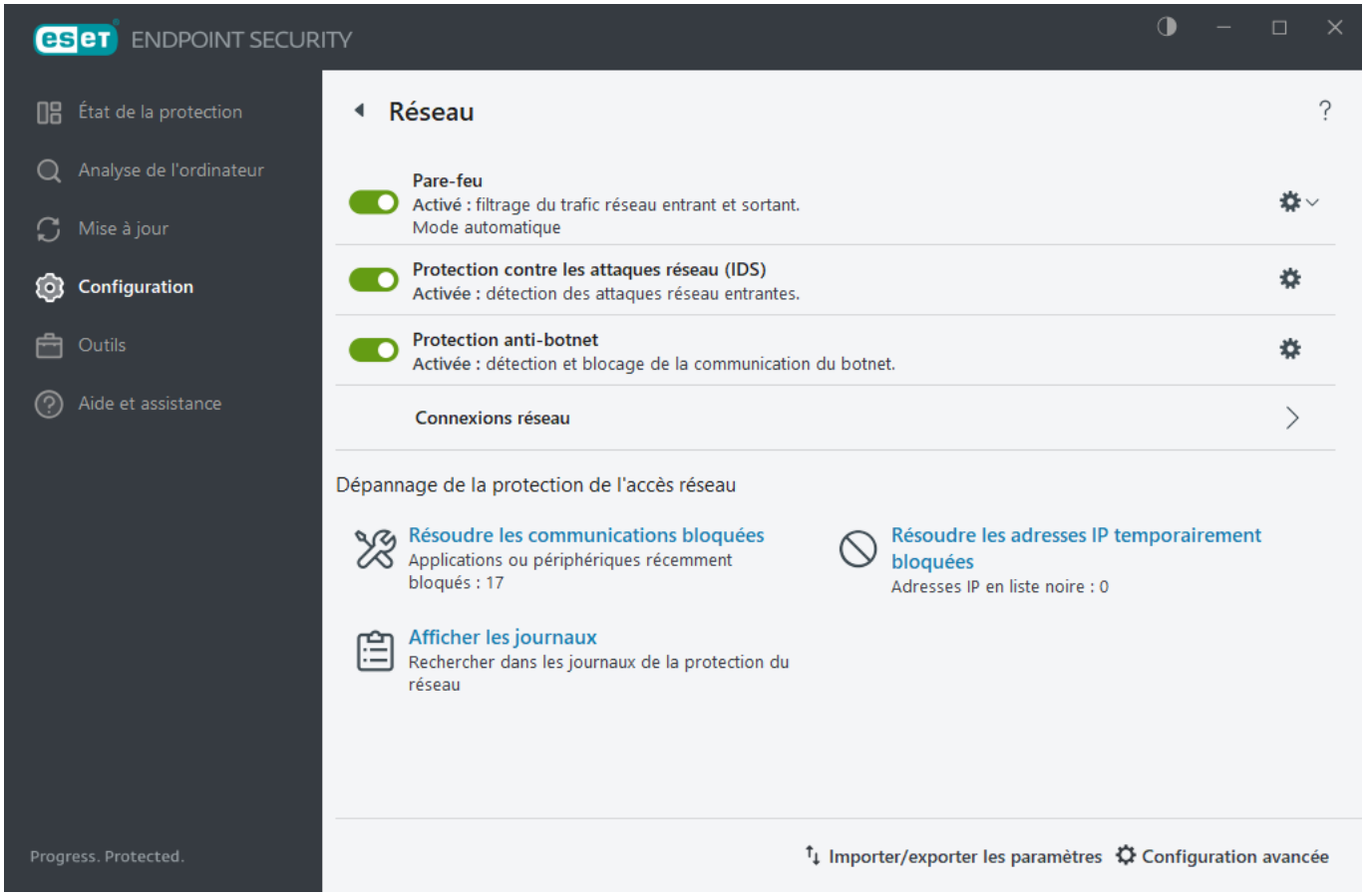
Anti-botnet – Identifie rapidement et précisément les logiciels malveillants sur le système.

Connexions réseau – Indique les réseaux auxquels les adaptateurs réseau sont connectées avec des informations détaillées.

Résoudre les communications bloquées – Permet de résoudre les problèmes de connectivité liés au pare-feu ESET. Pour plus d'informations, reportez-vous à l'assistant de dépannage.

Résoudre les adresses IP temporairement bloquées – Afficher 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.

Afficher les journaux – Ouvre le fichier journal de la protection du réseau.



Connexions réseau

Indique les réseaux auxquels les cartes réseau sont connectées. Pour afficher les connexions réseau, ouvrez la fenêtre principale du programme > **Configuration** > **Réseau** > **Connexions réseau**.

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

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

- **Modifier** – Ouvre la fenêtre Configurer la protection du réseau dans laquelle vous pouvez attribuer un profil de protection du réseau à un réseau spécifique.

- **Oublier** – Réinitialise la configuration de la connexion réseau par défaut.

Détails des connexions réseau

Double-cliquez sur une connexion dans la liste des connexions réseau pour afficher ses détails ainsi que ceux de l'adaptateur réseau. Les détails de la connexion réseau et de l'adaptateur réseau permettent d'identifier le réseau que vous essayez de configurer dans la Protection de l'accès réseau.

Détails des connexions réseau :

- État de la connexion réseau
- Date et heure de la première détection réseau
- Dernière fois que le réseau a été actif
- Temps total passé connecté à ce réseau
- Profil de connexion réseau
- Profil de connexion réseau défini dans Windows
- Configuration de la protection du réseau (si le réseau est approuvé)

Détails de l'adaptateur réseau :

- Type de connexion (câblé, virtuel, etc.)
- Nom de la carte réseau
- Description de l'adaptateur
- Adresse IP avec adresse MAC
- L'adresse IPv4 et IPv6 du réseau avec sous-réseau
- Suffixe DNS
- Adresse IP du serveur DNS
- Adresse IP du serveur DHCP
- Adresses IP et MAC de la passerelle par défaut
- Adresse MAC de l'adaptateur

Dépannage de l'accès réseau

L'assistant de dépannage permet de résoudre les problèmes de connectivité liés au pare-feu. L'option **Dépannage de l'accès réseau** figure dans la fenêtre principale du programme > **Configuration** > **Réseau** > **Résoudre les communications bloquées**.

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

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 **création d'une autre règle** et toutes les communications précédemment bloquées sont autorisées. Si le problème persiste, redémarrez l'ordinateur.

Cliquez sur **Ouvrir les règles du pare-feu** pour afficher les règles créées par l'assistant. Par ailleurs, vous pouvez afficher les règles créées par l'assistant dans Configurations avancées > **Protections** > **Protection de l'accès réseau** > **Pare-feu** > **Règles** > **Modifier**.

Les articles suivants de la base de connaissances ESET peuvent être disponibles uniquement en anglais :
- Ajout d'une exception de pare-feu à l'aide de l'assistant de dépannage

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

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, ouvrez la fenêtre principale du programme > **Configuration** > **Protection du réseau** > **Résoudre les adresses IP temporairement bloquées**. Les adresses IP temporairement bloquées le sont pendant 1 heure.

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.

Journaux de la protection du réseau

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

Les fichiers journaux peuvent servir à détecter des erreurs et à révéler des intrusions dans le système. La Protection du réseau contient les données suivantes :

- Date et heure de l'événement
- Nom de l'événement
- Source
- Adresse réseau cible
- Protocole de communication réseau

- Règle appliquée ou nom du ver s'il est identifié
- Chemin d'accès et nom de l'application
- Hachage
- Utilisateur
- Signataire de l'application (éditeur)
- Nom du package
- Nom du service

Une analyse approfondie de ces données peut aider à détecter des tentatives visant à compromettre la sécurité du système. Beaucoup d'autres facteurs peuvent informer l'utilisateur sur les risques potentiels de sécurité et l'aident à minimiser leur effet : connexions fréquentes en provenance de sites inconnus, multiples tentatives d'établissement de connexion, communications issues d'applications inconnues ou utilisation de numéros de ports inhabituels.

> **Exploitation d'une vulnérabilité de la sécurité**
> Le message relatif à l'exploitation d'une vulnérabilité de la sécurité est consigné même si la vulnérabilité en question a déjà été corrigée depuis la détection et le blocage de la tentative d'exploitation au niveau du réseau avant que l'exploitation ne puisse être effectivement exploitée.

Résolution des problèmes liés à la protection du réseau ESET

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

Pour obtenir de l'aide pour la résolution des problèmes liés au Protection du réseau ESET, consultez les rubriques suivantes :

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

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

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

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

> Utilisez la consignation pour déterminer l'ordre dans lequel le Protection du réseau 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 Security 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 Security doit être configuré avec les paramètres suivants :

1. Définition de la verbosité minimale des journaux sur **Diagnostic** dans Configuration avancée > **Outils** > **Fichiers journaux**.
2. Activez **Avertir lors d'attaques entrantes contre les failles de sécurité** dans Configurations avancées > **Protections** > **Protection de l'accès réseau** > **Protection contre les attaques réseau Options avancées** > **Détection des intrusions**.

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

Lorsque le pare-feu 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.

> 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 avancée de la protection du réseau

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

1. Ouvrir Configuration avancée > **Outils** > **Diagnostics** et activez l'option **Activer la journalisation avancée de la protection du réseau**.
2. Essayez de reproduire le problème que vous rencontrez.
3. Désactivez la journalisation avancée de la protection du réseau.
4. Le fichier journal PCAP, créé par la journalisation avancée de la protection du réseau, se trouve dans le même répertoire où sont générés les fichiers d'image mémoire de diagnostic :*C:\ProgramData\ESET\ESET Security\Diagnostics*

Résolution des problèmes liés à l'analyseur du trafic réseau

Si vous rencontrez des problèmes avec votre navigateur ou votre client de messagerie, vous devez d'abord déterminer si l'analyseur du trafic réseau en est la cause. Pour ce faire, désactivez temporairement l'analyseur du trafic réseau dansConfigurations avancées > **Moteur de détection** > **Analyseur du trafic réseau** (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 l'option SSL/TLS est activée, essayez de la désactiver temporairement. Vous pouvez continuer à utiliser SSL/TSL et effectuer la mise à jour en excluant la communication qui pose problème :
  Désactiver SSL/TLS. 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 de la protection de l'accès web (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 pouvez pas à utiliser les fonctionnalités d'un appareil 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 de la protection de l'accès web 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 SSL/TLS, ESET Endpoint Security vérifie que les applications installées approuvent le filtrage du protocole SSL en important un certificat dans leur magasin de certificats. Certaines applications peuvent nécessiter un redémarrage pour importer un certificat. 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. Ensuite, désactivez l'option SSL/TLS et réactivez-la. L'importation est réexécutée.

Menace réseau bloquée

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

Vous pouvez trouver le type de menace et l'adresse IP de l'appareil associé dans la notification. Cliquez sur **Modifier la gestion de cette menace** pour afficher les options suivantes :

Continuer le blocage – Bloque la menace détectée. Si vous ne souhaitez plus recevoir de notifications sur ce type de menace à partir d'une adresse distante spécifique, cliquez sur la case d'option en regard de l'option **Ne pas avertir** avant de cliquer sur **Continuer le blocage**. Une règle IDS (Intrusion Detection Service) est alors créée avec la configuration suivante : **Bloquer** - par défaut, **Notifier** - non, **Consigner** - non.

Autoriser – Crée une règle IDS (Intrusion Detection Service) pour autoriser la menace détectée. Sélectionnez l'une des options suivantes avant de cliquer sur **Autoriser** pour spécifier les paramètres de la règle :

- **Avertir uniquement lorsque cette menace est bloquée** – Configuration de la règle : **Bloquer** - non, **Notifier** - non, **Consigner** - non.
- **Avertir lorsque cette menace se produit** – Configuration de la règle : **Bloquer** - non, **Notifier** - par défaut, **Consigner** - par défaut.
- **Ne pas avertir** – Configuration de la règle : **Bloquer** - non, **Notifier** - non, **Consigner** - non.

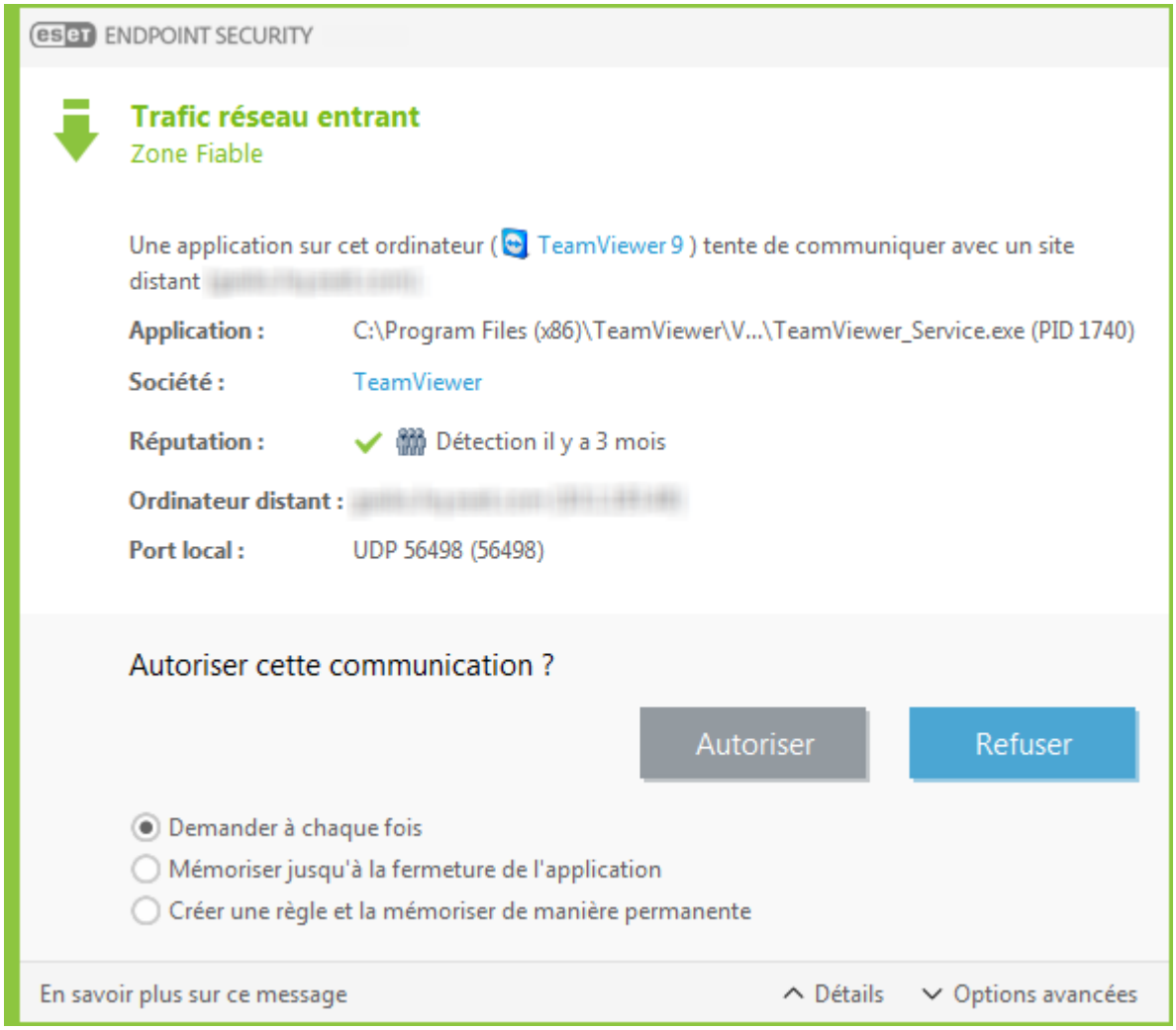
> Les informations affichées dans cette fenêtre de notification peuvent varier selon le type de la menace détectée.
> Pour plus d'informations sur les menaces et d'autres termes associés, reportez-vous aux sections Types d'attaques distantes ou Types de détections.
> Pour résoudre les **adresses IP en double lors d'un événement réseau**, consultez cet article de la base de connaissances ESET.

Établissement d'une connexion – détection

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

Le **mode interactif** affiche une fenêtre d'information qui signale la détection d'une nouvelle connexion réseau et donne des informations détaillées sur la connexion. Vous pouvez choisir d'**autoriser** ou de **refuser** (bloquer) la connexion. Si vous autorisez toujours la même connexion dans la boîte de dialogue, il est recommandé de créer une nouvelle règle pour la connexion. Sélectionnez **Créer une règle et la mémoriser de manière permanente** et sauvegardez l'action comme une nouvelle règle pour le pare-feu. Si le pare-feu personnel reconnaît

ultérieurement cette connexion, il applique la règle existante sans intervention de l'utilisateur.



Lors de la création de nouvelles règles, n'autorisez que les connexions que vous savez sécurisées. Si toutes les connexions sont autorisées, le pare-feu n'a aucune raison d'exister. Voici les paramètres importants pour les connexions :

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

Signataire – Nom de l'éditeur de l'application. Cliquez sur le texte pour afficher un certificat de sécurité pour la société.

Réputation – Niveau de risque de la connexion. Un niveau de risque est attribué aux connexions : OK (vert), Inconnu (orange) ou Risqué (rouge), à l'aide d'une série de règles heuristiques qui examinent les caractéristiques de chaque connexion, le nombre d'utilisateurs et l'heure de détection. Ces informations sont collectées par la technologie ESET LiveGrid®.

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

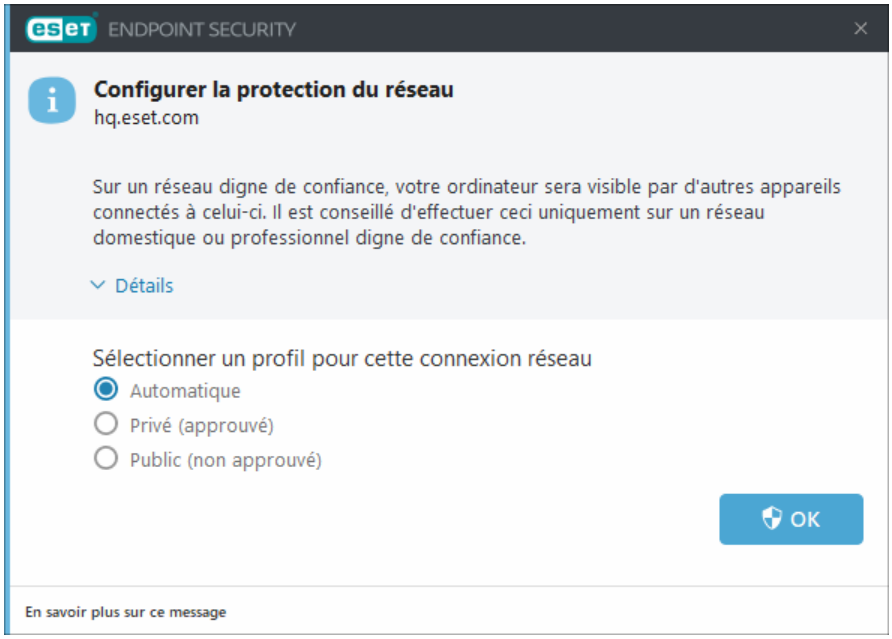
Ordinateur distant – Adresse de l'appareil distant. Autorise uniquement les connexions aux adresses fiables et connues.

Port distant – Port de communication. Les communications via les ports communs (le port 80 443 pour le trafic Internet par exemple) doivent toujours être autorisées en situation normale.

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

Nouveau réseau détecté

Par défaut, ESET Endpoint Security utilise les paramètres Windows lorsqu'une nouvelle connexion réseau est détectée. Pour afficher une boîte de dialogue lorsqu'un nouveau réseau est détecté, définissez l'attribution de profil de protection du réseau sur **Demander**. La protection du réseau s'effectue dès que votre ordinateur se connecte à un nouveau réseau.



Vous pouvez effectuer un choix parmi les profils de connexion réseau suivants :

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

Privé : pour des réseaux approuvés (réseau domestique ou professionnel). Votre ordinateur et les fichiers partagés stockés sur votre ordinateur sont visibles par les autres utilisateurs du réseau, et les ressources du système sont accessibles aux autres utilisateurs du réseau (l'accès aux fichiers et imprimantes partagés est activé, la communication RPC entrante est activée et le partage du bureau à distance est disponible). Il est recommandé d'utiliser ce paramètre lors des accès à un réseau local sécurisé. Ce profil est automatiquement attribué à une connexion réseau s'il est configuré en tant que domaine ou réseau privé dans Windows.

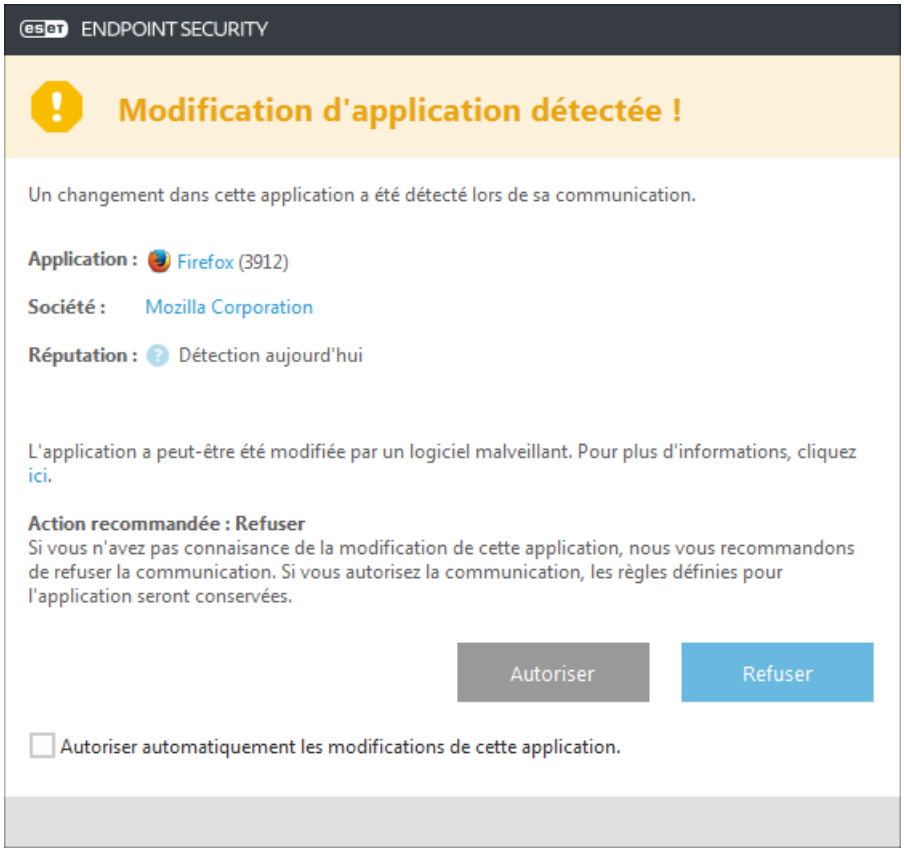
Non : pour des réseaux non approuvés (réseau public). les fichiers et les dossiers de votre système ne sont pas partagés ou visibles par les autres utilisateurs du réseau et les partages des ressources système sont désactivés. Il est recommandé d'utiliser ce paramètre lors des accès à des réseaux sans fil. Ce profil est automatiquement attribué à toute connexion réseau qui n'est pas configurée en tant que domaine ou réseau privé dans Windows.

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

⚠ Une configuration incorrecte du réseau peut compromettre la sécurité de votre ordinateur.

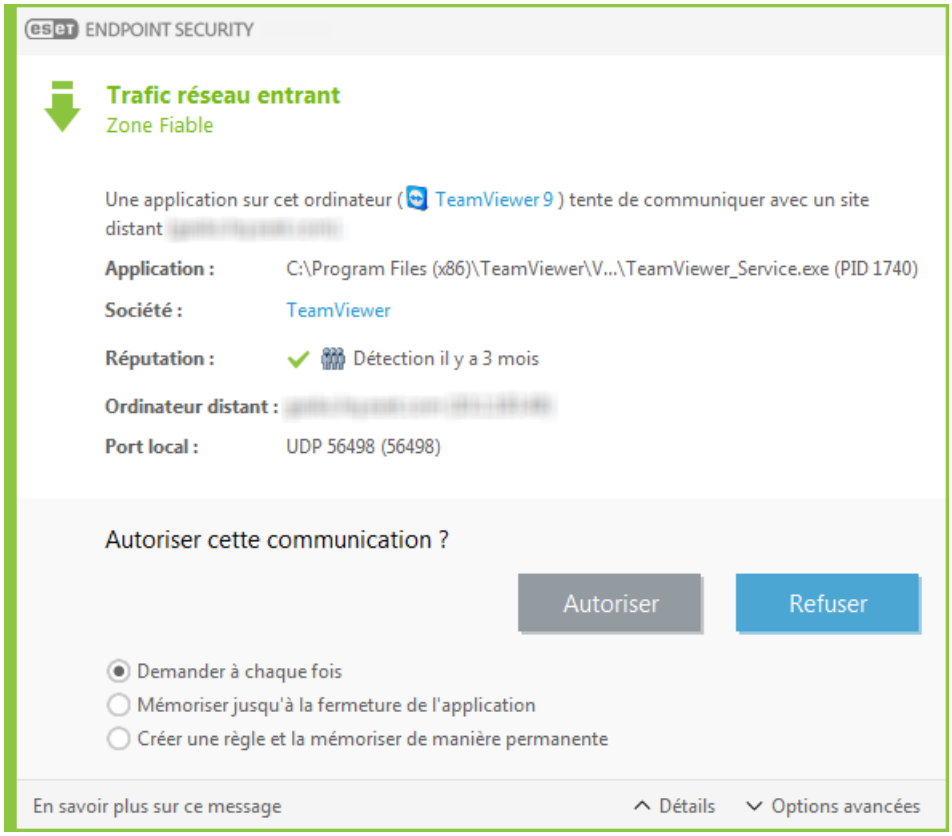
Changement d'application

Le pare-feu a détecté une modification dans une application utilisée pour établir des connexions sortantes à partir de l'ordinateur. Il se peut que l'application ait simplement été mise à jour. Mais une modification peut aussi être due à une application malveillante. Si vous n'êtes pas au courant d'une modification légitime qui ait pu avoir lieu, nous recommandons de refuser la connexion et d'analyse intelligente avec le moteur de détection le plus récent. Si vous êtes sûr de la modification et si vous autorisez les communications à l'aide de la case à cocher **Autoriser automatiquement les modifications de cette application**, la règle appliquée pour cette application est conservée.



Communication fiable entrante

Exemple de connexion entrante dans la zone Fiable :
un ordinateur distant dans la zone Fiable tente d'établir une communication avec une application locale s'exécutant sur votre ordinateur.



Application – Application contactée par un appareil distant.

Chemin de l'application – Emplacement de l'application.

Application Microsoft Store – Nom de l'application dans Microsoft Store.

Signataire – Nom de l'éditeur de l’application. Cliquez sur le texte pour afficher un certificat de sécurité pour la société.

Réputation – Réputation de l'application, telle qu'obtenue par la technologie ESET LiveGrid®.

Service – Nom du service en cours d'exécution sur l'ordinateur.

Ordinateur distant – Ordinateur distant tentant d'établir une communication avec l'application sur votre ordinateur.

Port distant – Port utilisé pour la communication.

Demander à chaque fois – Si l'action par défaut d'une règle est définie sur **Demander**, une boîte de dialogue apparaît à chaque déclenchement de la règle.

Mémoriser jusqu'à la fermeture de l'application – ESET Endpoint Security mémorise l'action choisie jusqu'au prochain redémarrage.

Créer une règle et la mémoriser de manière permanente – Si vous activez cette option avant d'autoriser ou de refuser une communication, ESET Endpoint Security mémorise l'action et la réutilise si le serveur distant tente de nouveau de contacter l'application.

Autoriser – Autorise la communication entrante.

Refuser – Refuse la communication entrante.

Modifier la règle – Permet de personnaliser les propriétés de la règle à l'aide de l'éditeur de règles du pare-feu.

Communication sortante fiable

Exemple de connexion sortante dans la zone Fiable :
une application locale tente d'établir la connexion avec un autre ordinateur se trouvant dans le réseau local ou dans un réseau situé à l'intérieur de la zone Fiable.

Application – Application contactée par un appareil distant.

Chemin de l'application – Emplacement de l'application.

Application Microsoft Store – Nom de l'application dans Microsoft Store.

Signataire – Nom de l'éditeur de l'application. Cliquez sur le texte pour afficher un certificat de sécurité pour la société.

Réputation – Réputation de l'application, telle qu'obtenue par la technologie ESET LiveGrid®.

Service – Nom du service en cours d'exécution sur l'ordinateur.

Ordinateur distant – Ordinateur distant tentant d'établir une communication avec l'application sur votre ordinateur.

Port distant – Port utilisé pour la communication.

Demander à chaque fois – Si l'action par défaut d'une règle est définie sur **Demander**, une boîte de dialogue apparaît à chaque déclenchement de la règle.

Mémoriser jusqu'à la fermeture de l'application – ESET Endpoint Security mémorise l'action choisie jusqu'au prochain redémarrage.

Créer une règle et la mémoriser de manière permanente – Si vous activez cette option avant d'autoriser ou de refuser une communication, ESET Endpoint Security mémorise l'action et la réutilise si le serveur distant tente de nouveau de contacter l'application.

Autoriser – Autorise la communication entrante.

Refuser – Refuse la communication entrante.

Modifier la règle – Permet de personnaliser les propriétés de la règle à l'aide de l'éditeur de règles du pare-feu.

Communication entrante

Exemple de connexion Internet entrante :
un ordinateur distant tente de communiquer avec une application s'exécutant sur cet ordinateur.

Application – Application contactée par un appareil distant.

Chemin de l'application – Emplacement de l'application.

Application Microsoft Store – Nom de l'application dans Microsoft Store.

Signataire – Nom de l'éditeur de l'application. Cliquez sur le texte pour afficher un certificat de sécurité pour la société.

Réputation – Réputation de l'application, telle qu'obtenue par la technologie ESET LiveGrid®.

Service – Nom du service en cours d'exécution sur l'ordinateur.

Ordinateur distant – Ordinateur distant tentant d'établir une communication avec l'application sur votre ordinateur.

Port distant – Port utilisé pour la communication.

Demander à chaque fois – Si l'action par défaut d'une règle est définie sur **Demander**, une boîte de dialogue apparaît à chaque déclenchement de la règle.

Mémoriser jusqu'à la fermeture de l'application – ESET Endpoint Security mémorise l'action choisie jusqu'au prochain redémarrage.

Créer une règle et la mémoriser de manière permanente – Si vous activez cette option avant d'autoriser ou de refuser une communication, ESET Endpoint Security mémorise l'action et la réutilise si le serveur distant tente de nouveau de contacter l'application.

Autoriser – Autorise la communication entrante.

Refuser – Refuse la communication entrante.

Modifier la règle – Permet de personnaliser les propriétés de la règle à l'aide de l'éditeur de règles du pare-feu.

Communication sortante

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

Application – Application contactée par un appareil distant.

Chemin de l'application – Emplacement de l'application.

Application Microsoft Store – Nom de l'application dans Microsoft Store.

Signataire – Nom de l'éditeur de l'application. Cliquez sur le texte pour afficher un certificat de sécurité pour la société.

Réputation – Réputation de l'application, telle qu'obtenue par la technologie ESET LiveGrid®.

Service – Nom du service en cours d'exécution sur l'ordinateur.

Ordinateur distant – Ordinateur distant tentant d'établir une communication avec l'application sur votre ordinateur.

Port distant – Port utilisé pour la communication.

Demander à chaque fois – Si l'action par défaut d'une règle est définie sur **Demander**, une boîte de dialogue apparaît à chaque déclenchement de la règle.

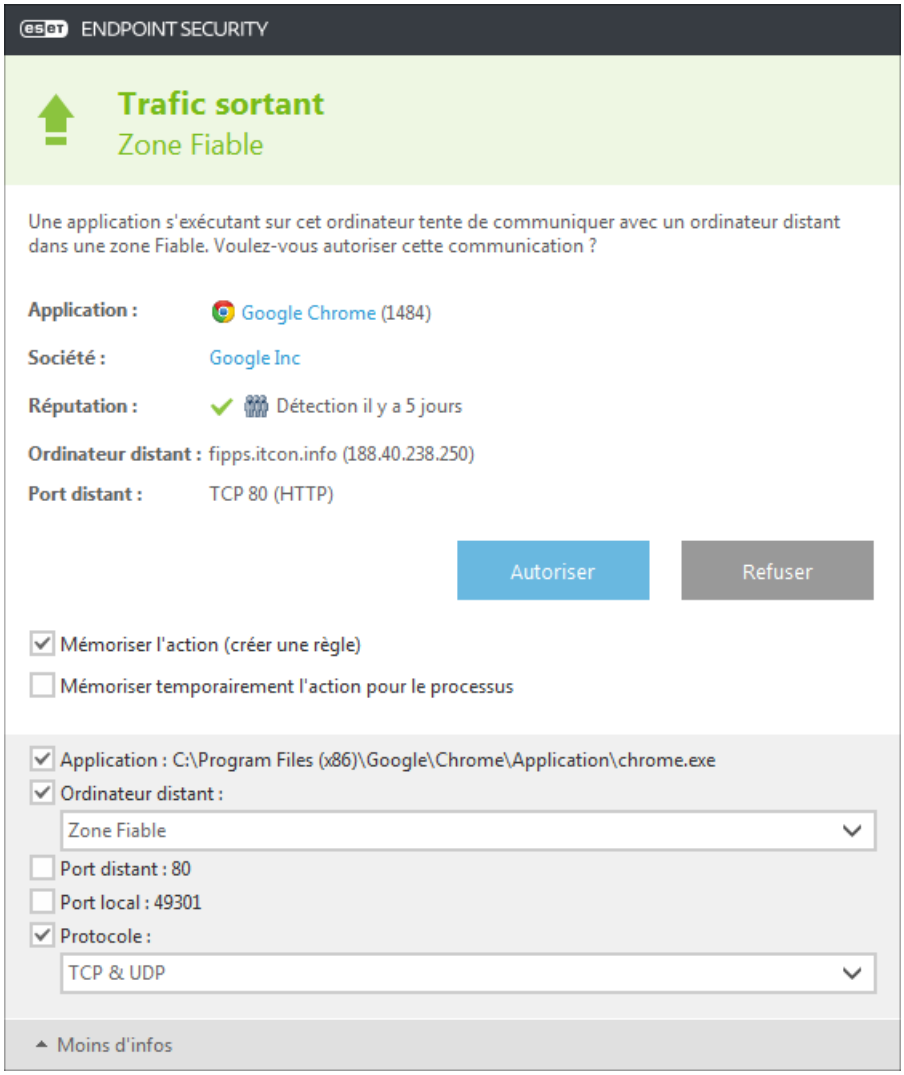
Mémoriser jusqu'à la fermeture de l'application – ESET Endpoint Security mémorise l'action choisie jusqu'au prochain redémarrage.

Créer une règle et la mémoriser de manière permanente – Si vous activez cette option avant d'autoriser ou de refuser une communication, ESET Endpoint Security mémorise l'action et la réutilise si le serveur distant tente de nouveau de contacter l'application.

Autoriser – Autorise la communication entrante.

Refuser – Refuse la communication entrante.

Modifier la règle – Permet de personnaliser les propriétés de la règle à l'aide de l'éditeur de règles du pare-feu.



Configuration de l'affichage des connexions

Cliquez avec le bouton droit sur une connexion pour afficher les options supplémentaires suivantes :

Résoudre les noms – Dans la mesure du possible, toutes les adresses réseau sont affichées dans le format DNS et non dans le format d'adresse IP numérique.

Afficher uniquement les connexions TCP – Cette liste affiche uniquement les connexions appartenant à la suite du protocole TCP.

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

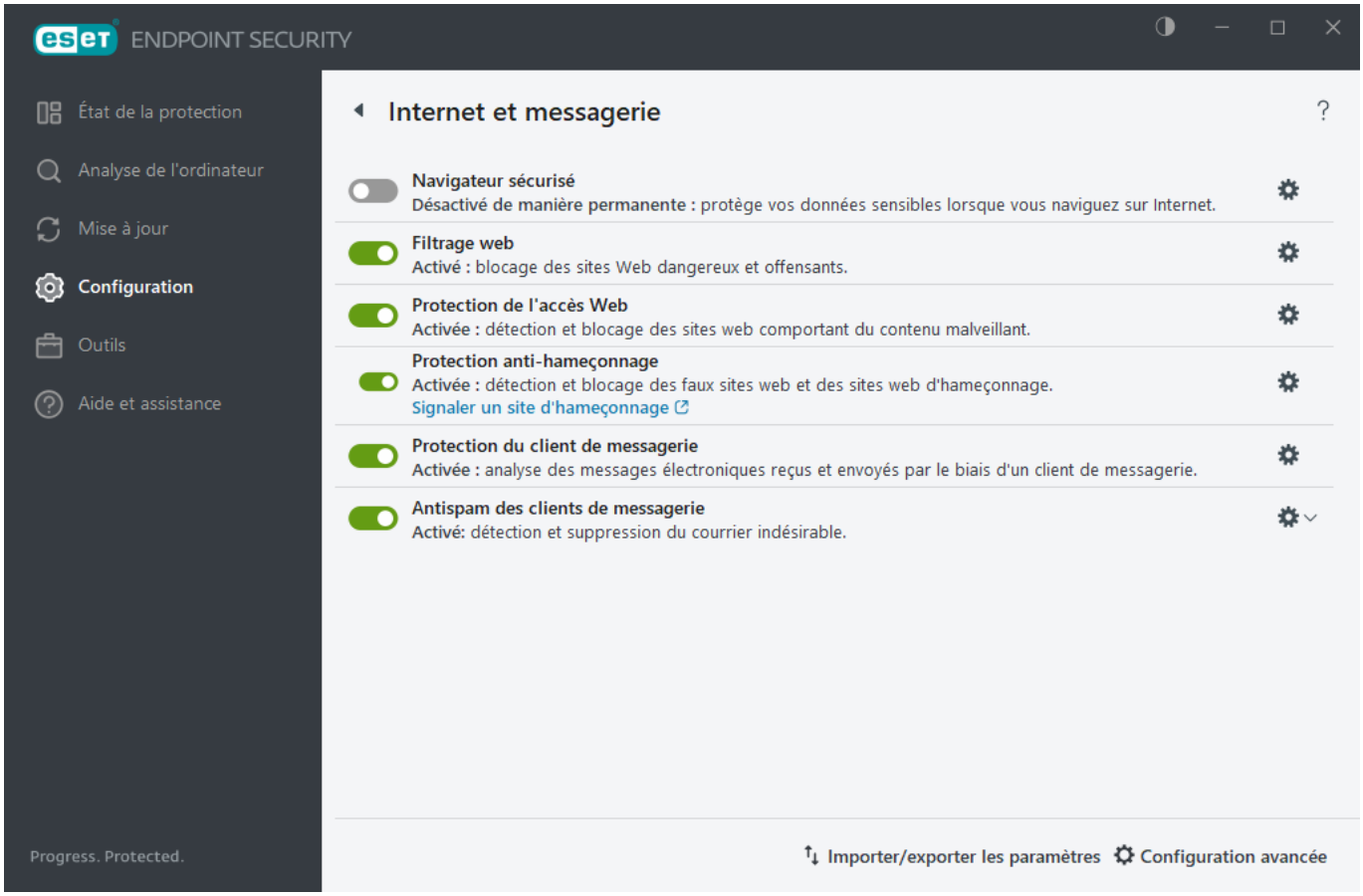
Afficher les connexions internes à l'ordinateur – Cette option permet de n'afficher que les connexions où le côté distant est un système local ; ces connexions sont appelées connexions hôte local.

Internet et messagerie

La connectivité internet est une fonctionnalité standard dans un ordinateur personnel, mais aussi le principal moyen de transfert de code malveillant. Ouvrez la fenêtre principale du programme > **Configuration** > **Internet et messagerie** pour configurer les fonctionnalités d'ESET Endpoint Security qui accroissent la protection internet.

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

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



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

Navigateur sécurisé : Protège vos données sensibles lorsque vous naviguez sur Internet.

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

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

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

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

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

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

L'antispam des clients de messagerie filtre les e-mails non sollicités.

Pour l'**antispam des clients de messagerie**, cliquez sur l'icône d'engrenage et sélectionnez l'une des options suivantes :

- **Configurer** : affiche les paramètres avancés de l'antispam des clients de messagerie.
- **Liste d'adresses de l'utilisateur** (si activée) : ouvre une boîte de dialogue dans laquelle vous pouvez ajouter, modifier ou supprimer des adresses pour définir les règles antispam. Les règles de cette liste seront appliquées à l'utilisateur actuel.
- **Liste d'adresses globale** (si activée) : ouvre une boîte de dialogue dans laquelle vous pouvez ajouter, modifier ou supprimer des adresses pour définir les règles antispam. Les règles de cette liste seront appliquées à tous les utilisateurs.

Protection antihameçonnage

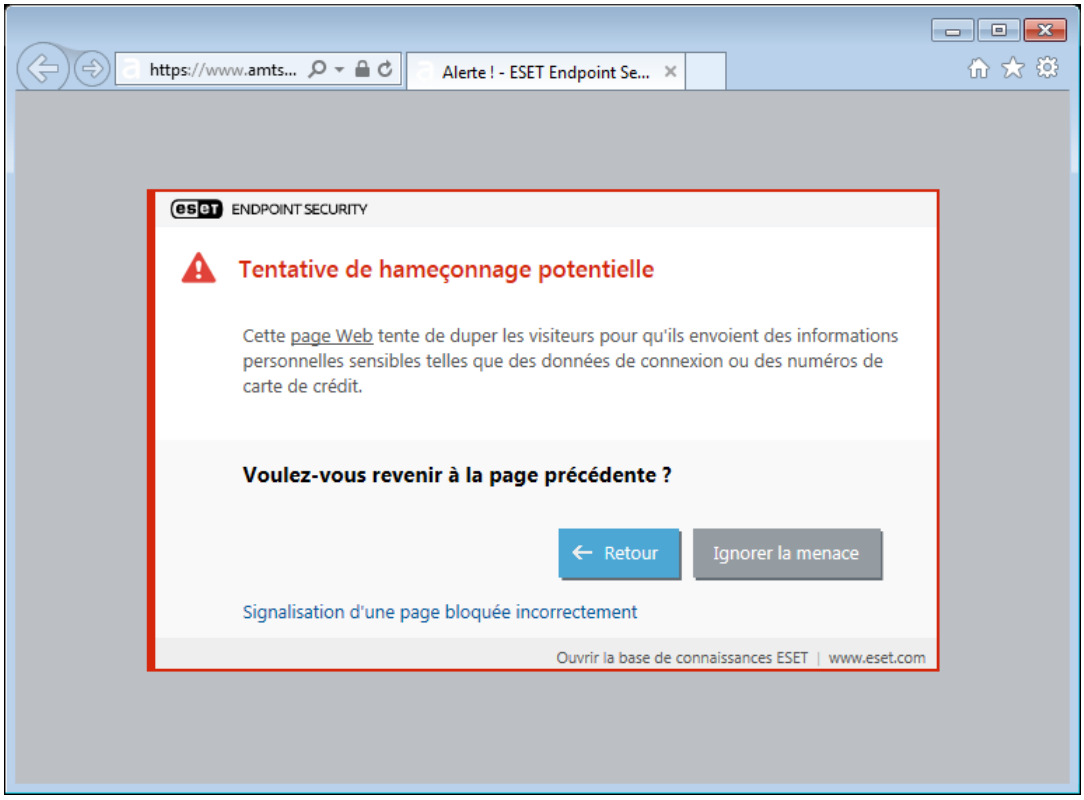
L'hameçonnage est une activité criminelle qui utilise l'ingénierie sociale (manipulation des utilisateurs pour obtenir des informations confidentielles). Il est utilisé pour accéder à des données sensibles telles que des numéros de compte bancaire, des codes PIN, etc. Pour plus d'informations, reportez-vous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

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

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

Accès à un site Web d'hameçonnage

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



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

Signaler un site d'hameçonnage

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

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

Importer et exporter les paramètres

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

Instructions illustrées

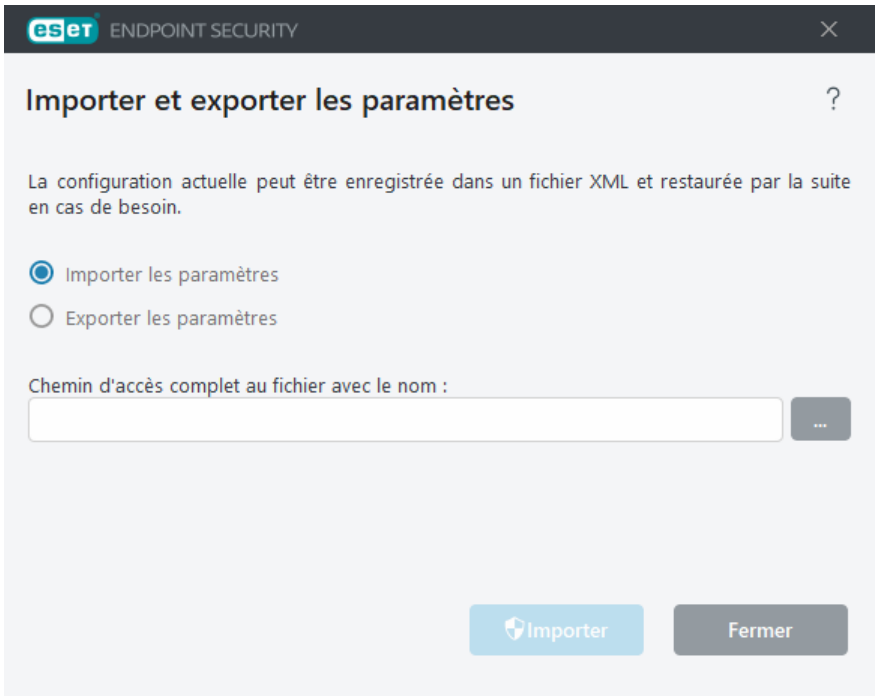
Pour obtenir des instructions illustrées disponibles en anglais et dans plusieurs autres langues, consultez Importer ou exporter les paramètres de configuration ESET à l'aide d'un fichier .xml.

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

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

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

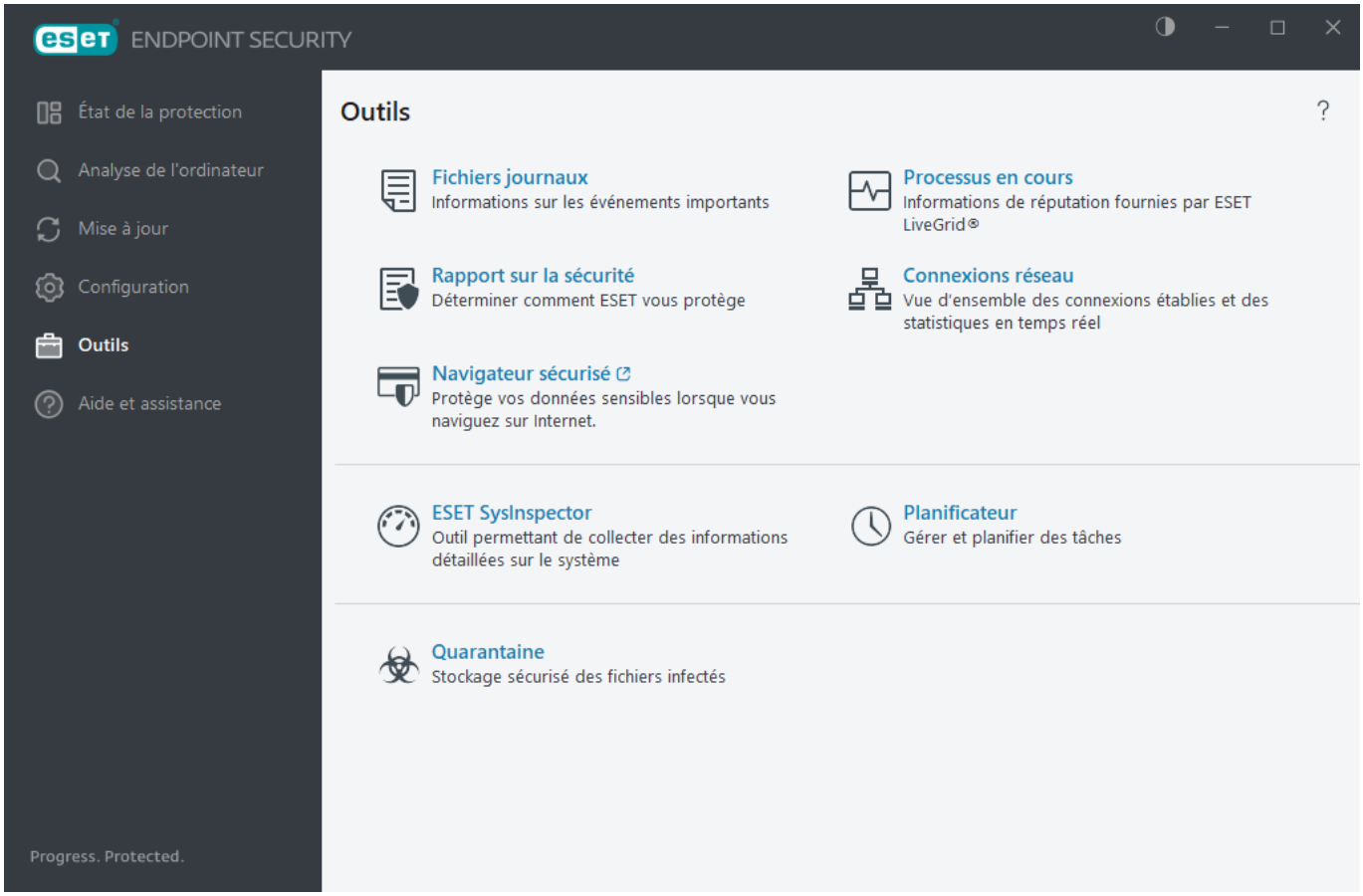
Vous pouvez rencontrer une erreur lors de l'exportation des paramètres si vous ne disposez pas de suffisamment de droits pour écrire le fichier exporté dans le répertoire spécifié.



Outils

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

- Fichiers journaux
- Processus en cours (si ESET LiveGrid® est activé dans ESET Endpoint Security)
- Rapport sur la sécurité (pour les endpoints non administrés)
- Connexions réseau (si le pare-feu est activé dans ESET Endpoint Security)
- ESET SysInspector
- Planificateur
- Soumettre un échantillon pour analyse – Permet de soumettre un fichier suspect pour analyse au laboratoire d'ESET (cette option peut ne pas être disponible selon la configuration d'ESET LiveGrid®).
- Quarantaine



Fichiers journaux

Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées. 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. Vous pouvez consulter les messages texte et les journaux directement à partir de l'environnement ESET Endpoint Security. Il est aussi possible d'archiver les fichiers journaux.

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

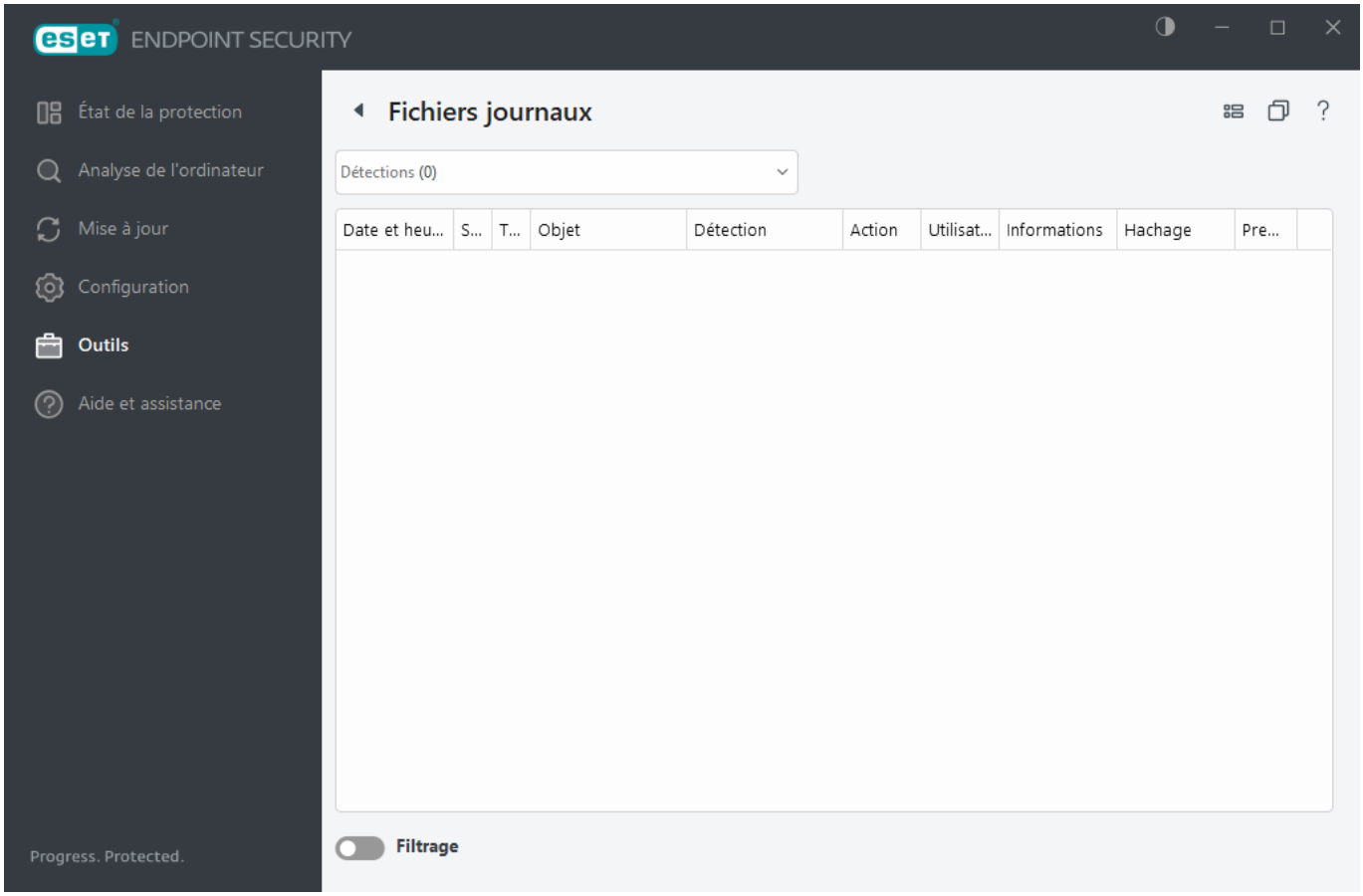
- **Détections** – Ce journal contient des informations sur les détections et infiltrations détectées par les modules de ESET Endpoint Security. Ces informations comprennent l'heure de détection, le nom de la détection, l'emplacement, l'action exécutée et le nom de l'utilisateur connecté au moment où 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 Security sont enregistrées dans le journal des événements. Le journal des événements contient des informations sur les événements qui se sont produits dans le programme. Il permet aux administrateurs système et aux utilisateurs de résoudre des problèmes. Les informations qu'il contient peuvent aider à trouver une solution à un problème qui s'est produit dans le programme.
- **Analyse de l'ordinateur** – Tous les résultats des analyses sont affichés dans cette fenêtre. Chaque ligne

correspond à un seul contrôle d'ordinateur. Double-cliquez sur une entrée pour afficher les détails de l'analyse correspondante.

- **Fichiers bloqués** – Contient les entrées des fichiers bloqués qui n'étaient pas accessibles lors de la connexion à ESET Enterprise Inspector. 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. Pour plus d'informations, consultez leguide de l'utilisateur en ligne de ESET Enterprise Inspector.
- **Fichiers envoyés** – Contient les entrées des fichiers qui ont été envoyés à ESET LiveGrid® ou ESET LiveGuard 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.
- **Navigateur sécurisé** – Contient des enregistrements de fichiers non vérifiés/non fiables chargés dans le navigateur.
- **Protection du réseau** – Le journal du pare-feu affiche toutes les attaques distantes détectées par la protection contre les attaques réseau ou 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 la protection du réseau permet de détecter à temps les tentatives d'infiltration du système et d'éviter tout accès non autorisé à votre système. Pour plus d'informations sur les attaques réseau, consultez Options IDS avancées.

- **Sites Web filtrés** – Cette liste est utile si vous souhaitez afficher la liste des sites web bloqués par la protection de l'accès web ou le contrôle web. Ces journaux permettent de voir l'heure, l'URL, l'utilisateur et l'application ayant ouvert une connexion au site Web en question.

- **Antispam des clients de messagerie** – Contient des entrées relatives aux messages marqués comme spam.
- **Contrôle Web** – Affiche les adresses URL bloquées ou autorisées et les détails sur leurs catégories. La colonne Action effectuée indique comment les règles de filtrage ont été appliquées.
- **Contrôle de périphérique** : contient des enregistrements des supports amovibles ou périphériques qui ont été connectés à l'ordinateur. Seuls les périphériques auxquels correspond une règle de contrôle de périphérique seront enregistrés dans le fichier journal. Si la règle ne correspond pas à un périphérique connecté, aucune entrée de journal ne sera créée pour un périphérique connecté. Des détails figurent également tels que le type de périphérique, le numéro de série, le nom du 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** – Après avoir cliqué sur cette option, vous pouvez définir des critères de filtrage pour des entrées de journal spécifiques dans la fenêtre Filtrage des journaux.
- **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.
- **Copier la cellule** – Copie le contenu de la cellule sur laquelle vous avez cliqué avec le bouton droit.
- **Supprimer/Supprimer tout** – Supprime les entrées sélectionnées ou toutes les entrées affichées. Vous devez disposer des privilèges d'administrateur pour effectuer cette action.
- **Exporter** – 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, vous pouvez définir des critères de filtrage pour sélectionner l'entrée spécifique à l'aide de la fenêtre Filtrage des journaux.
- **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.

Journal de vérification

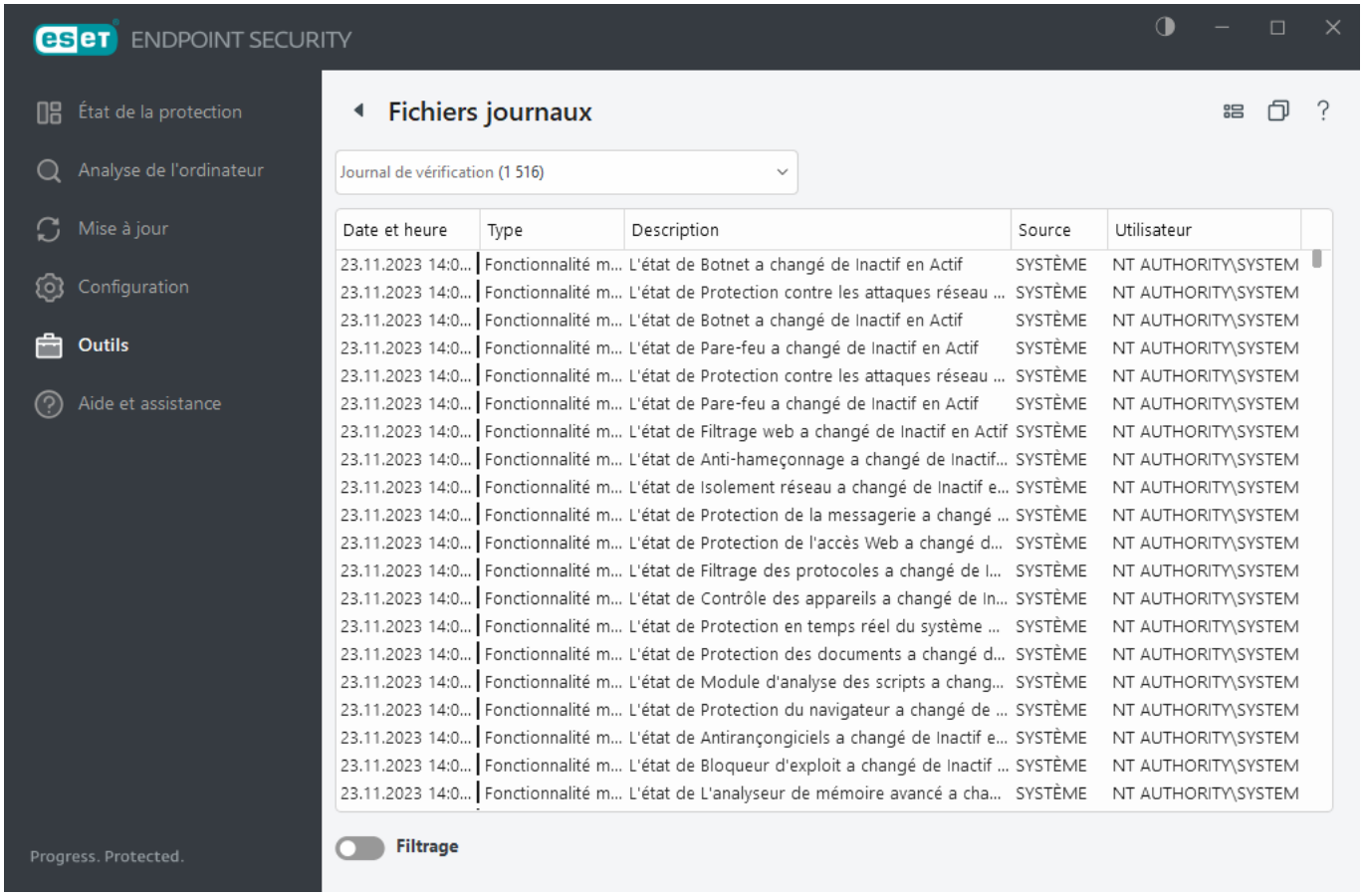
Un environnement d'entreprise comprend généralement plusieurs utilisateurs avec des droits d'accès définis pour la configuration des endpoints. Comme la modification de la configuration du produit peut avoir une incidence considérable sur le fonctionnement de celui-ci, il est essentiel que les administrateurs 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 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.



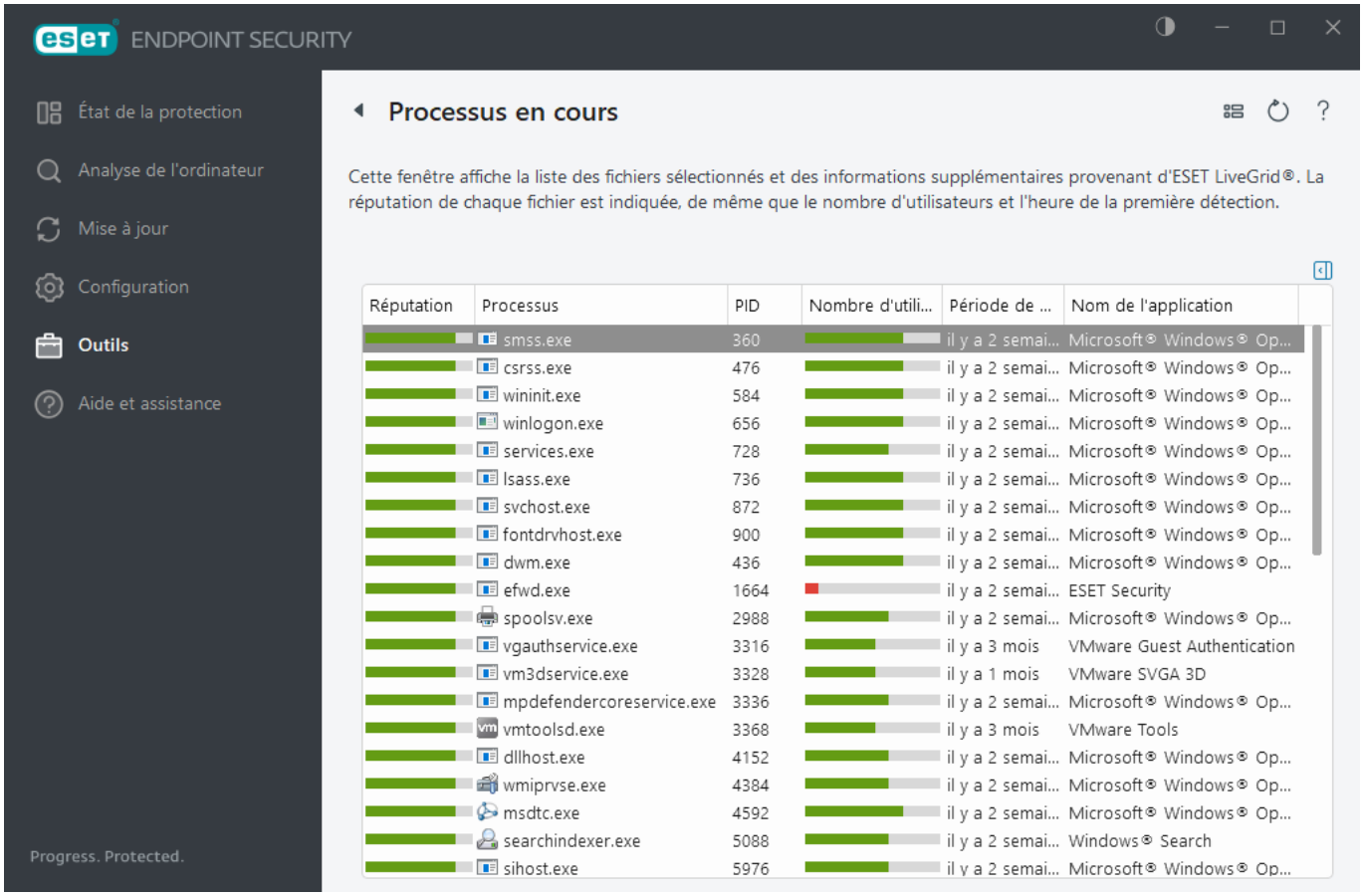
Cliquez avec le bouton droit sur un des **Paramètres modifiés** du journal d'audit dans la fenêtre Fichiers journaux, puis sélectionnez **Afficher les modifications** dans le menu contextuel pour afficher des informations détaillées sur la modification apportée. Vous pouvez en outre restaurer la modification de la configuration en cliquant sur **Restaurer** dans le menu contextuel (non disponible pour un produit géré par ESET PROTECT On-Prem). 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.

Processus en cours

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



Réputation : dans la majorité des cas, ESET Endpoint Security 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.

> 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®.

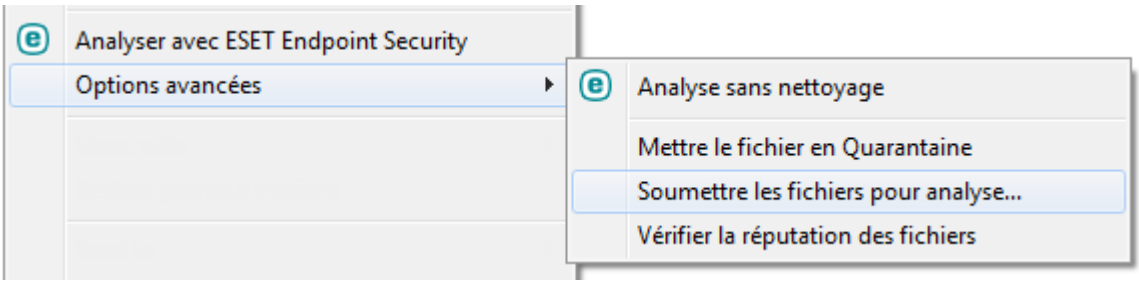
> Une application marquée avec le niveau de sécurité Inconnu (orange) n'est pas nécessairement un logiciel malveillant. Il s'agit généralement d'une nouvelle application. Vous pouvez soumettre un fichier pour analyse au laboratoire ESET si ce fichier vous semble suspect. Si le fichier s'avère être une 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.
- **Description** – Caractéristiques du fichier basées sur sa description du système d'exploitation.
- **Version** – Informations fournies par l'éditeur de l'application.
- **Société** – Nom du fournisseur ou du processus de l'application.
- **Produit** – Nom de l'application et/ou nom de l'entreprise.
- **Taille** – Taille du fichier en Ko (kilo-octets) ou Mo (méga-octets).
- **Date de création** – Date et heure de création d'une application.
- **Date de modification** – Date et heure de dernière modification d'une application.

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 d'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.
- **Pages Web bloquées dans le filtrage web** – Indique le nombre de pages web bloquées dans le filtrage web.
- **Application potentiellement indésirable détectée** – Indique le nombre d'applications potentiellement indésirables.
- **Courrier indésirable détecté** – Indique le nombre de courriers indésirables détectés.
- **Documents analysés** – Indique le nombre d'objets de document analysés.
- **Applications analysées** – Indique le nombre d'objets exécutables analysés.
- **Autres objets analysés** – Indique le nombre d'autres objets analysés.
- **Objets des pages Web analysés** – Indique le nombre d'objets de pages Web analysés.
- **Objets des e-mails analysés** – Indique le nombre d'objets d'e-mail analysés.

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

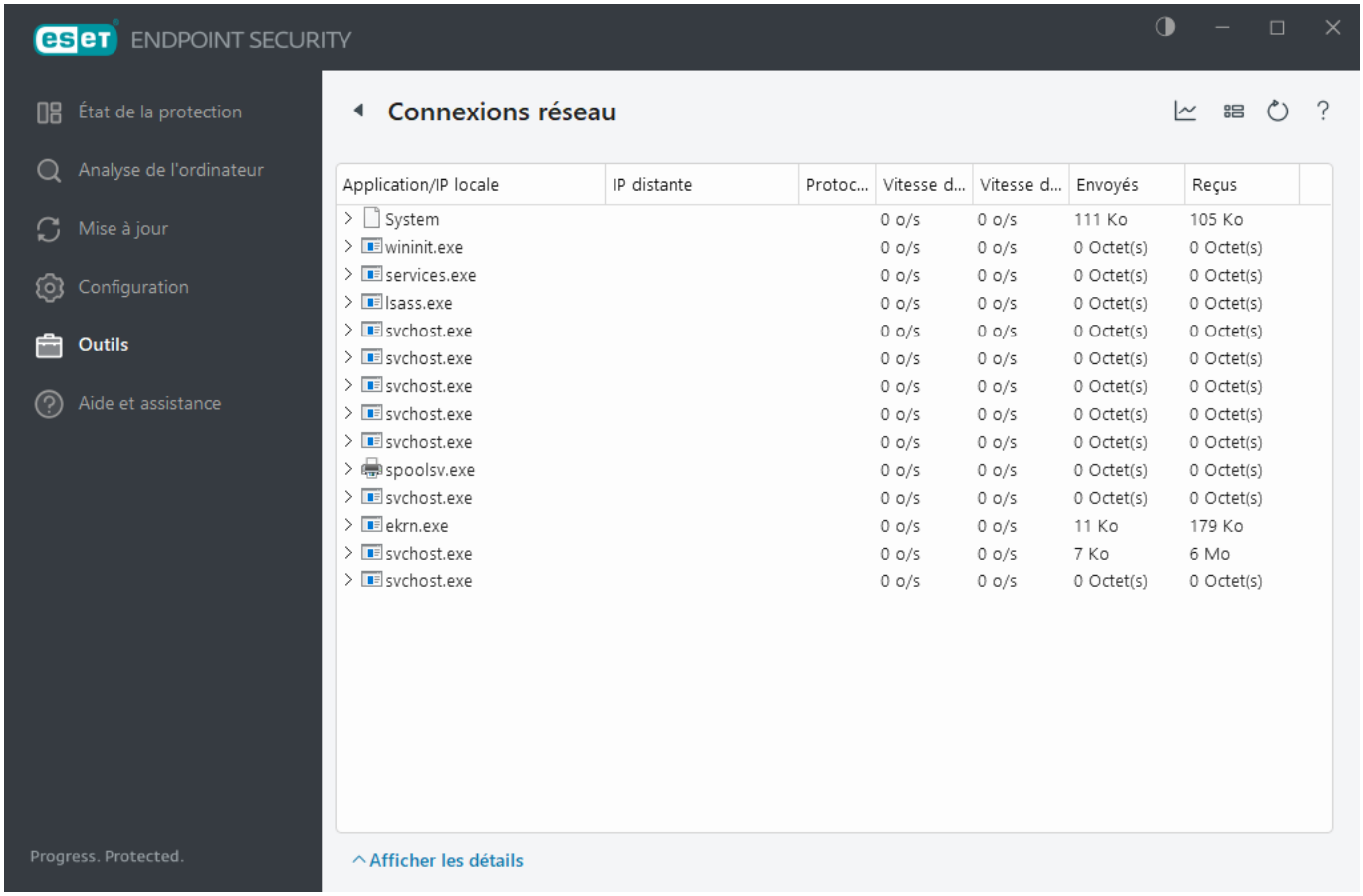
Cliquez sur l'engrenage dans le coin supérieur droit pour **activer/désactiver les notifications des rapports** ou sélectionner si les données des 30 derniers jours ou depuis l'activation du produit doivent être affichées. Si ESET

Endpoint Security est installé depuis moins de 30 jours, seul le nombre de jours depuis l'installation peut être sélectionné. La période de 30 jours est définie par défaut.

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

Connexions réseau

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



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

La première ligne affiche le nom de l'application et la vitesse de transfert de données. Pour afficher la liste des connexions établies par l'application (ainsi que des informations plus détaillées), cliquez sur **>**.

Colonnes

Application/IP locale – Nom de l'application, adresses IP locales et ports de communication.

Adresse IP distante – Adresse IP et numéro de port d'un ordinateur distant spécifique.

Protocole – Protocole de transfert utilisé.

Vitesse montante/descendante – Vitesse actuelle des données sortantes et entrantes.

Envoyé/Reçu – Quantité de données échangées sur la connexion.

Afficher les détails – Permet d'afficher les informations détaillées de la connexion sélectionnée.

Sélectionnez une application ou une adresse IP dans l'écran Connexions réseau, puis cliquez avec le bouton droit dessus pour afficher un menu contextuel dont la structure est la suivante :

Résoudre les noms – Dans la mesure du possible, toutes les adresses réseau sont affichées dans le format DNS et non dans le format d'adresse IP numérique.

Afficher uniquement les connexions TCP – Cette liste affiche uniquement les connexions appartenant à la suite du protocole TCP.

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

Afficher les connexions internes à l'ordinateur – Cette option permet de n'afficher que les connexions où le côté distant est un système local ; ces connexions sont appelées connexions hôte local.

Cliquez avec le bouton droit sur une connexion pour afficher les options supplémentaires suivantes :

Refuser la communication pour la connexion – Met fin à la connexion établie. Cette option n'est disponible que lorsque vous cliquez sur une connexion active.

Vitesse de rafraîchissement – Permet de choisir la fréquence de rafraîchissement des connexions actives.

Rafraîchir maintenant – Recharge la fenêtre des connexions réseau.

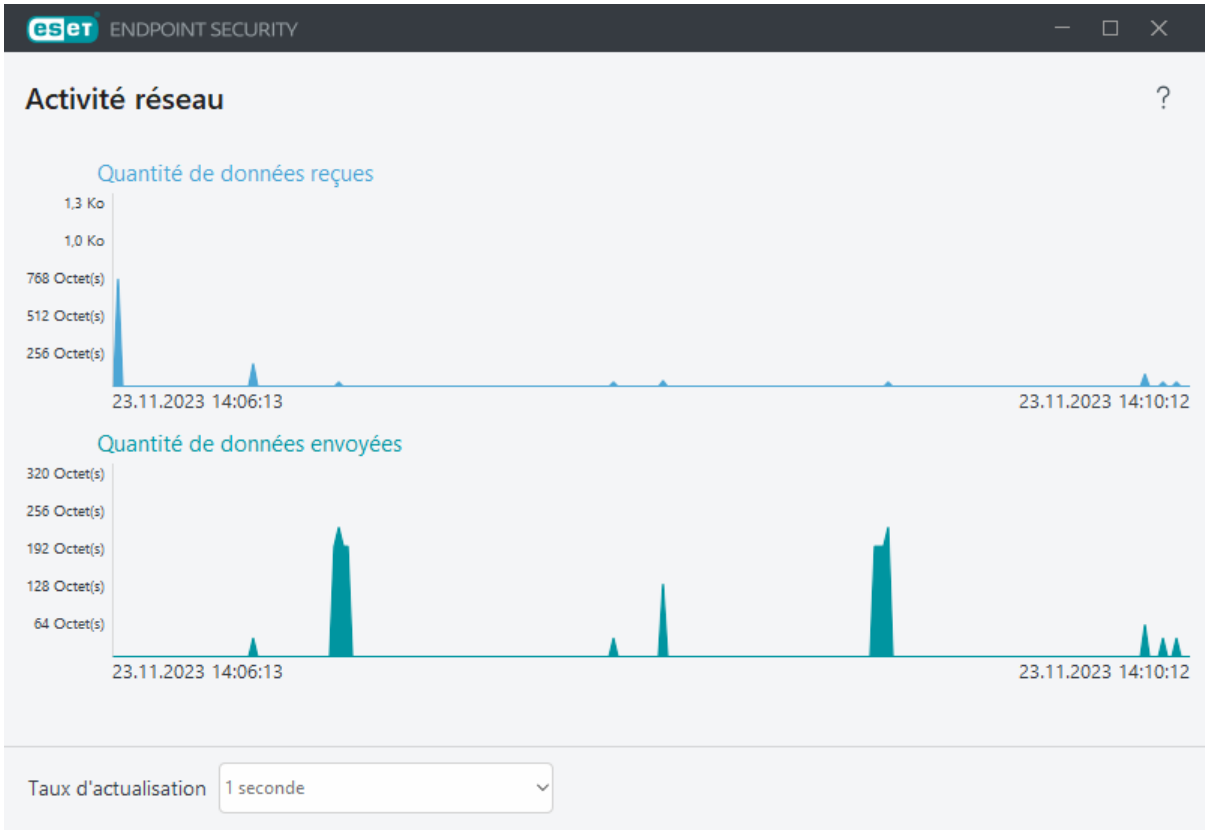
Les options suivantes ne sont disponibles que lorsque vous cliquez sur une application ou un processus, mais pas sur une connexion active :

Refuser temporairement la communication pour le processus – Rejette les connexions actuelles de l'application. Si une nouvelle connexion est établie, le pare-feu utilise une règle prédéfinie. Les paramètres sont décrits dans la section Règles de pare-feu.

Autoriser temporairement la communication pour le processus – Autorise les connexions actuelles de l'application. Si une nouvelle connexion est établie, le pare-feu utilise une règle prédéfinie. Les paramètres sont décrits dans la section Règles de pare-feu.

Activité réseau

Pour voir l'**activité réseau** actuelle sous forme graphique, cliquez sur **Outils** > **Connexions réseau**, puis sur l'icône de graphique . Au bas du graphique figure une chronologie qui enregistre en temps réel l'activité réseau sur la base de l'intervalle sélectionné. Pour modifier l'intervalle, sélectionnez la valeur adéquate dans le menu déroulant **Taux d'actualisation**.



Les options disponibles sont les suivantes :

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

L'axe vertical du graphique représente la quantité de données reçues ou envoyées. Pointez sur le graphique pour afficher la quantité exacte de données reçues/envoyées à une heure spécifique.

ESET SysInspector

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

La fenêtre ESET SysInspectoraffiche les informations suivantes sur les journaux :

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

Les actions disponibles sont les suivantes :

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

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

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

Planificateur

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

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

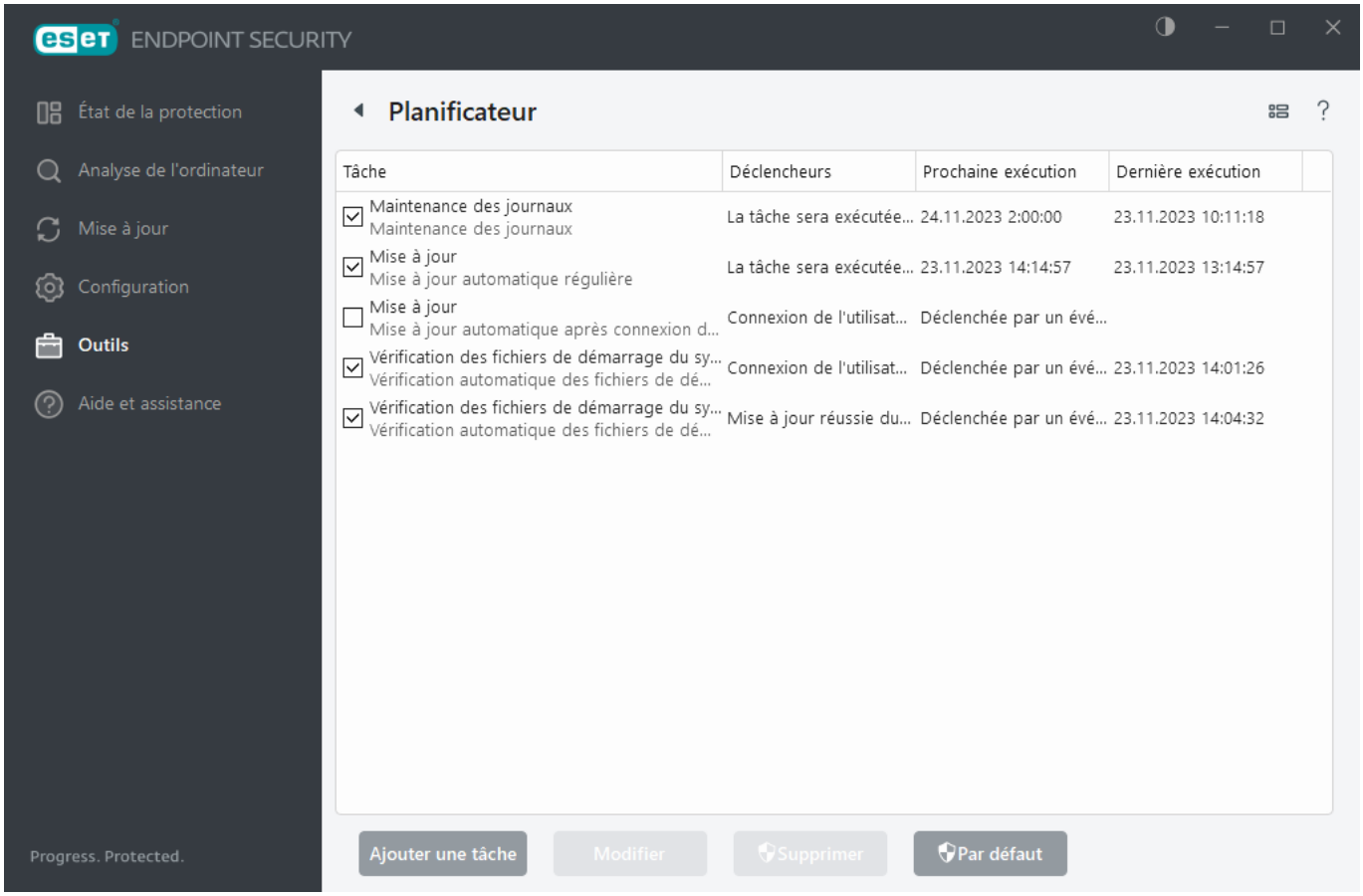
Il sert à planifier les tâches suivantes : la mise à jour du moteur de détection, l'analyse, le contrôle des fichiers de démarrage du système et la maintenance des journaux. Vous pouvez ajouter ou supprimer des tâches dans la fenêtre principale du planificateur (cliquez sur **Ajouter une tâche** ou **Supprimer** 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)

> Dans ESET PROTECT On-Prem, des délais d'exécution de tâche aléatoire peuvent être utilisés pour réduire la charge du serveur lors de l'exécution des tâches, en particulier sur les réseaux de grande envergure. Cette option permet de définir une durée au cours de laquelle une tâche doit être exécutée sur l'ensemble du réseau, plutôt que d'exécuter la tâche sur tous les postes de travail du réseau au même moment. Lorsqu'une tâche est exécutée, la valeur définie est segmentée de façon aléatoire pour allouer à chaque poste de travail du réseau une durée d'exécution unique de la tâche. Ceci permet d'éviter la surcharge des serveurs et les problèmes qui en découlent (certains serveurs peuvent par exemple signaler une attaque DoS lorsqu'une mise à jour en masse simultanée est effectuée sur tous les postes de travail du réseau).

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. Saisissez 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 avec le bouton droit dessus, puis cliquez sur **Afficher les détails des tâches**.

Options d'analyse planifiée

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

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

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

Vous pouvez définir l'exécution automatique d'une action au terme d'une analyse à l'aide du menu déroulant :

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

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

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

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

Consultez également la Progression de l'analyse.

Aperçu des tâches planifiées

Cette boîte de dialogue affiche des informations détaillées sur la tâche planifiée sélectionnée lorsque vous double-cliquez sur une tâche personnalisée ou que vous cliquez avec le bouton droit sur une tâche personnalisée du planificateur et cliquez sur **Afficher les détails des tâches**.

Détails de la tâche

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

- **Exécuter une application externe** – Permet de programmer l'exécution d'une application externe.
- **Maintenance des journaux** - Les fichiers journaux contiennent également des éléments provenant d'enregistrements supprimés. Cette tâche optimise régulièrement les entrées des fichiers journaux pour garantir leur efficacité.
- **Contrôle des fichiers de démarrage du système** – Vérifie les fichiers autorisés à s'exécuter au démarrage du système ou lors de l'ouverture de session de l'utilisateur.
- **Créer un rapport de l'état de l'ordinateur** – Crée un instantané ESET SysInspector de l'ordinateur et collecte des informations détaillées sur les composants système (pilotes, applications) et évalue le niveau de risque de chacun de ces composants.
- **Analyse de l'ordinateur à la demande** – Effectue une analyse des fichiers et des dossiers de votre ordinateur.
- **Mise à jour** – Planifie une tâche de mise à jour en mettant à jour les modules.

Planification de la tâche

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

- **Une fois** – La tâche est exécutée une fois, à la date et à l'heure prédéfinies.
- **Plusieurs fois** – La tâche est exécutée aux intervalles indiqués (en heures).
- **Quotidiennement** – La tâche est exécutée tous les jours à l'heure définie.
- **Chaque semaine** – La tâche est exécutée une ou plusieurs fois par semaine, au(x) jour(s) et à l'heure indiqués.
- **Déclenchée par un événement** – La tâche est exécutée après un événement particulier.

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

Planification de la tâche - Une fois

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

Planification de la tâche - Quotidienne

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

Planification de la tâche - Hebdomadaire

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

Planification de la tâche - Déclenchée par un événement

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

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

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

Tâche ignorée

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

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

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

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

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

• L'ordinateur sort du mode veille à 16 h 30. La première exécution ignorée de la tâche a eu lieu à 14 h 00. Deux heures et demie se sont écoulées depuis 14 h 00 ; la tâche sera donc exécutée immédiatement.

Détails de la tâche - Mise à jour

Pour mise à jour le programme à partir de deux serveurs de mise à jour, vous devez créer deux profils de mise à jour distincts. Si le premier ne permet pas de télécharger les fichiers de mise à jour, le programme bascule automatiquement vers le second. Ce procédé est notamment adapté aux portables dont la mise à jour s'effectue normalement depuis un serveur de mise à jour du réseau local, mais dont les propriétaires se connectent souvent à Internet à partir d'autres réseaux. Par conséquent, en cas d'échec du premier profil, le second télécharge automatiquement les fichiers de mise à jour à partir des serveurs de mise à jour d'ESET.

Détails de la tâche - Exécuter l'application

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

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

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

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

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

Soumission d'échantillons pour analyse

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

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, du courrier indésirable faux positif ou des sites web incorrectement classés par le module de filtrage web, 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.

> 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.

> 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.

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

Sélectionner un échantillon pour analyse - Site faux positif

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

Notes et autres informations : saisissez éventuellement d'autres informations ou une description qui faciliteront

le traitement du site web suspect.

Sélectionner un échantillon pour analyse - Autre

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

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

Quarantaine

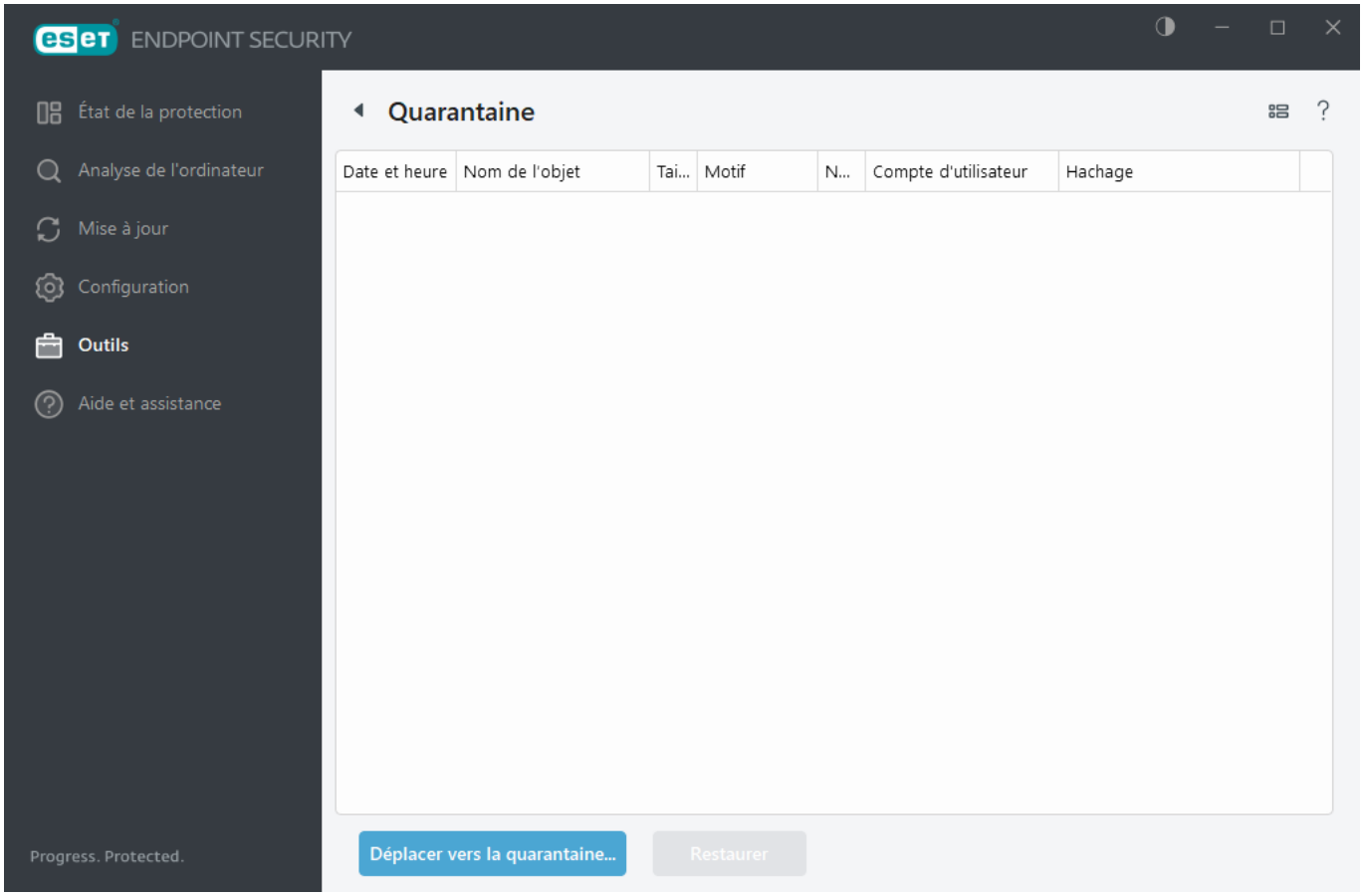
La fonction principale de la quarantaine est de stocker en toute sécurité les objets signalés (tels que les logiciels malveillants, les fichiers infectés ou les applications potentiellement indésirables).

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

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

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

Je gère à distance la quarantaine sur les postes de travail clients



Mise en quarantaine de fichiers

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

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

- ils ne peut pas être nettoyés ;
- s'il n'est pas sûr ou conseillé de les supprimer ;
- s'ils sont détectés à tort par ESET Endpoint Security ;
- si un fichier se comporte de manière suspecte, mais n'est pas détecté par le scanner.

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

- Utilisez la fonctionnalité glisser-déposer pour mettre manuellement en quarantaine un fichier ou un dossier en cliquant dessus, en déplaçant le pointeur de la souris vers la zone marquée tout en maintenant le bouton de la souris enfoncée, puis en le relâchant. L'application est ensuite placée au premier plan.
- Cliquez sur **Déplacer vers la quarantaine** dans la fenêtre principale du programme.
- Le menu contextuel peut également être utilisé à cet effet : cliquez avec le bouton droit dans la fenêtre de **Quarantaine** et sélectionnez **Mettre en quarantaine**.

Restoring from Quarantine

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

- Utilisez la fonctionnalité de **restauration** à cette fin. Celle-ci est disponible dans le menu contextuel en cliquant avec le bouton droit sur un fichier donné dans la quarantaine.

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

Suppression des éléments en quarantaine

Cliquez avec le bouton droit sur un élément donné, puis sélectionnez **Supprimer l'élément en quarantaine**. Vous pouvez également sélectionner l'élément à supprimer, puis appuyer sur **Suppr** sur votre clavier. Vous pouvez aussi sélectionner plusieurs éléments et les supprimer simultanément. Les éléments supprimés le seront définitivement de votre appareil et de la quarantaine.

Soumission de fichiers mis en quarantaine

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

Les articles suivants de la base de connaissances ESET peuvent être disponibles uniquement en anglais :
- Gérer la quarantaine dans ESET PROTECT On-Prem
- Mon produit ESET m'a signalé une détection. Que dois-je faire ?

Aide et assistance

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

Produit installé

- À propos d'ESET Endpoint Security – Affiche des informations sur votre copie d'ESET Endpoint Security.
- Résolution des problèmes liés aux produits : cliquez sur ce lien pour trouver des solutions aux problèmes les plus fréquents.
- Résolution des problèmes liés aux licences : cliquez sur ce lien pour trouver des solutions aux problèmes liés à l'activation ou au changement de licence.
- Changer de licence – Cliquez sur cette option pour ouvrir la fenêtre d'activation et activer votre produit.

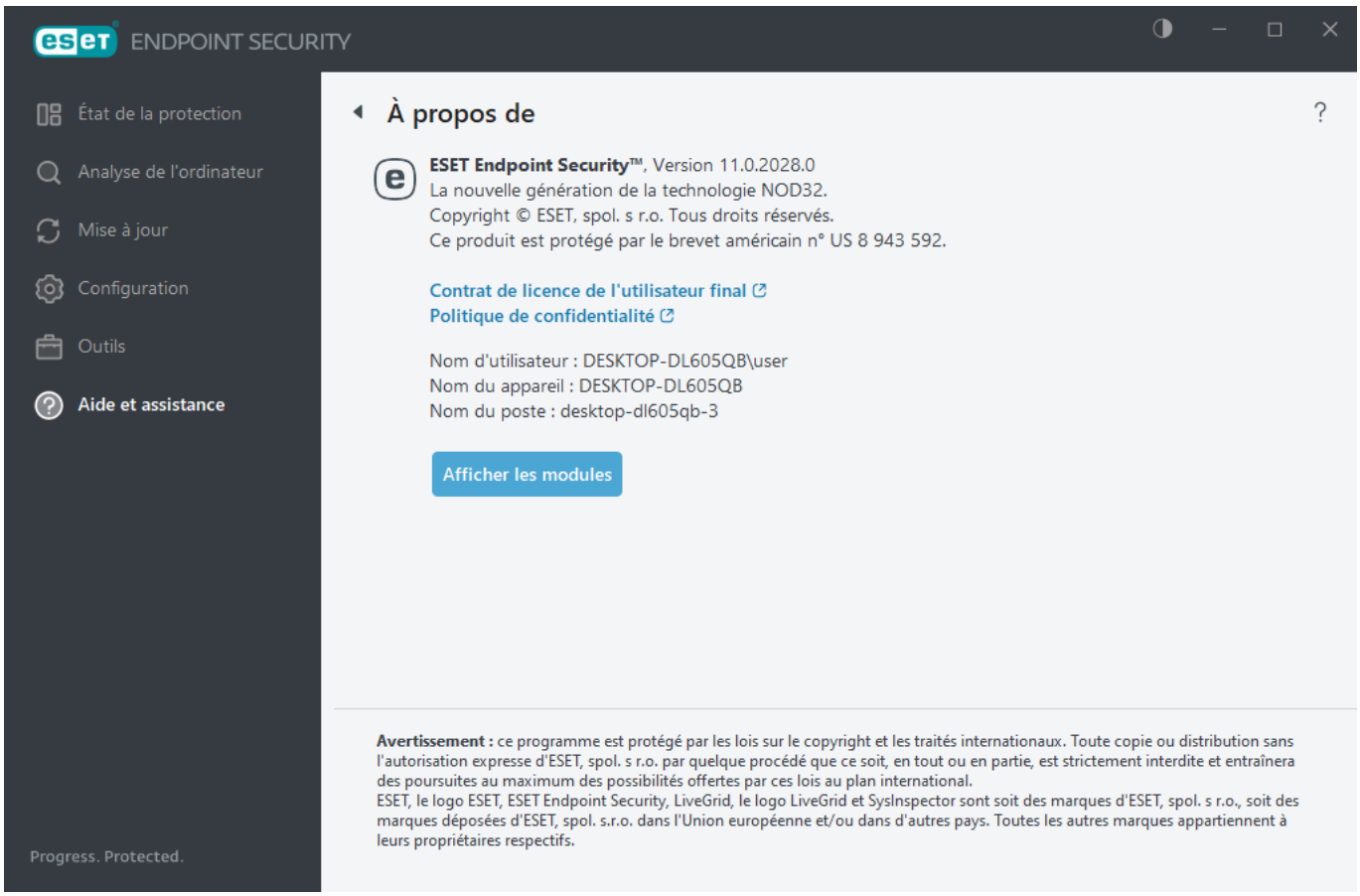
Page d'aide – Cliquez sur ce lien pour lancer les pages d'aide ESET Endpoint Security.

Assistance technique

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

À propos d'ESET Endpoint Security

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



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

- Vous pouvez copier les informations sur les modules dans le Presse-papiers en cliquant sur **Copier**. Ce procédé peut être utile pour la résolution des problèmes ou lorsque vous contactez l'assistance technique.
- Cliquez sur **Moteur de détection** dans la fenêtre Modules pour ouvrir ESET Virus radar, qui contient des informations sur chaque version du moteur de détection ESET.

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 Security, sur le système et les processus en cours (fichier journal ESET SysInspector), ainsi que les données du Registre. ESET utilise ces données uniquement pour fournir une assistance technique au client.

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

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

Diagnostics > Assistance technique.

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

Assistance technique

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

Contacter l'assistance technique

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

Obtenir des informations pour l'assistance technique

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

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

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

Configuration avancée

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

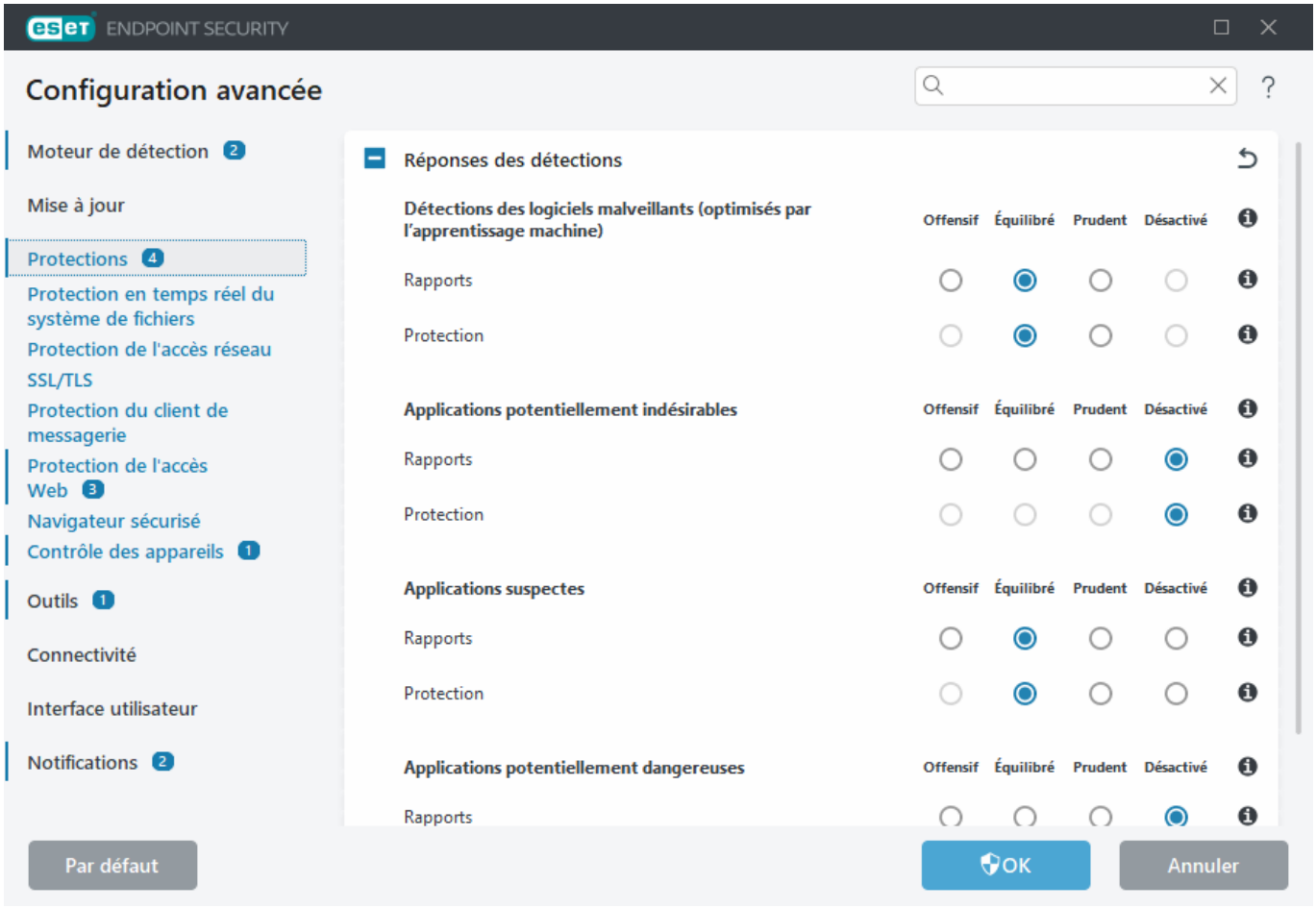
Pour ouvrir Configurations avancées, ouvrez la fenêtre principale du programme et appuyez sur la touche **F5** de votre clavier ou cliquez sur **Configuration** > **Configurations avancées**.

Lors de la création d'une stratégie à partir d'ESET PROTECT On-Prem 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'ESET PROTECT On-Prem.

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

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

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



Moteur de détection

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

- Exclusions
- Options avancées

- Analyseur du trafic réseau

Exclusions

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

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

Les exclusions de détection permettent d'exclure des objets du 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.

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

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

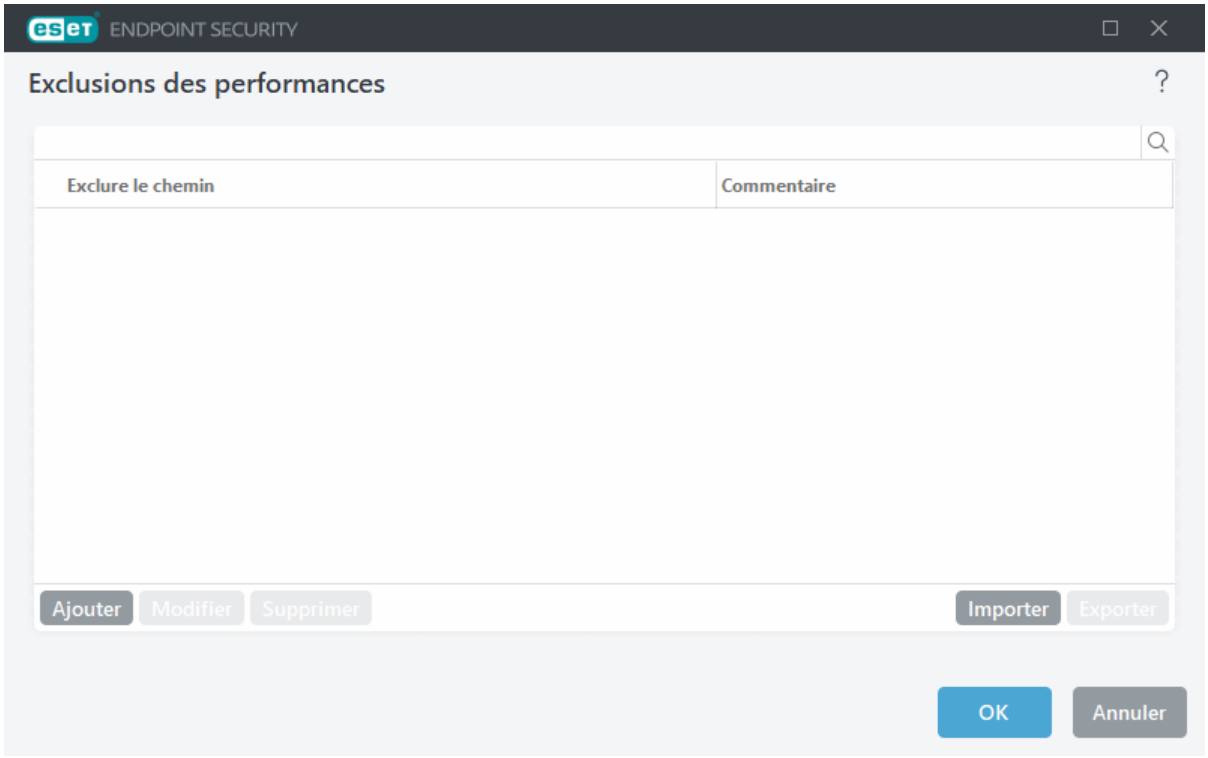
Exclusions des performances

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

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

Vous pouvez ajouter dans la liste des exclusions des fichiers et des dossiers à exclure de l'analyse via Configuration avancée > **Moteur de détection** > **Exclusions** > **Exclusions des performances** > **Modifier**.

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



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

Éléments de commande

- **Ajouter** – 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.

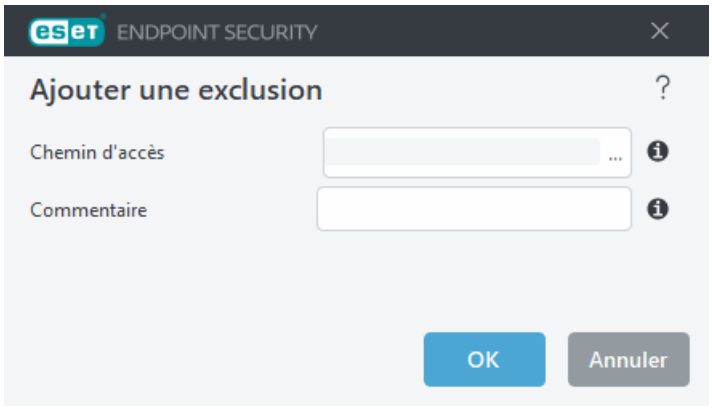
  Exemple du format de fichier d'importation/exportation

```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.PerformanceExclusions","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.

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.

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

Exemples :

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

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.

L'utilisation de caractères génériques au milieu d'un chemin (*C:\Tools*\Data\file.dat*, par exemple) peut fonctionner mais n'est pas officiellement prise en charge pour les exclusions de performances. 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 (comme pour les règles du pare-feu qui sont exécutées du haut vers le 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.

• Si vous souhaitez exclure tous les fichiers et sous-dossiers d'un dossier, saisissez le chemin d'accès au dossier et utilisez le masque *
• Si vous ne souhaitez exclure que les fichiers doc, utilisez le masque **.doc*
• Si le nom d'un fichier exécutable comporte un certain nombre de caractères variés dont vous ne connaissez que le premier (par exemple, « D »), utilisez le format suivant :
D????.exe (Les points d'interrogation remplacent les caractères manquants/inconnus.)
Exemples :
• *C:\Tools** – Le chemin doit se terminer par une barre oblique inverse (\) et un astérisque (*) pour indiquer qu'un dossier et que tout son contenu (fichiers et sous-dossiers) seront exclus.
• *C:\Tools*.** – Même comportement que *C:\Tools**
• *C:\Tools* – Le dossier *Tools* ne sera pas exécuté. Du point de vue du scanner, *Tools* peut aussi être un nom de fichier.
• *C:\Tools*.dat* – Cette exclusion exclut les fichiers .dat du dossier *Tools*.
• *C:\Tools\sg.dat* exclut ce fichier se trouvant exactement dans ce chemin.

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**

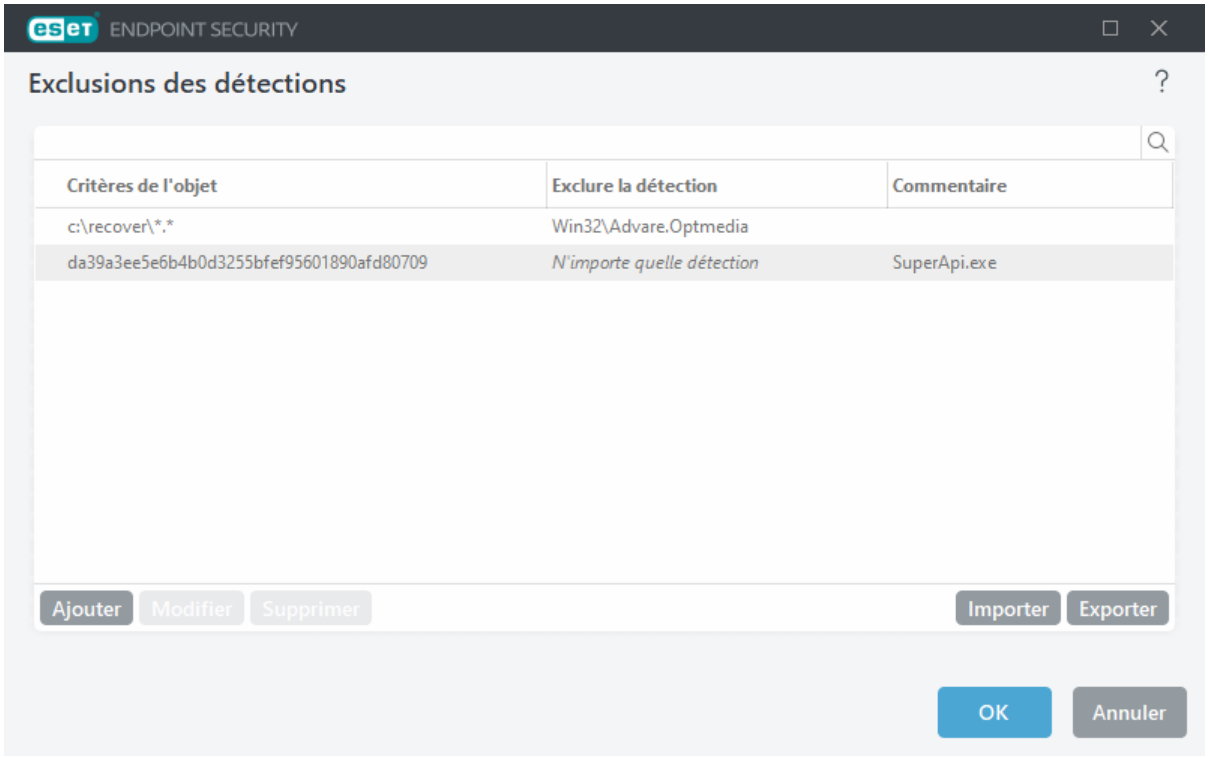
Développer la liste des variables système prises en charge

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.

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



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

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

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

Pour les applications potentiellement indésirables et les applications potentiellement dangereuses, l'exclusion par nom de détection peut être également créée :

- Dans la fenêtre d'alerte signalant la détection (cliquez sur **Afficher les options avancées**, puis sélectionnez **Exclure de la détection**).
- Dans le menu contextuel Fichiers journaux, à l'aide de l'Assistant de création d'exclusion de détection.
- En cliquant sur **Outils** > **Quarantaine** et **Restaurer et exclure de l'analyse** dans le menu contextuel.

Critères d'objet des exclusions de détection

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

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

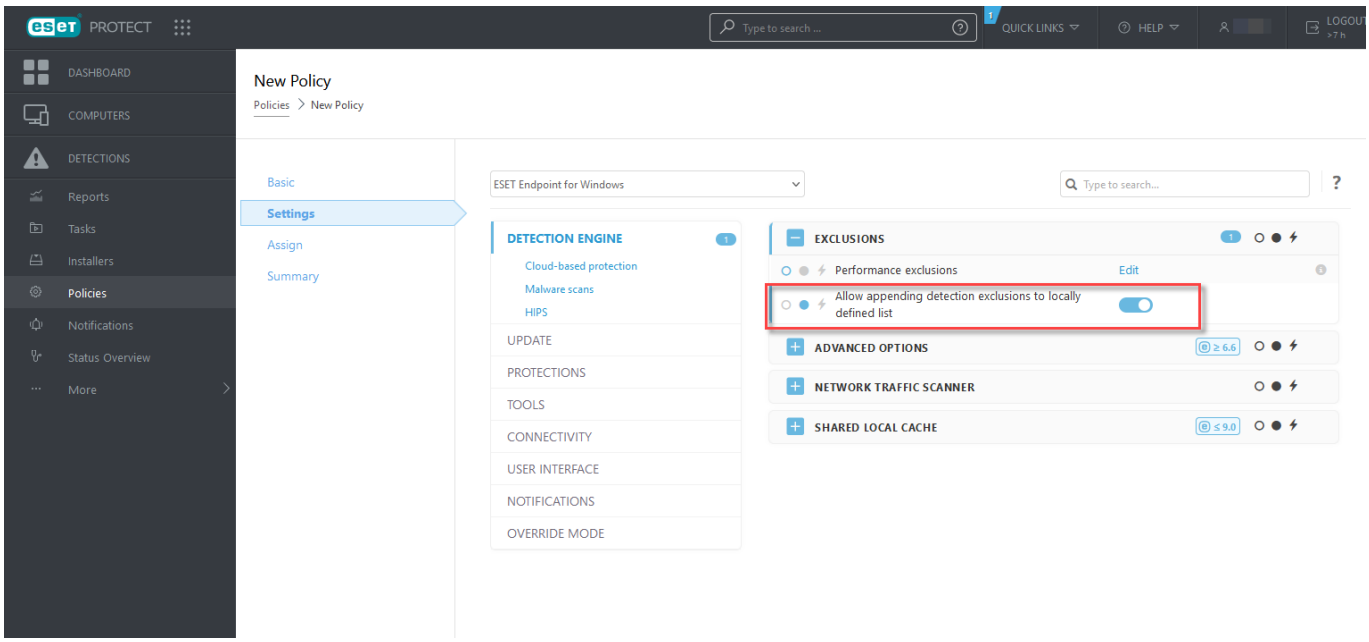
```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","File Hash"]}

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

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

Configuration des exclusions de détection dans ESET PROTECT On-Prem

Assistant pour la gestion des exclusions de détection d'ESET PROTECT On-Prem : permet de créer une exclusion de détection et de l'appliquer à d'autres ordinateurs/groupes.

Remplacement possible des exclusions de détection d'ESET PROTECT On-Prem

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'ESET PROTECT On-Prem fonctionnera comme prévu.

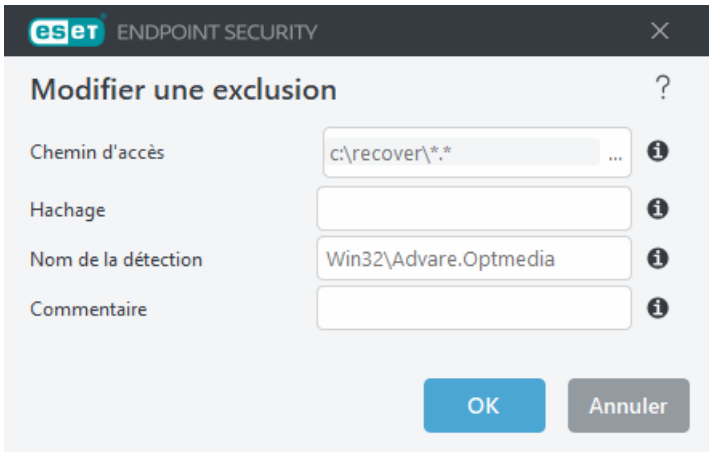


Ajout ou modification d'une exclusion de détection

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 Security. Les exclusions pour les infiltrations réelles sont très dangereuses ; envisagez d'exclure uniquement les fichiers/répertoires concernés en cliquant sur **...** dans le champ **Masque** et/ou seulement pendant une période temporaire. Les exclusions s'appliquent également aux applications potentiellement indésirables, aux applications potentiellement dangereuses et aux applications suspectes.

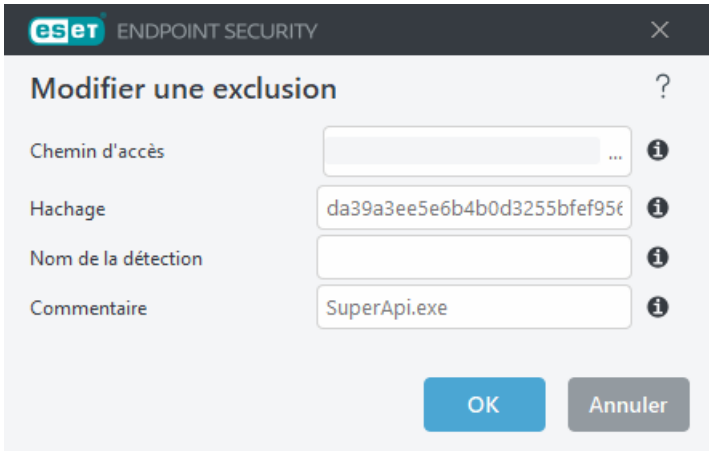
Consultez également Format d'exclusion de chemin.



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

Exclure le hachage

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



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 Security :
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Éléments de commande

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

Assistant de création d'exclusion de détection

Une exclusion de détection peut également être créée à partir du menu contextuel Fichiers journaux (non disponible pour les détections de logiciels malveillants) :

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

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

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

L'option recommandée est présélectionnée en fonction du type de détection.

Vous pouvez éventuellement ajouter un **commentaire** avant de cliquer sur **Créer une exclusion**.

Options avancées du moteur de détection

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

Analyseur du trafic réseau

L'analyseur du trafic réseau fournit une protection contre les logiciels malveillants pour les protocoles d'application, qui intègre plusieurs techniques avancées d'analyse des logiciels malveillants. Il analyse automatiquement les protocoles HTTP(S), POP3(S) et IMAP(S), quel que soit le navigateur internet ou le client de

messagerie. Vous pouvez activer/désactiver l'analyseur du trafic réseau dans Configurations avancées > **Moteur de détection** > **Analyseur du trafic réseau**.

Activer l'analyseur du trafic réseau : si vous désactivez cette option, les protocoles HTTP(S), POP3(S) et IMAP(S) ne seront pas analysés. Notez que les fonctionnalités d'ESET Endpoint Security suivantes nécessitent l'activation de l'analyseur du trafic réseau :

- Protection de l'accès Web
- Contrôle Web
- Navigateur sécurisé
- SSL/TLS
- Protection antihameçonnage
- Protection du client de messagerie

Protection dans le cloud

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

Les options disponibles sont les suivantes :

Option 1 : Activation du système de réputation ESET LiveGrid®

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

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

Option 2 : Activation du système de commentaires ESET LiveGrid®

En plus du système de réputation ESET LiveGrid®, le système de commentaires ESET LiveGrid® collecte sur votre ordinateur des informations concernant les nouvelles menaces détectées. Ces informations comprennent un échantillon ou une copie du fichier dans lequel la menace est apparue, le chemin et le nom du fichier, la date et l'heure, le processus par lequel la menace est apparue sur votre ordinateur et des informations sur le système d'exploitation de votre ordinateur.

Par défaut, ESET Endpoint Security est configuré pour soumettre les fichiers suspects au laboratoire d'ESET pour une analyse détaillée. Les fichiers ayant une extension définie (*.doc* ou *.xls* par exemple) sont toujours exclus. Vous pouvez également ajouter d'autres extensions si vous ou votre entreprise souhaitez éviter d'envoyer certains fichiers.

Option 3 : choisir de ne pas activer ESET LiveGrid®

Vous ne perdez rien de la fonctionnalité du logiciel, mais ESET Endpoint Security 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.

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 Security.

Configuration de la protection dans le cloud dans les configurations avancées

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

Activer le système de réputation ESET LiveGrid® (recommandé) – Le système de réputation ESET LiveGrid® améliore l'efficacité des solutions de protection contre les logiciels malveillants en comparant les fichiers analysés à une base de données d'éléments mis en liste blanche et noire dans le cloud.

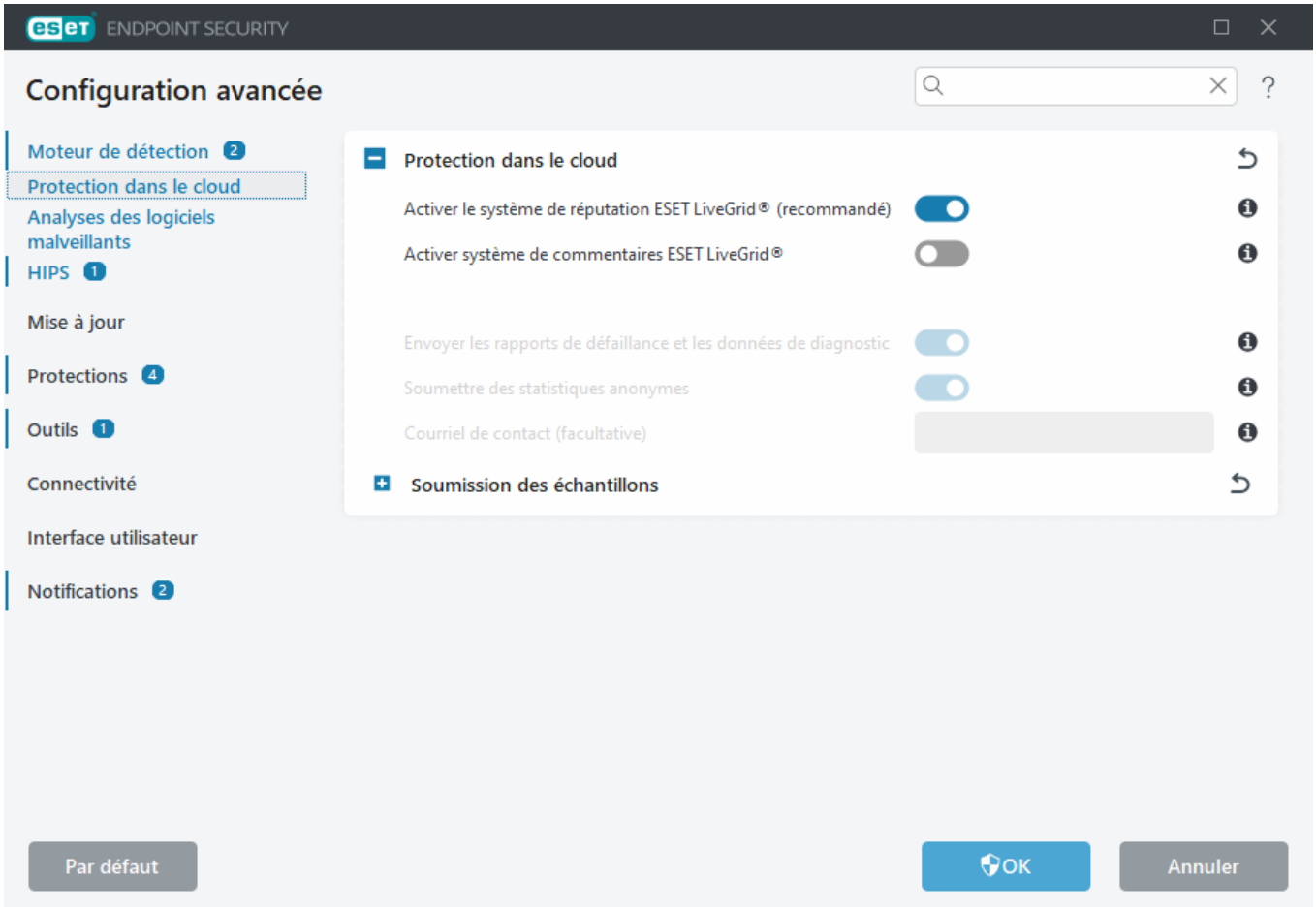
Activer le système de réputation ESET LiveGrid® – Envoie les données pertinentes de soumission (décrites dans la section **Soumission des échantillons** ci-dessous) ainsi que les rapports de défaillance et les statistiques au laboratoire de recherche ESET pour une analyse plus approfondie.

Activer ESET LiveGuard (ESET LiveGuard est une fonctionnalité supplémentaire vendue par ESET et n'est pas disponible par défaut) : ESET LiveGuard 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 manuelle des échantillons : permet de soumettre manuellement des échantillons à ESET à partir du menu contextuel Quarantaine ou Outils.

Soumission automatique des échantillons infectés

Sélectionnez quels échantillons seront soumis à ESET pour analyse afin d'améliorer les prochaines détections. Les options disponibles sont les suivantes :

- **Tous les échantillons détectés** – Tous les objets détectés par le moteur de détection (notamment les applications potentiellement indésirables lorsque cette option est activée dans les paramètres du scanner).
- **Tous les échantillons à l'exception des documents**– Tous les objets détectés à l'exception des **documents** (voir ci-dessous).
- **Ne pas envoyer** – Les objets détectés ne seront pas envoyés à ESET.

Soumission automatique des échantillons suspects

Ces échantillons seront également envoyés à ESET si le moteur de détection ne les a pas détectés. Il peut s'agir par exemple d'échantillons ayant failli ne pas être détectés ou qui semblent suspects ou dont le comportement n'est pas clair pour l'un des ESET Endpoint Security 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 fichiers/dossiers de la soumission (par exemple, il peut être utile d'exclure des fichiers qui peuvent comporter des informations confidentielles, telles que des documents ou des feuilles de calcul). Les fichiers de la liste ne seront jamais envoyés aux laboratoires d'ESET pour analyse, même s'ils contiennent un code suspect. Les fichiers les plus ordinaires sont exclus par défaut (.doc, etc.). Vous pouvez ajouter des fichiers à la liste des fichiers exclus si vous le souhaitez.

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

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

ESET LiveGuard

Pour activer le service ESET LiveGuard sur un ordinateur client à l'aide de la console web ESET PROTECT On-Prem Web Console, consultez la configuration ESET LiveGuard pour ESET Endpoint Security.

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.

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

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

Analyses des logiciels malveillants

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

Analyse à la demande

Profil sélectionné – Ensemble spécifique de paramètres utilisés par le scanner à la demande. Pour créer un profil, cliquez sur **Modifier** en regard de **Liste des profils**. Pour plus d'informations, consultez Profils d'analyse.

Après avoir sélectionné le profil d'analyse, vous pouvez configurer les options suivantes :

Cibles à analyser – Si vous souhaitez analyser une cible spécifique ou un groupe de cibles, cliquez sur **Modifier** en regard de **Cibles à analyser**, puis sélectionnez une option dans la structure (arborescence) des dossiers. Pour plus d'informations, consultez Cibles à analyser.

Analyse à la demande et réponses des détections : vous pouvez configurer des niveaux de création de rapports et de protection pour chaque profil d'analyse. Par défaut, les profils d'analyse utilisent la même configuration que celle définie dans la Protection en temps réel du système de fichiers. Désactivez le bouton bascule en regard de l'option **Utiliser les configurations de protection en temps réel** pour configurer des niveaux de rapport et de protection personnalisés. Consultez Protections pour une explication détaillée des niveaux de rapport et de protection.

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

Profils d'analyse

Il existe quatre profils d’analyse prédéfinis dans ESET Endpoint Security :

- **Analyse intelligente** : il s'agit du profil d'analyse avancée par défaut. Le profil d’analyse intelligente utilise la technologie d’optimisation intelligente qui exclut les fichiers qui ont été détectés comme étant non infectés lors d’une analyse précédente et qui n’ont pas été modifiés depuis. La durée d’analyse est ainsi réduite avec un impact minimal sur la sécurité du système.
- **Analyse par le menu contextuel** : vous pouvez lancer une analyse à la demande de n’importe quel fichier à partir du menu contextuel. Le profil d’analyse par le menu contextuel permet de définir une configuration d’analyse qui sera utilisée lorsque vous déclencherez l’analyse de cette manière.
- **Analyse approfondie** : Le profil d’analyse approfondie n’utilise pas l’optimisation intelligente par défaut. Par conséquent, aucun fichier n’est exclu de l’analyse à l’aide de ce profil.
- **Analyse de l'ordinateur** : il s’agit du profil par défaut utilisé dans l’analyse standard de l’ordinateur.

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

Pour créer un profil, ouvrez Configurations avancées > **Moteur de détection** > **Analyses des logiciels malveillants** > **Analyse à la demande** > **Liste des profils** > **Modifier**. La fenêtre **Gestionnaire de profils** dispose du menu déroulant **Profil sélectionné** contenant les profils d'analyse existants, ainsi qu'une option permettant de créer un

profil. Pour plus d'informations sur la création d'un profil d'analyse correspondant à vos besoins, reportez-vous à ThreatSense ; vous y trouverez une description de chaque paramètre de configuration de l'analyse.

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

Cibles à analyser

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

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

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

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

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

Analyse en cas d'inactivité

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

Analyse en cas d'inactivité

Activez le bouton bascule en regard de l'option **Activer l'analyse en cas d'inactivité** pour activer cette

fonctionnalité. Lorsque l'ordinateur n'est pas utilisé, une analyse silencieuse de l'ordinateur est effectuée sur tous les disques locaux.

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

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

Détection en cas d’inactivité

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

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

Détection en cas d’inactivité

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

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

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

Analyse au démarrage

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

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

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

Vérification automatique des fichiers de démarrage

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

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

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

Il existe en outre deux groupes spécifiques :

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

Les listes des fichiers à analyser sont fixées pour chaque groupe ci-dessus. Si vous choisissez une profondeur d'analyse inférieure pour les fichiers exécutés au démarrage du système, les fichiers non analysés seront analysés à l'ouverture ou à l'exécution.

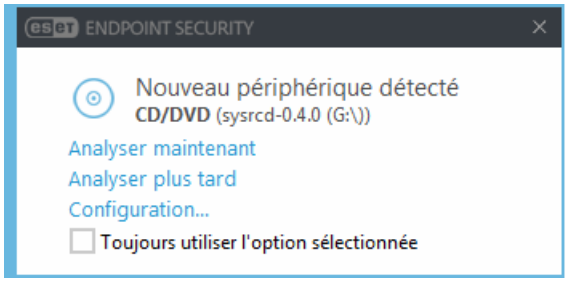
Priorité d'analyse – Niveau de priorité servant à déterminer le démarrage d'une analyse :

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

Supports amovibles

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

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



Options de cette boîte de dialogue :

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

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

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

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

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

Protection des documents

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

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

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

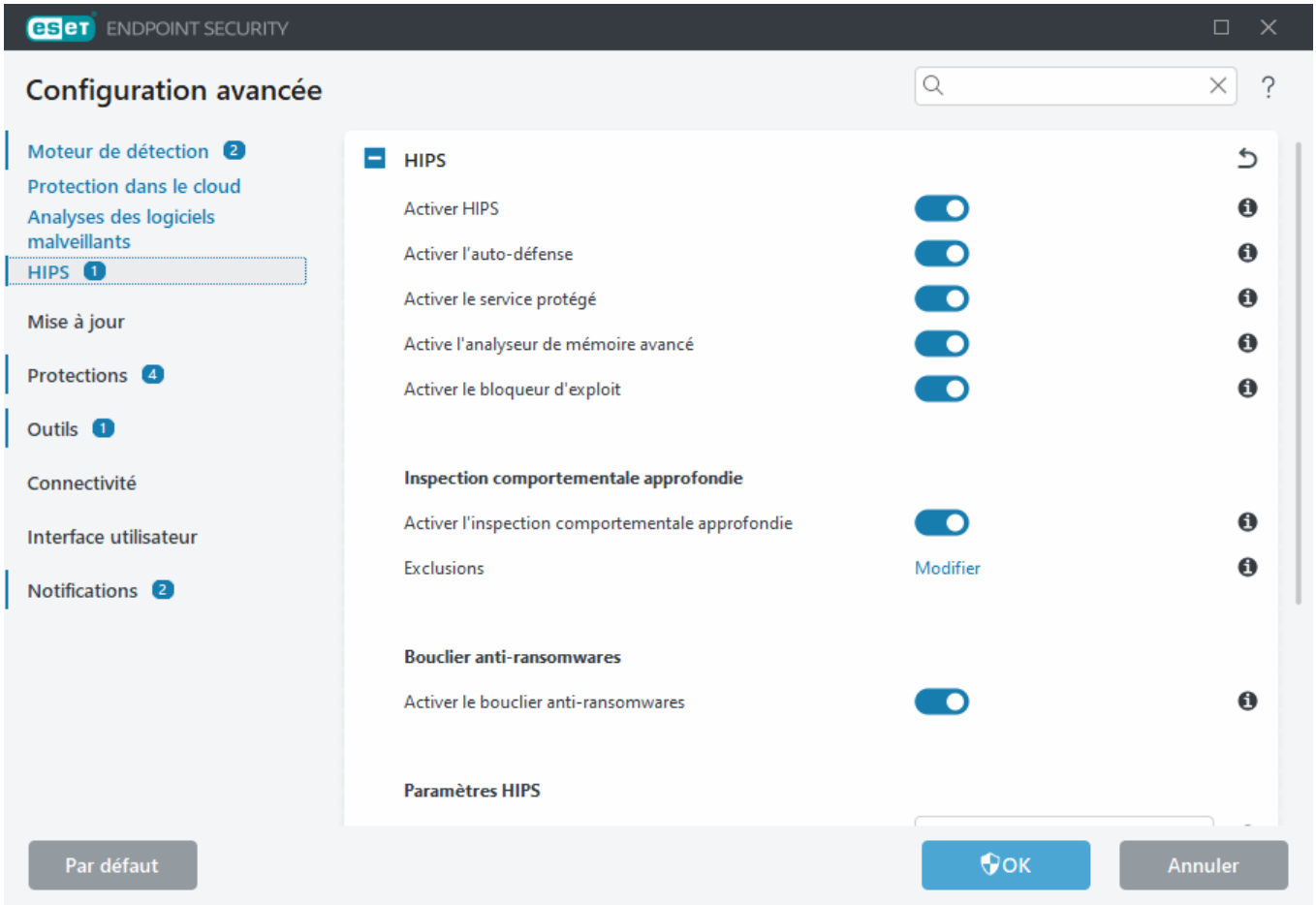
Cette fonctionnalité est activée par des applications utilisant Microsoft Antivirus API (par exemple Microsoft Office 2000 et versions ultérieures, ou Microsoft Internet Explorer 5.0 et versions ultérieures).

HIPS

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

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

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



HIPS

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

Activer l'auto-défense – ESET Endpoint Security 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 Intel® Threat Detection Technology : permet de détecter les attaques de ransomware en utilisant la télémétrie unique des processeurs Intel pour augmenter l'efficacité de la détection, réduire les alertes de faux positifs et étendre la visibilité afin de détecter les techniques d'évasion avancées. Consultez les processeurs pris en charge.

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 Security. Cette option est uniquement disponible dans ESET PROTECT On-Prem l'éditeur de configuration de politique.

Paramètres HIPS

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

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

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

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

Exclusions HIPS

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

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

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

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

Configuration avancée de HIPS

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

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

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

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

Pilotes dont le chargement est toujours autorisé

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

Ajouter – Ajoute un nouveau pilote.

Modifier – Modifie un pilote sélectionné.

Supprimer – Supprime un pilote de la liste.

Réinitialiser – Recharge un ensemble de pilotes système.

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

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

Les pilotes toujours autorisés à se charger sont spécifiques à chaque appareil et ne peuvent pas être modifiés à l'aide d'une politique ESET PROTECT On-Prem. Après l'installation, la liste des pilotes est vide. ESET Endpoint Security complète automatiquement la liste au fil du temps.

Fenêtre interactive HIPS

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

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

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

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

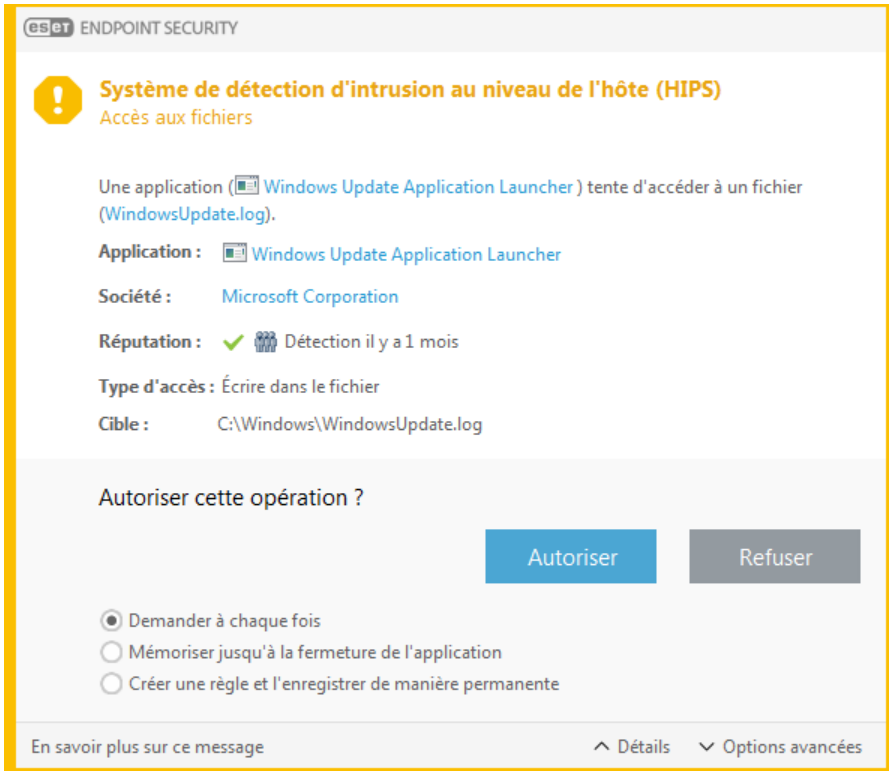
L'option **Créer une règle et l'enregistrer de manière permanente** créera une règle HIPS pouvant être modifiée ultérieurement dans la section Gestion des règles HIPS (requiert des privilèges d'administration).

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

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

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

Pour arrêter l'affichage des notifications, remplacez le mode de filtrage par **Mode automatique** dans Configuration avancée > **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**.

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.

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

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

Éléments de commande

Ajouter – Permet de créer une règle.

Modifier – Permet de modifier des entrées sélectionnées.

Supprimer – Supprime les entrées sélectionnées.

Priorité des règles HIPS

Aucune option ne permet d'ajuster le niveau de priorité des règles HIPS à l'aide des boutons haut/bas (comme pour les règles du pare-feu qui sont exécutées du haut vers le 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 le bouton bascule si vous souhaitez conserver la règle dans la liste, mais ne souhaitez pas l'appliquer.

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

Avertir l'utilisateur – Une notification apparaît dans le coin inférieur droit si un événement est déclenché.

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

Applications source – La règle est utilisée uniquement si l'événement est déclenché par cette ou ces applications. Dans le menu déroulant, sélectionnez **Applications spécifiques**, puis cliquez sur **Ajouter** pour ajouter de nouveaux fichiers. Vous pouvez également sélectionner **Toutes les applications** dans le menu déroulant pour ajouter toutes les applications.

Fichiers cibles – La règle est utilisée uniquement si l'opération est liée à cette cible. Dans le menu déroulant, sélectionnez **Fichiers spécifiques**, puis cliquez sur **Ajouter** pour ajouter de nouveaux fichiers ou dossiers. Vous pouvez également sélectionner **Tous les fichiers** dans le menu déroulant pour ajouter tous les fichiers.

Applications – La règle est utilisée uniquement si l'opération est liée à cette cible. Dans le menu déroulant, sélectionnez **Applications spécifiques**, puis cliquez sur **Ajouter** pour ajouter de nouveaux fichiers ou dossiers. Vous pouvez également sélectionner **Toutes les applications** dans le menu déroulant pour ajouter toutes les applications.

Entrées du Registre – La règle est utilisée uniquement si l'opération est liée à cette cible. Dans le menu déroulant, sélectionnez **Entrées spécifiques**, puis cliquez sur **Ajouter** pour ajouter de nouveaux fichiers ou dossiers. Vous pouvez également sélectionner **Toutes les entrées** dans le menu déroulant pour ajouter toutes les entrées.

> 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.

> Lors de la spécification d'un chemin, C:\example affecte les actions avec le dossier et C:\example*.* affecte les fichiers du dossier.

Opérations sur l'application

- **Déboguer une autre application** – Ajout d'un système de débogage au processus. Lors du débogage d'une application, de nombreux détails concernant son comportement peuvent être affichés et modifiés. Vous pouvez également accéder à ses données.
- **Intercepter les événements d'une autre application** – L'application source essaie de récupérer les événements destinés à une application spécifique (il peut s'agir par exemple d'un programme keylogger d'enregistrement des touches qui essaie de capturer les événements d'un navigateur).
- **Arrêter/Mettre en attente une autre application** – Met un processus en attente, le reprend ou l'arrête (accessible directement depuis l'explorateur des processus ou le volet des processus).
- **Démarrer une nouvelle application** – Démarrage de nouvelles applications et de nouveaux processus.
- **Modifier l'état d'une autre application** – L'application source essaie d'écrire dans la mémoire de l'application cible ou d'exécuter du code en son nom. Cette fonctionnalité peut être utile pour protéger

une application importante : vous la configurez en tant qu'application cible dans une règle qui bloque l'utilisation de cette opération.

Opérations sur le Registre

- **Modifier les paramètres de démarrage** – Toute modification apportée aux paramètres qui définissent les applications à exécuter au démarrage de Windows. Elles peuvent notamment être recherchées à l'aide de la clé Run du registre Windows.
- **Supprimer du registre** – Suppression d'une clé de registre ou de sa valeur.
- **Renommer la clé de registre** – Changement du nom des clés de registre.
- **Modifier le registre** – Création de nouvelles valeurs de clés de registre, modification de valeurs existantes, déplacement de données dans l'arborescence de base de données ou configuration des droits d'utilisateur ou de groupe pour les clés de registre.

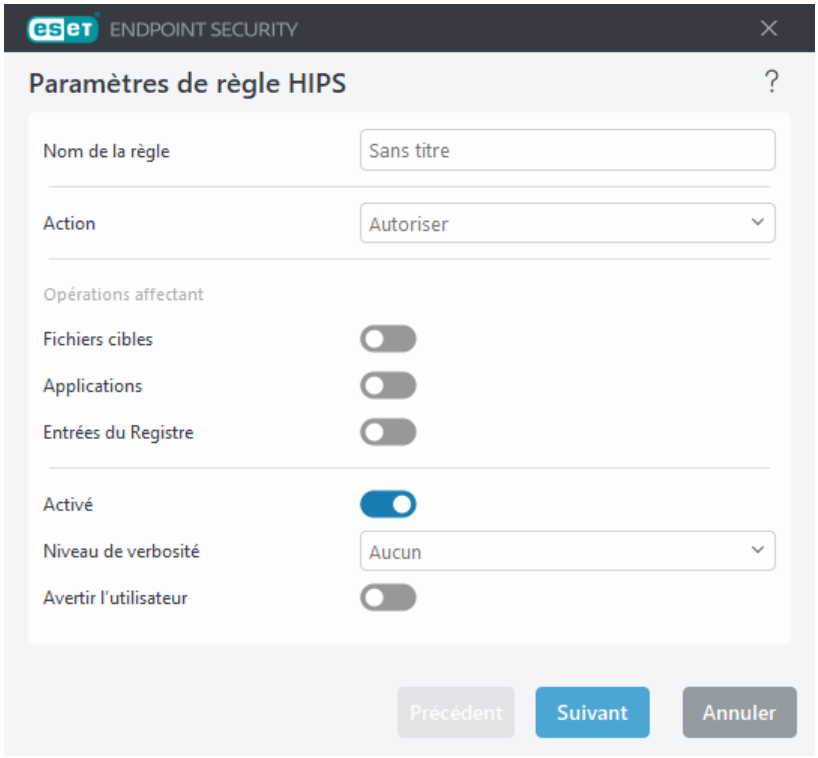
Utilisation des caractères génériques dans les règles
L'astérisque peut uniquement être utilisé dans les règles afin de remplacer une clé particulière, par exemple « HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start ». Les autres utilisations des caractères génériques ne sont pas prises en charge.

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.

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.



Ajouter le chemin de l'application/du registre pour HIPS

Sélectionnez un chemin d'application de fichier en cliquant sur l'option **...** Lors de la sélection d'un dossier, toutes les applications situées dans cet emplacement sont incluses.

L'option **Ouvrir l'Éditeur du Registre** démarrer l'éditeur du registre Windows (regedit). Lors de l'ajout d'un chemin de registre, saisissez l'emplacement correct dans le champ **Valeur**.

Exemples du chemin de fichier ou de registre :

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Mettre à jour

Les options de configuration de mise à jour sont disponibles dans Configurations avancées > **Mise à jour**. Cette section permet de spécifier les informations concernant les sources des mises à jour, telles que les serveurs de mise à jour utilisés et les données d'authentification donnant accès à ces serveurs.

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).

Mettre à jour

Le profil de mise à jour en cours d'utilisation est affiché dans le menu déroulant **Sélectionner le profil de mise à**

jour par défaut.

Pour créer un profil, consultez la section Profils de mise à jour.

Changement automatique de profil : permet de définir un profil de mise à jour pour un profil de connexion réseau spécifique.

Configurer les notifications de mise à jour – 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.

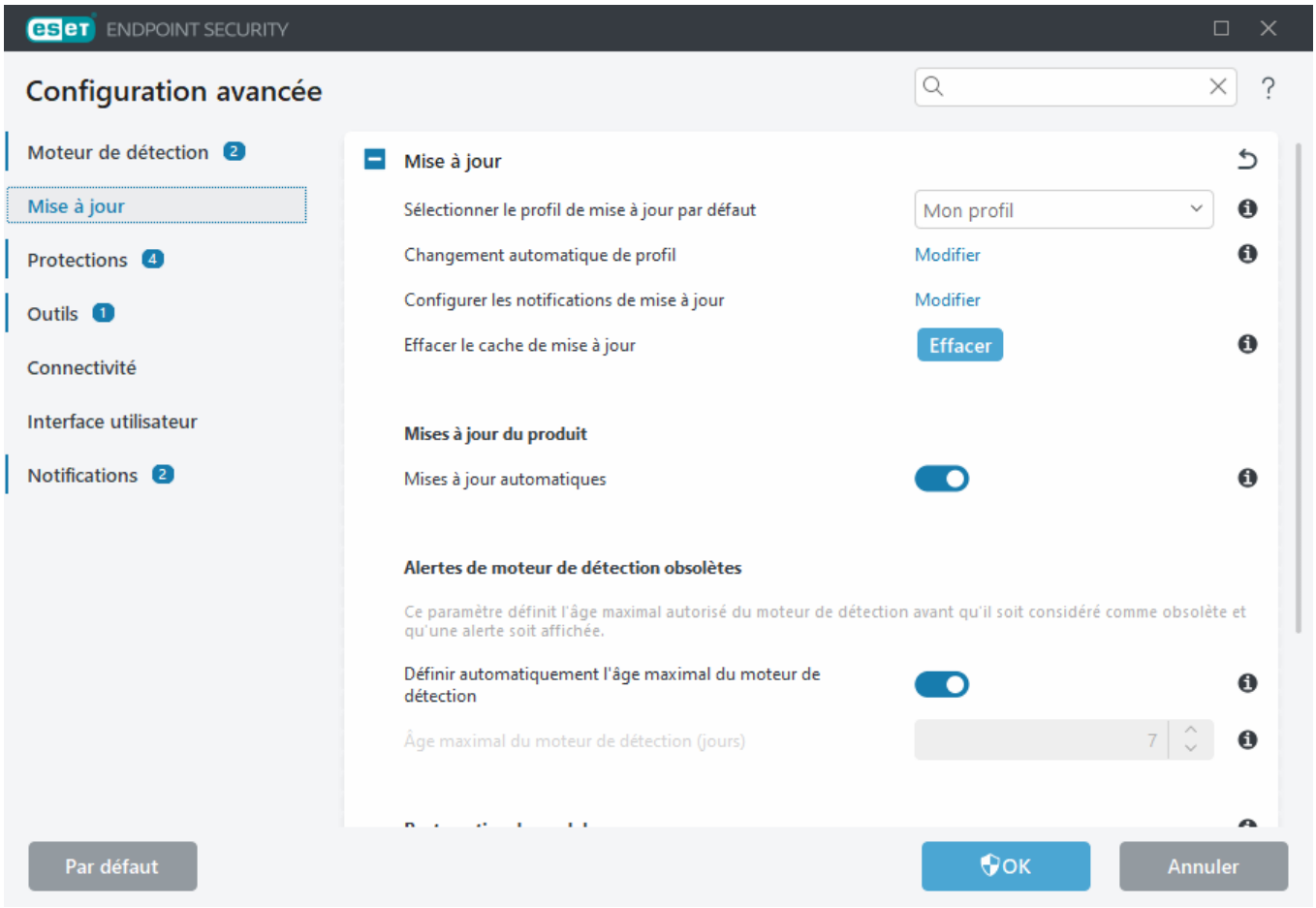
Si vous rencontrez des problèmes lors du téléchargement des mises à jour des modules, cliquez sur **Effacer** en regard de l'option **Vider le cache de mise à jour** pour supprimer les fichiers de mise à jour/le cache temporaires.

Alertes de moteur de détection obsolètes

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**.

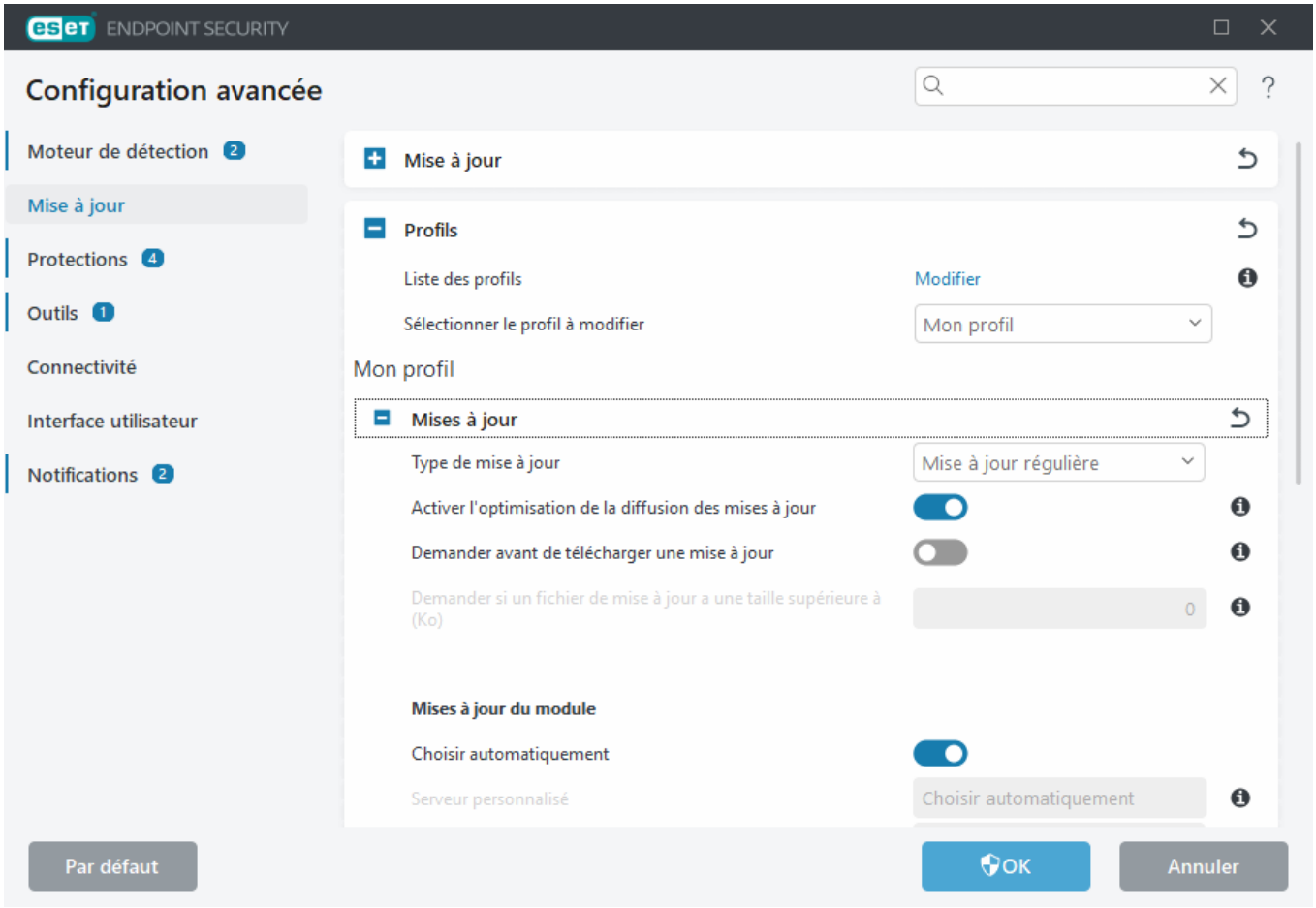
Pour créer un profil, cliquez sur **Modifier** en regard de **Liste des profils**, saisissez un nom dans **Nom du profil**, puis cliquez sur **Ajouter**.

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 appareils 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_partagé

> Le numéro de port du serveur HTTP spécifié dans les exemples ci-dessus dépend du port écouté par votre serveur HTTP/HTTPS.

Mises à jour du produit

Consultez Mises à jour du produit.

Options de connexion

Voir Options de connexion.

Miroir de mise à jour

Voir Miroir de mise à jour.

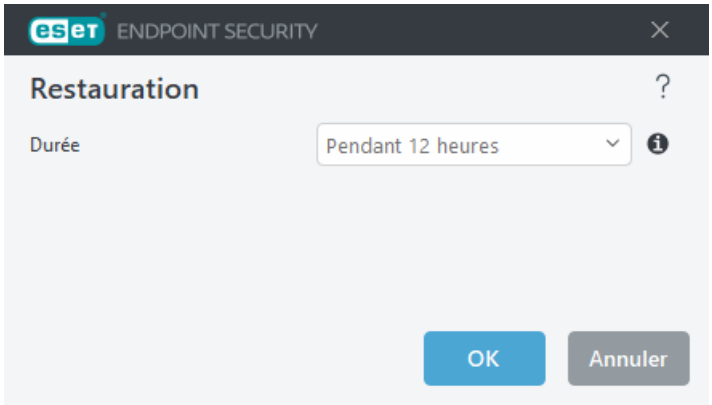
Paramètres avancés de mises à jour

Si vous pensez qu'une mise à jour du moteur de détection ou que des modules du programme sont instables ou corrompus, vous pouvez restaurer la version précédente et désactiver temporairement les mises à jour. D'un autre côté, il est aussi possible d'activer les mises à jour précédemment désactivées si vous les avez reportées pour une durée indéterminée.

ESET Endpoint Security enregistre des instantanés du moteur de détection et de modules du programme à utiliser avec la fonctionnalité de restauration. Pour créer des instantanés de la base de virus, conservez l'option **Créer des instantanés des modules** activée. Lorsque cette option est activée, le premier instantané est créé pendant la première mise à jour. Le deuxième est créé après 48 heures. Le champ **Nombre d'instantanés stockés localement** définit le nombre d'instantanés du moteur de détection stockés.

> Lorsque le nombre maximal d'instantanés est atteint (3, par exemple), l'instantané le plus ancien est remplacé par un nouveau toutes les 48 heures. ESET Endpoint Security restaure les versions des mises à jour du moteur de détection et des modules du programme en fonction de l'instantané le plus ancien.

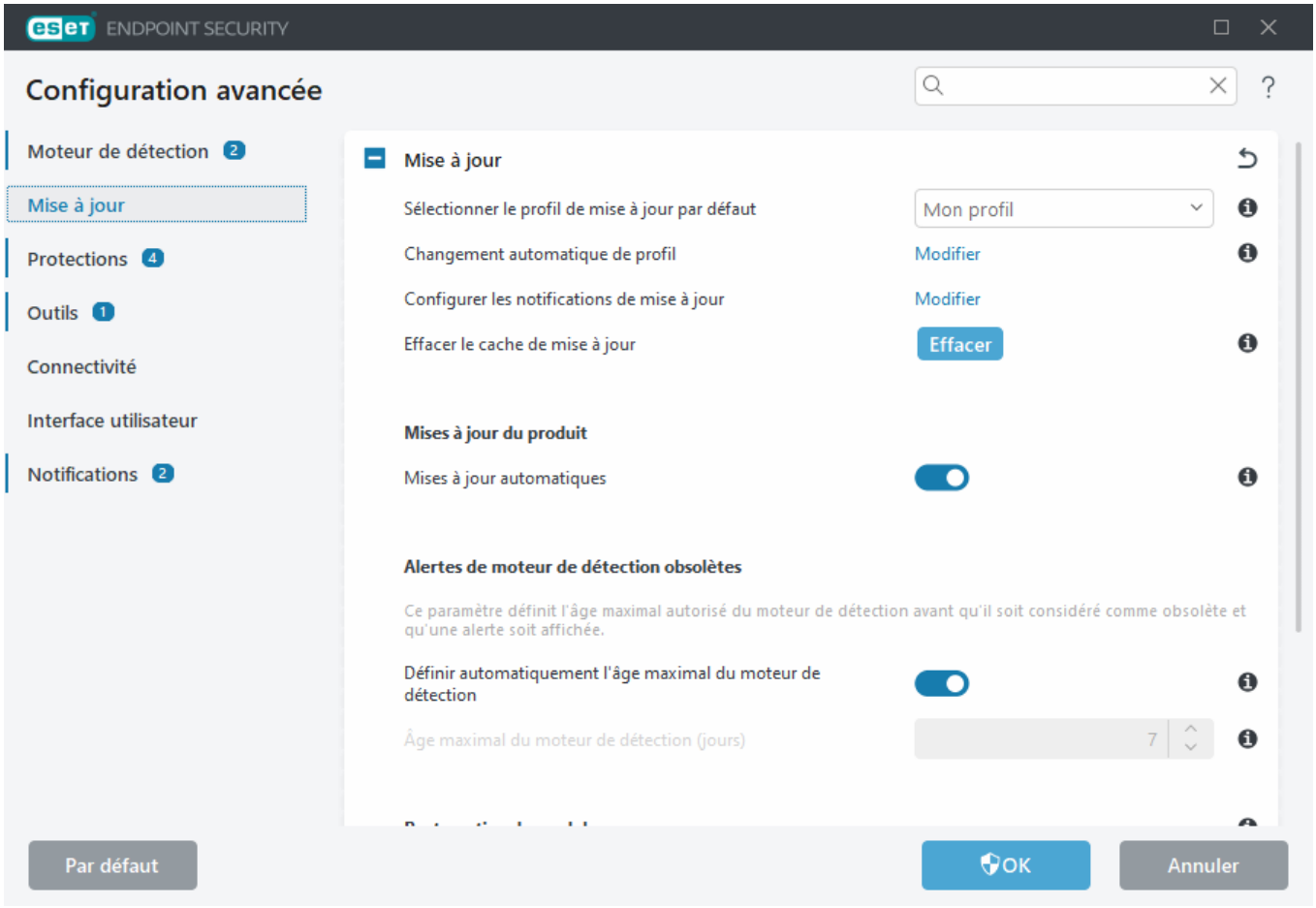
Ouvrez Configurations avancées > **Mise à jour** > **Mise à jour** > **Restauration du module** > **Restaurer** pour sélectionner un intervalle de temps dans le menu déroulant **Durée**.



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.

Si une restauration est exécutée, le bouton **Restaurer** devient **Autoriser les mises à jour**. Aucune mise à jour n'est autorisée pendant la durée sélectionnée dans le menu déroulant **Suspendre les mises à jour**. La version du moteur de détection revient à la version la plus ancienne disponible, stockée sous forme d'instantané dans le

système de fichiers de l'ordinateur local.



Supposons que le numéro 22700 correspond au numéro de version le plus récent du moteur de détection. Les moteurs de détection 22698 et 22696 sont stockés sous forme d'instantanés. Notez que le numéro 22697 n'est pas disponible. Dans cet exemple, l'ordinateur était éteint pendant la mise à jour 22697 et une mise à jour plus récente a été mise à disposition avant que la version 22697 n'ait été téléchargée. Si le champ **Nombre d'instantanés stockés localement** est défini sur 2 et que vous cliquez sur **Restaurer**, le moteur de détection (y compris les modules du programme) sera restauré à la version numéro 22696. Ce processus peut prendre un certain temps. Vérifiez si le moteur de détection est bien retourné à une version antérieure dans l'écran Mise à jour.

Mises à jour du produit

La section **Mises à jour du produit** contient des options relatives aux mises à jour du produit. Le programme vous permet de prédéfinir son comportement lorsqu'une nouvelle mise à jour du produit est disponible.

Les mises à jour du produit 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. Une fois une mise à jour du produit installée, un redémarrage de l'ordinateur peut être nécessaire.

Mises à jour automatiques : la suspension des mises à jour automatiques pour des profils de mise à jour spécifiques désactive temporairement les mises à jour automatiques du produit lorsqu'il est connecté à Internet à l'aide d'autres réseaux ou de connexions limitées. Gardez ce paramètre activé pour avoir un accès permanent aux dernières fonctionnalités et à la meilleure protection possible. Pour plus d'informations sur les mises à jour automatiques, consultez le FAQ sur les mises à jour.

Par défaut, les mises à jour du produit 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 du produit.

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

1. Définissez le chemin d'accès aux mises à jour du produit, 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 du produit à l'aide d'une mise à jour ESET Endpoint Security standard.

La sélection de l'option la plus appropriée dépend du poste de travail sur lequel les paramètres sont appliqués. 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 produit peut causer des dommages significatifs pour votre entreprise.

Options de connexion

Pour accéder aux options de configuration du serveur proxy pour un profil de mise à jour spécifique, ouvrez Configurations avancées > **Mise à jour** > **Profils** > **Mises à jour** > **Options de connexion**.

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 la configuration de serveur proxy déjà spécifiée dans Configurations avancées > **Connectivité** > **Serveur proxy**.

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

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 Security. 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 Security se connecte à un serveur proxy pour les mises à jour.
- Votre ordinateur est connecté à Internet par l'intermédiaire d'un serveur proxy. Les paramètres sont pris dans navigateur 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.

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

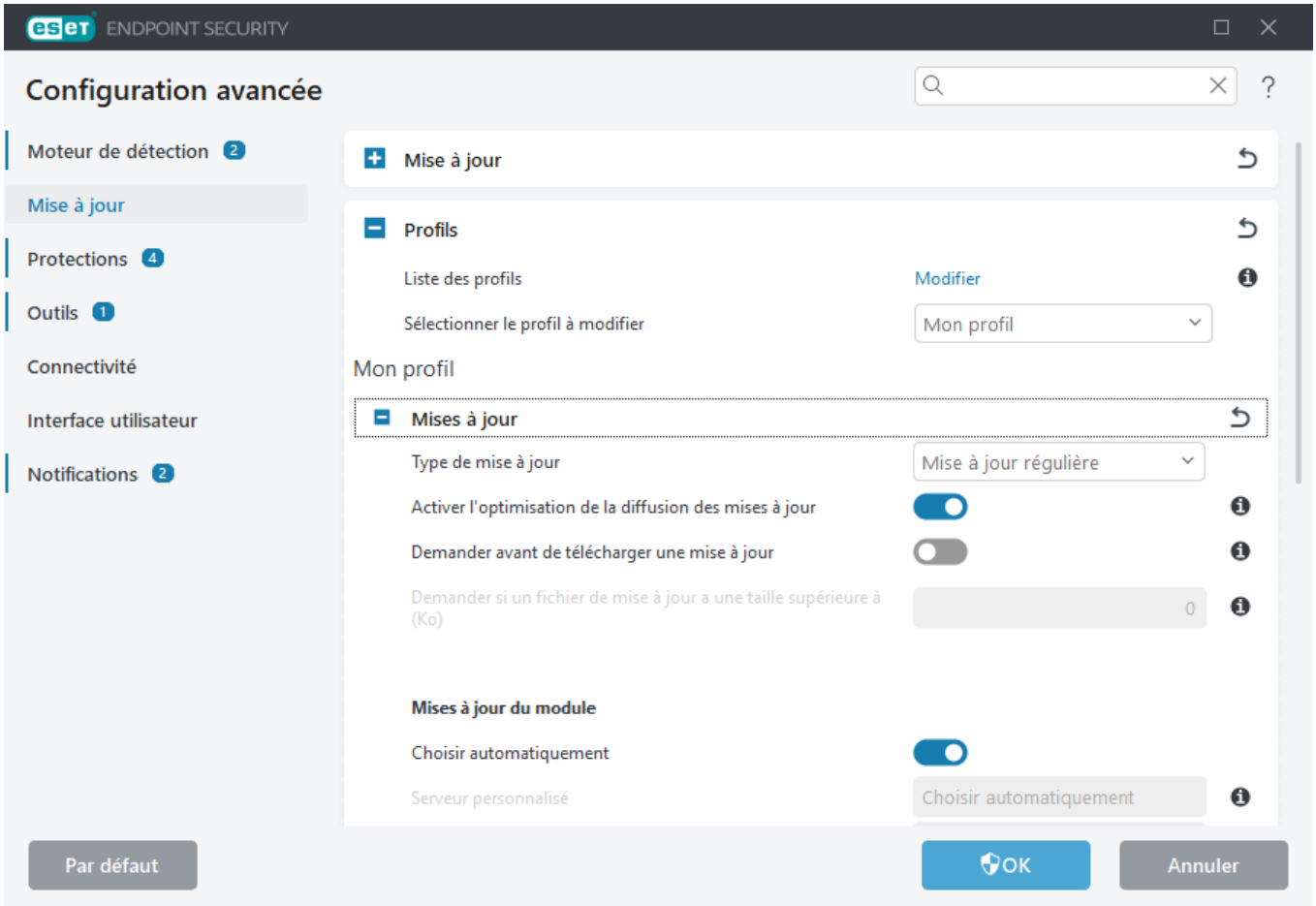
ESET Endpoint Security permet de créer des copies des fichiers de mises à jour afin de les utiliser pour la mise à jour d'autres postes de travail du réseau. L'utilisation d'un miroir, copie des fichiers de mise à jour dans l'environnement du réseau local, s'avère pratique puisque les fichiers de mise à jour doivent être téléchargés du serveur de mise à jour du fournisseur de manière répétée, pour toutes les stations de travail. Les mises à jour sont

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

Le miroir de mise à jour crée des copies des fichiers de mise à jour qui peuvent être utilisées pour mettre à jour les postes de travail qui exécutent la même génération du produit ESET Endpoint Security pour Windows. (Par exemple, ESET Endpoint Security pour Windows version 10.x crée des fichiers de mise à jour uniquement pour la version 10.x d'ESET Endpoint Antivirus pour Windows et ESET Endpoint Security pour Windows.)

Pour limiter le trafic Internet sur les réseaux sur lesquels ESET PROTECT On-Prem ou ESET PROTECT est utilisé pour gérer un grand nombre de clients, il est recommandé d'utiliser ESET Bridge au lieu de configurer un client en tant que miroir. ESET Bridge peut être installé avec ESET PROTECT On-Prem ou ESET PROTECT à l'aide du programme d'installation tout-en-un ou en tant que composant autonome. Pour plus d'informations et pour connaître les différences entre ESET Bridge, le proxy HTTP Apache, l'outil Mirror Tool et la connectivité directe, consultez la page d'aide en ligne d'<%ESET PROTECT%>.

Les options de configuration du serveur miroir local figurent dans Configurations avancées > **Mise à jour** > **Profils** > **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 Security\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 doit être entré sous le format *Domaine/Utilisateur* ou *Workgroup/Utilisateur*. N'oubliez pas de fournir les mots de passe correspondants.

Serveur HTTP et protocole SSL pour le miroir

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**.

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.

Les données d'authentification telles que **Nom d'utilisateur** et **Mot de passe** permettent uniquement d'accéder au serveur HTTP miroir. Ne remplissez ces champs que si un nom d'utilisateur et un mot de passe sont requis.

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 fournir les fichiers de mise à jour à télécharger. Il est presque impossible de suivre les transferts de données et les identifiants de connexion à l'aide de ce protocole. L'option **Type de clé privée** est définie sur **Intégrée** par défaut (l'option **Fichier de clé privée** est donc désactivée par défaut). Cela signifie que la clé privée fait partie du fichier de chaîne de certificat sélectionné.

Certificats auto-signés pour le miroir HTTPS
Si vous utilisez un serveur miroir HTTPS, vous devez importer son certificat dans le magasin racine approuvé sur tous les ordinateurs clients. Consultez la section Installation du certificat racine approuvé dans Windows.

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.

Le miroir de mise à jour crée des copies des fichiers de mise à jour qui peuvent être utilisées pour mettre à jour les postes de travail qui exécutent la même génération du produit ESET Endpoint Security pour Windows. (Par exemple, ESET Endpoint Security pour Windows version 10.x crée des fichiers de mise à jour uniquement pour la version 10.x d'ESET Endpoint Antivirus pour Windows et ESET Endpoint Security pour Windows.)

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 de mise à jour**, 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**.

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.

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

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 à partir du miroir. Il est conseillé d'accéder à Configuration avancée > **Mise à jour** > **Profils** > **Miroir de mise à jour** 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 :

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

Accès au miroir via le partage des systèmes

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

Configurez ensuite l'accès au miroir dans l'onglet Configuration avancée > **Mise à jour** > **Profils** > **Miroir de mise à jour** en désactivant l'option **Activer le serveur HTTP**. 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 et cliquez sur **Mise à jour** > **Profils** > **Mises à jour** > **Options de connexion** > **Partages Windows** > **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 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*.

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 ESET PROTECT On-Prem 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/ep10`

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 **Mises à jour du produit** 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 du produit.

Dépannage des problèmes de miroir de mise à jour

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

fréquents qui peuvent se produire lors d'une mise à jour depuis le miroir :

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

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

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

ESET Endpoint Security 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.

Protections

Les protections vous prémunissent des attaques contre le système en contrôlant les échanges de fichiers et d'e-mails, ainsi que les communications internet. Par exemple, si un objet classé comme logiciel malveillant est détecté, la correction commence. Les protections peuvent l'éliminer en le bloquant, puis en le nettoyant, en le supprimant ou en le mettant en quarantaine.

Pour configurer en détail les protections, ouvrez Configurations avancées > **Protections**.

> ⚠ Les modifications apportées aux protections ne doivent être effectuées que par un utilisateur expérimenté. Une configuration incorrecte des paramètres peut entraîner une diminution du niveau de protection.

Dans cette section :

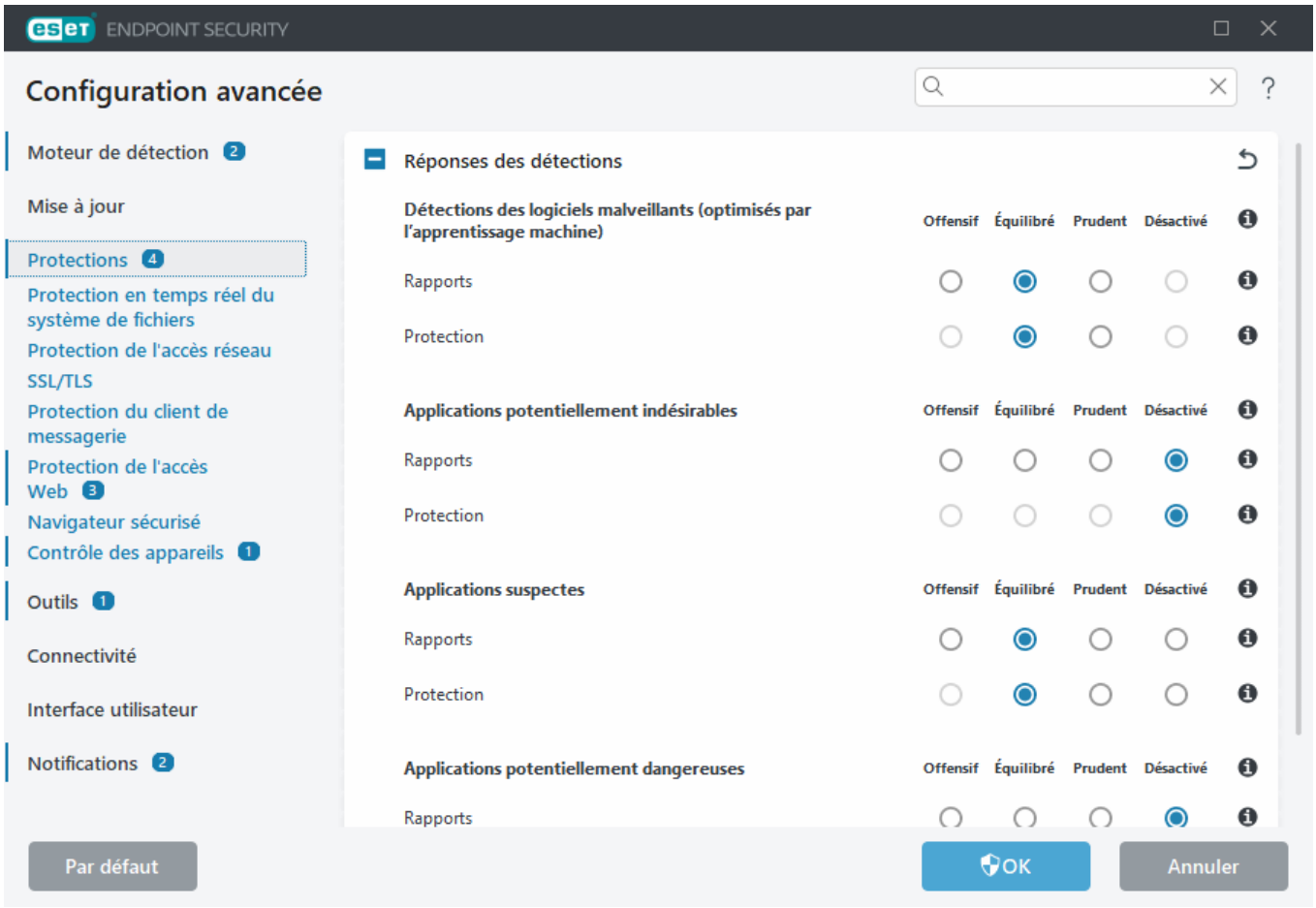
Réponses des détections

Les réponses des détections vous permettent de configurer les niveaux de rapport et de protection pour les catégories suivantes :

- **Détections des logiciels malveillants (optimisés par l'apprentissage machine)** – Un virus d'ordinateur est

un fragment de code malveillant ajouté à des fichiers qui sont sur votre ordinateur. Le terme « virus » est souvent utilisé de manière incorrecte. Le terme « logiciel malveillant »(malware, en anglais) est plus précis. La détection des logiciels malveillants est effectuée par le module du moteur de détection associé au composant d'apprentissage machine. Pour plus d'informations sur ce type de protection, reportez-vous au glossaire.

- **Applications potentiellement indésirables** : un grayware (ou application potentiellement indésirable) est un type de logiciel dont l'objectif n'est pas nécessairement malveillant, contrairement à d'autres types de logiciels malveillants comme les virus et les chevaux de Troie. Il peut toutefois installer d'autres logiciels non souhaités, modifier le comportement de l'appareil numérique, ou effectuer des activités non approuvées ou non attendues par l'utilisateur. Pour plus d'informations sur ce type de protection, reportez-vous au glossaire.
- **Les applications suspectes** comprennent des programmes compressés par des compresseurs ou des programmes de protection. Ces types de protections sont souvent exploités par des créateurs de logiciels malveillants pour contourner les détections.
- **Applications potentiellement dangereuses** : il s'agit de logiciels commerciaux légitimes susceptibles d'être utilisés à des fins malveillantes. Cette catégorie comprend les programmes d'accès à distance, les applications de décodage des mots de passe ou les keyloggers (programmes qui enregistrent chaque frappe au clavier de l'utilisateur). Pour plus d'informations sur ce type de protection, reportez-vous au glossaire.



Amélioration de la protection

L'apprentissage machine avancé fait maintenant partie des protections en tant que couche de protection avancée qui améliore la détection reposant sur l'apprentissage machine. Pour plus d'informations sur ce type de protection, reportez-vous au glossaire.

Configuration du signalement

Lorsqu'une détection est effectuée (une menace est détectée et classée comme étant un logiciel malveillant, par exemple), les informations sont consignées dans le journal Détections. Des notifications de bureau s'affichent aussi si elles sont configurées dans ESET Endpoint Security.

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

1. Détections de logiciels malveillants
2. Applications potentiellement indésirables
3. Applications potentiellement dangereuses
4. Applications suspectes

Signalement effectué avec le moteur de détection, y compris le composant d'apprentissage machine. Vous pouvez définir un seuil de signalement supérieur à celui de la protection. Ces paramètres de signalement n'ont aucun impact sur le blocage, le nettoyage et la suppression des objets.

Lisez ce qui suit avant de modifier un seuil (ou un niveau) pour les signalements de CATÉGORIE :

Seuil	Explication
Offensif	Rapports sur CATÉGORIE configurés sur une sensibilité maximale. D'autres détections sont signalées. Le paramètre **Offensif** peut identifier à tort des objets comme étant CATÉGORIE.
Équilibré	Rapports sur CATÉGORIE configurés comme étant équilibrés. Cette configuration est optimisée pour équilibrer les performances et la précision des taux de détection et le nombre d'objets signalés à tort.
Prudent	Rapports sur CATÉGORIE configurés pour réduire le nombre d'objets identifiés à tort tout en maintenant un niveau de protection suffisant. Les objets ne sont signalés que lorsque la probabilité est évidente et correspond au comportement CATÉGORIE.
Désactivé	Les rapports sur CATÉGORIE ne sont pas actifs. Les détections de ce type ne sont pas recherchées, signalées ni nettoyées. Par conséquent, cette configuration désactive la protection de ce type de détection. Le paramètre Désactivé n'est pas disponible pour les rapports sur les logiciels malveillants. La valeur par défaut est celle des applications potentiellement dangereuses.

Disponibilité des modules de protection ESET Endpoint Security

La disponibilité (activé ou désactivé) d'un module de protection pour un seuil de CATÉGORIE sélectionné est la suivante :

	Offensif	Équilibré	Prudent	Désactivé*
Module d'apprentissage machine avancé	✔ (mode offensif)	✔ (mode conservateur)	X	X
Module du moteur de détection	✔	✔	✔	X
Autres modules de protection	✔	✔	✔	X

* Non recommandé.

Détermination de la version du produit, des versions des modules du programme et des dates de version

1. Cliquez sur **Aide et assistance** > **À propos d'ESET Endpoint Security**.
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** 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 Security 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.

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

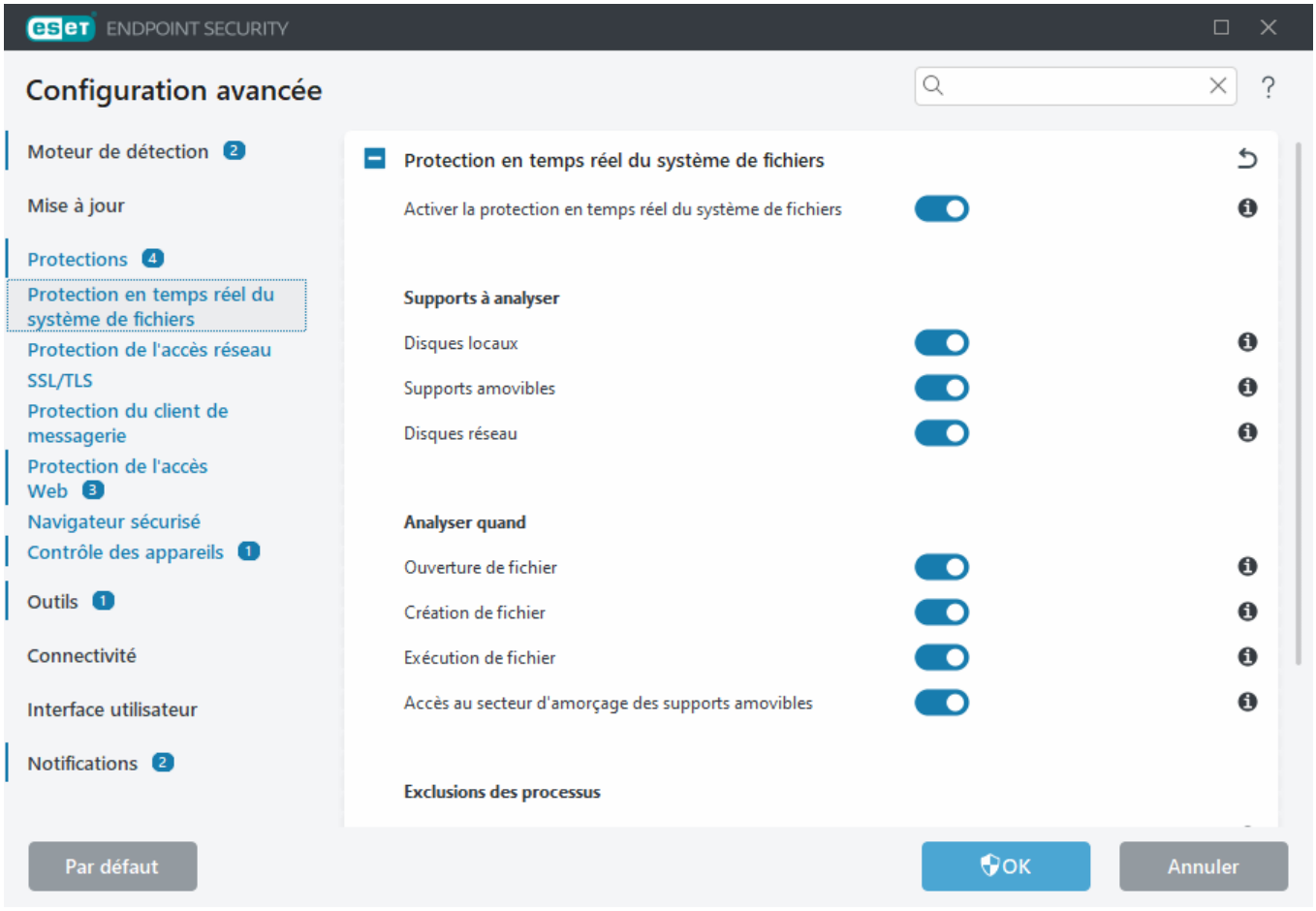
- Mettez en œuvre la « phase de production » sur certains postes de travail à titre de test (pas pour tous les postes de travail du réseau).

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 Security.
- 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 ESET PROTECT On-Prem pour rechercher une détection manquante éventuelle.

Protection en temps réel du système de fichiers

La protection en temps réel du système de fichiers contrôle tous les fichiers du système pour rechercher du code malveillant lors de leur ouverture, création ou exécution.



Par défaut, la protection en temps réel du système de fichiers est lancée au démarrage du système et assure une analyse ininterrompue. Il n'est pas recommandé de désactiver l'option **Activer la protection en temps réel du système de fichiers** dans Configurations avancées > **Protections** > **Protection en temps réel du système de fichiers** > **Protection en temps réel du système de fichiers**.

Supports à analyser

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

- **Disques locaux** – Analyse tous les disques durs système et fixes (par exemple : *C:*\, *D:*\).
- **Supports amovibles** – Analyse les CD/DVD, clés USB, cartes mémoire, etc.
- **Lecteurs réseau** – Analyse tous les lecteurs réseau mappés (par exemple : *H:*\ comme *store04*) ou les lecteurs réseau à accès direct (par exemple : *store08*).

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

Analyser quand

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

- **Ouverture de fichier** – Lance l'analyse lorsqu'un fichier est ouvert.
- **Création de fichier** – Analyse un fichier créé ou modifié.
- **Exécution de fichier** – Lance l'analyse lorsqu'un fichier est exécuté.

- **Accès au secteur d'amorçage des appareils amovibles** – Lorsqu'un appareil amovible contenant un secteur d'amorçage est inséré dans l'appareil, celui-ci est immédiatement analysé. Cette option n'active pas l'analyse des fichiers d'appareil amovible. Cette analyse se trouve dans **Supports à analyser** > **Appareils amovibles**. Pour que l'**accès au secteur d'amorçage des supports amovibles** fonctionne correctement, gardez l'option **Secteurs d'amorçage/UEFI** activée dans ThreatSense.

Exclusions des processus

Consultez Exclusions des processus.

ThreatSense

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

Pour garantir un impact minimal de la protection en temps réel sur le système, les fichiers déjà analysés ne sont pas analysés plusieurs fois (sauf s'ils ont été modifiés). Les fichiers sont immédiatement réanalysés après chaque mise à jour du moteur de détection. Ce comportement est contrôlé à l'aide de l'**optimisation intelligente**. Si l'**optimisation intelligente** est désactivée, tous les fichiers sont analysés à chaque accès. Pour modifier ce paramètre, ouvrez Configurations avancées > **Protections** > **Protection en temps réel du système de fichiers**. Cliquez ensuite sur **ThreatSense** > **Autre**, puis sélectionnez ou désélectionnez **Activer l'optimisation intelligente**.

La protection en temps réel du système de fichiers vous permet également de configurer des paramètres ThreatSense supplémentaires.

Exclusions des processus

La fonctionnalité Exclusions des processus permet d'exclure des processus d'application de la protection en temps réel du système de fichiers. Pour améliorer la vitesse de sauvegarde, l'intégrité des processus et la disponibilité du service, certaines techniques (connues pour entrer en conflit avec la protection contre les logiciels malveillants au niveau des fichiers) sont utilisées pendant la sauvegarde. Le seul moyen efficace d'éviter les deux situations est de désactiver le programme contre les logiciels malveillants. En excluant des processus spécifiques (par exemple ceux de la solution de sauvegarde), toutes les opérations sur les fichiers attribuées à ce processus exclu sont ignorées et considérées comme sûres, minimisant ainsi les interférences avec le processus de sauvegarde. Un outil de sauvegarde exclu peut accéder aux fichiers infectés sans déclencher d'alerte. C'est pourquoi les autorisations étendues ne sont autorisées que dans le module de protection en temps réel.

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

Les exclusions de processus permettent de réduire le risque de conflits potentiels et d'améliorer les performances des applications exclues, ce qui a un effet positif sur les performances globales et la stabilité du système d'exploitation. L'exclusion d'un processus/d'une application est une exclusion de son fichier exécutable (*.exe*).

Vous pouvez ajouter des fichiers exécutables à la liste des processus exclus dans Configurations avancées > **Protections** > **Protection en temps réel du système de fichiers** > **Protection en temps réel du système de fichiers** > **Exclusions des processus**.

Cette fonctionnalité a été conçue pour exclure les outils de sauvegarde. Exclure le processus de l'outil de sauvegarde de l'analyse garantit non seulement la stabilité du système, mais aussi celles des performances de la sauvegarde, car celle-ci n'est pas ralentie pendant son exécution.

Cliquez sur **Modifier** pour ouvrir la fenêtre de gestion **Exclusions des processus**, dans laquelle vous pouvez ajouter des exclusions et accéder au fichier exécutable (*Backup-tool.exe*, par exemple) qui sera exclu de l'analyse.
Dès que le fichier *.exe* est ajouté aux exclusions, l'activité de ce processus n'est pas surveillée par ESET Endpoint Security et aucune analyse n'est effectuée sur les opérations de fichier effectuées par celui-ci.

Si vous n'utilisez pas la fonction de navigation lors de la sélection de l'exécutable de processus, vous devez entrer manuellement le chemin complet de l'exécutable. Sinon, l'exclusion ne fonctionnera pas correctement et HIPS pourra signaler des erreurs.

Vous pouvez aussi **modifier** des processus existants ou les **supprimer** des exclusions.

La protection de l'accès web ne tient pas compte de cette exclusion. Par conséquent, si vous excluez le fichier exécutable de votre navigateur web, les fichiers téléchargés sont toujours analysés. Ainsi, une infiltration peut toujours être détectée. Ce scénario n'est qu'un exemple et nous vous déconseillons de créer des exclusions pour les navigateurs web.

Ajouter ou modifier des exclusions de processus

Cette boîte de dialogue permet d'**ajouter** des processus exclus du moteur de détection. Les exclusions de processus permettent de réduire le risque de conflits potentiels et d'améliorer les performances des applications exclues, ce qui a un effet positif sur les performances globales et la stabilité du système d'exploitation. L'exclusion d'un processus/d'une application est une exclusion de son fichier exécutable (*.exe*).

Sélectionnez le chemin d'accès au fichier d'une application visée par l'exception en cliquant sur ... (*C:\Program Files\Firefox\Firefox.exe*, par exemple). NE saisissez PAS le nom de l'application.
Dès que le fichier *.exe* est ajouté aux exclusions, l'activité de ce processus n'est pas surveillée par ESET Endpoint Security et aucune analyse n'est effectuée sur les opérations de fichier effectuées par celui-ci.

Si vous n'utilisez pas la fonction de navigation lors de la sélection de l'exécutable de processus, vous devez entrer manuellement le chemin complet de l'exécutable. Sinon, l'exclusion ne fonctionnera pas correctement et HIPS pourra signaler des erreurs.

Vous pouvez aussi **modifier** des processus existants ou les **supprimer** des exclusions.

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

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

Après l'installation de ESET Endpoint Security, tous les paramètres sont optimisés pour garantir le niveau maximum de système de sécurité aux utilisateurs. Pour restaurer les paramètres par défaut, cliquez sur ↺ en regard de Configurations avancées > **Protections** > **Réponses des détections**.

Vérification de la protection en temps réel

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

Le fichier peut être téléchargé à l'adresse suivante : http://www.eicar.org/download/eicar.com
Une fois que vous avez saisi cette URL dans votre navigateur, un message doit s'afficher pour vous indiquer que la menace a été supprimée.

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

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

La protection en temps réel est désactivée

Si un utilisateur désactive par mégarde la protection en temps réel, vous devez réactiver la fonctionnalité. Pour réactiver la protection en temps réel, sélectionnez **Configuration** dans la fenêtre principale du programme et cliquez sur **Ordinateur** > **Protection en temps réel du système de fichiers**.

Si la protection en temps réel ne se lance pas au démarrage du système, c'est probablement parce que l'option **Activer la protection en temps réel du système de fichiers** est désactivée. Pour vous assurer que cette option est activée, ouvrez Configurations avancées > **Protections** > **Protection en temps réel du système de fichiers**.

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

Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si deux programmes antivirus sont installés, ils risquent de provoquer des conflits. Nous recommandons de désinstaller tout autre antivirus de votre système avant d'installer ESET.

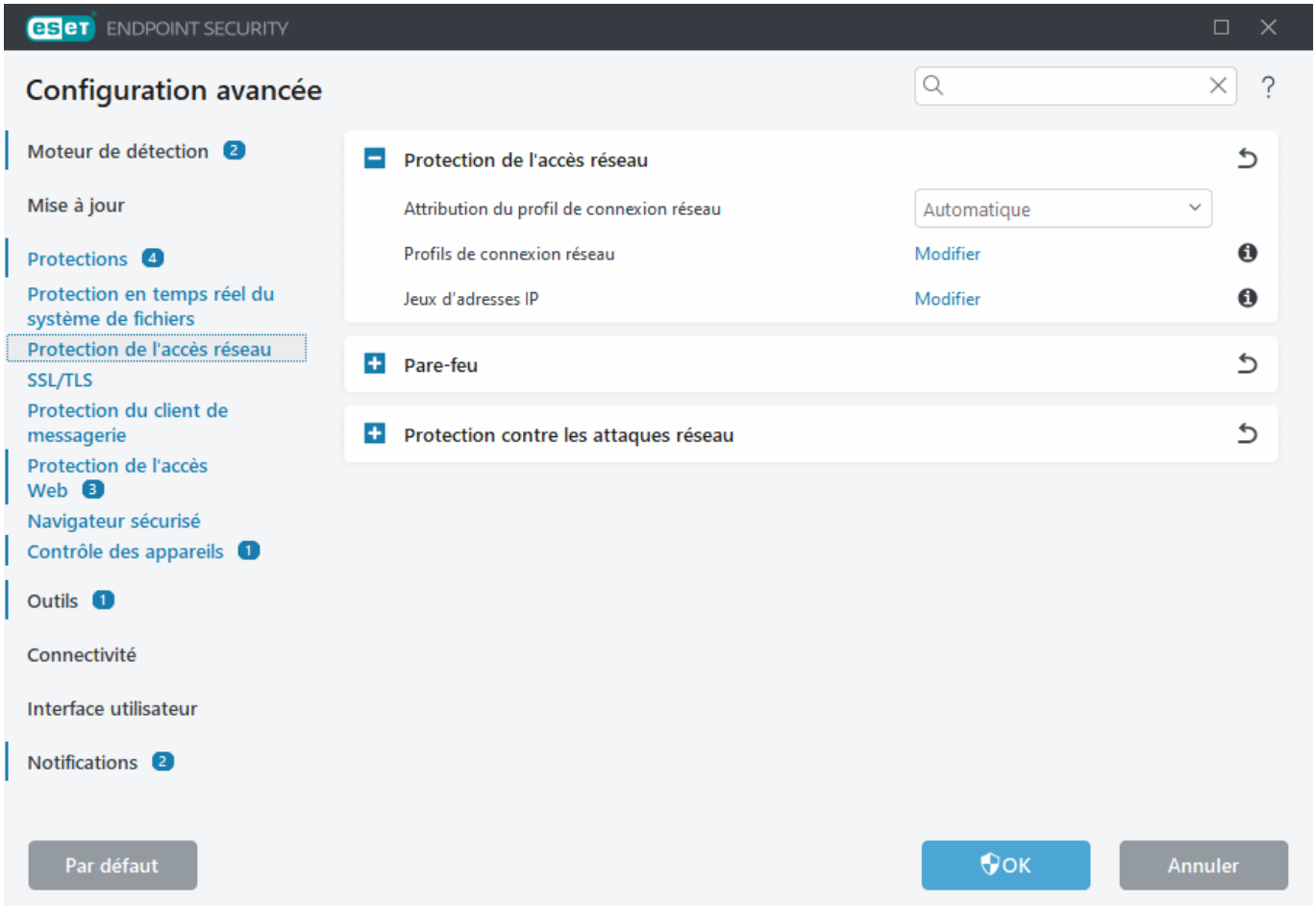
La protection en temps réel ne démarre pas

Si la protection en temps réel n'est pas lancée au démarrage du système (et si **Activer la protection en temps réel du système de fichiers** est activé), le problème peut provenir de conflits avec d'autres programmes. Pour résoudre ce problème, créez un journal ESET SysInspector et envoyez-le à l'assistance technique ESET pour analyse.

Protection de l'accès réseau

La protection de l'accès réseau vous permet de configurer toutes vos connexions réseau. Vous pouvez autoriser/refuser l’accès à votre ordinateur sur des réseaux spécifiques, autoriser/refuser l’accès aux périphériques réseau à partir de votre ordinateur et plus encore en fonction de la configuration. Par défaut, ESET Endpoint Security dispose de règles de pare-feu préconfigurées et d'une protection de l'accès réseau pour une

sécurité maximale. Toutefois, des environnements spécifiques peuvent nécessiter une configuration personnalisée. La modification des configurations par défaut ne doit être effectuée que par un utilisateur expérimenté.



Vous pouvez configurer les paramètres suivants dans Configurations avancées > **Protections** > **Protection de l'accès réseau** (cliquez sur les liens ci-dessous pour obtenir une description détaillée de chaque option de la protection de l'accès réseau) :

Protection de l'accès réseau

Profils de connexion réseau : les profils peuvent être utilisés pour contrôler la protection d'accès réseau et le pare-feu pour des connexions réseau spécifiques.

Jeux d'adresses IP : vous pouvez définir des ensembles d'adresses IP qui créent un groupe d'adresses IP logique, que vous pouvez utiliser pour les règles du pare-feu et de la protection contre les attaques par force brute.

Pare-feu

Protection contre les attaques réseau

Profils de connexion réseau

Des profils peuvent être utilisés pour contrôler le comportement de la protection d'accès réseau ESET Endpoint Security pour une connexion réseau spécifique. Lors de la création ou de la modification de règles de pare-feu, de règles IDS ou de règles de la protection contre les attaques par force brute, vous pouvez l'attribuer à un profil

spécifique ou l'appliquer à tous les profils. Lorsqu'un profil est actif sur une connexion réseau, seules les règles globales (sans aucun profil indiqué) et les règles attribuées à ce profil sont appliquées. Vous pouvez créer plusieurs profils avec des règles différentes attribuées aux connexions réseau pour modifier facilement le comportement du pare-feu.

Vous pouvez configurer des profils de connexion réseau dans Configurations avancées > **Protections** > **Protection de l'accès réseau** > **Protection de l'accès réseau**.

Attribution du profil de connexion réseau : permet de choisir si les connexions réseau nouvellement découvertes se voient automatiquement attribuer (sélectionnez **Auto** dans le menu déroulant) un profil prédéfini ou personnalisé en fonction des activateurs configurés dans les profils de connexion réseau ou si vous souhaitez être invité (sélectionnez **Demander** dans le menu déroulant) à configurer la protection du réseau et à attribuer un profil manuellement chaque fois qu'une nouvelle connexion réseau est détectée.

Vous pouvez également attribuer manuellement un profil de connexion réseau spécifique dans la fenêtre principale du programme > **Configuration** > **Réseau** > **Connexions réseau**. Pointez sur une connexion réseau spécifique et cliquez sur l'icône de menu ⋮ > **Modifier** pour ouvrir la fenêtre Configurer la protection du réseau et sélectionner un profil.

Profils de connexion réseau : cliquez sur **Modifier** pour ajouter ou modifier des profils de connexion réseau.

Les profils suivants sont prédéfinis et ne peuvent pas être modifiés/supprimés :

Privé : pour des réseaux approuvés (réseau domestique ou professionnel). Votre ordinateur et les fichiers partagés stockés sur votre ordinateur sont visibles par les autres utilisateurs du réseau, et les ressources du système sont accessibles aux autres utilisateurs du réseau (l'accès aux fichiers et imprimantes partagés est activé, la communication RPC entrante est activée et le partage du bureau à distance est disponible). Il est recommandé d'utiliser ce paramètre lors des accès à un réseau local sécurisé. Ce profil est automatiquement attribué à une connexion réseau s'il est configuré en tant que domaine ou réseau privé dans Windows.

Non : pour des réseaux non approuvés (réseau public). les fichiers et les dossiers de votre système ne sont pas partagés ou visibles par les autres utilisateurs du réseau et les partages des ressources système sont désactivés. Il est recommandé d'utiliser ce paramètre lors des accès à des réseaux sans fil. Ce profil est automatiquement attribué à toute connexion réseau qui n'est pas configurée en tant que domaine ou réseau privé dans Windows.

Lorsque la connexion réseau bascule vers un autre profil, une notification apparaît dans l'angle inférieur droit de votre écran.

Ajout ou modification de profils de connexion réseau

Vous pouvez ajouter ou modifier des profils de connexion réseau dans Configurations avancées > **Protections** > **Protection de l'accès réseau** > **Protection de l'accès réseau** > **Profils de connexion réseau** > **Modifier**. Pour modifier un profil, il doit être sélectionné dans la liste de la fenêtre **Profils de connexion réseau**.

Les profils suivants sont prédéfinis et ne peuvent pas être modifiés/supprimés :

Privé : pour des réseaux approuvés (réseau domestique ou professionnel). Votre ordinateur et les fichiers partagés stockés sur votre ordinateur sont visibles par les autres utilisateurs du réseau, et les ressources du système sont accessibles aux autres utilisateurs du réseau (l'accès aux fichiers et imprimantes partagés est activé, la communication RPC entrante est activée et le partage du bureau à distance est disponible). Il est recommandé d'utiliser ce paramètre lors des accès à un réseau local sécurisé. Ce profil est automatiquement attribué à une

connexion réseau s'il est configuré en tant que domaine ou réseau privé dans Windows.

Non : pour des réseaux non approuvés (réseau public). les fichiers et les dossiers de votre système ne sont pas partagés ou visibles par les autres utilisateurs du réseau et les partages des ressources système sont désactivés. Il est recommandé d'utiliser ce paramètre lors des accès à des réseaux sans fil. Ce profil est automatiquement attribué à toute connexion réseau qui n'est pas configurée en tant que domaine ou réseau privé dans Windows.

Monter/Descendre  – Vous permet d'ajuster le niveau de priorité des profils de connexion réseau (les profils de connexion réseau sont évalués et appliqués en fonction de leur priorité. Le premier profil correspondant est toujours appliqué).

Ajout ou modification d'un profil

Le profil de connexion réseau personnalisé vous permet d'appliquer des règles de pare-feu, des règles de protection contre les attaques par force brute et de définir des paramètres supplémentaires pour des connexions réseau spécifiques. Vous allez spécifier à quelles connexions réseau le profil personnalisé sera attribué dans la section Activateurs.

Pour ouvrir l'éditeur de profils, dans la fenêtre **Profils de connexion réseau** :

- Cliquez sur **Ajouter**.
- Sélectionnez l'un des profils existants et cliquez sur **Modifier**.
- Sélectionnez l'un des profils existants et cliquez sur **Copier**.

Nom – Nom personnalisé de votre profil.

Description – Description du profil pour faciliter son identification.

Autres adresses fiables – Les adresses définies ici sont ajoutées à la zone fiable de la connexion réseau à laquelle ce profil est appliqué (quel que soit le type de protection du réseau).

Connexion approuvée – Votre ordinateur et les fichiers partagés stockés sur votre ordinateur sont visibles par les autres utilisateurs du réseau, et les ressources du système sont accessibles aux autres utilisateurs du réseau (l'accès aux fichiers et imprimantes partagés est activé, la communication RPC entrante est activée et le partage du bureau à distance est disponible). Nous vous recommandons d'utiliser ce paramètre lors de la création d'un profil pour une connexion réseau locale sécurisée. Tous les sous-réseaux du réseau directement connectés sont également considérés comme approuvés. Par exemple, si un adaptateur réseau est connecté à ce réseau avec l'adresse IP 192.168.1.5 et le masque de sous-réseau 255.255.255.0, le sous-réseau 192.168.1.0/24 est ajouté à la zone Fiable de la connexion réseau. Si l'adaptateur possède plus d'adresses/de sous-réseaux, ils seront tous approuvés.

Signaler un chiffrement Wi-Fi faible – ESET Endpoint Security affiche une notification sur le Bureau lorsque vous vous connectez à un réseau sans fil sans protection ou à un réseau avec une faible protection.

Activateurs – Conditions personnalisées à remplir pour affecter ce profil de connexion réseau à une connexion réseau. Consultez Activateurs pour une explication détaillée.

Activateurs

Les activateurs sont des conditions personnalisées qui doivent être remplies pour attribuer un profil de connexion réseau à une connexion réseau. Si le réseau connecté possède les mêmes attributs que ceux définis dans les activateurs d'un profil de réseau connecté, le profil sera appliqué au réseau. Un profil de connexion réseau peut avoir un ou plusieurs activateurs. Dans le cas de plusieurs activateurs, la logique OU s'applique (au moins une condition doit être remplie). Vous pouvez définir des activateurs dans l'éditeur de profil de connexion réseau. La création de profils de connexion réseau personnalisés doit être effectuée par un utilisateur expérimenté.

Les activateurs suivants sont disponibles (si vous souhaitez connaître les détails du réseau auquel vous êtes actuellement connecté, consultez Connexions réseau) :

Adaptateur

Type d'adaptateur : applique le profil si la connexion réseau est établie sur le type de carte sélectionné.
Nom de l'adaptateur : applique le profil si le nom de l'adaptateur correspond.
IP de l'adaptateur : applique le profil si l'adresse IP de l'adaptateur réseau correspond.

DNS

Suffixe DNS : applique le profil si le nom du domaine correspond.
IP DNS : applique le profil si l'adresse IP du serveur DNS correspond.

WINS

Applique le profil si l'adresse IP Windows Internet Name Service (WINS) mappée correspond.

DHCP

IP DHCP : correspond à l'adresse IP du serveur DHCP.

Passerelle par défaut

IP : applique le profil si l'adresse IP de la passerelle par défaut correspond.
Adresse MAC : applique le profil si l'adresse MAC de la passerelle par défaut correspond.

Wi-Fi

SSID : applique le profil si le SSID (nom du Wi-Fi) correspond.
Nom du profil : applique le profil si le nom du profil Wi-Fi correspond.
Type de sécurité : applique le profil si le type de sécurité correspond à celui sélectionné dans le menu déroulant. (Si vous voulez en faire correspondre plus d'un, créez un autre activateur).
Type de chiffrement : applique le profil si le type de chiffrement correspond à celui sélectionné dans le menu déroulant. (Si vous voulez en faire correspondre plus d'un, créez un autre activateur).
Sécurité réseau : applique le profil si le réseau est **ouvert/sécurisé**.

Profil Windows

Applique le profil si le réseau est configuré dans Windows en tant que **domaine/privé/public**.

Authentification

L'authentification réseau recherche un serveur spécifique sur le réseau et utilise le chiffrement asymétrique (algorithme RSA) pour authentifier le serveur. Le nom du réseau authentifié doit correspondre au nom défini dans les paramètres du serveur d'authentification. Le nom respecte la casse. Le nom du serveur peut être saisi sous la forme d'une adresse IP, d'un nom DNS ou d'un nom NetBios.
Téléchargez ESET Authentication Server.
La clé publique peut être importées à l'aide d'un des types de fichier suivants :
• Clé publique chiffrée PEM (.pem) ; vous pouvez générer cette clé à l'aide d'ESET Authentication Server.
• Clé publique chiffrée
• Certificat de clé publique (.crt)
Cliquez sur **Tester** pour tester vos paramètres. Si l'authentification aboutit, Authentification de serveur réussie s'affiche. Si l'authentification n'est pas configurée correctement, l'un des messages d'erreur suivants s'affiche :
Authentification de serveur échouée. Signature non valide ou non correspondante.
La signature du serveur ne correspond pas à la clé publique saisie.
Authentification de serveur échouée. Le nom du réseau ne correspond pas.
Le nom du réseau configuré ne correspond pas au nom de le réseau du serveur d'authentification. Vérifiez les deux noms et assurez-vous qu'ils soient identiques.
Authentification de serveur échouée. Réponse non valide ou inexistante du serveur.
Aucune réponse n'est reçue si le serveur n'est pas en cours d'exécution ou accessible. Une réponse non valide peut être reçue si un autre serveur HTTP est en cours d'exécution sur l'adresse spécifiée.
Clé publique non valide.
Vérifiez que le fichier de clé publique n'est pas endommagé.

Jeux d’adresses IP

Un jeu d'adresses IP représente un ensemble d'adresses IP qui créent un groupe logique d'adresses IP ; ce procédé est utile lorsque vous devez réutiliser un même ensemble d'adresses dans plusieurs règles du pare-feu ou règles de la protection contre les attaques par force brute. ESET Endpoint Security contient également des jeux d'adresses IP prédéfinis pour lesquels des règles internes sont appliquées. La **zone Fiable** est un exemple de groupe. La zone fiable représente un groupe d'adresses réseau où votre ordinateur et les fichiers partagés stockés sur votre ordinateur sont visibles par les autres utilisateurs du réseau, et où les ressources du système sont accessibles aux autres utilisateurs du réseau.

Pour ajouter un jeu d'adresses IP :

1. Ouvrez Configurations avancées > **Protections** > **Protection de l'accès réseau** > **Jeux d'adresses IP** > **Modifier**.
2. Cliquez sur **Ajouter**, saisissez un **nom** et une **description** pour la zone, puis tapez une adresse IP distante dans **Adresse de l'ordinateur distant (IPv4/IPv6, plage, masque)**.
3. Cliquez sur **OK**.

Pour plus d'informations, consultez Modifier des jeux d'adresses IP.

Modification de jeux d'adresses IP

Pour plus d'informations sur les jeux d'adresses IP, consultez Jeux d'adresses IP.

Colonnes

Nom – Nom d'un groupe d'ordinateurs distants.

Description – Description générale du groupe.

Adresses IP – Adresses IP distantes qui appartiennent à un jeu d'adresses IP.

Éléments de commande

Lorsque vous **ajoutez** ou **modifiez** un jeu d'adresses IP, les champs suivants sont disponibles :

Nom – Nom d'un groupe d'ordinateurs distants.

Description – Description générale du groupe.

Adresse de l'ordinateur distant (IPv4, IPv6, plage, masque) – permet d'ajouter une adresse distante, une plage d'adresses ou un sous-réseau.

Supprimer – Supprime une zone de la liste.

Les jeux d'adresses IP prédéfinis ne peuvent pas être supprimés.

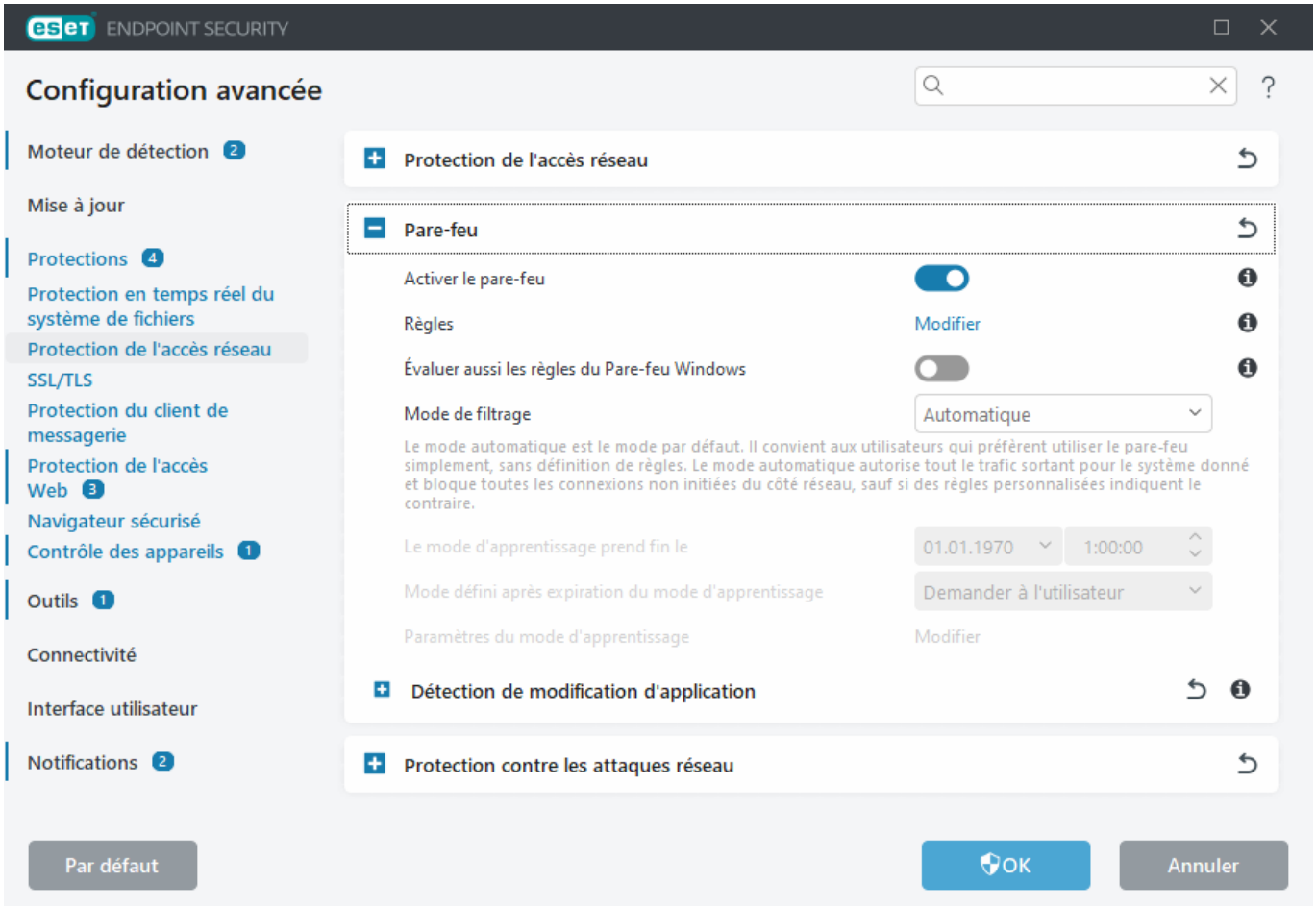
Exemples d'adresses IP

Ajouter une adresse IPv4:
Adresse unique – Ajoute l'adresse IP d'un ordinateur (par exemple, *192.168.0.10*).
Plage d'adresses – Saisissez l'adresse IP de début et de fin pour définir la plage IP de plusieurs ordinateurs (par exemple *192.168.0.1 à 192.168.0.99*).
Sous-réseau – Le sous-réseau (groupe d'ordinateurs) est défini par une adresse IP et un masque. Par exemple, 255.255.255.0 est le masque de réseau pour le sous-réseau 192.168.1.0. Pour exclure tout le type de sous-réseau dans *192.168.1.0/24*.
Ajouter une adresse IPv6:
Adresse unique – Ajoute l'adresse IP d'un ordinateur auquel la règle doit être appliquée, par exemple *2001:718:1c01:16:214:22ff:fec9:ca5*.
Sous-réseau – Le sous-réseau (groupe d'ordinateurs) est défini par une adresse IP et un masque (par exemple : *2002:c0a8:6301:1::1/64*).

Pare-feu

Le pare-feu contrôle tout le trafic réseau entrant et sortant de votre ordinateur sur la base de règles internes et de règles définies par vous. Il autorise ou refuse les différentes connexions réseau. Le pare-feu fournit une protection contre les attaques en provenance d'appareils distants et permet de bloquer certains services potentiellement dangereux.

Pour configurer le pare-feu, ouvrez Configurations avancées > **Protections** > **Protection de l'accès réseau** > **Pare-feu**.



Pare-feu

Activer le pare-feu

Il est recommandé de laisser cette fonctionnalité activée pour assurer la protection de votre système. Lorsque le pare-feu est activé, le trafic réseau est analysé dans les deux sens.

Règles

La configuration des règles permet de voir et modifier toutes les règles du pare-feu appliquées au trafic généré par des applications dans des connexions approuvées et sur Internet.

Les règles du pare-feu Windows configurées à l'aide d'une stratégie de groupe (GPO) ne sont pas évaluées.

Vous pouvez créer une règle IDS lors des attaques Botnet de votre ordinateur. Une règle peut être modifiée dans Configurations avancées > **Protections** > **Protection de l'accès réseau** > **Protection contre les attaques réseau** > **Règles IDS**, en cliquant sur **Modifier**.

Évaluer aussi les règles du Pare-feu Windows

En mode de filtrage automatique, le trafic entrant autorisé par les règles du pare-feu Windows est évalué et traité, sauf en cas de blocage explicite par les règles ESET.

Mode de filtrage

Le comportement du pare-feu change en fonction du mode de filtrage. Les modes de filtrage affectent également

le niveau d'interaction de l'utilisateur.

Les modes de filtrage suivants sont disponibles pour le pare-feu de ESET Endpoint Security :

Mode de filtrage	Description
Mode automatique	Mode par défaut. Ce mode convient aux utilisateurs qui préfèrent utiliser le pare-feu simplement, sans définition de règles. Des règles personnalisées définies par l'utilisateur peuvent être créées, mais ne sont pas nécessaires en **mode automatique**. Le mode automatique autorise tout trafic sortant du système donné et bloque la plupart du trafic entrant, à l'exception du trafic à partir de la zone Fiable (comme indiqué dans Options IDS avancées/Services autorisés) et aux réponses aux communications sortantes récentes.
Mode interactif	Mode interactif : vous permet d'élaborer une configuration personnalisée pour votre pare-feu. Lors de la détection d'une communication à laquelle aucune règle ne s'applique, une boîte de dialogue s'affiche pour signaler une connexion inconnue. Cette boîte de dialogue permet d'autoriser ou de refuser la communication, cette décision pouvant être enregistrée comme nouvelle règle pour le pare-feu. Si vous choisissez de créer une règle, toutes les connexions ultérieures de ce type sont autorisées ou refusées, conformément à la règle.
Mode basé sur des politiques	Le mode basé sur des règles personnalisées bloque toute connexion ne faisant pas l'objet d'une règle spécifique l'autorisant. Ce mode permet aux utilisateurs expérimentés de définir des règles qui n'autorisent que des connexions souhaitées et sûres. Toutes les autres connexions spécifiées sont bloquées par le pare-feu.
Mode d'apprentissage	Crée et enregistre automatiquement des règles. Ce mode convient à la configuration initiale du pare-feu, mais il ne doit pas être utilisé pendant des périodes prolongées. Aucune intervention de l'utilisateur n'est requise, car ESET Endpoint Security enregistre les règles conformément aux paramètres prédéfinis. Le mode d'apprentissage n'étant pas sécurisé, il est recommandé de ne l'utiliser que jusqu'à ce que toutes les règles aient été créées pour éviter les risques de sécurité.

Le mode d'apprentissage prend fin le : définissez la date et l'heure auxquelles le mode d'apprentissage se termine automatiquement. Vous pouvez également désactiver le mode d'apprentissage manuellement à tout moment.

Mode défini après expiration du mode d'apprentissage – Définissez à quel mode de filtrage sera rétabli le pare-feu une fois le mode d'apprentissage terminé. Pour en savoir plus sur les modes de filtrage, consultez le tableau ci-dessus. Une fois terminé, l'option **Demander à l'utilisateur** requiert des privilèges administratifs pour effectuer un changement au mode de filtrage du pare-feu.

Paramètres du mode d'apprentissage : cliquez sur **Modifier** pour configurer les paramètres d'enregistrement des règles créées en mode d'apprentissage.

Détection de modification d'application

La fonctionnalité de détection de modification d'application affiche des notifications si des applications modifiées pour lesquelles il existe une règle de pare-feu tentent d'établir des connexions.

Paramètres du mode d'apprentissage

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

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

Sélectionnez **Apprentissage** dans le menu déroulant dans Configurations avancées > **Protections** > **Protection de l'accès réseau** > **Pare-feu** > **Pare-feu** > **Mode de filtrage** pour activer les options du mode d'apprentissage. Cliquez sur **Modifier** en regard de **Paramètres du mode d'apprentissage** pour configurer les options suivantes :

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

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

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

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

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

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

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

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

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

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

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

Boîte de dialogue - Fin du mode d'apprentissage

Lorsque la période d'utilisation du mode d'apprentissage est écoulée, vous êtes invité à passer en mode de filtrage **interactif** ou **basé sur des règles personnalisées**. Lorsque le pare-feu est en mode d'apprentissage, de nouvelles règles sont créées sans l'intervention de l'utilisateur.

Pour plus d'informations sur chaque mode de filtrage, reportez-vous à la section Modes de filtrage.

> Il est recommandé d'examiner les règles créées en mode d'apprentissage en cliquant sur **Ouvrir l'éditeur de règles**.

Règles du pare-feu

Les règles de pare-feu représentent un ensemble de conditions utilisées pour tester de façon significative toutes les connexions réseau, ainsi que toutes les actions affectées à ces conditions. À l'aide des règles du pare-feu, vous pouvez définir l'action à entreprendre si une connexion réseau (de différents types) est établie.

Les règles sont évaluées de haut en bas et vous pouvez voir leur priorité dans la première colonne. L'action de la première règle correspondante est utilisée pour chaque connexion réseau évaluée.

Les connexions peuvent être divisées en connexions entrantes et sortantes. Les connexions entrantes sont initiées par un appareil distant qui tente d'établir une connexion avec le système local. Les connexions sortantes fonctionnent en sens inverse : c'est le système local qui contacte un appareil distant.

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

Vous pouvez afficher et modifier les règles du pare-feu dans Configurations avancées > **Protections** > **Protection de l'accès réseau** > **Pare-feu** > **Règles** > **Modifier**.

Si les règles du pare-feu sont nombreuses, vous pouvez utiliser un filtre pour n'afficher que des règles spécifiques. Pour filtrer les règles du pare-feu, cliquez sur **Autres filtres** au-dessus de la liste des règles du pare-feu. Vous pouvez filtrer les règles selon les critères suivants :

- Origine
- Direction
- Action
- Disponibilité

Par défaut, les règles du pare-feu prédéfinies sont masquées. Pour afficher toutes les règles prédéfinies, désactivez le bouton bascule en regard de l'option **de Masquer les règles intégrées (prédéfinies)**. Vous pouvez désactiver ces règles, mais vous ne pouvez pas les supprimer.

> Cliquez sur l'icône de recherche dans le coin supérieur droit pour rechercher un ou des règles.

Colonnes

Priorité : les règles sont évaluées de haut en bas et vous pouvez voir leur priorité dans la première colonne.

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

Application : application à laquelle la règle s'applique.

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

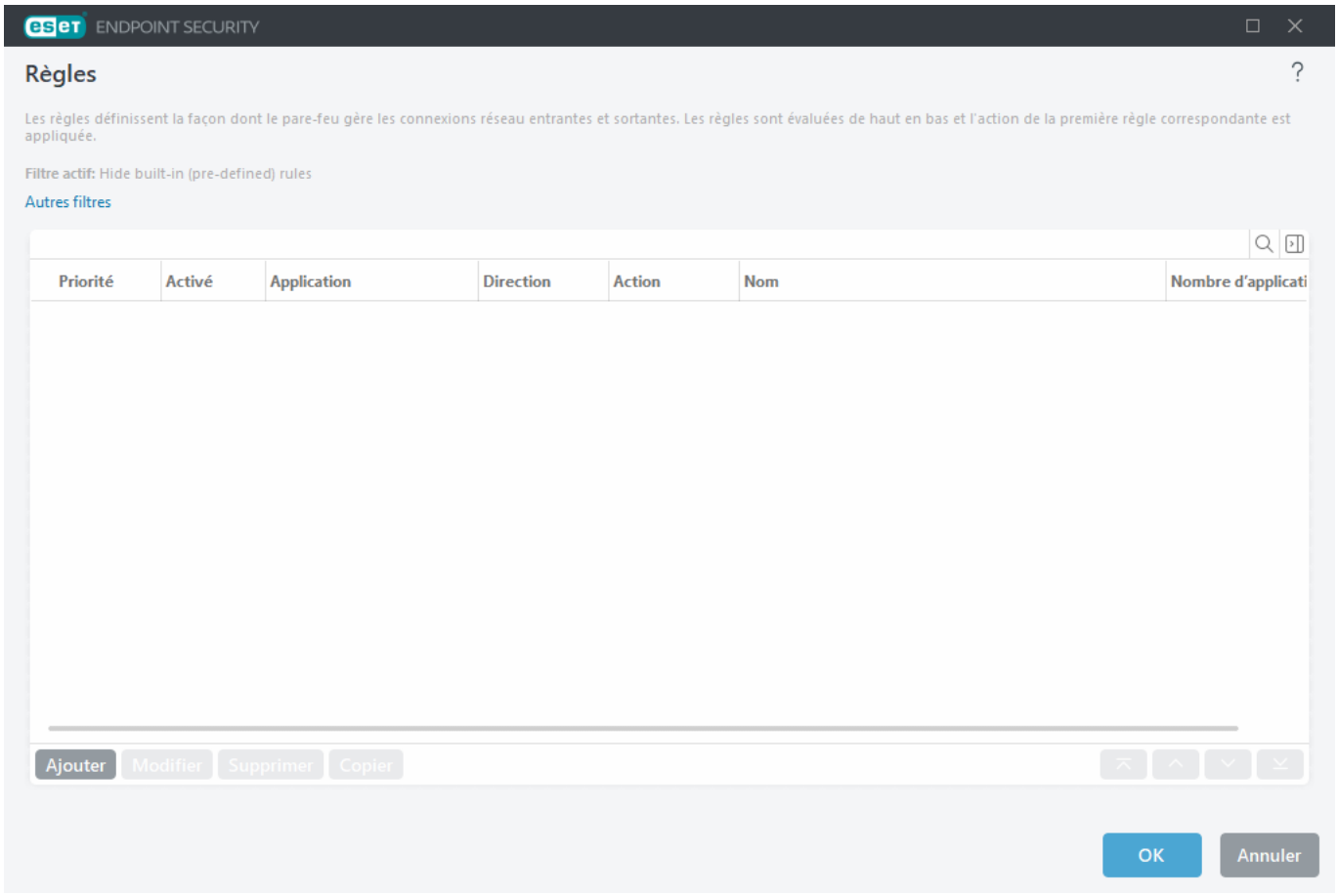
Action : indique l'état de la communication (bloquer/autoriser/demander).

Nom : nom de la règle. L'icône ESET représente une règle prédéfinie.

Nombre d'applications : nombre total de fois que la règle a été appliquée.

Cliquez sur l'icône de développement pour afficher les détails de la règle.

Vous pouvez choisir les colonnes à afficher en cliquant avec le bouton droit sur l'en-tête du tableau.



Éléments de commande

Ajouter – Permet de créer une règle.

Modifier : modifie une règle existante.

Supprimer : permet de supprimer une règle existante.

Copier : permet de créer une copie d'une règle sélectionnée.

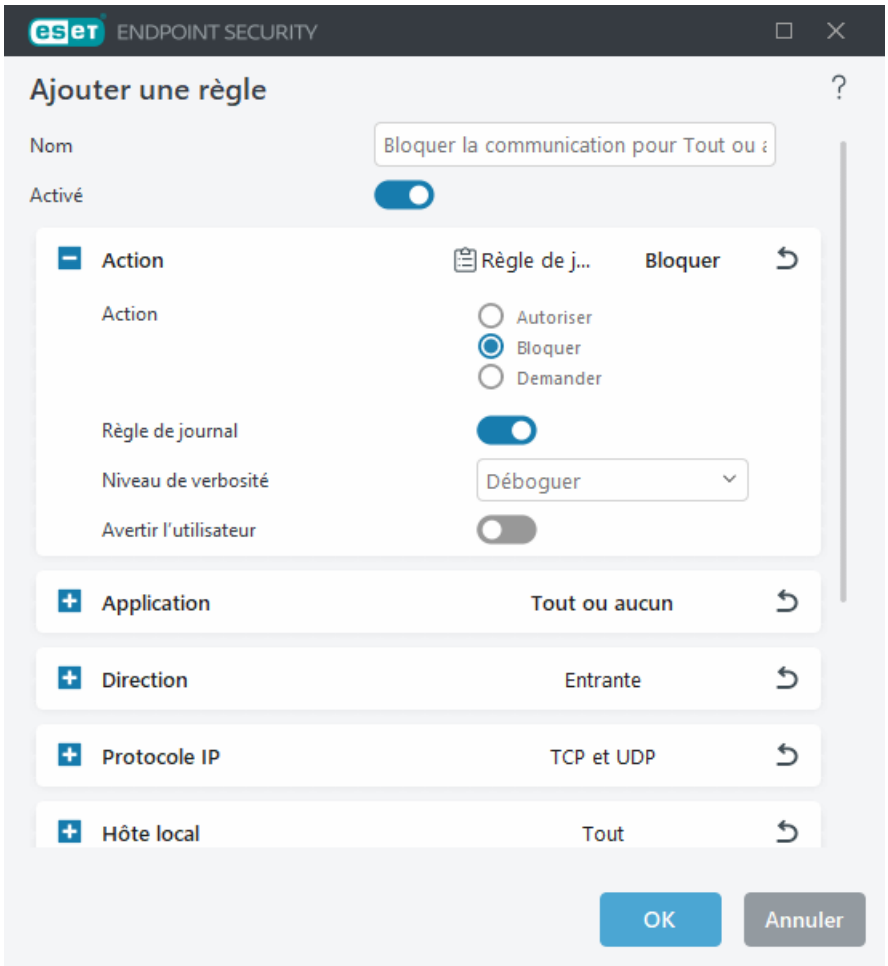
Haut/Monter/Bas/Descendre : permet d'ajuster le niveau de priorité des règles (les règles sont exécutées du haut vers le bas).

Ajout ou modification de règles du pare-feu

Les règles de pare-feu représentent des conditions utilisées pour tester de façon significative toutes les connexions réseau, ainsi que les actions affectées à ces conditions. Il peut être nécessaire de modifier ou d'ajouter des règles de pare-feu lorsque les paramètres du réseau changent (par exemple, lorsque l'adresse réseau ou le numéro de port du côté distant a changé) afin de garantir le bon fonctionnement d'une application affectée par une règle. Un utilisateur expérimenté doit créer des règles de pare-feu personnalisées.

Les articles suivants de la base de connaissances ESET peuvent être disponibles uniquement en anglais :
- Créer ou modifier des règles du pare-feu dans ESET Endpoint Security
- Créer ou modifier des règles du pare-feu pour les stations de travail clientes dans ESET PROTECT On-Prem

Pour ajouter ou modifier une règle de pare-feu, ouvrez Configurations avancées > **Protections** > **Protection de l'accès réseau** > **Pare-feu Règles** > **Modifier**. Dans la fenêtre Règles du pare-feu, cliquez sur **Ajouter** ou **Modifier**.



Nom : saisissez un nom pour la règle.

Activée : activez le bouton bascule pour activer la règle.

Ajoutez des actions et des conditions pour la règle du pare-feu :

Action

Action : sélectionnez cette option si vous souhaitez **autoriser/bloquer** les communications qui correspondent aux conditions définies dans cette règle ou si vous souhaitez qu'ESET Endpoint Security vous **pose la question** chaque fois que les communications s'établissent.
Règle de journal : si la règle est appliquée, elle est enregistrée dans les Fichiers journaux.
Journalisation de la gravité : sélectionnez la gravité de l'entrée de journal pour cette règle.
L'option **Notifier l'utilisateur** affiche une notification lorsque la règle est appliquée.

Application :

Spécifiez une application pour laquelle cette règle sera appliquée.
Chemins de l'application : cliquez sur **...** et accédez à une application ou saisissez le chemin d'accès complet à l'application (C:\Program Files\Firefox\Firefox.exe, par exemple). NE saisissez PAS uniquement le nom de l'application.
Signature de l'application : vous pouvez appliquer la règle aux applications en fonction de leur signature (nom de l'éditeur). Sélectionnez dans le menu déroulant si vous souhaitez appliquer la règle aux applications avec **Toute signature valide** ou aux applications avec **Signature par un signataire spécifique**. Si vous sélectionnez les applications avec **Signature par un signataire spécifique**, vous devez définir le signataire dans le champ **Nom du signataire**.
Application Microsoft Store : sélectionnez dans le menu déroulant une application installée à partir du Microsoft Store.
Service : vous pouvez sélectionner un service système au lieu d'une application. Ouvrez le menu déroulant pour sélectionner un service.
Appliquer aux processus enfants : certaines applications peuvent exécuter plus de processus alors que vous ne voyez qu'une seule fenêtre d'application. Activez ce bouton bascule pour vous assurer que la règle s'appliquera à tous les processus de l'application spécifiée.

Direction

Sélectionnez la **Direction** des communications auxquelles cette règle s'appliquera :
• **Les deux** : communications entrantes et sortantes
• **Entrée** : communications entrantes uniquement
• **Sortie** : communications sortantes uniquement

Protocole IP

Sélectionnez **Protocole** dans le menu déroulant si vous souhaitez que cette règle ne s'applique qu'à un protocole spécifique.

Hôte local

Adresses, plage d'adresses ou sous-réseau locaux pour lesquels cette règle est appliquée. Si aucune adresse n'est spécifiée, la règle s'applique à toutes les communications avec les hôtes locaux. Vous pouvez ajouter des adresses IP, des plages d'adresses ou des sous-réseaux directement dans le champ **IP** ou sélectionner des jeux d'adresses existants en cliquant sur **Modifier** en regard de **Jeux d'adresses IP**.

Port local

Numéros des **ports** locaux. Si aucun numéro n'est spécifié, la règle s'applique à n'importe quel port. Vous pouvez ajouter un port de communication ou une plage de ports de communication.

Hôte distant

Adresse, plage d'adresses ou sous-réseau distants pour lesquels cette règle est appliquée. Si aucune adresse n'est spécifiée, la règle s'applique à l'ensemble des communications avec les hôtes distants. Vous pouvez ajouter des adresses IP, des plages d'adresses ou des sous-réseaux directement dans le champ **IP** ou sélectionner des jeux d'adresses existants en cliquant sur **Modifier** en regard de **Jeux d'adresses IP**.

Port distant

Numéros des **ports** distants. Si aucun numéro n'est spécifié, la règle s'applique à n'importe quel port. Vous pouvez ajouter un port de communication ou une plage de ports de communication.

Profil

Une règle de pare-feu peut être appliquée à des profils de connexion réseau spécifiques.
Toute : la règle s'applique à toute connexion réseau malgré le profil utilisé.
Sélectionné : la règle sera appliquée à une connexion réseau spécifique en fonction du profil sélectionné. Cochez la case en regard des profils à sélectionner.

Nous créons une nouvelle règle pour autoriser le navigateur Web Firefox à accéder au sites web du réseau Internet/local.
1. Dans la section **Action**, sélectionnez **Action** > **Autoriser**.
2. Dans la section **Application**, spécifiez le **Chemin de l'application** du navigateur web (par exemple C:\Program Files\Firefox\Firefox.exe). NE saisissez PAS uniquement le nom de l'application.
3. Dans la section **Direction**, sélectionnez **Direction** > **Sortie**.
4. Dans la section **Protocole IP**, sélectionnez **TCP et UDP** dans le menu déroulant **Protocole**.
5. Dans la section **Port distant**, ajoutez les numéros de **port** : *80 443* pour permettre la navigation standard.

La modification des règles prédéfinies est limitée.

Détection de modification d'application

La fonctionnalité de détection de modification d'application affiche des notifications si des applications modifiées pour lesquelles il existe une règle de pare-feu tentent d'établir des connexions. La modification d'application est un mécanisme qui remplace temporairement ou définitivement une application d'origine par une autre application à l'aide d'un exécutable différent (protection contre les règles de pare-feu abusives).

Veuillez noter que cette fonctionnalité ne vise pas à détecter les modifications apportées à une application en général. L'objectif est d'éviter de tromper les règles du pare-feu existantes. Seules les applications pour lesquelles il existe des règles du pare-feu spécifiques sont contrôlées.

Pour modifier la **détection de modification d'application**, ouvrez Configurations avancées > **Protections** > **Protection de l'accès réseau Pare-feu** > **Détection de modification d'application**.

Activer la détection de modifications des applications – Si cette option est sélectionnée, le programme surveille les modifications apportées aux applications (mises à jour, infections ou autres modifications). Quand une application modifiée tente d'établir une connexion, vous êtes averti par le pare-feu.

Autoriser la modification d'applications signées (fiables) – N'affiche pas de notification si l'application possède la même signature numérique valide avant et après la modification.

Liste des applications exclues de la détection – Cette fenêtre permet d'ajouter ou de supprimer des applications pour lesquelles les modifications sont autorisées sans notification.

Liste des applications exclues de la détection

Le pare-feu d'ESET Endpoint Security détecte les modifications apportées aux applications pour lesquelles des règles existent (voir Détection de modification d'application).

Dans certains cas, vous pouvez décider de ne pas utiliser cette fonctionnalité pour certaines applications si vous souhaitez les exclure de la vérification par le pare-feu.

Ajouter : ouvre une fenêtre dans laquelle vous pouvez sélectionner une application à ajouter à la liste des applications exclues de la détection des modifications. Vous pouvez effectuer un choix dans une liste d'applications en cours d'exécution avec une communication réseau ouverte pour laquelle une règle de pare-feu existe. Vous pouvez également ajouter une application spécifique.

Modifier : ouvre une fenêtre dans laquelle vous pouvez modifier l'emplacement d'une application qui figure dans la liste des applications exclues de la détection des modifications. Vous pouvez effectuer un choix dans une liste d'applications en cours d'exécution avec une communication réseau ouverte pour laquelle une règle de pare-feu existe. Vous pouvez également modifier l'emplacement manuellement.

Supprimer : supprime des entrées de la liste des applications exclues de la détection des modifications.

Protection contre les attaques réseau (IDS)

La protection contre les attaques réseau (IDS) améliore la détection des exploits pour rechercher des vulnérabilités connues. Pour en savoir plus sur la protection contre les attaques réseau, consultez le Glossaire. Pour configurer la protection contre les attaques réseau, ouvrez Configurations avancées > **Protections** > **Protection de l'accès réseau** > **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 contre les botnets, consultez le Glossaire.

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

Tous les événements importants détectés par la protection du réseau sont enregistrés dans un fichier journal. Pour plus d'informations, consultez le journal de la protection du réseau.

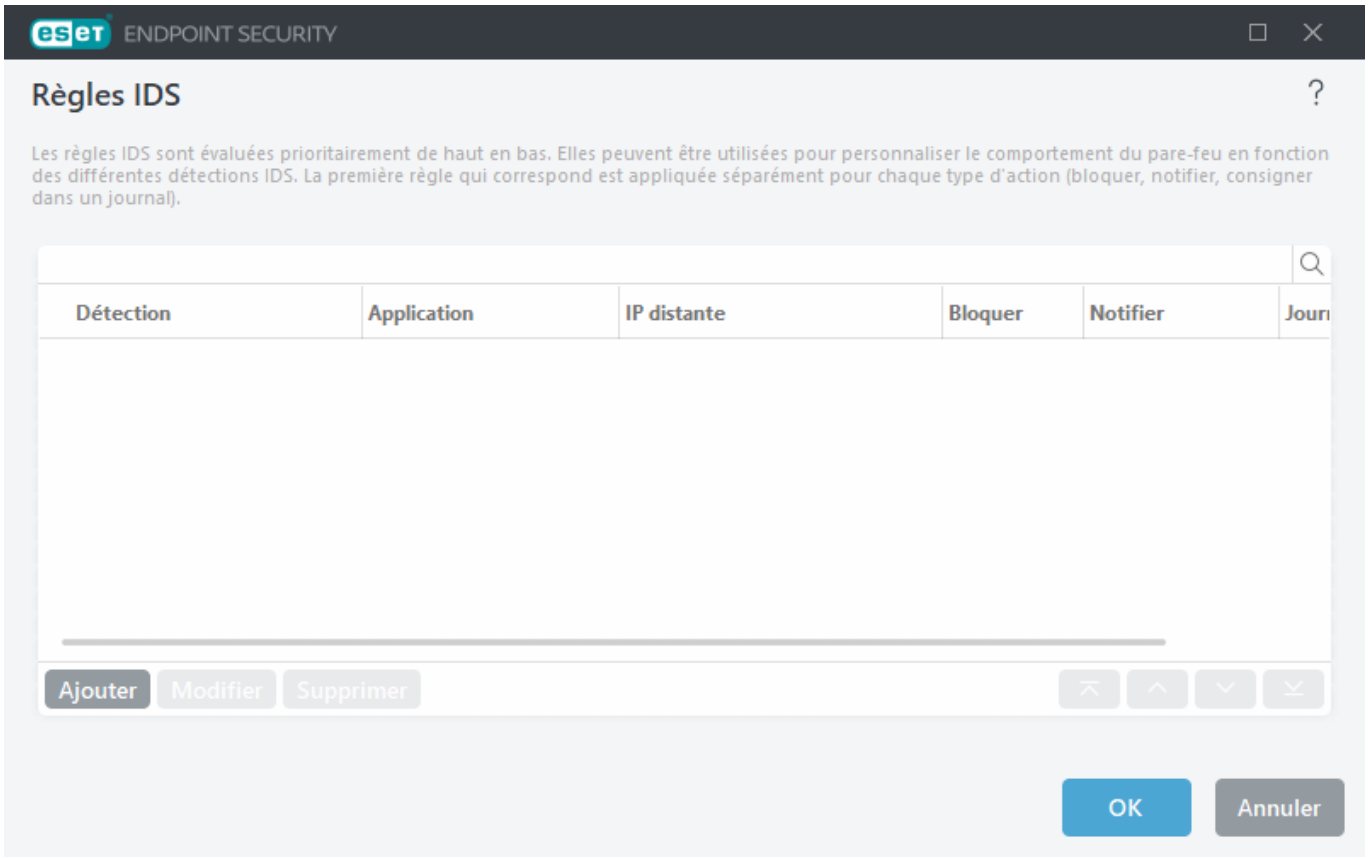
Règles IDS

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.

Les articles suivants de la base de connaissances ESET peuvent être disponibles uniquement en anglais :
- Créer des règles IDS sur les postes de travail clients dans ESET Endpoint Security
- Créer des règles IDS pour les postes de travail clients dans ESET PROTECT On-Prem

Gestion des règles IDS

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



Des **exclusions** d'onglet s'affichent si un administrateur crée des exclusions IDS dans la console web ESET PROTECT On-Prem Web Console. Les exclusions IDS peuvent contenir des règles uniquement et sont évaluées avant les règles IDS.

Éditeur de règle

Détection : type de détection.

Nom de la menace : vous pouvez spécifier un nom de menace pour certaines des détections disponibles.

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 une virgule.

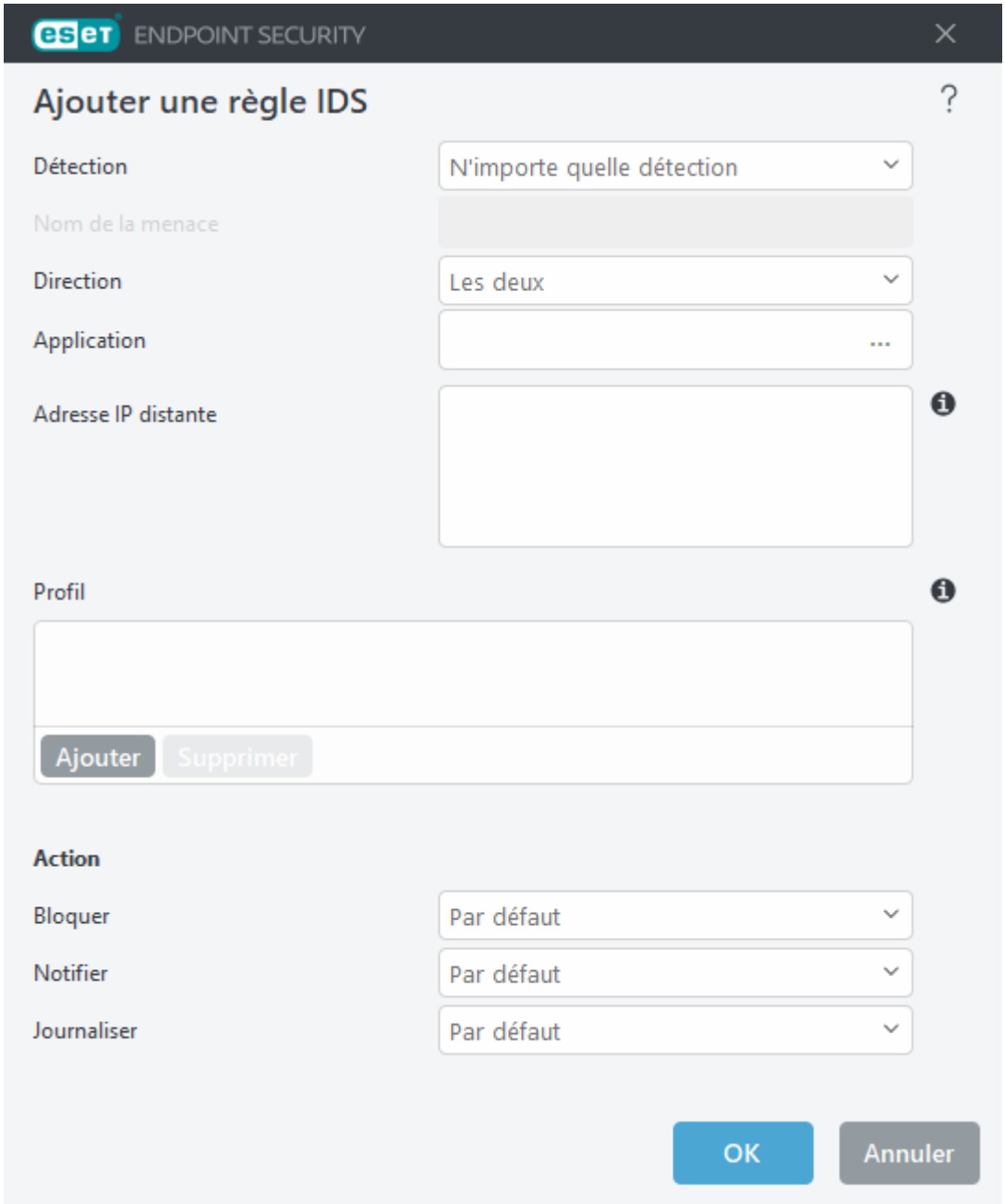
Profil : vous pouvez choisir un profil de connexion réseau auquel cette règle s'appliquera.

Action

Bloquer : chaque processus système possède son propre comportement et une action affectée (bloquer ou autoriser). Pour remplacer le comportement par défaut de ESET Endpoint Security, 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 Security. Sélectionnez **Non** si vous ne souhaitez pas consigner les événements. Les valeurs disponibles sont **Par défaut/Oui/Non**.



Vous souhaitez afficher une notification et créer un journal chaque fois que l'événement se produit :
1. Cliquez sur **Ajouter** pour ajouter une règle IDS.
2. Sélectionnez une alerte spécifique dans le menu déroulant **Détection**.
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 Security.
5. Définissez les menus déroulants **Notifier** et **Consigner** sur **Oui**.
6. Cliquez sur **OK** pour enregistrer cette notification.

Vous souhaitez supprimer les notifications récurrentes pour un type de détection 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 **Détection**, par exemple **Session SMB sans extensions de sécurité** ou **Attaque par balayage de ports TCP**.
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.

Protection contre les attaques par force brute

La protection contre les attaques par force brute bloque les attaques par devinette de mot de passe pour les services RDP et SMB. Une attaque par force brute est une méthode permettant de deviner un mot de passe ciblée en essayant systématiquement toutes les combinaisons de lettres, de chiffres et de symboles. Pour configurer la protection contre les attaques par force brute, ouvrez Configurations avancées > **Protections** > **Protection de l'accès réseau** > **Protection contre les attaques réseau** > **Protection contre les attaques par force brute**.

Activer la protection contre les attaques par force brute : ESET Endpoint Security inspecte le contenu du trafic réseau et bloque les tentatives d'attaques par devinette de mot de passe.

Règles : permettent de créer, de modifier et d'afficher des règles pour les connexions réseau entrantes et sortantes. Pour plus d'informations, consultez Règles.

Exclusions : liste des détections exclues définies par une adresse IP ou un chemin d'accès d'application. Vous pouvez créer et modifier des exclusions dans ESET PROTECT On-Prem. Pour plus d'informations, consultez Exclusions.

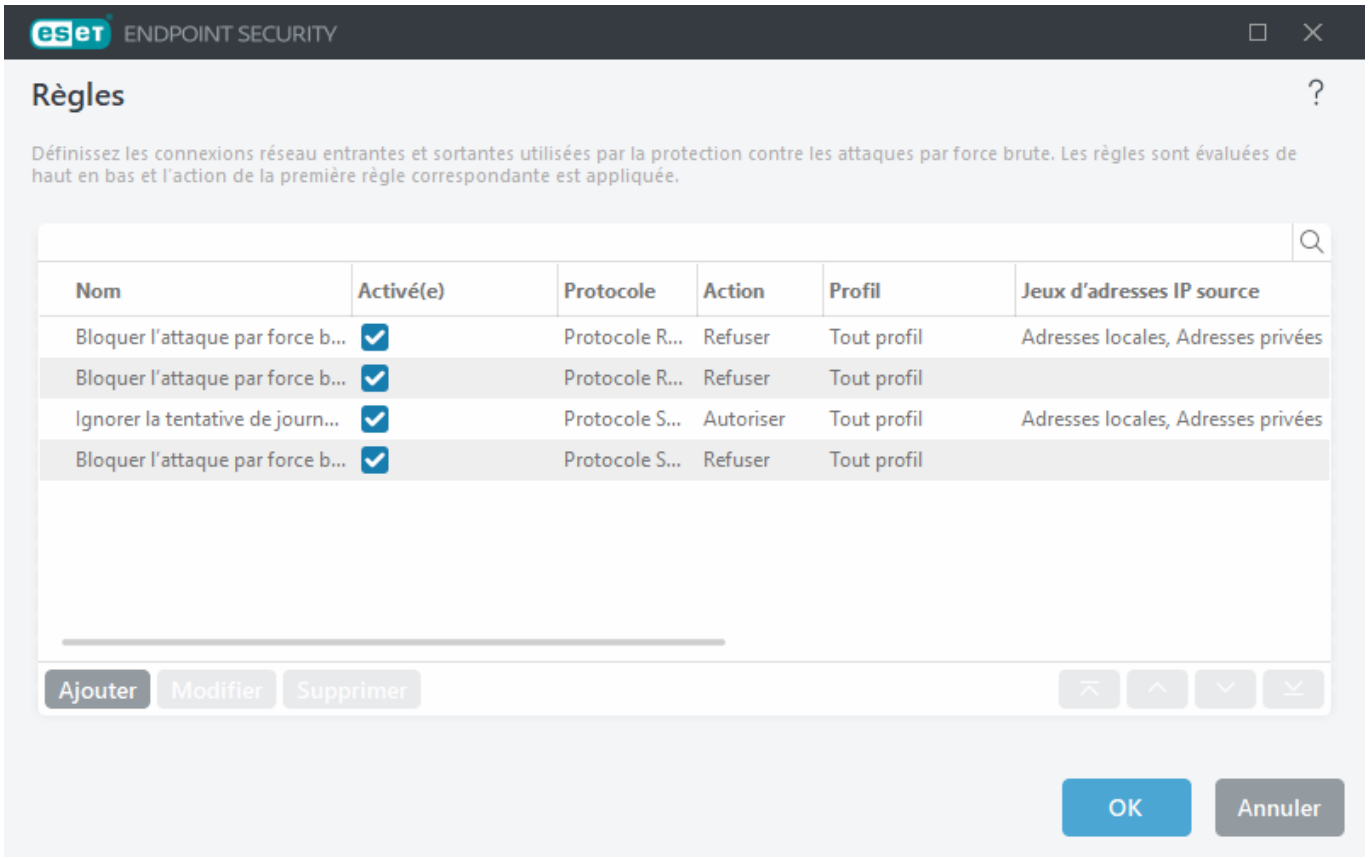
Pour plus d'informations sur la protection contre les attaques par force brute, consultez l'article Guide de sécurité numérique d'ESET.

Règles

Les règles de protection contre les attaques par force brute vous permettent de créer, de modifier et d'afficher des règles pour les connexions réseau entrantes et sortantes. Les règles prédéfinies ne peuvent pas être modifiées ni supprimées.

Gestion des règles de protection contre les attaques par force brute

- **Ajouter** : cliquez sur cette option pour créer une règle de protection contre les attaques par force brute.
- **Modifier** : cliquez sur cette bouton pour modifier une règle existante de protection contre les attaques par force brute.
- **Supprimer** : cliquez sur cette option si vous souhaitez supprimer une exception existante de la liste des règles IDS.
- **Haut/Monter/Bas/Descendre** : permet d'ajuster le niveau de priorité des règles.



> Pour garantir la meilleure protection possible, la règle de blocage ayant la valeur **Nombre maximal de tentatives** la plus faible est appliquée même si la règle est positionnée plus bas dans la liste des règles lorsque plusieurs règles de blocage correspondent aux conditions de détection.

Éditeur de règle

Nom : nom de la règle.

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

Action : choisissez de **refuser** ou d'**autoriser** la connexion si les paramètres de la règle sont respectés.

Protocole : protocole de communication que cette règle inspecte.

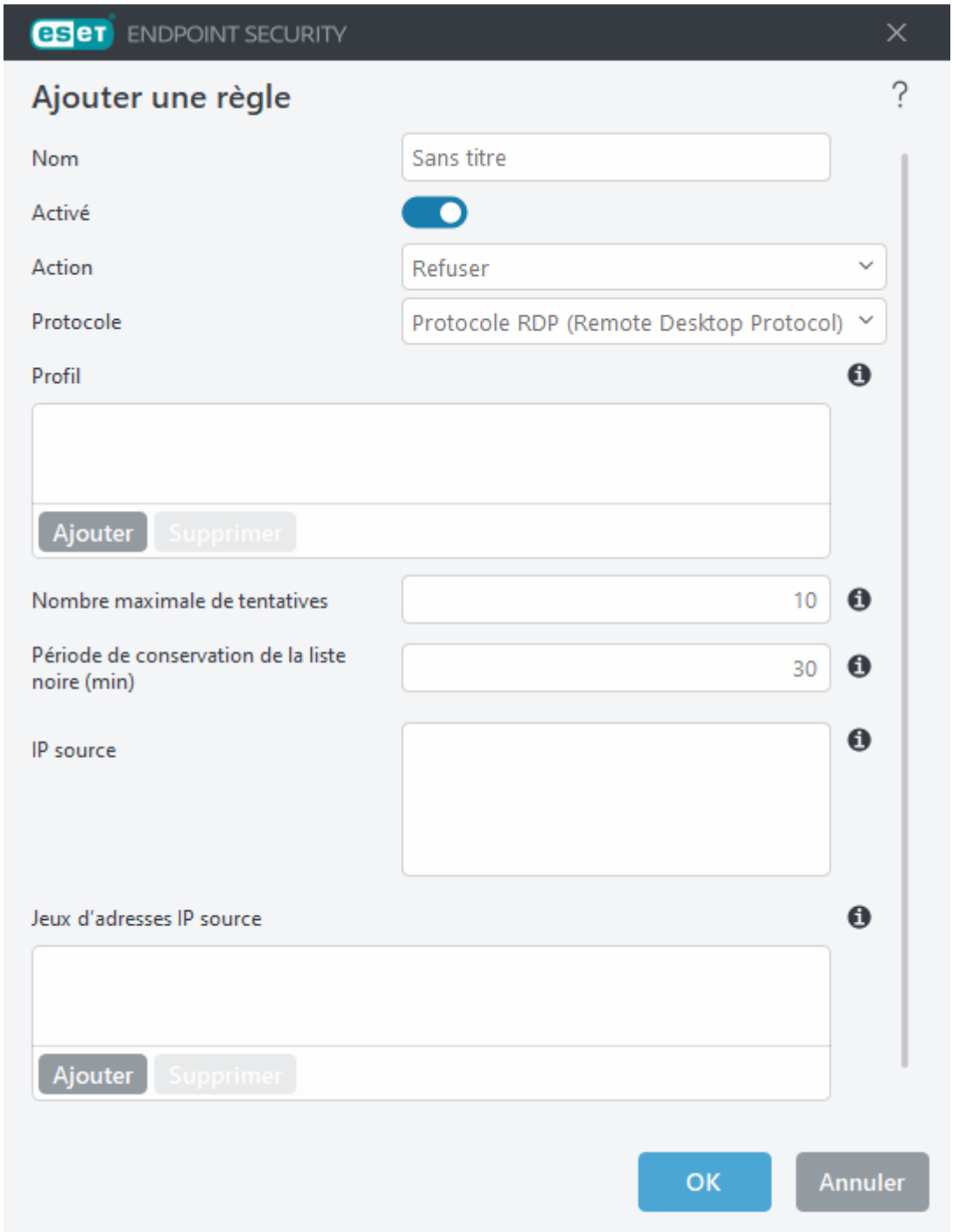
Profil : vous pouvez choisir un profil de connexion réseau auquel cette règle s'appliquera.

Nombre maximale de tentatives : Nombre maximal de tentatives autorisées de répétition d'attaques jusqu'à ce que l'adresse IP soit bloquée et ajoutée à la liste noire.

Période de conservation de la liste noire (min) : définit la date et l'heure d'expiration de l'adresse dans la liste noire.

IP source : liste des sous-réseaux, des plages et des adresses IP. Plusieurs adresses doivent être séparées par une virgule.

Jeux d'adresses IP source : jeu d'adresses IP que vous avez déjà défini dans les jeux d'adresses IP.



Exclusions

Les exclusions de force brute peuvent être utilisées pour supprimer la détection de force brute pour des critères spécifiques. Ces exclusions sont créées dans ESET PROTECT On-Prem en fonction de la détection de force brute.

Colonnes

- **Détection** : type de détection.
- **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 une virgule.

Gestion des exclusions

Les exclusions s'affichent si un administrateur crée des exclusions de force brute dans la console web ESET PROTECT On-Prem Web Console. Les exclusions peuvent contenir des règles uniquement et sont évaluées avant les règles IDS.

Options avancées

Dans Configurations avancées > **Protections** > **Protection de l'accès réseau** > **Protection contre les attaques réseau** > **Options avancées**, vous pouvez activer ou désactiver la détection de plusieurs types d'attaques et d'exploits susceptibles d'endommager votre ordinateur.

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.

Certaines options spécifiques de cette fenêtre peuvent varier selon le type ou la version de votre produit ESET et du module de pare-feu ainsi que de la version de votre système d'exploitation.

Détection d'intrusion

- **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).
- **Détection d'attaque par empoisonnement ARP** – Détection d'attaque par empoisonnement ARP déclenchée par des attaques man-in-the-middle ou détection de sniffing au niveau du commutateur réseau. Le protocole ARP (Address Resolution Protocol) est utilisé par une application ou un périphérique réseau pour déterminer l'adresse Ethernet.
- **Détection d'attaque par analyse de ports TCP/UDP** – Détecte les attaques des applications d'analyse de ports, conçues pour sonder les ports ouverts d'un ordinateur hôte en envoyant des requêtes client vers une plage d'adresses de ports dans le but de découvrir des ports actifs et d'exploiter la vulnérabilité du

service. Pour en savoir plus sur ce type d'attaque, consultez le glossaire.

- **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. Vous pouvez définir la **Période de conservation de la liste noire** , qui définit la durée pendant laquelle l'adresse sera bloquée après la détection de l'attaque.
- **Avertir lors de la détection d'une attaque** – Active une notification qui apparaît dans la zone de notification Windows, 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

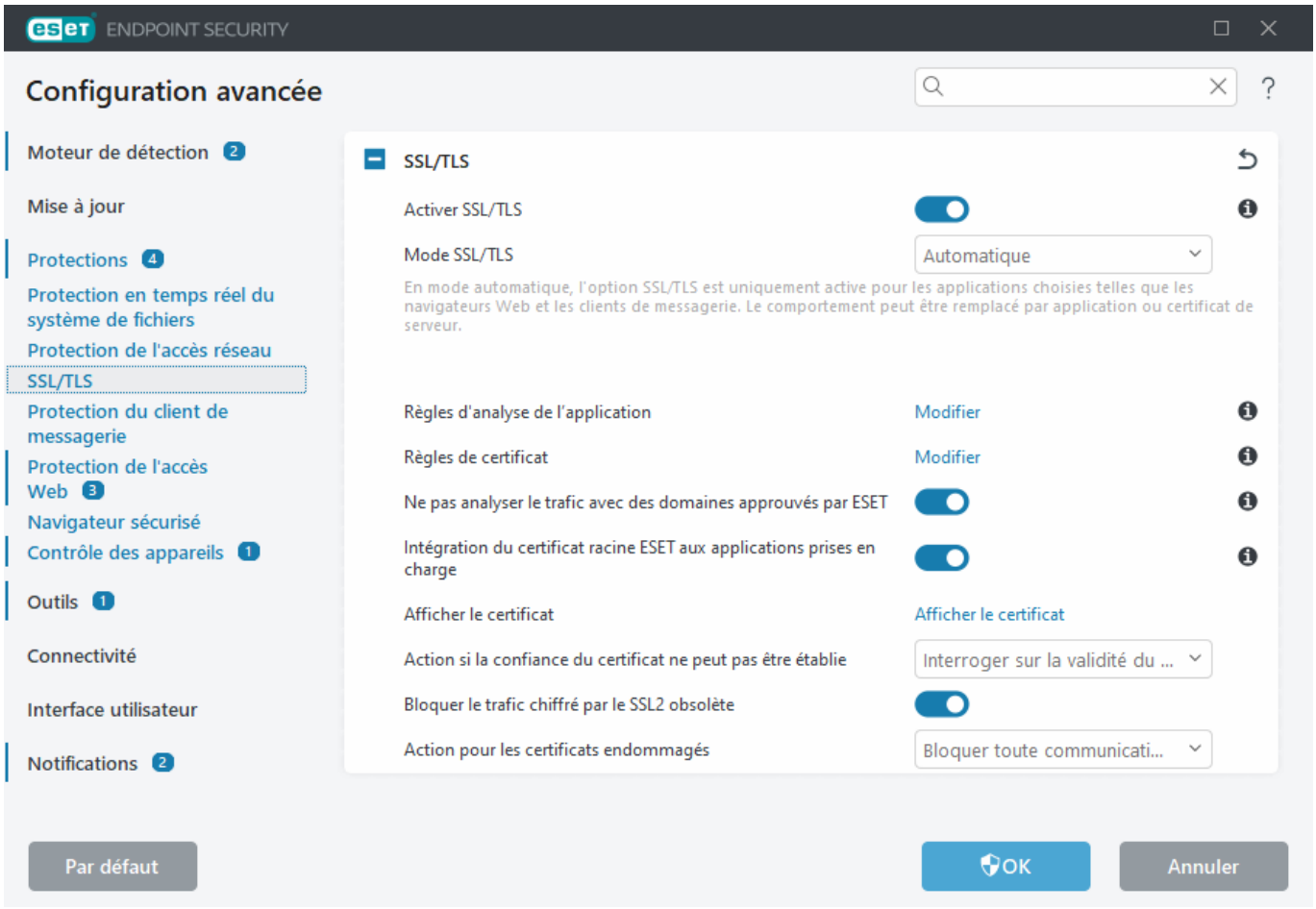
- **Autoriser les connexions entrantes aux partages administratifs du protocole SMB** : les partages administratifs sont les partages réseau par défaut qui partagent les partitions de disque dur (*C$*, *D$*, ...) au sein du système, ainsi que le répertoire système (*ADMIN$*). Désactiver la connexion 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.
- **Refuser l'ouverture de fichiers exécutables sur un serveur hors de la zone Fiable dans le protocole SMB** – Refuse la connexion lorsque vous tentez d'ouvrir un fichier exécutable (.exe, .dll, etc.) à partir d'un dossier partagé du serveur qui n'appartient pas à la zone Fiable dans le pare-feu. Veuillez noter que la copie de fichiers exécutables depuis des sources fiables peut être légitime. Toutefois, cette détection devrait limiter les risques issus de l'ouverture involontaire d'un fichier sur un serveur malveillant (par exemple en cas de clic d'un utilisateur sur un lien hypertexte menant à un fichier exécutable partagé malveillant).
- **Refuser l'authentification NTLM dans le protocole SMB pour la connexion d'un serveur à l'intérieur ou à l'extérieur de la zone Fiable** – Les protocoles qui utilisent les schémas d'authentification NTLM (toutes versions) sont sujets à des attaques par transfert d'identifiants (connues sous le nom d'attaques par relai SMB dans le cas du protocole SMB). Refuser l'authentification NTLM avec un serveur hors de la zone Fiable devrait limiter les risques de transfert d'identifiants par un serveur malveillant hors de la zone Fiable. De la même façon, vous pouvez refuser l'authentification NTLM avec des serveurs dans la zone Fiable.
- **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** : autres services MSRPC. 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).

SSL/TLS

ESET Endpoint Security peut rechercher les menaces de communication qui utilisent le protocole SSL. Vous pouvez utiliser plusieurs modes de filtrage pour examiner les communications SSL protégées à l'aide de certificats approuvés, de certificats inconnus ou de certificats exclus de la vérification des communications SSL protégées. Pour modifier les paramètres SSL/TLS, ouvrez Configurations avancées > **Protections** > **SSL/TLS**.



Activer SSL/TLS : si cette option est désactivée, ESET Endpoint Security n'analyse pas les communications sur SSL/TLS.

Le mode SSL/TLS est disponible dans les options suivantes :

Mode de filtrage	Description
Automatique	Ce mode par défaut n'analyse que les applications appropriées telles que les navigateurs Web et les clients de messagerie. Vous pouvez le remplacer en sélectionnant les applications dans lesquelles les communications sont analysées.
Interactif	Si vous entrez un nouveau site protégé par SSL (avec un certificat inconnu), une boîte de dialogue de sélection d'action s'affiche. Ce mode vous permet de créer la liste des certificats SSL/applications qui seront exclus de l'analyse.
Basé sur des politiques	Sélectionnez cette option pour analyser toutes les communications SSL protégées, à l'exception des communications protégées par des certificats exclus de la vérification. Si une nouvelle communication utilisant un certificat signé inconnu est établie, vous n'êtes pas informé et la communication est automatiquement filtrée. Lorsque vous accédez à un serveur disposant d'un certificat non approuvé indiqué comme approuvé (il figure dans la liste des certificats approuvés), la communication vers le serveur est autorisée et le contenu du canal de communication est filtré.

Règles d'analyse de l'application : permet de personnaliser le comportement d'ESET Endpoint Security pour des applications spécifiques.

Règles de certificat : permet de personnaliser le comportement d'ESET Endpoint Security pour des certificats SSL spécifiques.

Ne pas analyser le trafic avec des domaines approuvés par ESET : lorsque cette option est activée, les communications avec les domaines approuvés sont exclues de l'analyse. Une liste blanche intégrée gérée par ESET détermine la fiabilité d'un domaine.

Intégration du certificat racine ESET aux applications prises en charge : pour que la communication SSL fonctionne correctement dans les navigateurs/clients de messagerie, il est essentiel d'ajouter le certificat racine pour ESET à la liste des certificats racines connus (éditeurs). Lorsque cette option est activée, ESET Endpoint Security ajoute automatiquement le certificat ESET SSL Filter CA aux navigateurs connus (Opera par exemple). Pour les navigateurs utilisant le magasin de certification système, le certificat est ajouté automatiquement. Par exemple, Firefox est automatiquement configuré pour approuver les autorités racines dans le magasin de certification système.

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

Action si la confiance du certificat ne peut pas être établie : dans certains cas, un certificat de site web ne peut pas être vérifié à l'aide du magasin TRCA (par exemple, un certificat arrivé à expiration, un certificat non approuvé, un certificat non valide pour le domaine spécifique ou une signature qui peut être analysée mais qui ne signe pas correctement le certificat). Les sites web légitimes utilisent toujours des certificats approuvés. S'ils n'en fournissent pas, cela peut signifier qu'un pirate déchiffre vos communications ou que le site web connaît des difficultés techniques.

Si **Interroger sur la validité du certificat** est activé (sélectionné par défaut), vous êtes invité à sélectionner une action lorsque la communication chiffrée est établie. Une boîte de dialogue de sélection d'action apparaît ; vous pouvez marquer le certificat comme étant fiable ou exclu. Si le certificat ne figure pas dans la liste TRCA, la fenêtre est rouge. S'il y figure, la fenêtre est verte.

Vous pouvez sélectionner **Bloquer toute communication utilisant le certificat** pour toujours mettre fin à la connexion chiffrée au site utilisant le certificat non approuvé.

Bloquer le trafic chiffré par le SSL2 obsolète : les communications utilisant la version antérieure du protocole SSL seront automatiquement bloquées.

Action pour les certificats endommagés : un certificat endommagé est un certificat qui utilise un format non reconnu par ESET Endpoint Security ou qui a été reçu endommagé (par exemple, écrasé par des données aléatoires). Dans ce cas, nous recommandons de conserver l'option **Bloquer toute communication utilisant le certificat** activée. Si l'option **Interroger sur la validité du certificat** est sélectionnée, l'utilisateur est invité à sélectionner une action à exécuter lorsque la communication chiffrée est établie.

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

Règles d'analyse de l'application

Les **Règles d'analyse de l'application** peuvent être utilisées pour personnaliser le comportement d'ESET Endpoint Security pour des applications spécifiques et mémoriser les actions choisies lorsque le **Mode SSL/TLS** est en **Mode interactif**. La liste peut être consultée et modifiée dans Configurations avancées > **Protections** > **SSL/TLS** > **Règles d'analyse de l'application** > **Modifier**.

La fenêtre **Règles d'analyse de l'application** comprend les éléments suivants :

Colonnes

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

Action d'analyse – Sélectionnez **Analyser** ou **Ignorer** pour analyser ou ignorer la communication. Sélectionnez **Automatique** pour effectuer une analyse en mode automatique et demander quelle action entreprendre en mode interactif. Sélectionnez **Demander** pour demander toujours à l'utilisateur quelle action effectuer.

Éléments de commande

Ajouter – Ajoute une application filtrée.

Modifier – Sélectionnez l'application à configurer, puis cliquez sur **Modifier**.

Supprimer – Sélectionnez l'application à supprimer, puis cliquez sur **Supprimer**.

Importer/Exporter – Importez des applications depuis un fichier ou enregistrez votre liste actuelle d'applications dans un fichier.

OK/Annuler – Cliquez sur **OK** si vous souhaitez enregistrer les modifications. Sinon, cliquez sur **Annuler** pour quitter sans enregistrer.

Règles de certificat

Les **Règles de certificat** peuvent être utilisées pour personnaliser le comportement d'ESET Endpoint Security pour des certificats SSL spécifiques et mémoriser les actions choisies lorsque le **Mode SSL/TLS** est en **Mode interactif**. La liste peut être consultée et modifiée dans Configurations avancées > **Protections** > **SSL/TLS** > **Règles de certificat** > **Modifier**.

La fenêtre **Règles de certificat** est composée des éléments suivants :

Colonnes

Nom : nom du certificat.

Émetteur du certificat : nom du créateur du certificat.

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

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

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

Éléments de commande

Ajouter : Ajoutez un nouveau certificat et définissez ses paramètres en ce qui concerne l'accès et les options d'analyse.

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

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

OK/Annuler – Cliquez sur **OK** si vous souhaitez enregistrer les modifications. Sinon, cliquez sur **Annuler** pour quitter sans enregistrer.

Trafic réseau chiffré

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

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

n'est pas considéré comme étant approuvé.

Lorsque l'option **Mode SSL/TLS** est définie sur **Mode interactif**, une boîte de dialogue demande pour chaque site web d'**analyser** ou d'**ignorer** le trafic. Certaines applications vérifient que le trafic SSL n'est ni modifié ni inspecté par quelqu'un. Dans ce cas, ESET Endpoint Security 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 Windows
> • « Trafic réseau chiffré : certificat non approuvé » s'affiche lors de la consultation de pages web

Dans les deux cas, l'utilisateur peut choisir de mémoriser l'action sélectionnée. Les actions enregistrées sont stockées dans les règles de certificat.

Protection du client de messagerie

Pour configurer la protection du client de messagerie, ouvrez Configurations avancées > **Protections** > **Protection du client de messagerie** et choisissez une option de configuration parmi les suivantes :

- Protection du transport des messages
- Protection des boîtes aux lettres
- Gestion des listes d'adresses
- ThreatSense

Protection du transport des messages

Les protocoles IMAP(S) et POP3(S) sont les protocoles les plus répandus qui permettent de recevoir des e-mails dans une application cliente de messagerie. Le protocole IMAP (Internet Message Access Protocol) est un autre protocole Internet pour la récupération des e-mails. IMAP présente certains avantages par rapport à POP3, par exemple, plusieurs clients peuvent se connecter simultanément à la même boîte aux lettres et conserver des informations sur l'état des messages, telles que le type de lecture, de réponse ou de suppression des messages. Le module de protection qui fournit ce contrôle est automatiquement initié au démarrage du système et est alors actif dans la mémoire.

ESET Endpoint Security protège ces protocoles, quel que soit le client de messagerie utilisé, sans avoir à reconfigurer le client de messagerie. Par défaut, toutes les communications via les protocoles POP3 et IMAP sont analysées, quels que soient les numéros de port POP3/IMAP par défaut.
Le protocole MAPI n'est pas analysé. Toutefois, les communications avec le serveur Microsoft Exchange peuvent être analysées par le module d'intégration dans les clients de messagerie tels que Microsoft Outlook.

> ESET Endpoint Security prend également en charge l'analyse des protocoles IMAPS (585, 993) et POP3S (995) qui utilisent un canal chiffré pour transférer des informations entre un serveur et un client. ESET Endpoint Security contrôle la communication à l'aide des protocoles SSL (Secure Socket Layer) et TLS (Transport Layer Security).
> Les communications chiffrées seront analysées par défaut. Pour consulter la configuration de l'analyseur, ouvrez Configurations avancées > **Protections** > SSL/TLS.

Pour configurer la protection du transport des messages, ouvrez Configurations avancées > **Protections** > **Protection du client de messagerie** > **Protection du transport des messages**.

Activer la protection du transport des messages : lorsque cette option est activée, les communications du transport des messages sont analysées par ESET Endpoint Security.

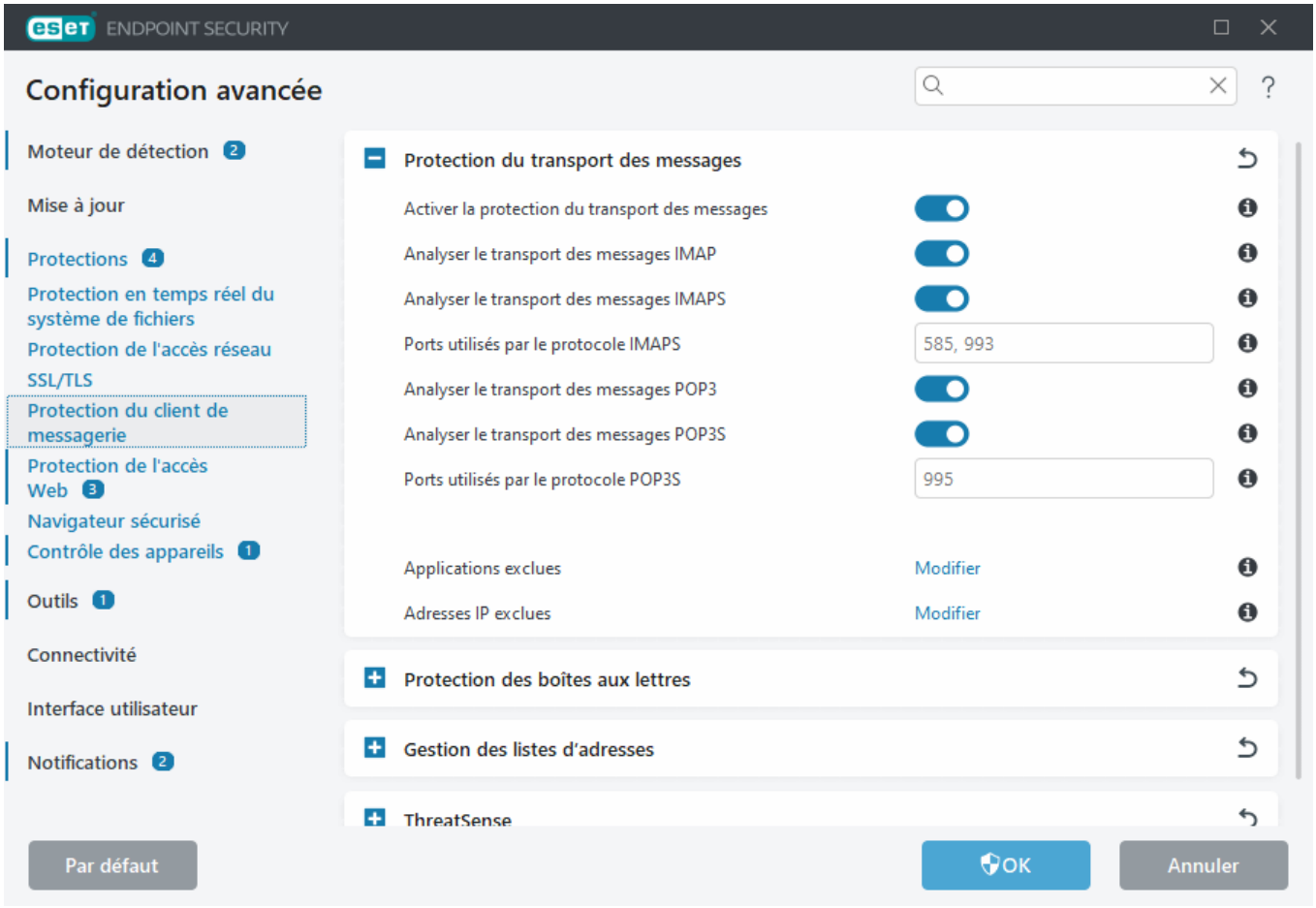
Vous pouvez choisir les protocoles de transport des messages qui seront analysés en cliquant sur le bouton bascule situé en regard des options suivantes (par défaut, l'analyse de tous les protocoles est activée) :

- **Analyser le transport des messages IMAP**
- **Analyser le transport des messages IMAPS**
- **Analyser le transport des messages POP3**
- **Analyser le transport des messages POP3S**

Par défaut, ESET Endpoint Security analyse les communications IMAPS et POP3S sur les ports standard. Pour ajouter des ports personnalisés pour les protocoles IMAPS et POP3S, ajoutez-les au champ de texte en regard de **Ports utilisés par le protocole IMAPS** ou **Ports utilisés par le protocole POP3S**. Plusieurs numéros de ports doivent être séparés par une virgule.

Applications exclues : permet d'exclure des applications spécifiques de l'analyse par la protection du transport des messages. Cette option s'avère utile lorsque la protection de l'accès web entraîne des problèmes de compatibilité.

Adresses IP exclues : permet d'exclure des adresses distantes spécifiques de l'analyse par la protection du transport des messages. Cette option s'avère utile lorsque la protection de l'accès web entraîne des problèmes de compatibilité.



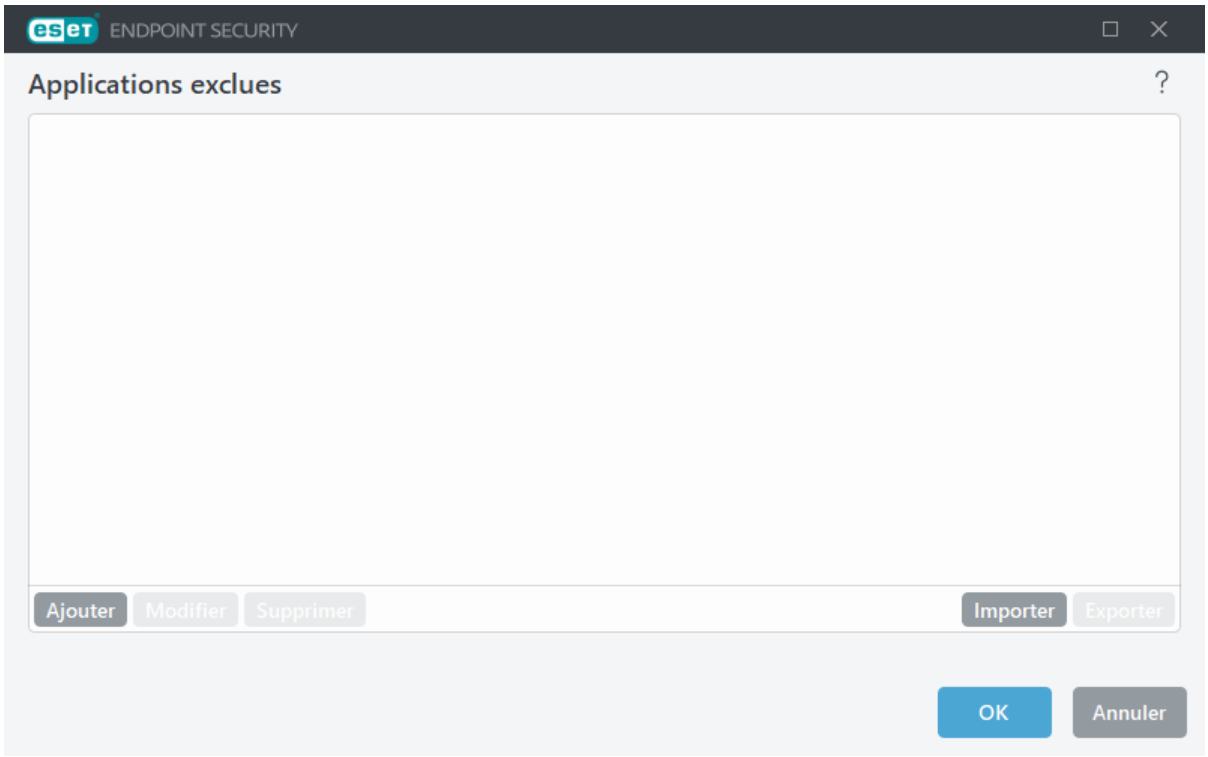
Applications exclues

Pour exclure l'analyse des communications pour des applications spécifiques, ajoutez-les à la liste. Les communications HTTP(S)/POP3(S)/IMAP(S) liées aux adresses sélectionnées ne font pas l'objet d'une détection des menaces. Il est recommandé d'utiliser cette option uniquement pour les applications qui ne fonctionnent pas correctement lorsque leur communication est vérifiée.

L'exécution des applications et des services est disponible automatiquement lorsque vous cliquez sur **Ajouter**. Cliquez sur **...** et accédez à une application pour ajouter manuellement l'exclusion.

Modifier – Modifie les entrées sélectionnées de la liste.

Supprimer – Supprime les entrées sélectionnées de la liste.



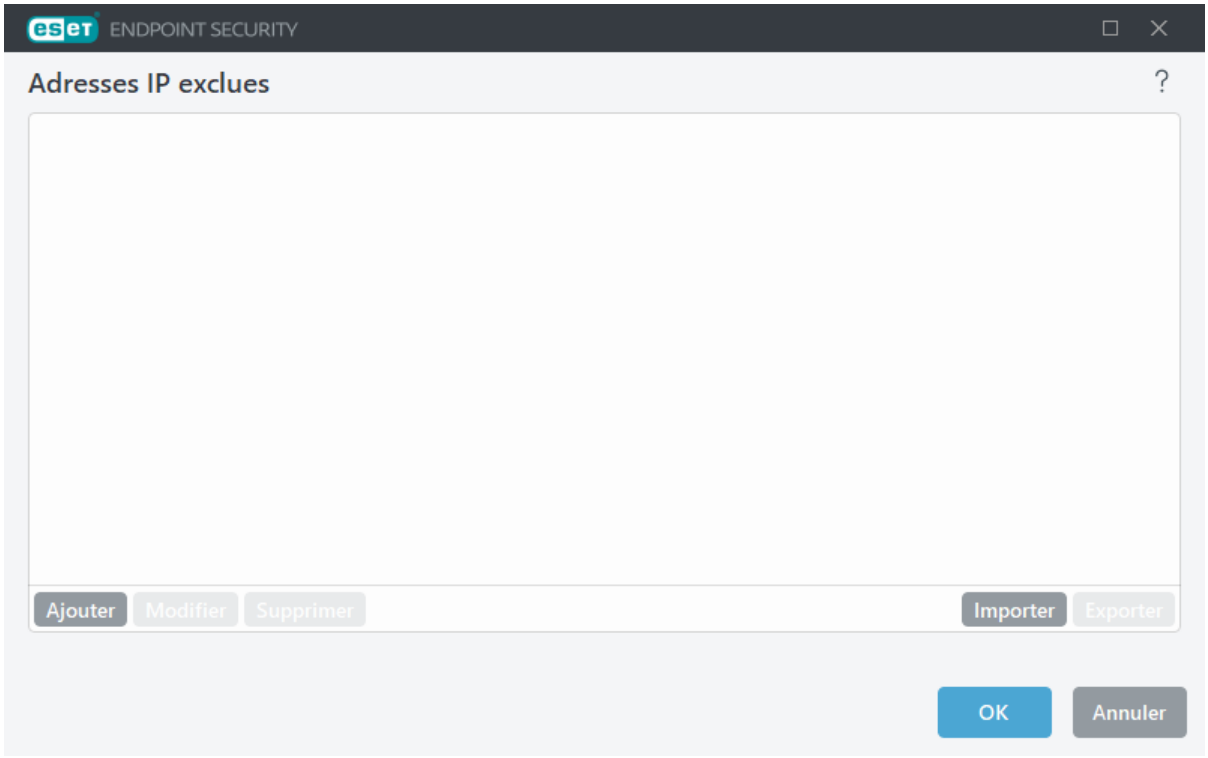
Adresses IP exclues

Les adresses figurant dans cette liste sont exclues de l'analyse. Les communications HTTP(S)/POP3(S)/IMAP(S) liées aux adresses sélectionnées ne font pas l'objet d'une détection des menaces. Il est recommandé d'utiliser cette option uniquement pour les adresses que vous savez être fiables.

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.



Exemples d'adresses IP

Ajouter une adresse IPv4:

Adresse unique – Ajoute l'adresse IP d'un ordinateur (par exemple, *192.168.0.10*).

Plage d'adresses – Saisissez l'adresse IP de début et de fin pour définir la plage IP de plusieurs ordinateurs (par exemple *192.168.0.1 à 192.168.0.99*).

Sous-réseau – Le sous-réseau (groupe d'ordinateurs) est défini par une adresse IP et un masque. Par exemple, 255.255.255.0 est le masque de réseau pour le sous-réseau 192.168.1.0. Pour exclure tout le type de sous-réseau dans *192.168.1.0/24*.

Ajouter une adresse IPv6:

Adresse unique – Ajoute l'adresse IP d'un ordinateur auquel la règle doit être appliquée, par exemple *2001:718:1c01:16:214:22ff:fec9:ca5*.

Sous-réseau – Le sous-réseau (groupe d'ordinateurs) est défini par une adresse IP et un masque (par exemple : *2002:c0a8:6301:1::1/64*).

Protection des boîtes aux lettres

L'intégration d'ESET Endpoint Security à votre boîte aux lettres augmente le niveau de protection active contre le code malveillant dans les e-mails.

Pour configurer la protection des boîtes aux lettres, ouvrez Configurations avancées > **Protections** > **Protection du client de messagerie** > **Protection des boîtes aux lettres**.

Activer la protection de la messagerie par les modules d'extension clients – Lorsque cette option est désactivée, la protection par les modules d'extension des clients de messagerie est désactivée.

Sélectionnez les e-mails à analyser :

- **Courrier reçu**
- **Courrier envoyé**
- **Courrier lu**

- **E-mail modifié**

> Il est recommandé de conserver l'option **Activer la protection de la messagerie par les modules d'extension clients** activée. Même si l'intégration n'est pas activée ou fonctionnelle, les communications par messagerie demeurent protégées par la protection du transport des messages (IMAP/IMAPS et POP3/POP3S).

Rechercher du courrier indésirable

Le courrier non sollicité, ou courrier indésirable, constitue l'un des plus grands problèmes liés à la communication électronique. Le spam représente jusqu'à 30 % de toutes les communications par messagerie électronique. L'antispam des clients de messagerie sert de protection contre ce problème. En combinant plusieurs principes de sécurité de messagerie, l'antispam des clients de messagerie garantit un meilleur filtrage pour que votre boîte de réception reste saine. La détection du courrier indésirable reconnaît le courrier non sollicité d'après des listes prédéfinies d'adresses fiables (autorisées) et de courrier indésirable (bloquées).

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

Activer l'antispam des clients de messagerie – Lorsque cette option est activée, les messages reçus sont analysés pour rechercher du courrier indésirable.

Utiliser l'outil de recherche de courrier indésirable avancé – Des données antispam supplémentaires seront téléchargées périodiquement, ce qui augmentera les capacités antispam et donnera de meilleurs résultats.

Consignation du score définissant un message comme étant du courrier indésirable – Le moteur du blocage de courrier indésirable ESET Endpoint Security attribue à chaque message analysé un score de courrier indésirable. Le message est enregistré dans le journal de l'antispam (fenêtre principale du programme > **Outils** > **Fichiers journaux** > **Antispam des clients de messagerie**).

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

> Lorsque vous cliquez sur un message dans le dossier de courrier indésirable, vous pouvez sélectionner **Reclassifier les messages comme NON-courrier indésirable** pour le déplacer vers la boîte de réception. Lorsque vous cliquez sur un message que vous identifiez comme étant du courrier indésirable dans la boîte de réception, sélectionnez **Reclassifier les messages comme courrier indésirable** pour le déplacer vers le dossier de courrier indésirable. Vous pouvez sélectionner plusieurs messages et agir simultanément sur tous.

Intégrations : vous permet d'intégrer la protection des boîtes aux lettres à votre client de messagerie. Pour plus d'informations, consultez Intégrations.

Réponse : permet de personnaliser la gestion du courrier indésirable. Pour plus d'informations, consultez Réponse.

Intégrations

L'intégration d'ESET Endpoint Security au client de messagerie augmente le niveau de protection active contre le code malveillant dans les e-mails. Si votre client de messagerie est pris en charge, vous pouvez activer l'intégration dans ESET Endpoint Security. Une fois le produit intégré à votre client de messagerie, la barre d'outils d'ESET Endpoint Security est insérée directement dans le client de messagerie, ce qui permet une protection plus efficace des messages. Pour modifier les paramètres d'intégration, ouvrez Configurations avancées > **Protections** > **Protection du client de messagerie Protection des boîtes aux lettres** > **Intégration**.

Intégrer à Microsoft Outlook : Microsoft Outlook est actuellement le seul client de messagerie pris en charge. La protection de la messagerie fonctionne comme un module d'extension. L'avantage principal du plugin réside dans le fait qu'il est indépendant du protocole utilisé. Lorsqu'un client de messagerie reçoit un message chiffré, il le déchiffre et l'envoie au scanner de virus. Pour obtenir la liste complète des versions de Microsoft Outlook prises en charge, consultez cet article de la base de connaissances ESET

Traitement avancé du client de messagerie : traite les événements Outlook Messaging API (MAPI) supplémentaires : Objet modifié (`fnevObjectModified`) and Objet créé (`fnevObjectCreated`). Si vous constatez un ralentissement du système lors de l'utilisation du client de messagerie, désactivez cette option.

Barre d'outils Microsoft Outlook

La protection Microsoft Outlook fonctionne comme un module d'extension. Une fois ESET Endpoint Security installé, cette barre d'outils contenant la protection antivirus et l'antispam des clients de messagerie options est ajoutée à Microsoft Outlook :

Courrier indésirable – Marque les messages choisis comme étant du courrier indésirable. Après marquage, une « empreinte » du message est envoyée à un serveur central de stockage des signatures de courrier indésirable. Si le serveur reçoit d'autres empreintes semblables de plusieurs utilisateurs, le message est classé ensuite comme courrier indésirable.

Non-courrier indésirable – Marque les messages sélectionnés comme n'étant pas du courrier indésirable.

Adresse de courrier indésirable (bloquée, une liste d'adresses de courrier indésirable) – Ajoute une adresse d'expéditeur à la liste d'adresses en tant qu'adresse bloquée. Tous les messages reçus de la liste sont automatiquement classés comme courrier indésirable.

> ⚠ Prenez garde au « spoofing » : ce système usurpe l'adresse des expéditeurs de messages électroniques afin d'amener les destinataires à les lire et à y répondre.

Adresse fiable (autorisée, une liste d'adresses fiables) – Ajoute une adresse d'expéditeur à la liste d'adresses en tant qu'adresse autorisée. Tous les messages reçus des adresses autorisées ne sont jamais classés automatiquement comme courrier indésirable.

ESET Endpoint Security – Double-cliquez sur l'icône pour ouvrir la fenêtre principale d'ESET Endpoint Security.

Analyser à nouveau les messages – Vous permet de lancer manuellement la vérification des messages. Vous pouvez indiquer les messages à vérifier et activer une nouvelle analyse du message reçu. Pour plus d'informations, consultez Protection des boîtes aux lettres.

Configuration de l'analyseur – Affiche les options de configuration de la protection des boîtes aux lettres.

Configuration du blocage du courrier indésirable – Affiche les options de configuration de la protection des boîtes aux lettres.

Liste d'adresses antispam – Ouvre la fenêtre de la gestion des listes d'adresses dans laquelle vous pouvez accéder à des listes d'adresses exclues, fiables et de courrier indésirable.

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 Security intégrée dans les clients de messagerie permet aux utilisateurs de spécifier plusieurs options pour la vérification du courrier électronique. L'option **Analyser à nouveau les messages** offre deux modes d'analyse :

Tous les messages du dossier en cours – Analyse les messages du dossier affiché.

Messages sélectionnés uniquement – Analyse uniquement les messages marqués par l'utilisateur.

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

Réponse

En fonction des résultats de l'analyse des messages, ESET Endpoint Security peut déplacer les messages analysés ou ajouter du texte personnalisé à leur objet. Vous pouvez configurer ces paramètres dans Configurations avancées > **Protections** > **Protection du client de messagerie** > **Protection des boîtes aux lettres** > **Réponse**.

L'antispam des clients de messagerie d'ESET Endpoint Security permet de configurer les paramètres suivants pour les messages :

Ajouter un texte à l'objet des messages – Permet d'ajouter une chaîne de caractères personnalisée à la ligne de l'objet des messages classés comme courrier indésirable. Le **texte** par défaut est « [SPAM] ».

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

Déplacer vers le dossier personnalisé – Lorsque cette option est activée, le courrier indésirable est déplacé vers un dossier spécifié ci-dessous.

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

Si un message contient une détection, ESET Endpoint Security tente de le nettoyer par défaut. Si le message ne peut pas être nettoyé, vous pouvez choisir une **Action à entreprendre si le nettoyage est impossible** :

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

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

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

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

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

- **Jamais** – Aucune notification ne sera ajoutée.
- **Lorsqu'une détection se produit** – Seuls les messages contenant un code malveillant sont marqués comme contrôlés (valeur par défaut).
- **À tous les e-mails lors de l'analyse** – Le programme ajoute des messages à tous les e-mails analysés.

Mettre à jour l'objet d'un e-mail reçu et lu/Mettre à jour l'objet d'un e-mail envoyé – Activez cette option pour ajouter le texte personnalisé spécifié ci-dessous au message.

Texte ajouté à l'objet des messages détectés – Modifiez ce texte si vous souhaitez modifier le format du préfixe de l'objet d'un e-mail infecté. Cette fonction remplace l'objet du message "Bonjour" au format suivant : « [détection %DETECTIONNAME%] ». La variable %DETECTIONNAME% représente la détection.

Gestion des listes d’adresses

La fonctionnalité antispam des clients de messagerie d'ESET Endpoint Security permet de configurer divers paramètres pour les listes d'adresses. Pour configurer des listes d'adresses, ouvrez Configurations avancées > **Protections** > **Protection du client de messagerie** > **Gestion des listes d'adresses**.

Activer la liste d'adresses de l'utilisateur : activez cette option pour activer la liste d'adresses de l'utilisateur.

Liste d'adresses de l'utilisateur : liste d’adresses e-mail dans laquelle vous pouvez ajouter, modifier ou supprimer des adresses pour définir les règles antispam. Les règles de cette liste seront appliquées à l'utilisateur actuel.

Activer la liste d’adresses globale : activez cette option pour activer la liste d'adresses globale partagée par tous les utilisateurs sur cet appareil.

Liste d'adresses globale : liste d’adresses e-mail dans laquelle vous pouvez ajouter, modifier ou supprimer des adresses pour définir les règles antispam. Les règles de cette liste seront appliquées à tous les utilisateurs.

Autoriser automatiquement et ajouter à la liste d’adresses de l’utilisateur

Traiter les adresses du carnet d'adresses comme des adresses autorisées : Les adresses de votre liste de contacts seront traitées comme des adresses approuvées sans être ajoutées à la liste d'adresses de l'utilisateur.

Ajouter les adresses des destinataires des messages sortants : ajoutez les adresses des destinataires des messages envoyés à la liste d'adresses de l'utilisateur en tant qu'autorisées.

Ajouter les adresses des messages reclassées comme NON-courrier indésirable : ajoutez les adresses des expéditeurs reclassées comme NON-courrier indésirable à la liste d'adresses de l'utilisateur en tant qu'autorisées.

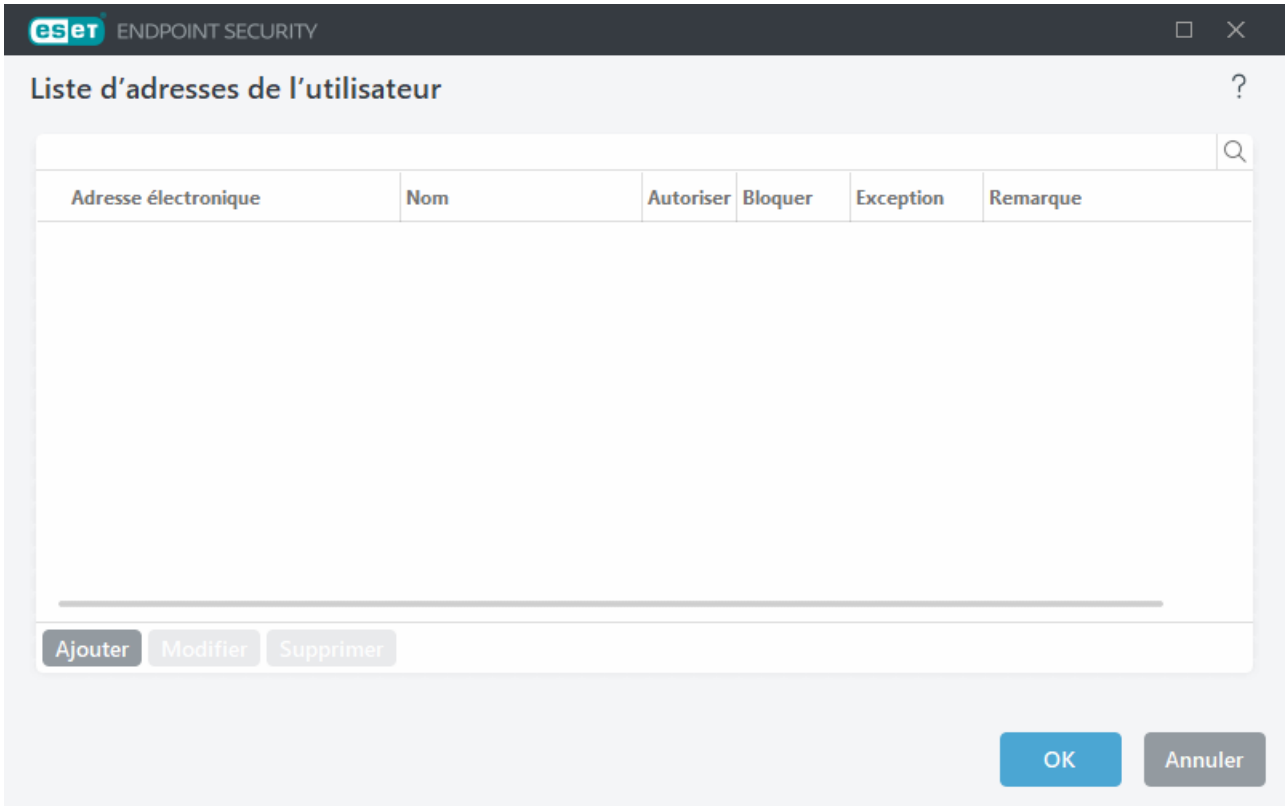
Ajouter automatiquement en tant qu'exception à la liste d’adresses de l’utilisateur

Ajouter les adresses à partir des comptes : ajoutez les adresses des comptes clients de messagerie existants à la à la liste d'adresses de l'utilisateur en tant qu'exception.

Listes d'adresses

Pour vous protéger contre les messages non sollicités, ESET Endpoint Security permet de classer des adresses de messagerie dans des listes d'adresses.

Pour modifier des listes d'adresses, ouvrez Configurations avancées > **Protections** > **Protection du client de messagerie** > **gestion des listes d'adresses**, puis cliquez sur **Modifier** en regard de **Liste d'adresses de l'utilisateur** ou **Liste d'adresses globale**.



Colonnes

Adresse e-mail – Adresse à laquelle la règle s'applique.

Nom – Nom de la règle personnalisée.

Autoriser/Bloquer/Exception – Cases d'option utilisés pour déterminer l'action à entreprendre pour l'adresse e-mail (cliquez sur la case d'option dans la colonne de votre choix pour modifier rapidement l'action) :

- **Autoriser** – Adresses considérées comme sûres et desquelles vous souhaitez recevoir des messages.
- **Bloquer** – Adresses considérées comme dangereuses/indésirables et desquelles vous ne souhaitez pas recevoir de messages.
- **Exception** – Adresses qui font toujours l'objet d'une recherche de courrier indésirable et qui peuvent être usurpées et utilisées pour l'envoi de courrier indésirable.

Note – Informations sur la création de la règle et si elle s'applique à l'ensemble du domaine /domaines de niveau inférieur.

Gestion des adresses

- **Ajouter** – Cliquez sur cette option pour ajouter une règle pour une nouvelle adresse.
- **Modifier** – Sélectionnez et cliquez sur cette option pour modifier une règle existante.
- **Supprimer** – Sélectionnez et cliquez sur cette option si vous souhaitez supprimer une règle de la liste d'adresses.

Ajouter/Modifier une adresse

Cette fenêtre permet d'ajouter ou de modifier une adresse dans la gestion des listes d'adresses et de configurer l'action à entreprendre :

Adresse e-mail – Adresse à laquelle la règle s'applique. Les caractères génériques ne sont pas pris en charge.

Nom – Nom de la règle personnalisée.

Action – Action à entreprendre si l'adresse e-mail du contact correspond à l'adresse spécifiée dans le champ **Adresse e-mail** :

- **Autoriser** – Adresses considérées comme sûres et desquelles vous souhaitez recevoir des messages.
- **Bloquer** – Adresses considérées comme dangereuses/indésirables et desquelles vous ne souhaitez pas recevoir de messages.
- **Exception** – Adresses qui font toujours l'objet d'une recherche de courrier indésirable et qui peuvent être usurpées et utilisées pour l'envoi de courrier indésirable.

Domaine entier – Sélectionnez cette option pour le règle à appliquer à l'intégralité du domaine du contact (pas uniquement à l'adresse spécifiée dans le champ **Adresse e-mail**, mais à toutes les adresses de messagerie du domaine *address.info*).

Domaines de niveau inférieur – Sélectionnez cette option pour le règle à appliquer aux domaines de plus faible niveau du contact (*adresse.info* représente le domaine et *mon.adresse.info* représente un sous-domaine).

Résultat du traitement d'adresse

Lors de l'ajout de nouvelles adresses ou de la modification de l'action entreprise pour l'adresse e-mail, ESET Endpoint Security affiche des messages de notification. Le contenu de ces messages varie en fonction de l'action que vous essayez d'exécuter.

Cochez la case **Ne plus demander** pour exécuter l'action automatiquement sans afficher le message la fois suivante.

ThreatSense

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

les options de configuration de la technologie ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

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

Pour ouvrir la fenêtre de configuration, cliquez sur **ThreatSense** dans les Configurations avancées de chaque module utilisant la technologie ThreatSense (reportez-vous aux informations ci-dessous). Différents scénarios de sécurité peuvent nécessiter des configurations différentes. Dans cette optique, ThreatSense est configurable individuellement pour les modules de protection suivants :

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

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

Objets à analyser

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

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

Secteurs d'amorçage/UEFI – Analyse les secteurs d'amorçage afin de détecter la présence éventuelle de logiciels malveillants dans l'enregistrement d'amorçage principal. Pour plus d'informations sur UEFI, consultez le glossaire.

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

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

Archives auto-extractibles – Les archives auto-extractibles (SFX) sont des archives qui sont extraites automatiquement.

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

Options d'analyse

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

Heuristique – La méthode heuristique utilise un algorithme d'analyse de l'activité (malveillante) des programmes. Elle présente l'avantage d'identifier un code malveillant qui n'existait pas ou qui n'était pas connu par la version antérieure du moteur de détection. Cette méthode présente néanmoins l'inconvénient d'une probabilité (très

faible) de fausses alarmes.

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

Nettoyage

Les paramètres de nettoyage déterminent le comportement d'ESET Endpoint Security 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 d'ThreatSense vous permet de définir les types de fichiers à analyser.

Autre

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

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

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

Consigner tous les objets – Le journal d'analyse affiche tous les fichiers analysés dans des archives auto-extractibles, même ceux qui ne sont pas infectés (peut générer beaucoup de données et augmenter la taille du fichier du journal d'analyse).

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

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

Limites

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

Paramètres d’objet

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

Durée d’analyse maximale pour l’objet (s) – Définit la durée maximale de l’analyse des fichiers dans un objet conteneur (tel qu’une archive RAR/ZIP ou un e-mail avec plusieurs pièces jointes). Ce paramètre ne s’applique pas aux fichiers autonomes. Si une valeur définie par l’utilisateur a été saisie et que le temps s’est écoulé, une analyse s’arrêtera dès que possible, que l’analyse de chaque fichier d’un objet conteneur soit terminée ou non. Dans le cas d'une archive contenant des fichiers volumineux, l'analyse s'arrêtera dès qu'un fichier de l'archive sera extrait (par exemple, lorsqu'une variable définie par l'utilisateur est de 3 secondes, mais que l'extraction d'un fichier prend 5 secondes). Le reste des fichiers de l'archive ne sera pas analysé lorsque ce temps sera écoulé. Pour limiter le temps d'analyse, y compris pour les archives plus volumineuses, utilisez les options **Taille d’objet maximale** et **Taille maximale du fichier dans l'archive** (non recommandé en raison d'éventuels risques de sécurité). Valeur par défaut : illimitée.

Configuration de l’analyse d’archive

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

Taille maximale de fichier dans l'archive – Cette option permet de spécifier la taille maximale des fichiers (après extraction) à analyser contenus dans les archives. La valeur maximale est 3 Go.

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

Protection de l’accès Web

La protection de l'accès web vous permet de configurer les paramètres avancés du module Protection internet. Les options suivantes sont disponibles dans Configurations avancées > **Protections** > **Protection de l'accès web** > **Protection de l'accès web** :

Activer la protection de l'accès web – Lorsque cette option est désactivée, la protection de l'accès web et l'anti-hameçonnage ne sont pas assurés.

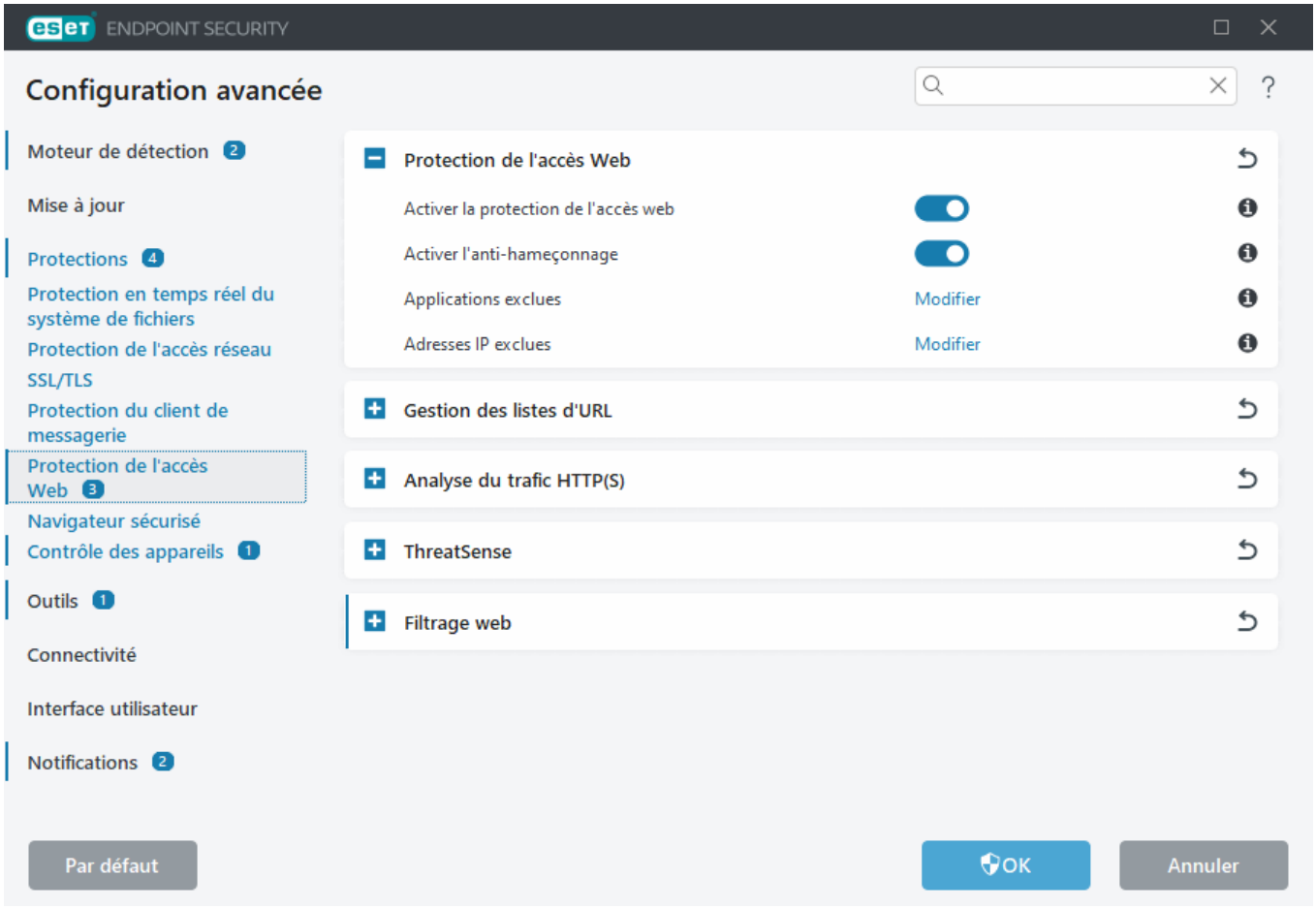
> Nous vous recommandons vivement de laisser la protection de l'accès web activée et de n'exclure aucune application ou adresse IP par défaut.

Analyser les scripts de navigateur : lorsque cette option est activée, le moteur de détection vérifie tous les programmes JavaScript exécutés par des navigateurs web.

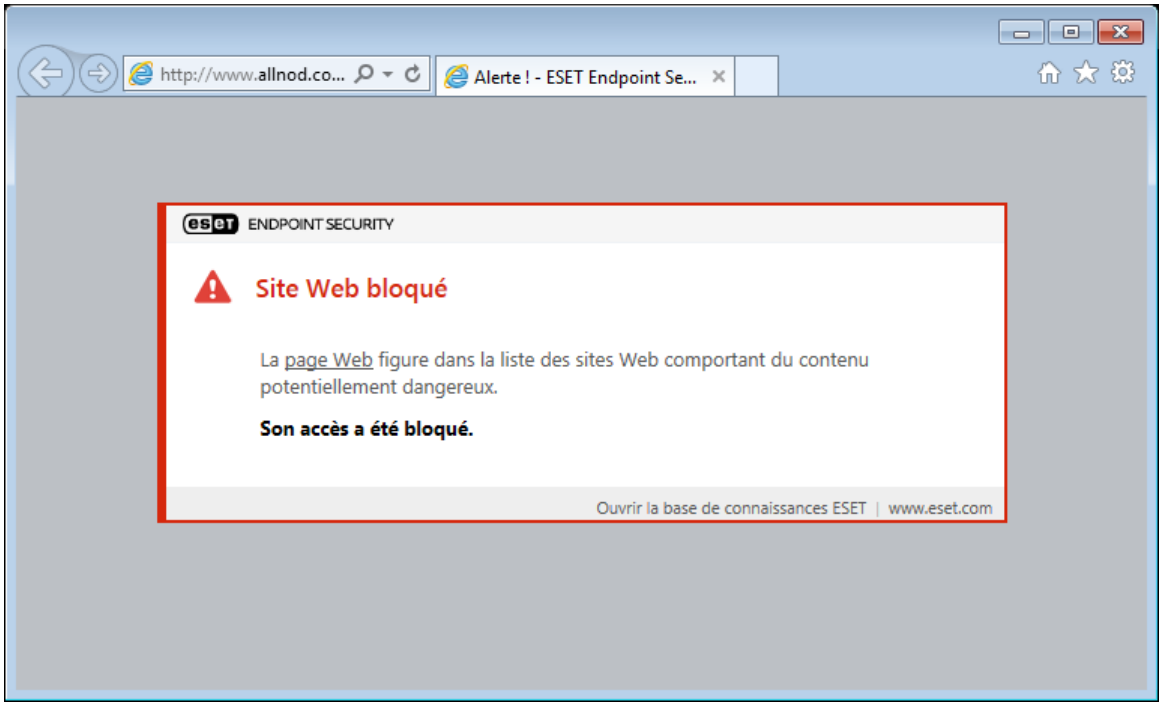
Activer l'anti-hameçonnage : lorsque cette option est activée, les pages web d'hameçonnage sont bloquées. Pour plus d'informations, reportez-vous à la section Protection antihameçonnage.

Applications exclues : permet d'exclure des applications spécifiques de l'analyse par la protection de l'accès web. Cette option s'avère utile lorsque la protection de l'accès web entraîne des problèmes de compatibilité.

Adresses IP exclues : permet d'exclure des adresses distantes spécifiques de l'analyse par la protection de l'accès web. Cette option s'avère utile lorsque la protection de l'accès web entraîne des problèmes de compatibilité.



Lorsque le site web est bloqué, la protection de l'accès web affiche le message suivant dans votre navigateur :



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 Security

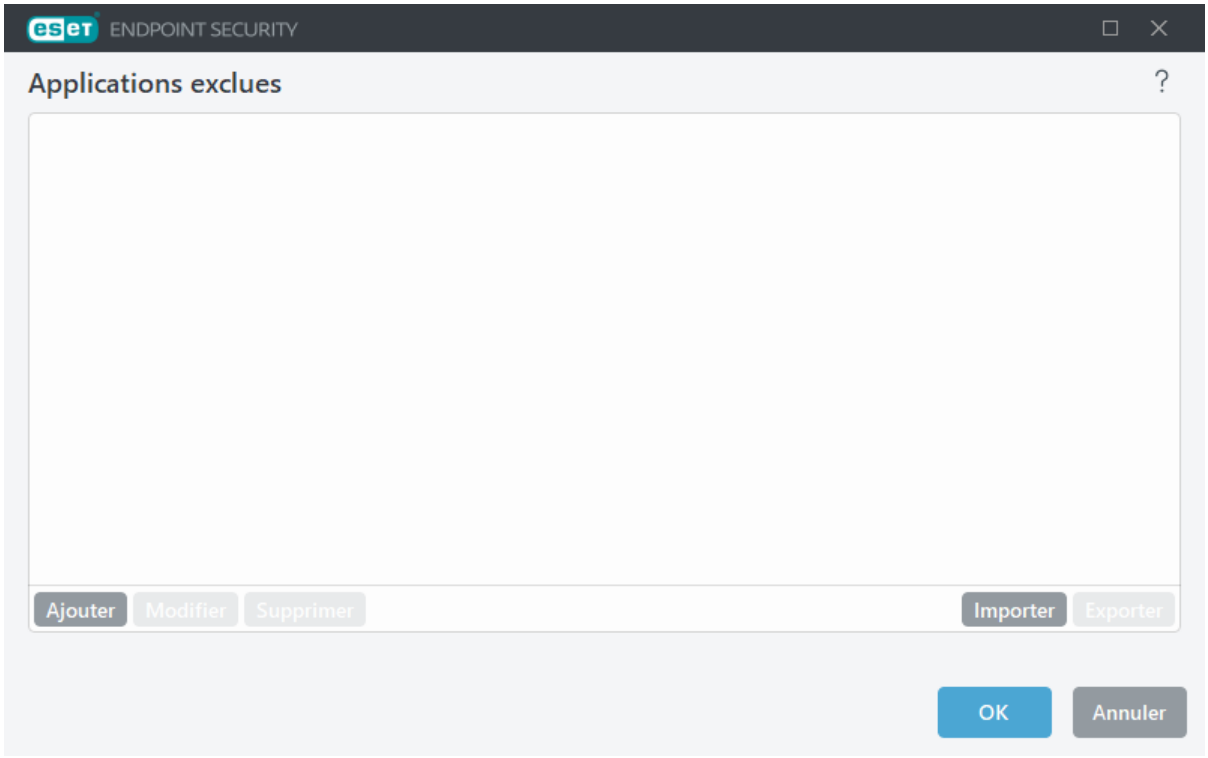
Applications exclues

Pour exclure l'analyse des communications pour des applications spécifiques, ajoutez-les à la liste. Les communications HTTP(S)/POP3(S)/IMAP(S) liées aux adresses sélectionnées ne font pas l'objet d'une détection des menaces. Il est recommandé d'utiliser cette option uniquement pour les applications qui ne fonctionnent pas correctement lorsque leur communication est vérifiée.

L'exécution des applications et des services est disponible automatiquement lorsque vous cliquez sur **Ajouter**. Cliquez sur **...** et accédez à une application pour ajouter manuellement l'exclusion.

Modifier – Modifie les entrées sélectionnées de la liste.

Supprimer – Supprime les entrées sélectionnées de la liste.



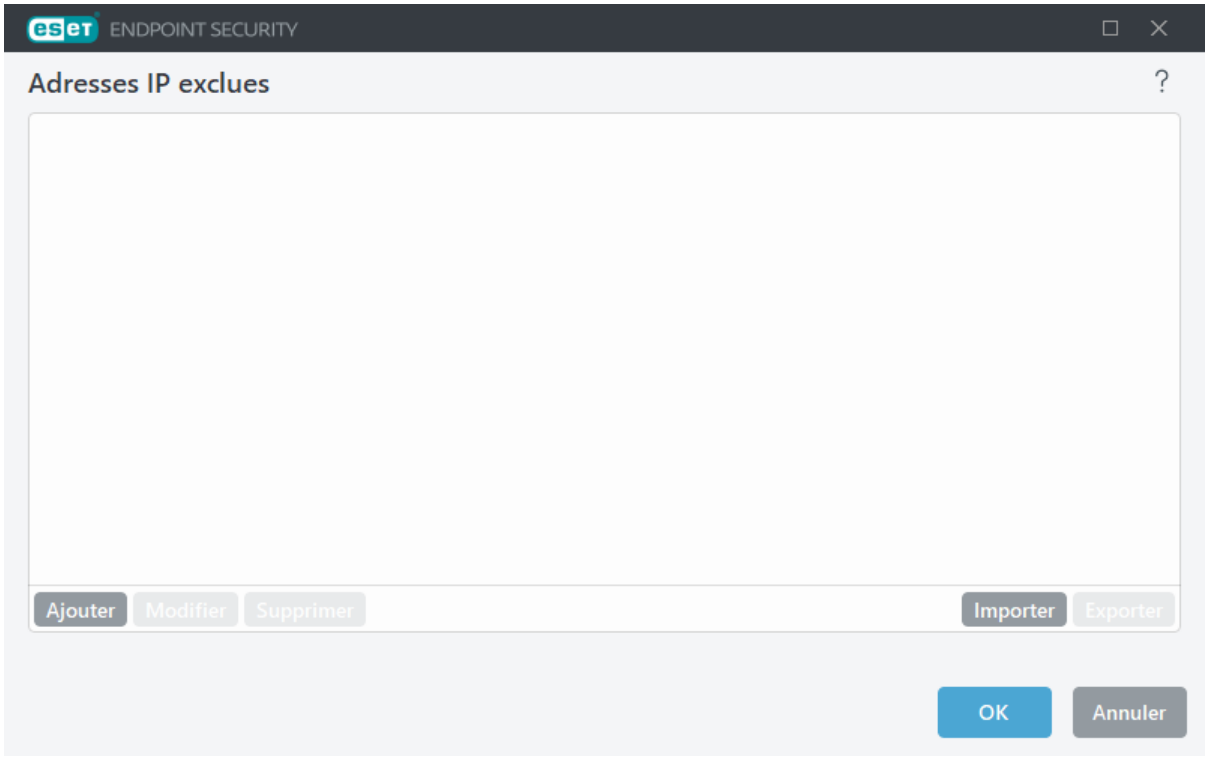
Adresses IP exclues

Les adresses figurant dans cette liste sont exclues de l'analyse. Les communications HTTP(S)/POP3(S)/IMAP(S) liées aux adresses sélectionnées ne font pas l'objet d'une détection des menaces. Il est recommandé d'utiliser cette option uniquement pour les adresses que vous savez être fiables.

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.



Exemples d'adresses IP

Ajouter une adresse IPv4:

Adresse unique – Ajoute l'adresse IP d'un ordinateur (par exemple, *192.168.0.10*).

Plage d'adresses – Saisissez l'adresse IP de début et de fin pour définir la plage IP de plusieurs ordinateurs (par exemple *192.168.0.1 à 192.168.0.99*).

Sous-réseau – Le sous-réseau (groupe d'ordinateurs) est défini par une adresse IP et un masque. Par exemple, 255.255.255.0 est le masque de réseau pour le sous-réseau 192.168.1.0. Pour exclure tout le type de sous-réseau dans *192.168.1.0/24*.

Ajouter une adresse IPv6:

Adresse unique – Ajoute l'adresse IP d'un ordinateur auquel la règle doit être appliquée, par exemple *2001:718:1c01:16:214:22ff:fec9:ca5*.

Sous-réseau – Le sous-réseau (groupe d'ordinateurs) est défini par une adresse IP et un masque (par exemple : *2002:c0a8:6301:1::1/64*).

Gestion des listes d'URL

La **Gestion des listes d'URL** dans Configurations avancées > **Protections** > **Protection de l'accès web** vous permet de spécifier les adresses HTTP à bloquer, autoriser ou exclure de l'analyse du contenu.

L'option SSL/TLS doit être activée si vous souhaitez filtrer les adresses HTTPS en plus des adresses HTTP. Sinon, seuls les domaines des sites HTTPS que vous avez visités sont ajoutés et non l'URL complète.

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

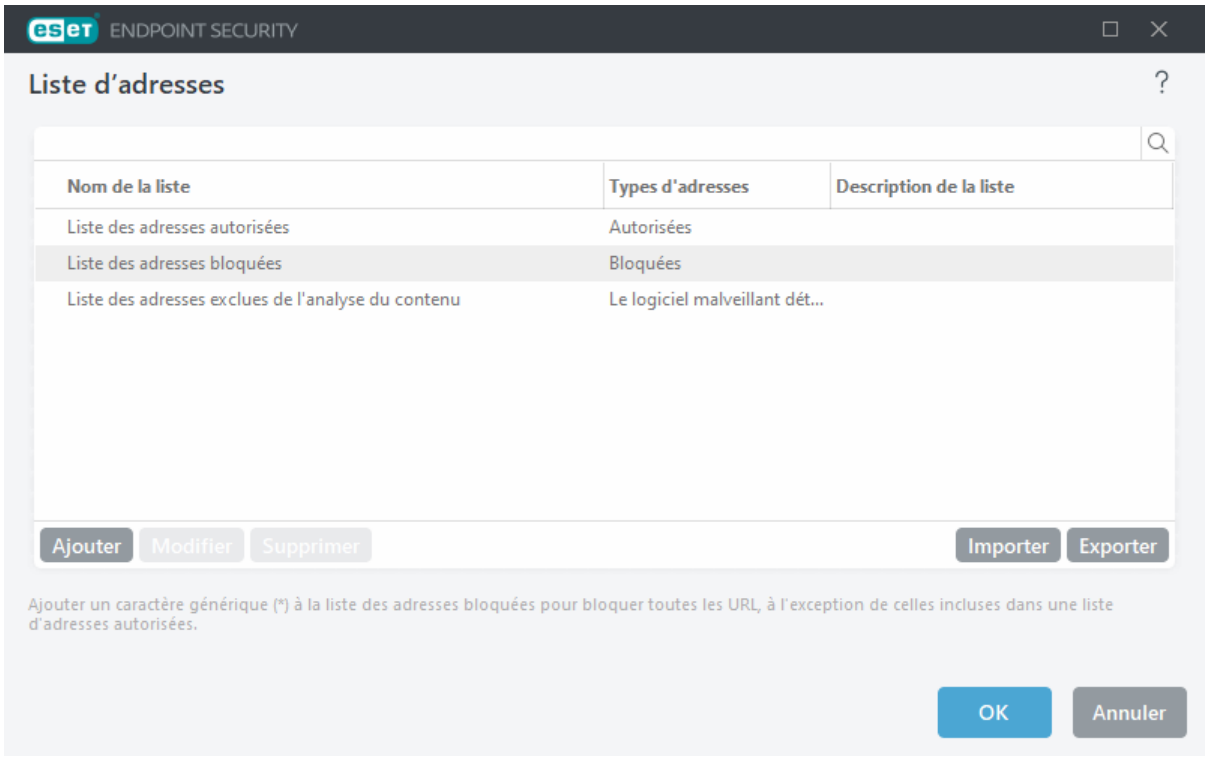
Si vous souhaitez bloquer toutes les adresses HTTP, à l'exception des adresses figurant dans la **liste des adresses autorisées** active, ajoutez un astérisque (*) à la **liste des adresses bloquées** active.

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

quel caractère. Faites attention lors la définition des adresses exclues, car la liste ne doit contenir que des adresses fiables et sûres. De la même manière, veillez à employer correctement les symboles « * » et « ? » dans cette liste. Reportez-vous à Ajout d'un masque de domaine/d'adresse HTTP pour déterminer comment faire correspondre un domaine complet avec tous ses sous-domaines en toute sécurité. Pour activer une liste, sélectionnez l'option **Liste active**. Si vous souhaitez être averti lors de la saisie d'une adresse figurant dans la liste actuelle, sélectionnez l'option **Notifier lors de l'application**.

Adresses approuvées par ESET

Si l'option **Ne pas analyser le trafic avec des domaines approuvés par ESET** est activée, les protocoles SSL/TLS et les domaines sur liste blanche gérés par ESET ne seront pas affectés par la configuration de la gestion des listes d'URL.



Éléments de commande

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

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

Supprimer : permet de supprimer les listes existantes. Cette option n'est disponible que pour les listes créées à l'aide de l'option **Ajouter** et non les listes par défaut.

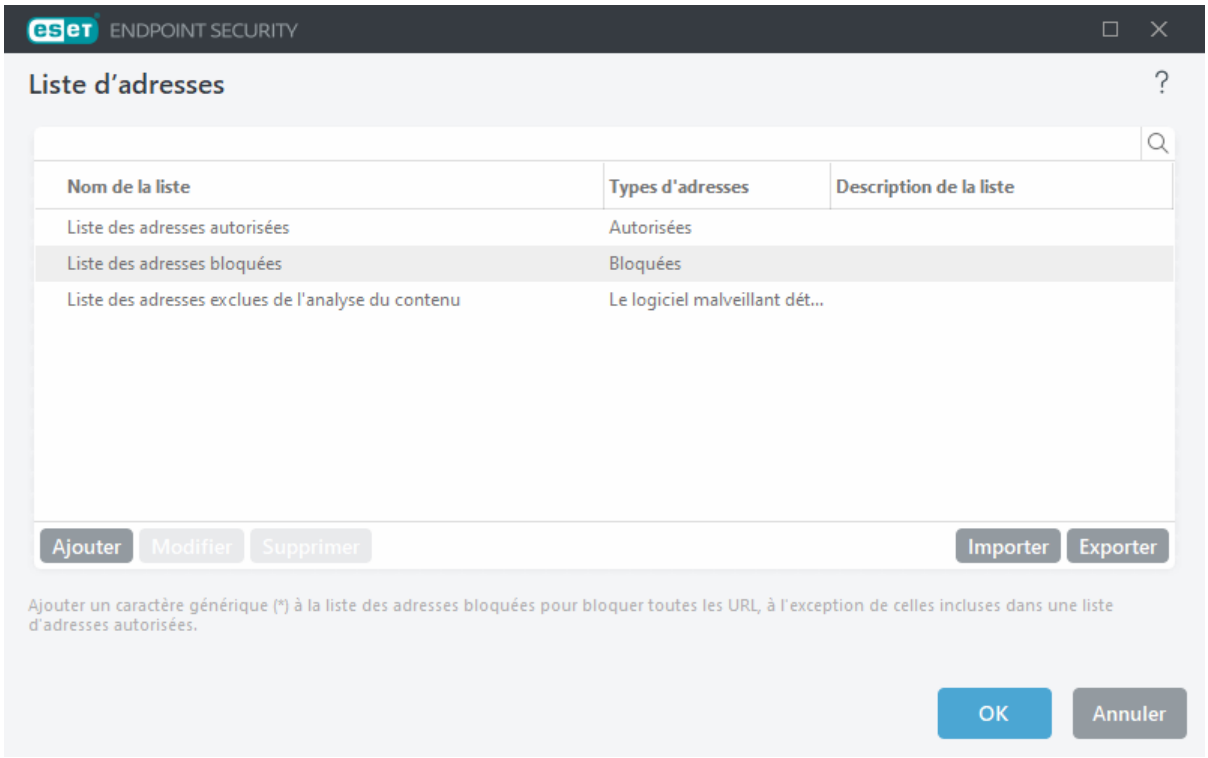
Liste d'adresses

Dans cette section, vous pouvez spécifier des listes d'adresses HTTP(S) qui seront bloquées, autorisées ou exclues de la vérification.

Par défaut, les trois listes suivantes sont disponibles :

- **Liste des adresses exclues de l'analyse du contenu** – Aucune vérification de la présence de code malveillant n'est effectuée pour les adresses répertoriées dans la liste.
- **Liste des adresses autorisées** – Si l'option N'autoriser l'accès qu'aux adresses HTTP figurant dans la liste des adresses autorisées est activée et si la liste des adresses bloquées contient un astérisque (correspond à tout), l'utilisateur n'est autorisé à accéder qu'aux adresses répertoriées dans cette liste. Les adresses de cette liste sont autorisées même si elles sont incluses dans la liste des adresses bloquées.
- **Liste des adresses bloquées** - L'utilisateur n'est pas autorisé à accéder aux adresses répertoriées dans cette liste, à moins qu'elles ne figurent également dans la liste des adresses autorisées.

Cliquez sur **Ajouter** pour créer une liste. Pour supprimer les listes sélectionnées, cliquez sur **Supprimer**.



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 Security

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

Création d'une liste d'adresses

Cette boîte de dialogue permet de configurer une nouvelle liste de masques/adresses URL qui seront, bloqués, autorisés ou exclus de la vérification.

Vous pouvez configurer les options suivantes :

Type de liste d'adresses : trois types de liste sont disponibles :

- **Le logiciel malveillant détecté est ignoré** – Aucune vérification de la présence de code malveillant n'est effectuée pour les adresses répertoriées dans la liste.
- **Bloqué** : l'accès aux adresses spécifiées dans cette liste est bloqué.
- **Autorisé** : l'accès aux adresses répertoriées dans cette liste est autorisé. Les adresses de cette liste sont autorisées même si elles correspondent aux adresses bloquées.

Nom de liste – Spécifiez le nom de la liste. Ce champ n'est pas disponible lors de la modification de l'une des listes prédéfinies.

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

Pour activer une liste, sélectionnez l'option **Liste active** en regard de celle-ci. Si vous souhaitez être averti lorsqu'une liste spécifique est utilisée lors de l'accès à des sites web, sélectionnez l'option **Notifier lors de l'application**. Vous recevrez par exemple une notification lorsqu'un site web sera bloqué ou autorisé en raison de son inclusion dans la liste des adresses bloquées ou autorisées. La notification contient le nom de la liste.

Niveau de verbosité – Sélectionnez le niveau de verbosité dans le menu déroulant. Les entrées avec la verbosité Avertissement peuvent être collectées par ESET PROTECT On-Prem.

Le niveau de détail de la consignation des informations et avertissements n'est disponible que pour les règles qui contiennent au moins deux composants sans caractère générique dans le domaine. Par exemple :
- *.domain.com/*
- *www.domain.com/*

Éléments de commande

Ajouter – Ajoutez une nouvelle adresse URL à la liste (entrez plusieurs valeurs avec un séparateur).

Modifier – Permet de modifier une adresse existante dans la liste. Disponible uniquement pour les adresses créées avec l'option **Ajouter**.

Supprimer – Permet de supprimer des adresses existantes de la liste. Disponible uniquement pour les adresses créées avec l'option **Ajouter**.

Importer – Importez un fichier comportant des adresses URL (séparez les valeurs par un saut de ligne, par exemple *.txt utilisant le codage UTF-8).

Pour plus d'informations, consultez le chapitre Ajout d'un masque d'URL.

Ajout d'un masque d'URL

Consultez les instructions de cette boîte de dialogue pour entrer le masque d'adresse/de domaine souhaité.

ESET Endpoint Security permet de bloquer l'accès à des sites Web spécifiques et d'empêcher le navigateur Internet d'en afficher le contenu. Vous pouvez également 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.).

Par exemple, le masque *x? représente toute adresse ayant un x comme avant-dernier caractère. Pour prendre

en compte le domaine entier, saisissez-le sous la forme **.domain.com/**. La spécification du préfixe du protocole (*http://*, *https://*) dans le masque est facultative. S'il est omis, le masque correspondra à n'importe quel protocole. 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 **.domain.com* ne correspondra pas à *http://anydomain.com/anypath#.domain.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 **.domain.com* correspond également à *http://domain.com*. L'utilisation de **domain.com* serait incorrecte, car ce masque correspondrait aussi à *http://anotherdomain.com*.

Le niveau de détail de la consignation des informations et avertissements n'est disponible que pour les règles qui contiennent au moins deux composants sans caractère générique dans le domaine. Par exemple :
- *.domain.com/*
- *www.domain.com/*

Analyse du trafic HTTP(S)

Par défaut, ESET Endpoint Security est configuré pour analyser le trafic HTTP et HTTPS utilisé par les navigateurs internet et d'autres applications. Vous ne devez désactiver l'analyse du trafic que si vous rencontrez des problèmes liés à des logiciels tiers et que vous souhaitez déterminer si le problème est causé par ESET Endpoint Security.

Activer l'analyse du trafic HTTP – Le trafic HTTP est toujours contrôlé sur tous les ports pour toutes les applications.

Activer l'analyse du trafic HTTPS – Le trafic HTTPS utilise un canal chiffré pour transférer des informations entre un serveur et un client. ESET Endpoint Security contrôle les communications à l'aide des protocoles SSL (Secure Socket Layer) et TLS (Transport Layer Security). Le programme analyse uniquement le trafic sur les ports définis dans **Ports utilisés par le protocole HTTPS**, quelle que soit la version du système d'exploitation (vous pouvez ajouter des ports aux ports prédéfinis 443 et 0 à 65 535).

ThreatSense

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

les options de configuration de la technologie ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

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

Pour ouvrir la fenêtre de configuration, cliquez sur **ThreatSense** dans les Configurations avancées de chaque module utilisant la technologie ThreatSense (reportez-vous aux informations ci-dessous). Différents scénarios de

sécurité peuvent nécessiter des configurations différentes. Dans cette optique, ThreatSense est configurable individuellement pour les modules de protection suivants :

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

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

Objets à analyser

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

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

Secteurs d'amorçage/UEFI – Analyse les secteurs d'amorçage afin de détecter la présence éventuelle de logiciels malveillants dans l'enregistrement d'amorçage principal. Pour plus d'informations sur UEFI, consultez le glossaire.

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

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

Archives auto-extractibles – Les archives auto-extractibles (SFX) sont des archives qui sont extraites automatiquement.

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

Options d’analyse

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

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

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

Nettoyage

Les paramètres de nettoyage déterminent le comportement d'ESET Endpoint Security 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 d'ThreatSense vous permet de définir les types de fichiers à analyser.

Autre

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

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

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

Consigner tous les objets – Le journal d'analyse affiche tous les fichiers analysés dans des archives auto-extractibles, même ceux qui ne sont pas infectés (peut générer beaucoup de données et augmenter la taille du fichier du journal d'analyse).

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

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

Limites

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

Paramètres d’objet

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

Durée d’analyse maximale pour l’objet (s) – Définit la durée maximale de l’analyse des fichiers dans un objet conteneur (tel qu’une archive RAR/ZIP ou un e-mail avec plusieurs pièces jointes). Ce paramètre ne s’applique pas aux fichiers autonomes. Si une valeur définie par l’utilisateur a été saisie et que le temps s’est écoulé, une analyse s’arrêtera dès que possible, que l’analyse de chaque fichier d’un objet conteneur soit terminée ou non. Dans le cas d'une archive contenant des fichiers volumineux, l'analyse s'arrêtera dès qu'un fichier de l'archive sera extrait (par exemple, lorsqu'une variable définie par l'utilisateur est de 3 secondes, mais que l'extraction d'un fichier prend 5 secondes). Le reste des fichiers de l'archive ne sera pas analysé lorsque ce temps sera écoulé. Pour limiter le temps d'analyse, y compris pour les archives plus volumineuses, utilisez les options **Taille d’objet maximale** et **Taille maximale du fichier dans l'archive** (non recommandé en raison d'éventuels risques de sécurité). Valeur par défaut : illimitée.

Configuration de l’analyse d’archive

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

Taille maximale de fichier dans l'archive – Cette option permet de spécifier la taille maximale des fichiers (après extraction) à analyser contenus dans les archives. La valeur maximale est 3 Go.

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

Contrôle Web

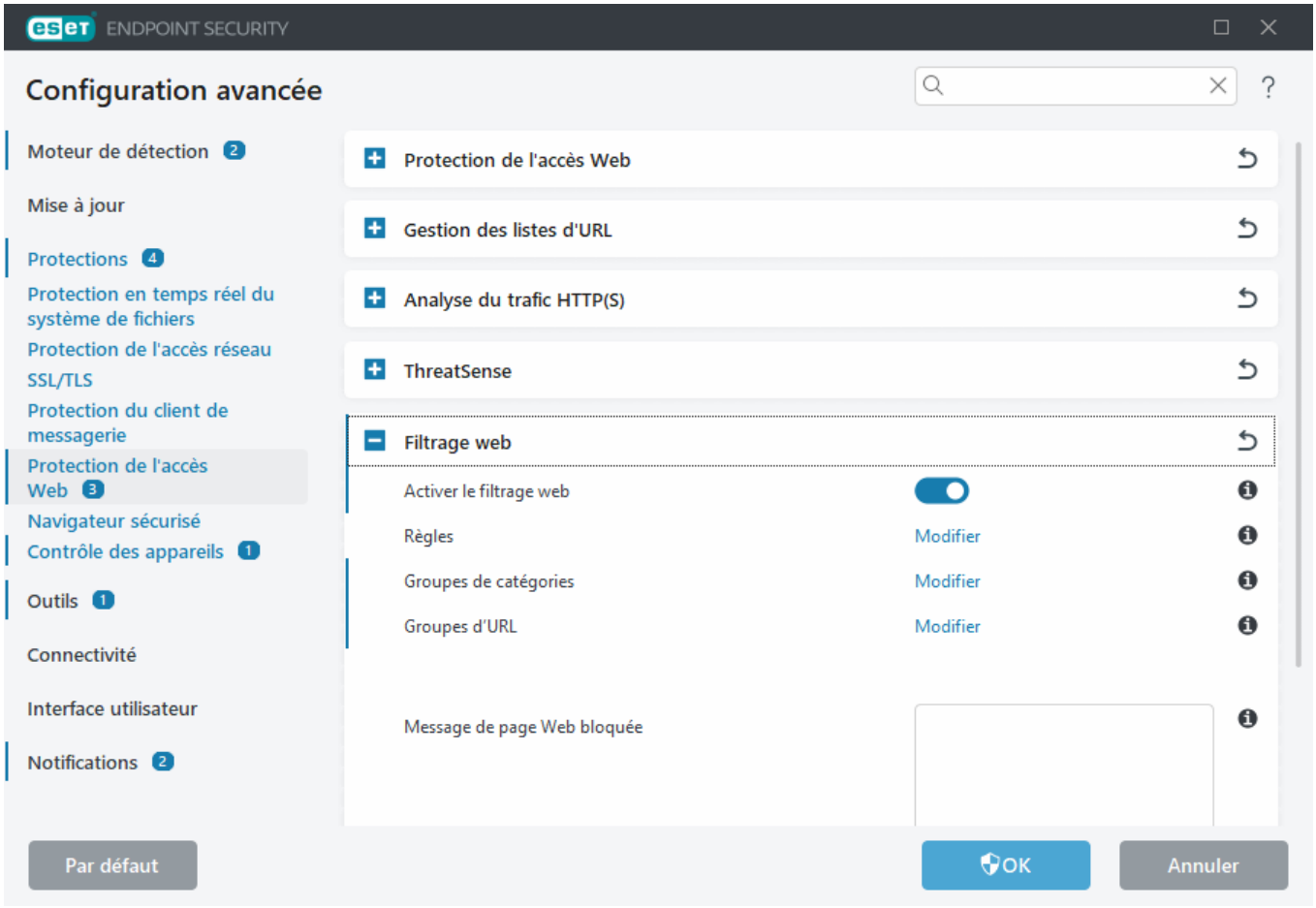
La section Contrôle Web permet de configurer des paramètres qui contribuent à protéger votre entreprise contre les responsabilités juridiques. Le Contrôle Web peut réglementer l'accès aux sites Web qui enfreignent les droits de propriété intellectuelle. L'objectif est d'empêcher les employés d'accéder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

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

Par défaut, le filtrage web est désactivé. Pour l'activer, procédez comme suit :

1. Ouvrez Configurations avancées > **Protections** > **Protection de l'accès web** > **Filtrage web**.
2. Activez le bouton bascule **Activer le filtrage web** pour activer le filtrage web dans ESET Endpoint Security.

3. Configurez l'accès à des pages web spécifiques. Cliquez sur **Modifier** en regard de **Règles** pour accéder à la fenêtre Éditeur de règles du Contrôle Web.

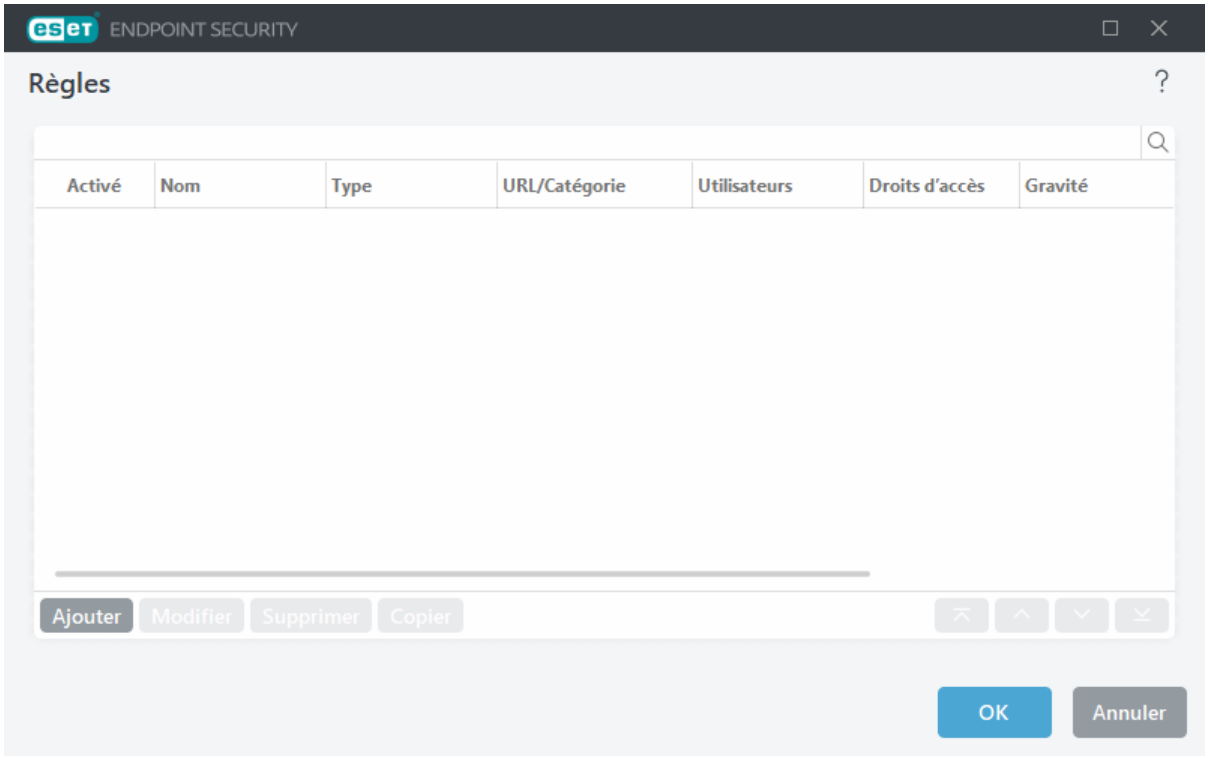


Les champs **Message de page Web bloquée** et **Image de page Web bloquée** vous permettent de personnaliser facilement le message affiché lorsqu'un site web est bloqué.

> Si vous souhaitez bloquer toutes les pages web et n'en laisser que certaines disponibles, utilisez la gestion des adresses URL.

Règles du filtrage web

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



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

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

Les règles sont triées dans l'ordre déterminant leur priorité (les règles dont la priorité est la plus élevée sont en haut). Pour modifier la priorité d'une règle, sélectionnez-la et cliquez sur le bouton fléché pour augmenter ou réduire sa priorité. Cliquez sur la double flèche pour déplacer la règle vers le haut ou le bas de la liste.

Voir aussi Création de règles.

Ajout de règles de contrôle web

La fenêtre Règles de contrôle web permet de créer ou de modifier manuellement une règle de contrôle web existante.

Nom

Entrez une description de la règle dans le champ **Nom** afin de mieux l'identifier.

Activé

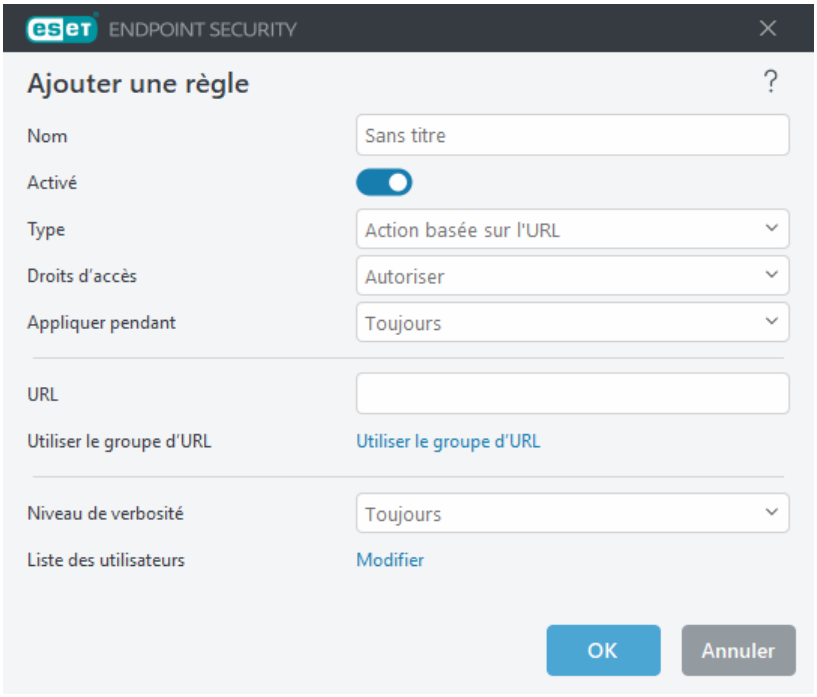
Cliquez sur le bouton bascule **Activé** pour désactiver ou activer la règle ; cela peut être utile si vous ne souhaitez pas supprimer la règle de façon définitive.

Action

Effectuez un choix entre **Action basée sur l'URL** ou **Action basée sur la catégorie** :

Action basée sur l'URL

Pour les règles qui contrôlent l'accès d'un site Web donné, saisissez l'URL dans le champ **URL**.
Les symboles spéciaux * (astérisque) et ? (point d'interrogation) ne peuvent pas être utilisés dans la liste d'adresses URL. Lorsque vous créez un groupe d'URL qui contient un site Web avec plusieurs domaines de niveau supérieur, vous devez ajouter séparément chacun d'entre eux. Si vous ajoutez un domaine au groupe, tout le contenu situé dans ce domaine et ses sous-domaines (par exemple *sous.pageexemple.com*) sera bloqué ou autorisé en fonction du choix d'action basée sur l'URL.
URL ou **Utiliser le groupe d'URL** - Définissez l'URL de lien ou le groupe d'URL de liens pour autoriser, bloquer ou afficher un avertissement lors de l'accès à l'une de ces URL.



Action basée sur la catégorie

La règle sera appliquée en fonction d'une catégorie de site web.
Catégorie d'URL ou **Utiliser le groupe** - Sélectionnez la catégorie de site web ou un groupe de catégories pour autoriser, bloquer ou afficher un avertissement lors de la détection de l'une de ces catégories.

Droits d'accès

- **Autoriser** – L'accès à l'adresse/la catégorie d'URL est autorisé.
- **Avertir** – bloque l'accès à l'adresse/la catégorie d'URL. Vous pouvez cliquer sur **Revenir en arrière** pour revenir au site web précédent ou cliquer sur **Continuer** pour accéder au site web. Si vous cliquez sur **Continuer**, la page de blocage ne s'affichera pas la prochaine fois que vous visiterez le site web.
- **Toujours avertir** – Bloque l'accès à l'adresse/la catégorie d'URL. Vous pouvez cliquer sur **Revenir en arrière** pour revenir au site web précédent ou cliquer sur **Continuer** pour accéder au site web. La page de blocage sera affichée chaque fois que vous visiterez le site web.
- **Bloquer** – Bloque l'accès à l'adresse/la catégorie d'URL. Vous pouvez cliquer sur **Revenir en arrière** pour revenir au site web précédent.

Appliquer pendant

Permet d'appliquer la règle créée pendant un certain temps. Sélectionnez le créneau horaire créé dans le menu déroulant **Appliquer pendant**. Informations supplémentaires sur les créneaux horaires

Journalisation de la gravité

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

> La gravité de la journalisation peut être configurée séparément pour chaque liste. Les journaux avec l'état **Avertissement** peuvent être collectés par ESET PROTECT On-Prem.

Liste de l'utilisateur

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

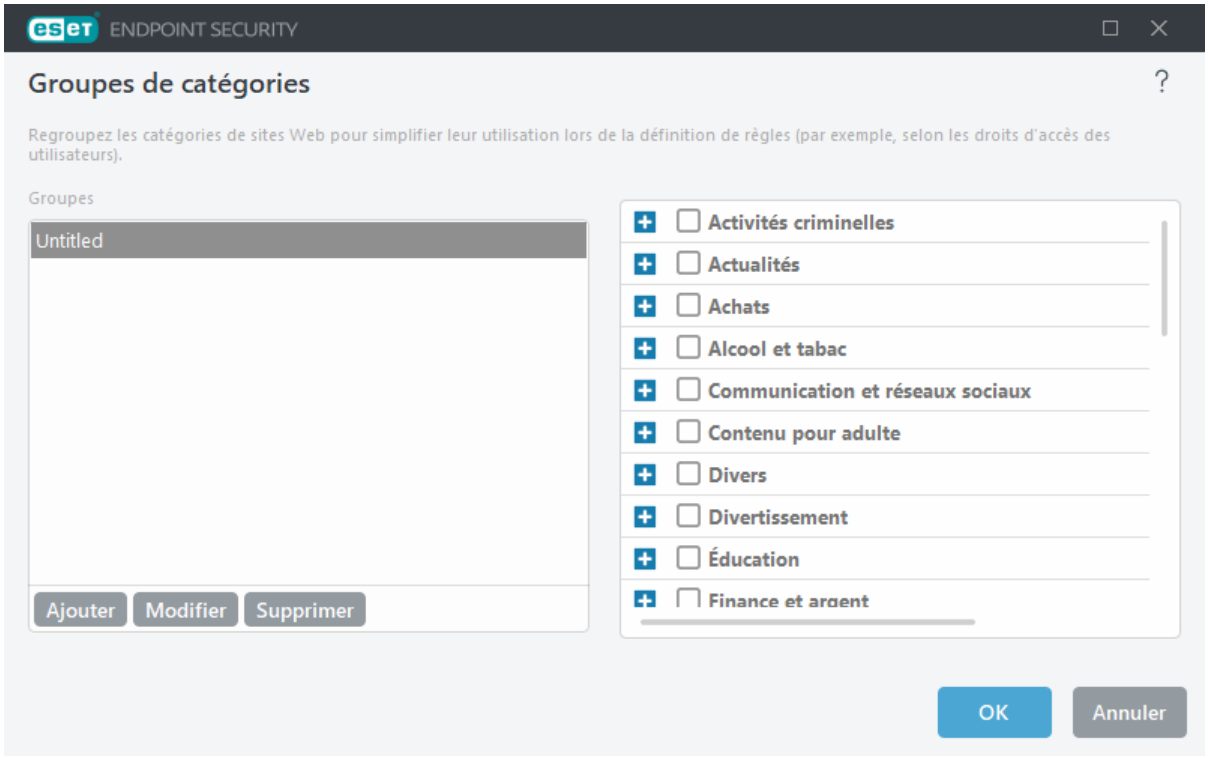
Groupes de catégories

La fenêtre Groupes de catégories se divise en deux parties. La partie gauche de la fenêtre contient une liste de groupes de catégories.

- **Ajouter** – Cliquez sur cette option pour créer un groupe de catégories.
- **Modifier** – Cliquez sur cette option pour modifier un groupe de catégories existant.
- **Supprimer** – Cliquez sur cette option si vous souhaitez supprimer un groupe de catégories de la liste de groupes de catégories.

La partie droite de la fenêtre contient une liste de catégories et sous-catégories. Sélectionnez une catégorie dans la liste Catégorie pour afficher les sous-catégories correspondantes. Chaque groupe contient des sous-catégories réservées aux adultes et/ou généralement inappropriées ainsi que des catégories généralement considérées comme acceptables. Lorsque vous ouvrez la fenêtre Groupes de catégories et cliquez sur le premier groupe, vous pouvez ajouter ou supprimer des catégories/sous-catégories de la liste des groupes appropriés (Violence ou Armes, par exemple). Les pages web au contenu inapproprié peuvent être bloquées et les utilisateurs peuvent être informés lorsqu'ils accèdent à une page web bloquée.

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



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

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

Vous pouvez signaler une catégorisation incorrecte d'une URL.

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

Groupes d'URL

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

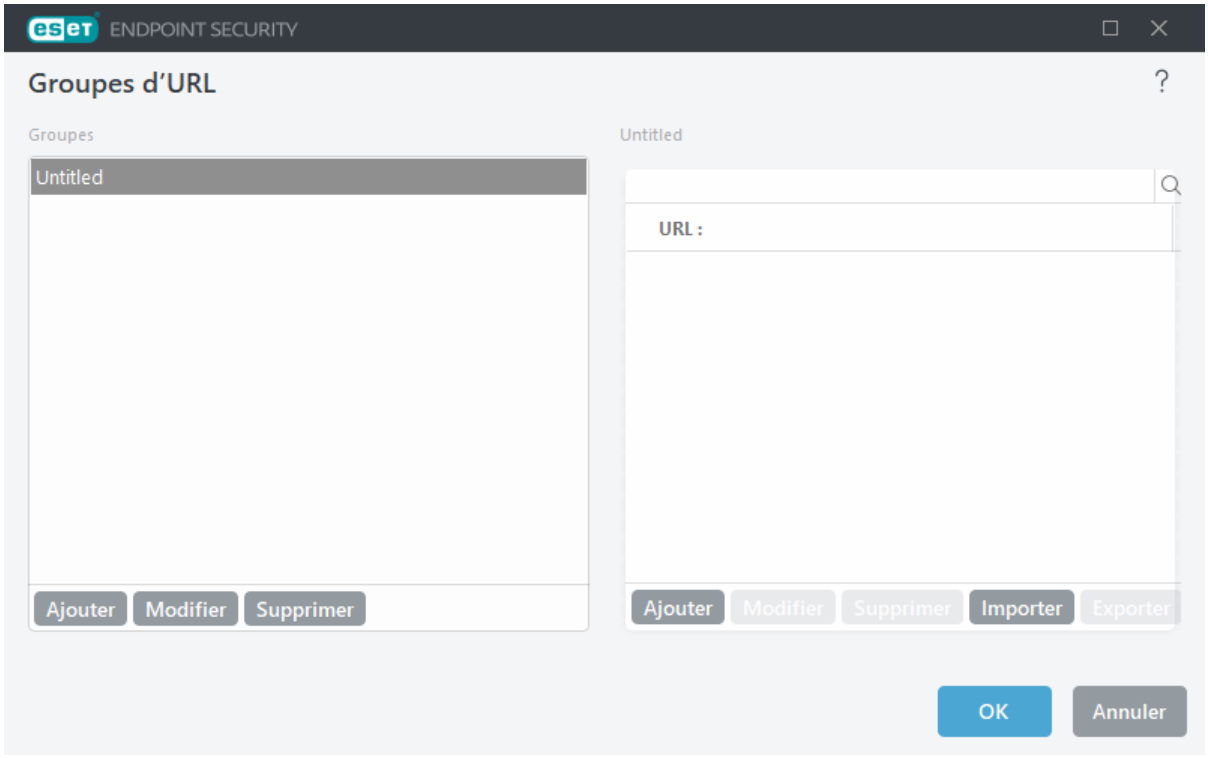
Création d'un groupe d'URL

Pour créer un groupe d'URL, cliquez sur **Ajouter** et saisissez son nom.

L'utilisation d'un groupe d'URL peut s'avérer utile lorsque l'administrateur souhaite créer une règle pour plusieurs

pages web (bloquées ou autorisées en fonction de votre choix).

Ajout d'adresses URL à la liste des groupes d'URL - manuel



Pour ajouter une adresse URL à la liste, sélectionnez un groupe d'URL et cliquez sur **Ajouter** en bas à droite de la fenêtre.

Les symboles spéciaux * (astérisque) et ? (point d'interrogation) ne peuvent pas être utilisés dans la liste d'adresses URL.

Il n'est pas nécessaire de saisir le nom complet du domaine avec http:// ou https://.

Si vous ajoutez un domaine au groupe, l'ensemble du contenu situé sur ce domaine et tous les sous-domaines (par exemple,, *sub.examplepage.com*) sera bloqué ou autorisé en fonction de votre choix d'action basée sur l'URL.

Si un conflit existe entre deux règles (la première règle bloque le domaine alors que la deuxième l'autorise), le domaine ou l'adresse IP spécifique sera de toute façon bloquée. Pour plus d'informations sur la création de règles, consultez Action basée sur l'URL.

Ajout d'adresses URL à la liste de groupes d'URL - importation à l'aide d'un fichier .txt

Cliquez sur **Importer** pour importer un fichier comportant une liste d'adresses URL (séparez les valeurs par un saut de ligne, par exemple, un fichier .txt utilisant le codage UTF-8). Les symboles spéciaux * (astérisque) et ? (point d'interrogation) ne peuvent pas être utilisés dans la liste d'adresses URL.

Utilisation de groupes d'URL dans le filtrage web

Si vous souhaitez définir une action à exécuter pour un groupe d'URL spécifique, ouvrez l'éditeur de règles de filtrage web, sélectionnez votre groupe d'URL à l'aide du menu déroulant, ajustez les autres paramètres, puis

cliquez sur **OK**.

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

Personnalisation du message de page web bloquée

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

Utilisation

Bloquons la catégorie de sites web « Armes ».

Exemple de message de page web bloquée :

```
La page web %URL_OR_CATEGORY% a été bloquée, car son contenu est considéré comme in
approprié ou nuisible.
Pour plus de détails, veuillez contacter l'administrateur.
```

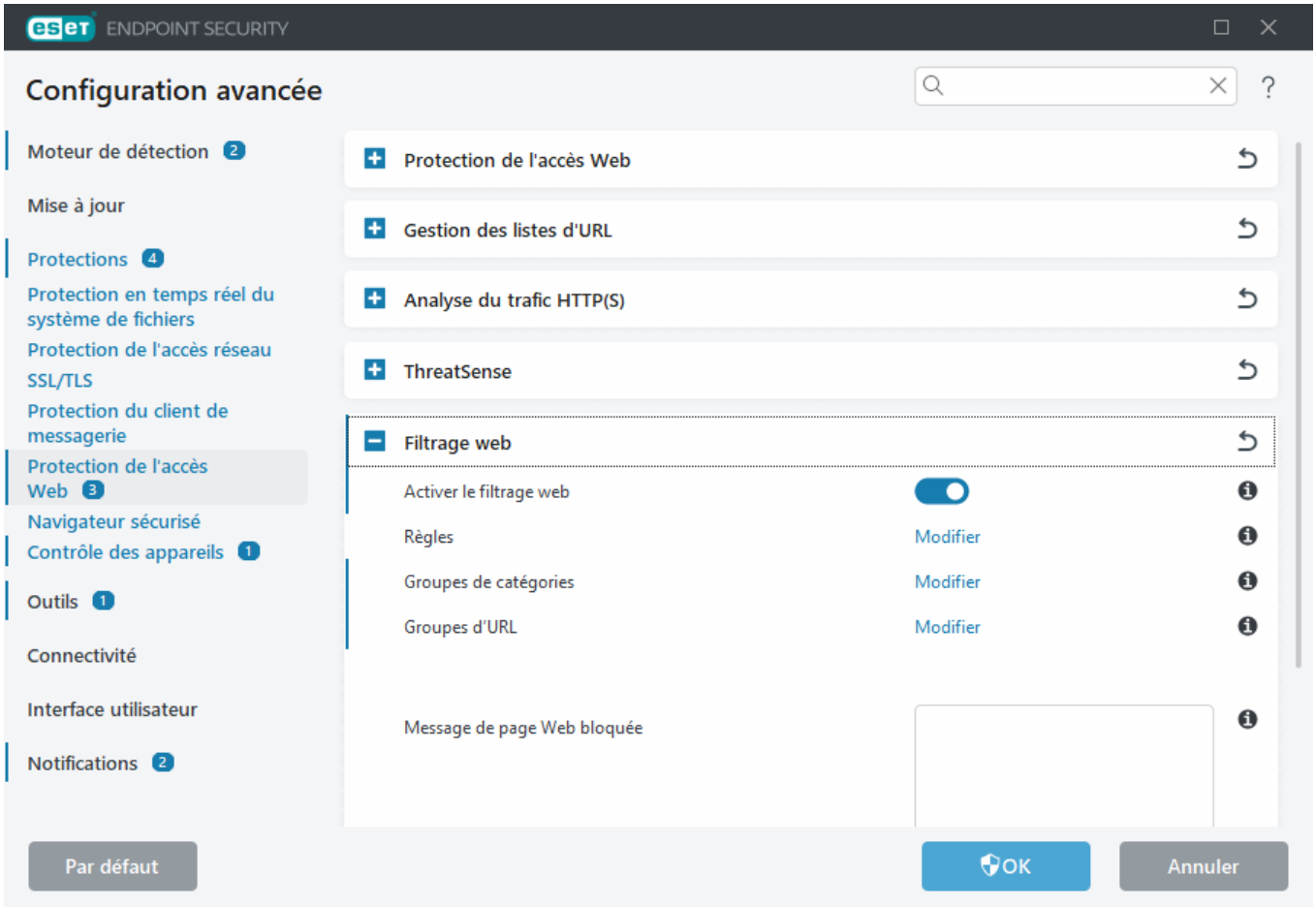
Variable	Description
%CATEGORY%	Catégorie de filtrage web bloquée.
%URL_OR_CATEGORY%	Site web ou catégorie de filtrage web bloquée (dépend de la règle de blocage du filtrage web).
%STR_GOBACK%	Valeur du bouton Retour.
%product_name%	Nom du produit ESET (ESET Endpoint Security)
%product_version%	Version du produit ESET.

Exemple de graphique de page web bloquée :

```
https://help.eset.com/tools/indexPage/products/antitheft.png
```

La taille de l'image (largeur/hauteur) sera automatiquement ajustée si elle est trop grande.

Dans ESET Endpoint Security, la configuration ressemblera à celle-ci :



Boîte de dialogue - Filtrage Web

La fonction principale du Contrôle Web est de contrôler les sites Web auxquels chaque utilisateur accède dans le réseau d'entreprise. L'administrateur réseau doit être en mesure de définir les catégories des sites Web auxquels les utilisateurs auront accès par utilisateur ou groupe d'utilisateurs. L'intégration aux services d'annuaire permet l'utilisation des groupes Active Directory pour la configuration du contrôle web. Cette fonctionnalité est désactivée par défaut. Si vous souhaitez l'activer, activez **Activer le filtrage web**. Cliquez sur **Modifier** pour accéder à l'Éditeur de règles. Cliquez sur **Modifier** en regard de Groupes de catégories pour modifier les groupes prédéfinis ou sur **Modifier** en regard de l'Éditeur de groupes d'URL pour ajouter un nouveau groupe d'URL.

Navigateur sécurisé

Le Navigateur sécurisé constitue une couche supplémentaire de protection conçue pour protéger vos données financières lors des transactions en ligne.

Le système de réputation ESET LiveGrid® doit être activé (activé par défaut) pour que le Navigateur sécurisé fonctionne correctement.

Pour configurer le comportement du Navigateur sécurisé, ouvrez Configurations avancées > **Protections** > **Navigateur sécurisé**.

Vous pouvez utiliser l'option de configuration suivante du Navigateur sécurisé :

- **Sécuriser tous les navigateurs** : tous les navigateurs web pris en charge démarrent en mode sécurisé. Vous

pouvez ainsi naviguer sur Internet, accéder à la banque en ligne et effectuer des achats et des transactions en ligne dans une fenêtre de navigateur sécurisé sans être redirigé.

Général

Protection du navigateur

Sécuriser tous les navigateurs : activez pour démarrer tous les navigateurs web pris en charge en mode sécurisé. Vous pouvez ainsi naviguer sur Internet, accéder à la banque en ligne et effectuer des achats et des transactions en ligne dans une fenêtre de navigateur sécurisé sans être redirigé.

Mode d'installation des extensions – Dans le menu déroulant, vous pouvez sélectionner les extensions qui seront autorisées à être installées sur un navigateur sécurisé par ESET : La modification du mode d'installation des extensions n'a aucune incidence sur les extensions de navigateur déjà installées :

- **Extensions essentielles** – Uniquement les extensions les plus importantes développées par un fabricant de navigateur spécifique.
- **Toutes les extensions** – Toutes les extensions qui sont prises en charge par un navigateur spécifique.

Navigateur sécurisé

Protection améliorée de la mémoire – Si cette option est activée, la mémoire du navigateur sécurisé sera protégée contre toute inspection de la part d'autres processus.

Protection du clavier – Si cette option est activée, les informations saisies à l'aide du clavier dans le navigateur sécurisé sont masquées pour les autres applications. Cela renforce la protection contre les keyloggers.

Cadre vert du navigateur – Si cette option est désactivée, la notification informative dans le navigateur et le cadre vert entourant le navigateur sont masqués.

Configurer les alertes interactives du Navigateur sécurisé – Permet d'ouvrir la fenêtre Alertes interactives.

> Dans certaines situations, une alerte interactive spécifique ne s'affiche que lorsqu'une erreur se produit lors du démarrage du Navigateur sécurisé. Pour plus d'informations, consultez Alertes interactives.

Notification dans le navigateur

Le navigateur sécurisé vous informe de son état actuel par des notifications dans le navigateur et par la couleur du cadre du navigateur.

Les notifications dans le navigateur sont affichées dans l'onglet situé sur le côté droit.

Pour développer la notification dans le navigateur, cliquez sur l'icône ESET. Pour réduire la notification, cliquez sur le texte de celle-ci. Pour ignorer la notification et le cadre vert du navigateur, cliquez sur l'icône Fermer.

Seuls les notifications informatives et le cadre vert du navigateur vert peuvent être ignorés.

Notification dans le navigateur

Type de notification	État
Notification informative et cadre de navigateur vert	Une protection maximale est assurée et la notification dans le navigateur est minimisée par défaut.
Avertissement et cadre de navigateur orange	Le navigateur sécurisé requiert votre attention pour un problème non critique. Pour plus d'informations sur le problème ou pour obtenir une solution, suivez les instructions de la notification dans le navigateur.
Alerte de sécurité et cadre de navigateur rouge	Le navigateur n'est pas protégé. Redémarrez le navigateur pour vous assurer que la protection est active. Pour résoudre un conflit avec les fichiers chargés dans le navigateur, ouvrez les fichiers journaux > **Navigateur sécurisé**, puis veillez à ce que les fichiers consignés ne soient pas chargés au prochain lancement du navigateur. Si le problème persiste, contactez l'assistance technique d'ESET en suivant les instructions de cet article de la base de connaissances.

Contrôle de périphérique

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

Périphériques externes pris en charge :

- Stockage sur disque (disque dur, disque amovible USB)
- CD/DVD
- Imprimante USB
- FireWireStockage
- Bluetooth Périphérique
- Lecteur de carte à puce
- Périphérique d'image
- Modem
- LPT/COM port
- Appareil portable (appareils alimentés par batterie tels que les lecteurs multimédia, les smartphones, les appareils plug-and-play, etc.)
- Tous les types de périphérique

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

Cliquez sur le bouton bascule **Activer le contrôle des appareils** pour activer la fonctionnalité Contrôle des appareils dans ESET Endpoint Security. Vous devez redémarrer votre ordinateur pour que cette modification prenne effet. Une fois le contrôle des appareils activé, vous pouvez définir des **règles** dans la fenêtre Éditeur de règles.

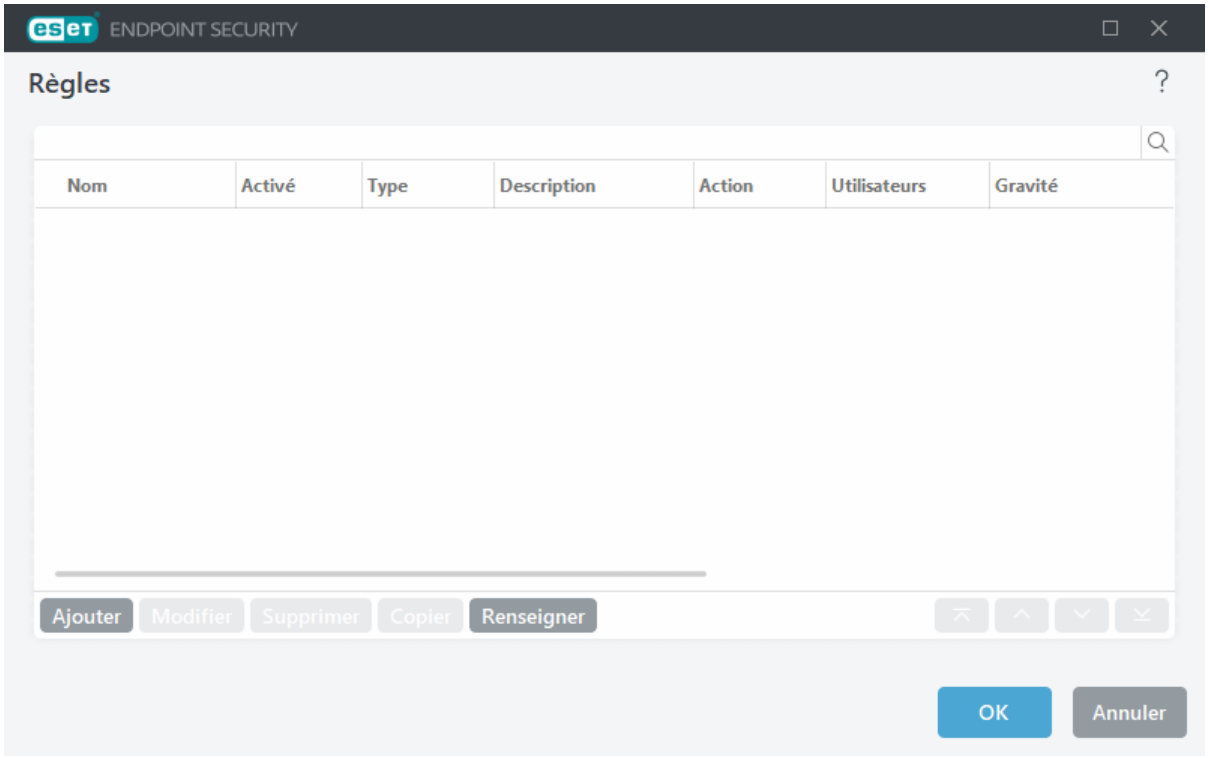
Vous pouvez importer un groupe de contrôle des appareils avec des règles d'un fichier xml à l'aide du planificateur. Pour plus d'informations et un guide détaillé, consultez cet article de la base de connaissances ESET.

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

Éditeur de règles de contrôle de périphérique

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

Les articles suivants de la base de connaissances ESET peuvent être disponibles uniquement en anglais : Ajouter et modifier des règles de contrôle des appareils à l'aide des produits endpoint ESET

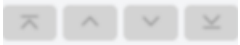


Des périphériques spécifiques peuvent être autorisés ou bloqués selon l'utilisateur, le groupe d'utilisateurs ou tout autre paramètre supplémentaire pouvant être spécifié dans la configuration des règles. La liste des règles contient plusieurs descriptions de la règle, telles que le nom, le type d'appareil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

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

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

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

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

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

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).

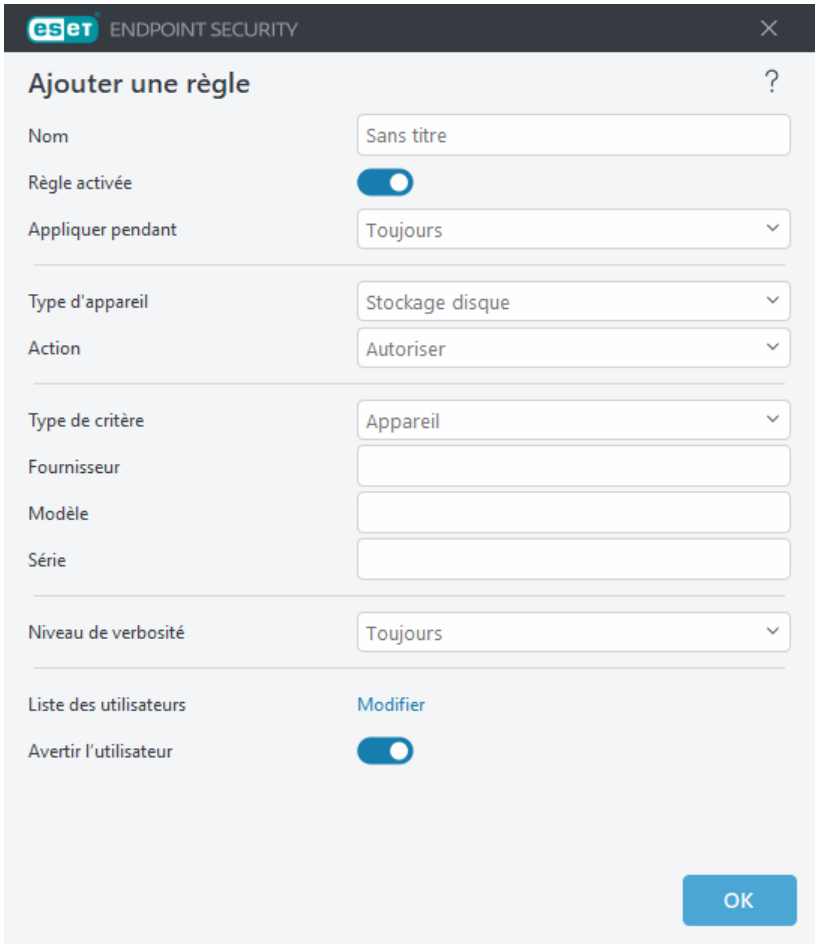
Sélectionnez un appareil dans la liste des appareils détectés, puis cliquez sur **OK** pour ajouter une règle de contrôle des appareils avec des informations prédéfinies (tous les paramètres peuvent être réglés).

Les appareils en mode de faible consommation (veille) sont signalés par une icône d'avertissement . Pour activer le bouton **OK** et ajouter une règle pour cet appareil :

- Reconnectez l'appareil.
- Utilisez l'appareil (par exemple, lancez l'application Caméra dans Windows pour mettre en éveil une webcam).

Ajout de règles de contrôle de périphérique

Une règle de contrôle des appareils définit une action à exécuter lorsqu'un appareil répondant aux critères de la règle est connecté à l'ordinateur.



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

Appliquer pendant – Permet d'appliquer la règle créée pendant un certain temps. Dans le menu déroulant, sélectionnez le créneau horaire créé. Consultez des informations supplémentaires sur les créneaux horaires.

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.

> 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 :

- **Autoriser** – L'accès complet au périphérique est autorisé.
- **Bloquer** – L'accès au périphérique est bloqué.
- **Blocage d'écriture** – L'accès en lecture seule au périphérique est autorisé.
- **Avertir** – À chaque connexion d'un périphérique, l'utilisateur est averti s'il est autorisé/bloqué, et une entrée est enregistrée dans le journal. Comme les 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 **Blocage d'écriture** n'étant pas disponible pour Bluetooth, un tel périphérique ne peut être qu'autorisé ou sujet à un avertissement).

Type de critère

Sélectionnez **Groupe de périphériques** ou **Périphérique**.

D'autres paramètres présentés ci-dessous peuvent être utilisés afin d'affiner les règles pour différents appareils. Tous les paramètres respectent la casse et prennent en charge les caractères génériques (*, ?) :

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

> Si ces paramètres ne sont pas définis, la règle ignore ces champs lors de la recherche de correspondances. Les paramètres de filtrage de tous les champs de texte respectent la casse et prennent en charge les caractères génériques (un point d'interrogation (?) représente un seul caractère tandis qu'un astérisque (*) représente une chaîne de zéro caractère ou plus).

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

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.

Limites de la liste des utilisateurs

La liste des utilisateurs ne peut pas être définie pour des règles avec des types d'appareilsspécifiques :

- Imprimante USB
- Périphérique Bluetooth
- Lecteur de carte à puce
- Périphérique d'image
- Modem
- Port LPT/COM

Avertir l'utilisateur – Si un appareil bloqué par une règle existante est inséré, une fenêtre de notification s'affiche.

Groupe de périphériques

Un périphérique connecté à votre ordinateur peut présenter un risque de sécurité.

La fenêtre Groupes de périphériques se divise en deux parties. La partie droite de la fenêtre contient la liste des périphériques appartenant à un groupe donné. La partie gauche comporte les groupes créés. Sélectionnez un groupe pour afficher les appareils dans le volet droit.

Lorsque vous ouvrez la fenêtre Groupes de périphériques et que vous sélectionnez un groupe, vous pouvez ajouter ou supprimer des périphériques de la liste. Une autre méthode pour ajouter des périphériques au groupe consiste à les importer à partir d'un fichier. Vous pouvez aussi cliquer sur le bouton **Renseigner** pour que tous les périphériques connectés à votre ordinateur soient répertoriés dans la fenêtre **Périphériques détectés**. Sélectionnez des appareils dans la liste renseignée, puis cliquez sur **OK** pour les ajouter au groupe.

Éléments de commande

Ajouter : vous pouvez ajouter un groupe en saisissant son nom ou un appareil à un groupe existant selon l'endroit de la fenêtre où vous avez cliqué sur le bouton.

Modifier : permet de modifier le nom du groupe sélectionné ou les paramètres du périphérique (fabricant, modèle, numéro de série, etc.).

Supprimer : permet de supprimer le groupe ou le périphérique sélectionné selon la partie de la fenêtre où vous avez cliqué sur le bouton.

Importer : permet d'importer une liste d'appareils à partir d'un fichier texte. L'importation d'appareils à partir d'un fichier texte demande une mise en forme correcte :

- Chaque appareil doit se trouver au début d'une nouvelle ligne.
- Le **fournisseur**, le **modèle** et la **série** doivent être indiqués pour chaque appareil et séparés par une virgule.

Voici un exemple de contenu de fichier texte :

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Exporter : permet d'exporter une liste d'appareils vers un fichier.

Le bouton **Renseigner** permet de donner une vue d'ensemble de tous les périphériques actuellement connectés avec des informations sur : le type de périphérique, le fournisseur, le modèle et le numéro de série (le cas

échéant).

> Vous pouvez importer un groupe de contrôle des appareils avec des règles d'un fichier xml à l'aide du planificateur. Pour plus d'informations et un guide détaillé, consultez cet article de la base de connaissances ESET.

Ajouter un appareil

Pour ajouter un appareil à un groupe existant, cliquez sur Ajouter dans la fenêtre à droite. D'autres paramètres présentés ci-dessous peuvent être utilisés afin d'affiner les règles pour différents appareils. Tous les paramètres respectent la casse et prennent en charge les caractères génériques (*, ?) :

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

> Si ces paramètres ne sont pas définis, la règle ignore ces champs lors de la recherche de correspondances. Les paramètres de filtrage de tous les champs de texte respectent la casse et prennent en charge les caractères génériques (un point d'interrogation (?) représente un seul caractère tandis qu'un astérisque (*) représente une chaîne de zéro caractère ou plus).

Cliquez sur **OK** pour enregistrer les modifications. Cliquez sur **Annuler** si vous souhaitez fermer la fenêtre **Groupes de périphériques** sans enregistrer les modifications.

> Une fois le groupe d'appareils créé, vous devez ajouter une nouvelle règle de contrôle des appareils pour le groupe d'appareils créé et sélectionner l'action à exécuter.

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

ThreatSense

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

les options de configuration de la technologie ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

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

Pour ouvrir la fenêtre de configuration, cliquez sur **ThreatSense** dans les Configurations avancées de chaque module utilisant la technologie ThreatSense (reportez-vous aux informations ci-dessous). Différents scénarios de sécurité peuvent nécessiter des configurations différentes. Dans cette optique, ThreatSense est configurable individuellement pour les modules de protection suivants :

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

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

Objets à analyser

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

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

Secteurs d'amorçage/UEFI – Analyse les secteurs d'amorçage afin de détecter la présence éventuelle de logiciels malveillants dans l'enregistrement d'amorçage principal. Pour plus d'informations sur UEFI, consultez le glossaire.

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

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

Archives auto-extractibles – Les archives auto-extractibles (SFX) sont des archives qui sont extraites automatiquement.

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

Options d'analyse

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

Heuristique – La méthode heuristique utilise un algorithme d'analyse de l'activité (malveillante) des programmes. Elle présente l'avantage d'identifier un code malveillant qui n'existait pas ou qui n'était pas connu par la version antérieure du moteur de détection. Cette méthode présente néanmoins l'inconvénient d'une probabilité (très

faible) de fausses alarmes.

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

Nettoyage

Les paramètres de nettoyage déterminent le comportement d'ESET Endpoint Security 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 d'ThreatSense vous permet de définir les types de fichiers à analyser.

Autre

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

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

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

Consigner tous les objets – Le journal d'analyse affiche tous les fichiers analysés dans des archives auto-extractibles, même ceux qui ne sont pas infectés (peut générer beaucoup de données et augmenter la taille du fichier du journal d'analyse).

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

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

Limites

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

Paramètres d’objet

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

Durée d’analyse maximale pour l’objet (s) – Définit la durée maximale de l’analyse des fichiers dans un objet conteneur (tel qu’une archive RAR/ZIP ou un e-mail avec plusieurs pièces jointes). Ce paramètre ne s’applique pas aux fichiers autonomes. Si une valeur définie par l’utilisateur a été saisie et que le temps s’est écoulé, une analyse s’arrêtera dès que possible, que l’analyse de chaque fichier d’un objet conteneur soit terminée ou non. Dans le cas d'une archive contenant des fichiers volumineux, l'analyse s'arrêtera dès qu'un fichier de l'archive sera extrait (par exemple, lorsqu'une variable définie par l'utilisateur est de 3 secondes, mais que l'extraction d'un fichier prend 5 secondes). Le reste des fichiers de l'archive ne sera pas analysé lorsque ce temps sera écoulé. Pour limiter le temps d'analyse, y compris pour les archives plus volumineuses, utilisez les options **Taille d’objet maximale** et **Taille maximale du fichier dans l'archive** (non recommandé en raison d'éventuels risques de sécurité). Valeur par défaut : illimitée.

Configuration de l’analyse d’archive

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

Taille maximale de fichier dans l'archive – Cette option permet de spécifier la taille maximale des fichiers (après extraction) à analyser contenus dans les archives. La valeur maximale est 3 Go.

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

Niveaux de nettoyage

Pour modifier les paramètres de niveau de nettoyage d'un module de protection souhaité, développez **ThreatSense** (par exemple, **Protection en temps réel du système de fichiers**), puis choisissez un **niveau de nettoyage** dans le menu déroulant.

ThreatSense comporte les niveaux de correction (nettoyage, par exemple) suivants :

Correction dans ESET Endpoint Security

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.

Extensions de fichier exclues de l'analyse

Les extensions de fichier exclues font partie d'ThreatSense. Pour configurer les extensions de fichier exclues, cliquez sur **ThreatSense** dans les Configurations avancées pour n'importe quel module utilisant la technologie ThreatSense.

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

> Ne confondez pas cette option avec Exclusions des processus, Exclusions HIPS ou Exclusions de fichier/dossier.

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

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

> Pour ajouter une nouvelle extension à la liste, cliquez sur **Ajouter**. Saisissez l'extension dans le champ correspondant (comme tmp) et cliquez sur **OK**. Lorsque vous sélectionnez **Entrer plusieurs valeurs**, vous pouvez ajouter plusieurs extensions de fichier en les séparant par des lignes, des virgules ou des points-virgules (par exemple, choisissez **Point-virgule** comme séparateur dans le menu déroulant et saisissez `edb;eml;tmp`).
> Vous pouvez utiliser un symbole spécial ? (point d'interrogation). Qui symbolise n'importe quel caractère (par exemple, `?db`).

> Pour voir l'extension exacte (le cas échant) d'un fichier dans un système d'exploitation Windows, vous devez cocher la case **Extensions de noms de fichiers** dans **Explorateur Windows** > **Affichage** (onglet).

Autres paramètres ThreatSense

Pour modifier ces paramètres, ouvrez Configurations avancées > **Protections** > **Protection en temps réel du système de fichiers** > **Paramètres ThreatSense supplémentaires**.

Autres paramètres ThreatSense pour les fichiers nouveaux et les fichiers modifiés

La probabilité d'infection de fichiers nouveaux ou modifiés est comparativement supérieure à celle de fichiers existants. Pour cette raison, le programme vérifie ces fichiers avec d'autres paramètres d'analyse. ESET Endpoint Security utilise l'heuristique avancée qui détecte les nouvelles menaces avant la mise à disposition de la mise à jour du moteur de détection avec les méthodes d'analyse basées sur les signatures.

Outre les nouveaux fichiers, l'analyse porte également sur les **archives auto-extractibles** (.sfx) et les **fichiers exécutables compressés** (en interne). Par défaut, les archives sont analysées jusqu'au dixième niveau d'imbrication et sont contrôlées indépendamment de leur taille réelle. Pour modifier les paramètres d'analyse d'archive, désactivez **Paramètres d'analyse d'archive par défaut**.

Autres paramètres ThreatSense pour les fichiers exécutés

Heuristique avancée à l'exécution du fichier : Par défaut, l'heuristique avancée est utilisée lorsque des fichiers sont exécutés. Lorsque ce paramètre est activé, il est fortement recommandé de conserver les options Optimisation intelligente et ESET LiveGrid® activées pour limiter l'impact sur les performances système.

Heuristique avancée lors de l'exécution de fichiers à partir de périphériques amovibles : L'heuristique avancée émule le code dans un environnement virtuel et évalue son comportement avant qu'il ne soit autorisé à s'exécuter à partir d'un support amovible.

Outils

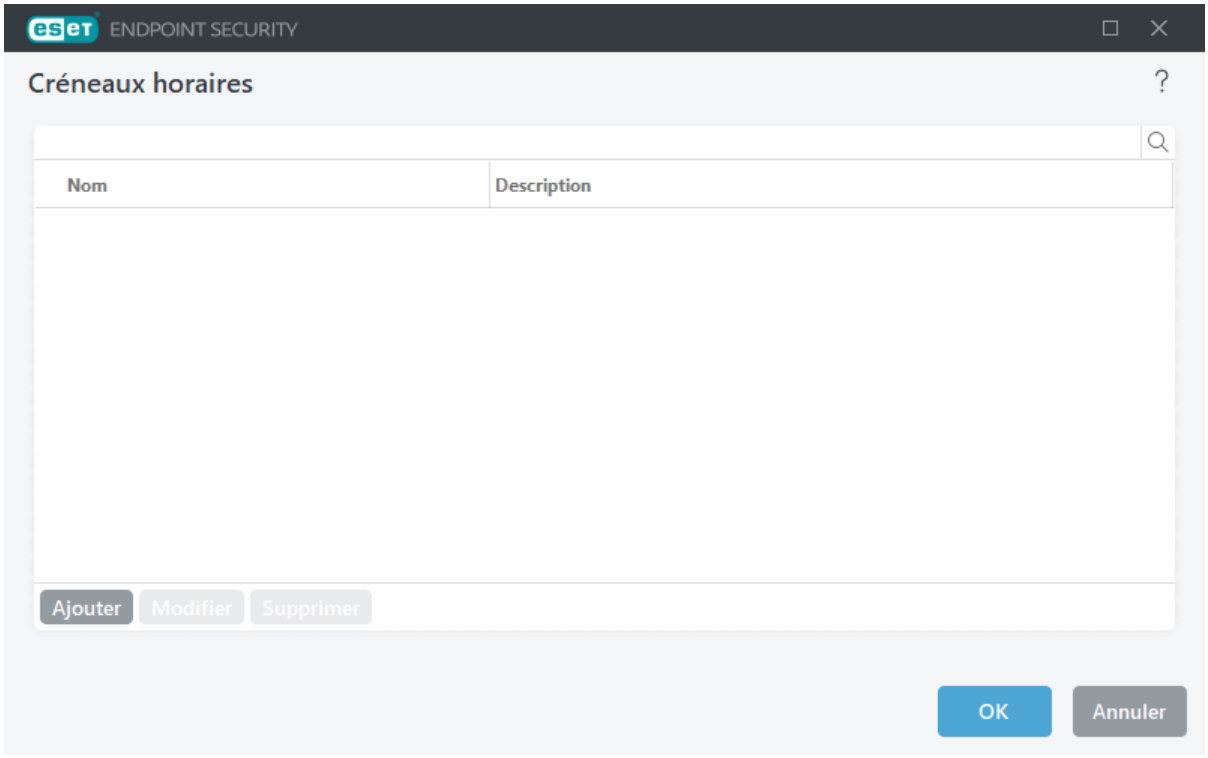
Vous pouvez configurer des paramètres avancés pour les fonctionnalités qui offrent une sécurité supplémentaire et simplifient l'administration d'ESET Endpoint Security dans Configurations avancées > **Outils**.

- Créneaux horaires
- Microsoft Windows Update
- ESET CMD
- Surveillance et administration à distance
- Intervalle de vérification des licences
- Fichiers journaux
- Mode de présentation
- Diagnostics

Créneaux horaires

Les créneaux horaires peuvent être créés et ensuite affectés aux règles pour **Contrôle des appareils** et **Filtrage web**. 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 ou la fenêtre de l'éditeur de règles de filtrage web.

Microsoft Windows Update

La fonctionnalité Windows Update est un élément important de la protection des utilisateurs contre les logiciels malveillants. C'est pourquoi il est essentiel d'installer les mises à jour de Microsoft Windows dès qu'elles sont disponibles. ESET Endpoint Security vous informe des mises à jour manquantes en fonction du niveau que vous spécifiez. Les niveaux suivants sont disponibles :

- **Pas de mise à jour** – Aucune mise à jour système n'est proposée au téléchargement.
- **Mises à jour optionnelles** – Les mises à jour marquées comme étant faiblement prioritaires et au-dessus sont proposées au téléchargement.
- **Mises à jour recommandées** – Les mises à jour marquées comme étant courantes et au-dessus sont proposées au téléchargement.
- **Mises à jour importantes** – Les mises à jour marquées comme étant importantes et au-dessus sont proposées au téléchargement.
- **Mises à jour critiques** – Seules les mises à jour critiques sont proposées pour le téléchargement.

Cliquez sur **OK** pour enregistrer les modifications. La fenêtre Mises à jour système s'affiche après la vérification de l'état à l'aide du serveur de mise à jour. C'est pourquoi les informations de mise à jour système ne sont peut-être pas immédiatement disponibles après l'enregistrement des modifications.

Boîte de dialogue - Mises à jour du système d'exploitation

Si des mises à jour sont disponibles pour votre système d'exploitation, la fenêtre d'accueil ESET Endpoint Security affiche une notification. Cliquez sur **Plus d'informations** pour ouvrir la fenêtre des mises à jour système.

La fenêtre Mises à jour système affiche la liste des mises à jour disponibles prêtes pour le téléchargement et l'installation. Le type de mise à jour s'affiche à côté du nom de la mise à jour.

Double-cliquez sur une mise à jour pour afficher la fenêtre Informations sur la mise à jour contenant des informations supplémentaires.

Cliquez sur **Exécuter une mise à jour système** pour télécharger et installer toutes les mises à jour du système d'exploitation répertoriées.

Mise à jour les informations

La fenêtre Mises à jour système affiche la liste des mises à jour disponibles prêtes pour le téléchargement et l'installation. Le niveau de priorité de chaque mise à jour s'affiche à côté de son nom.

Cliquez sur **Exécuter une mise à jour système** pour lancer le téléchargement et l'installation des mises à jour du système d'exploitation.

Cliquez avec le bouton droit sur une ligne de mise à jour et cliquez sur **Afficher les informations** pour afficher une nouvelle fenêtre comportant des informations supplémentaires.

ESET CMD

Il s'agit d'une fonctionnalité qui permet d'utiliser des commandes ecmd avancées. Vous pouvez exporter et 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 Security peut être exportée dans un fichier *.xml*.

Lorsqu'ESET CMD est activé, deux méthodes d'autorisation sont disponibles :

- **Aucune** : aucune autorisation. Il n'est pas recommandé d'utiliser cette méthode car elle permet l'importation de n'importe quelle configuration non signée, ce qui constitue un risque potentiel.
- **Mot de passe de configuration avancée** : un mot de passe est nécessaire pour importer une configuration à partir d'un fichier *.xml* devant être signé (reportez-vous à la section relative à la signature d'un fichier de configuration *.xml* plus bas). Le mot de passe spécifié dans la configuration de l'accès doit être fourni avant l'importation d'une nouvelle configuration. Si la configuration de l'accès n'est pas activée, que le mot de passe ne correspond pas ou que le fichier de configuration *.xml* n'est pas signé, la configuration n'est pas importée.

Une fois qu'ESET CMD est activé, vous pouvez utiliser la ligne de commande pour exporter ou importer des configurations de ESET Endpoint Security. Vous pouvez le faire manuellement ou créer un script pour l'automatisation.

Pour utiliser les commandes ecmd avancées, vous devez les exécuter avec des privilèges d'administrateur ou ouvrir une invite de commandes Windows (cmd) à l'aide de la commande **Exécuter en tant qu'administrateur**. Si vous ne procédez pas ainsi, le message **Error executing command** s'affiche. Le dossier de destination doit aussi exister lors de l'exportation d'une configuration. La commande d'exportation fonctionne toujours lorsque le paramètre ESET CMD est désactivé.

Les commandes ecmd ne peuvent être exécutées que localement. Leur suspension ne peut être gérée que via une tâche client **Exécuter une commande** à l'aide d'ESET PROTECT On-Prem.

Commande d'exportation des paramètres :
`ecmd /getcfg c:\config\settings.xml`
Commande d'importation des paramètres :
`ecmd /setcfg c:\config\settings.xml`

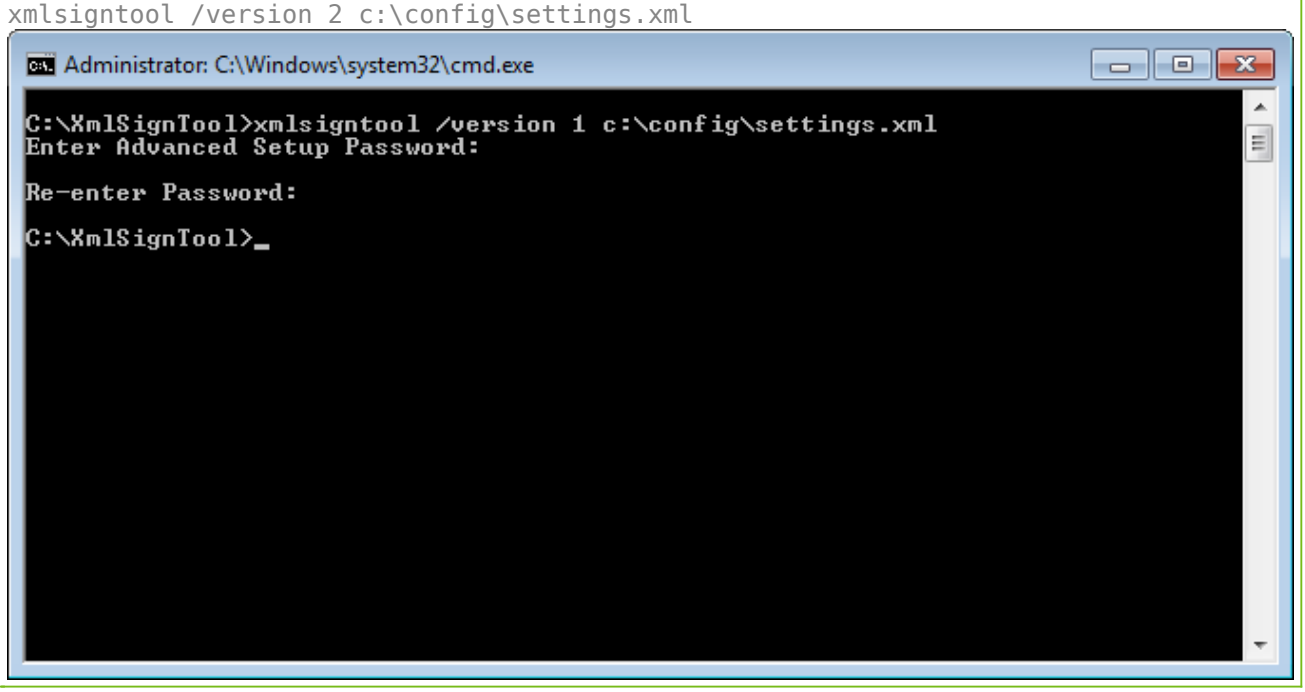
Signature d'un fichier de configuration *.xml* :

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>`

La valeur du paramètre `/version` dépend de la version d'ESET Endpoint Security. 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 Security avec ESET CMD à l'aide de la méthode d'autorisation du mot de passe.

Commande de signature du fichier de configuration exporté :
`xmlsigntool /version 2 c:\config\settings.xml`



Si le mot de passe de la configuration de l'accès change et si vous souhaitez importer une configuration qui a été signée avec un ancien mot de passe, vous devez signer de nouveau le fichier de configuration *.xml* à l'aide du mot de passe actuel. Vous pouvez ainsi utiliser un ancien fichier de configuration sans l'exporter sur un autre ordinateur exécutant ESET Endpoint Security avant l'importation.

Il n'est pas recommandé d'activer ESET CMD sans autorisation, car cela permet l'importation de configuration non signée. Définissez le mot de passe dans Configuration avancée > **Interface utilisateur** > **Configuration de l'accès** pour empêcher toute modification non autorisée par les utilisateurs.

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 ESET PROTECT On-Prem. 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 périphériques	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
Mode de présentation	ecmd /setfeature presentation pause	ecmd /setfeature presentation 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
Antispam des clients de messagerie	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Protection antihameçonnage	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

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 Security 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 Security

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 N-able N-central
- module d'extension ESET Direct Endpoint Management pour N-able RMM
- module d'extension ESET Direct Endpoint Management pour NinjaOne
- module d'extension ESET Direct Endpoint Management pour DattoRMM
- module d'extension ESET Direct Endpoint Management pour Kaseya VSA

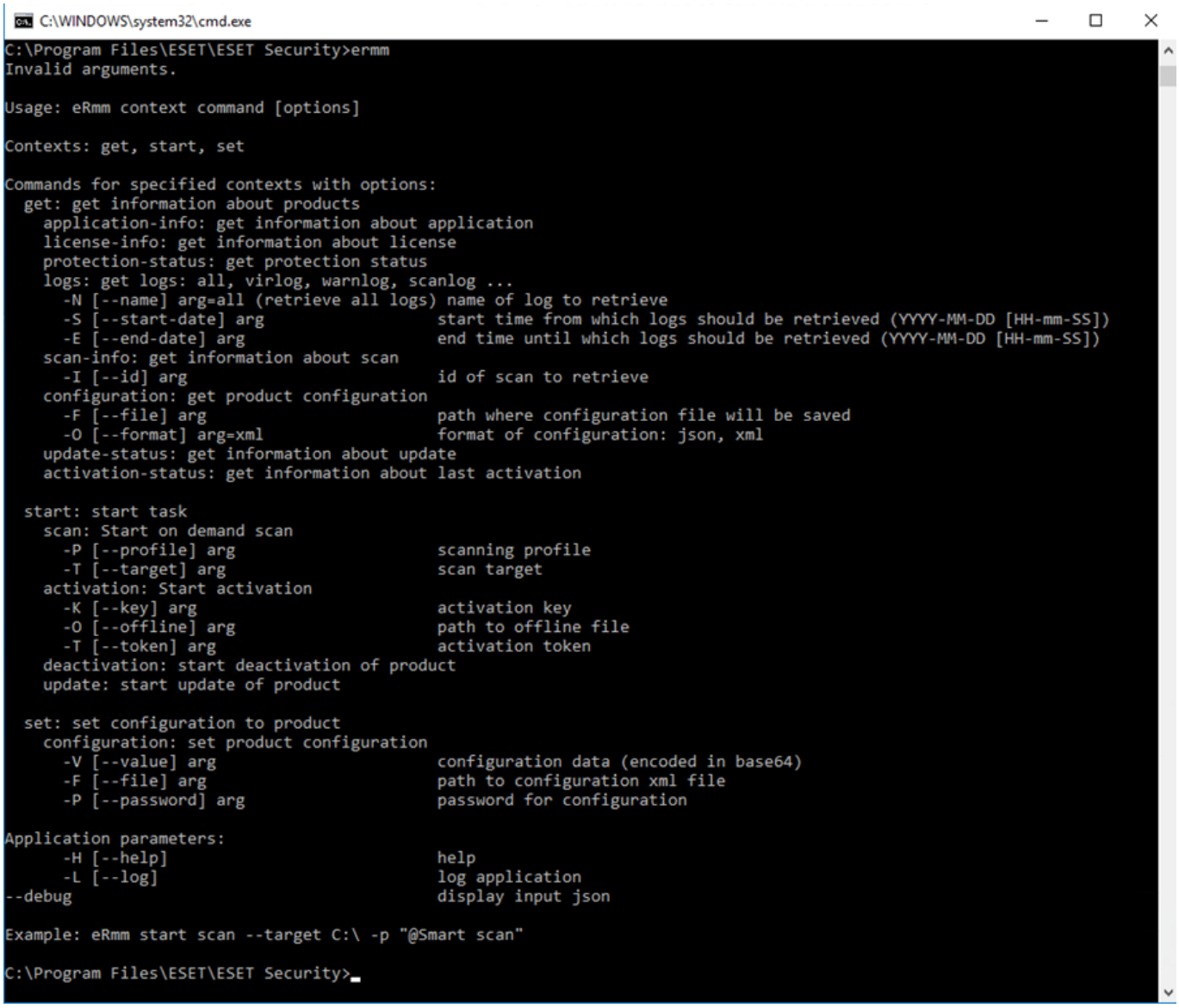
Ligne de commande ERMM

La gestion de la surveillance à distance est exécutée à l'aide de l'interface à ligne de commande. L'installation par défaut d'ESET Endpoint Security contient le fichier ermm.exe situé dans l'application Endpoint au sein du répertoire : *c:\Program Files\ESET\ESET Security*.

Exécutez l'invite de commande (cmd.exe) en tant qu'administrateur et accédez au chemin indiqué (pour ouvrir l'invite de commande, appuyez sur le bouton Windows + R du clavier, tapez cmd dans la fenêtre Exécuter, puis appuyez sur Entrée).

La syntaxe de la commande est la suivante : `ermm context command [options]`

Les paramètres des journaux respectent la casse.



ermm.exe utilise trois contextes de base : Obtenir, Démarrer et Définir. Le tableau ci-dessous vous permet de trouver des exemples de syntaxe de commandes. Cliquez sur le lien de la colonne Commande pour voir les autres options, paramètres et exemples d'utilisation. Une fois la commande exécutée, la partie « sortie » (résultat) s'affiche. Pour voir une partie d'entrée, ajoutez un paramètre `--debug` à la commande.

Contexte	Commande	Description
get		**Obtenir des informations sur les produits**
	application-info	Obtenir des informations sur le produit
	license-info	Obtenir des informations sur la licence
	protection-status	Obtenir l'état de la protection
	logs	Get logs
	scan-info	Obtenir des informations sur l'analyse en cours
	configuration	Obtenir la configuration du produit
	update-status	Obtenir des informations sur la mise à jour
	activation-status	Obtenir des informations sur la dernière activation
start		**Start task**
	scan	Démarrer l'analyse à la demande

Contexte	Commande	Description
	activation	Démarrer l’activation du produit
	deactivation	Démarrer la désactivation du produit
	update	Démarrer la mise à jour du produit
set		**Définir les options du produit**
	configuration	Définir la configuration sur le produit

Dans le résultat de chaque commande, les premières informations affichées sont un ID de résultat. Pour mieux comprendre les informations des résultats, consultez le tableau des ID ci-dessous.

ID de l'erreur	Erreur	Description
0	Success	
1	Command node not present	Nœud « Command » absent de l’entrée json
2	Command not supported	La commande n'est pas prise en charge.
3	General error executing the command	Erreur lors de l’exécution de la commande
4	Task already running	La tâche demandée est déjà en cours d’exécution et n’a pas été démarrée
5	Invalid parameter for command	Entrée utilisateur incorrecte
6	Command not executed because it's disabled	RMM n’est pas activé dans les paramètres avancés ni démarré en tant qu’administrateur

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

Ligne de commande

```
ermm.exe get protection-status
```

Paramètres

None

Exemple

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

Ligne de commande

```
ermm.exe get application-info
```

Paramètres

None

Exemple

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":"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

Ligne de commande

```
ermm.exe get license-info
```

Paramètres

None

Exemple

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

Ligne de commande

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-
date "2017-04-04 12-00-00"
```

Paramètres

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])

Exemple

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, running, failure }

Ligne de commande

```
ermm.exe get activation-status
```

Paramètres

None

Exemple

call

```
{
"command":"get_activation_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"status":"success"
},
"error":null
}
```

get scan-info

Obtenir des informations sur l'analyse en cours.

Ligne de commande

```
ermm.exe get scan-info
```

Paramètres

Aucun

Exemple

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 }

Ligne de commande

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

Paramètres

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Exemple

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 }

Ligne de commande

```
ermm.exe get update-status
```

Paramètres

None

Exemple

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

Ligne de commande

```
ermm.exe start scan --profile "profile name" --target "path"
```

Paramètres

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Exemple

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

Ligne de commande

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

Paramètres

Name	Value
key	Activation key

offline	Path to offline file

Exemple

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

Ligne de commande

```
ermm.exe start deactivation
```

Paramètres

None

Exemple

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

Ligne de commande

```
ermm.exe start update
```

Paramètres

None

Exemple

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 }

Ligne de commande

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Paramètres

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)

Exemple

call

```
{
"command":"set_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml",
"password": "pass"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

Intervalle de vérification des licences

ESET Endpoint Security doit se connecter automatiquement aux serveurs de licences ESET. Vous pouvez limiter le nombre de connexions au serveur de licences ESET dans Configurations avancées > **Outils** > **Licence**. Par défaut, la **Vérification de l'intervalle** est définie sur **Automatique** et la connexion est établie plusieurs fois par heure. En cas d'augmentation du trafic réseau, définissez la **Vérification de l'intervalle** sur **Limité** pour réduire la surcharge. Lorsque l'option **Limité** est sélectionnée, ESET Endpoint Security ne vérifie le serveur de licences qu'une fois par jour ou au redémarrage de l'ordinateur.

Si la configuration **Vérification de l'intervalle** est définie sur **Limité**, toutes les modifications associées aux licences effectuées via ESET PROTECT HUB/ESET MSP Administrator peuvent prendre jusqu'à un jour pour s'appliquer aux configurations d'ESET Endpoint Security.

Fichiers journaux

La configuration de la journalisation d'ESET Endpoint Security est accessible dans Configurations avancées > **Outils** > **Fichiers journaux**. La section des fichiers journaux permet de définir la manière dont les journaux sont gérés. Le programme supprime automatiquement les anciens fichiers journaux pour gagner de l'espace disque. Les options suivantes peuvent être spécifiées pour les fichiers journaux :

Verbosité minimale des journaux – Spécifie le niveau minimum de verbosité des événements à consigner :

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

- **Critique** – Consigne uniquement les erreurs critiques (erreur de démarrage de la protection antivirus, pare-feu intégré, etc.).

> Toutes les connexions bloquées sont enregistrées lorsque vous sélectionnez le niveau de verbosité **Diagnostic**.

Les entrées des journaux plus anciennes que le nombre de jours spécifiés dans le champ **Supprimer automatiquement les entrées plus anciennes que (jours)** seront automatiquement supprimées.

Optimiser automatiquement les fichiers journaux : si cette option est activée, ESET Endpoint Security défragmente automatiquement les fichiers journaux si le pourcentage de fragmentation est supérieur à la valeur spécifiée dans le champ **Si le nombre d'entrées inutilisées dépasse (%)**. L'optimisation est un processus de défragmentation des fichiers, ce qui signifie qu'<%PRODUCTNAME %> supprimera tous les enregistrements inutilisés.

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.

> Pour résoudre les problèmes plus rapidement, ESET peut vous demander de fournir les journaux de votre ordinateur. ESET Log Collector facilite la collecte des informations nécessaires. Pour plus d'informations sur ESET Log Collector, consultez cet article de la base de connaissances ESET.

Mode 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 de notification/d'alerte et veulent réduire les contraintes sur l'CPU. Il peut également être utilisé au cours de présentations qui ne peuvent pas être interrompues par l'activité antivirus. Lorsque cette fonctionnalité est activée, toutes les fenêtres contextuelles sont désactivées et l'activité du planificateur est complètement arrêtée. La protection du système continue à fonctionner en arrière-plan, mais n'exige aucune interaction de la part de l'utilisateur.

Vous pouvez activer ou désactiver le mode de présentation dans la fenêtre principale du programme en cliquant sur **Configuration** > **Ordinateur**, puis sur  ou  à côté de **Mode de présentation**. 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.

Activez l'option **Activer le mode de présentation automatiquement lors de l'exécution d'applications en mode plein écran** dans Configuration avancée > **Outils** > **Mode de présentation** pour que le mode de présentation démarre dès que vous lancez une application en mode plein écran et s'arrête lorsque vous quittez l'application.

Activez l'option **Désactiver automatiquement le mode de présentation après** pour définir une durée après laquelle le mode de présentation est automatiquement désactivé.

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

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 Security 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 moteur antispam – Enregistrez tous les événements qui se produisent pendant l'analyse antispam. Les développeurs peuvent ainsi diagnostiquer et résoudre les problèmes liés au moteur antispam ESET.

Activer la journalisation avancée de la protection du navigateur : Enregistrez tous les événements qui se produisent dans le Navigateur sécurisé pour permettre un diagnostic et la résolution des problèmes.

Activer la journalisation avancée de l'analyseur de l'ordinateur – Enregistrez tous les événements qui se produisent lors de l'analyse des fichiers et des dossiers par l'analyse de l'ordinateur ou la protection en temps réel du système de fichiers.

Activer la journalisation avancée du contrôle des appareils – Enregistrez tous les événements qui se produisent dans le contrôle des appareils. Les développeurs peuvent ainsi diagnostiquer et résoudre les problèmes liés au contrôle des appareils.

Activer la journalisation avancée de Direct Cloud : Enregistrez toutes les communications du produit entre celui-ci et les serveurs Direct Cloud.

Activer la journalisation avancée de la protection des documents – Enregistrez tous les événements qui se produisent dans la protection des documents pour permettre un diagnostic et la résolution des problèmes.

Activer la journalisation avancée de la protection du client de messagerie – Enregistrez tous les événements qui se produisent dans la protection du client de messagerie et le module d'extension du client de messagerie pour permettre un diagnostic et la résolution des problèmes.

Activer la journalisation avancée du noyau – Enregistrez tous les événements qui se produisent dans le service du noyau ESET (ekrn) pour permettre le diagnostic et la résolution des problèmes.

Activer la journalisation avancée des licences – Enregistrez toutes les communications du produit avec les serveurs d'activation et de licences ESET.

Activer le suivi de la mémoire – Enregistrez tous les événements qui permettront aux développeurs de diagnostiquer les fuites de mémoire.

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 de l'analyseur du trafic réseau : enregistrez toutes les données passant par l'analyseur du trafic réseau au format PCAP pour aider les développeurs à diagnostiquer et à résoudre les problèmes liés à l'analyseur du trafic réseau.

Activer la journalisation avancée du système d'exploitation – 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 des messages Push : Enregistrez tous les événements qui se produisent pendant les messages Push pour permettre les diagnostics et la résolution des problèmes.

Activer la journalisation avancée de la protection en temps réel du système de fichiers – Enregistrez tous les événements qui se produisent dans la protection en temps réel du système de fichiers pour permettre un diagnostic et la résolution des problèmes.

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 de la gestion des vulnérabilités et des correctifs – Enregistrez tous les événements qui se produisent dans la gestion des vulnérabilités et des correctifs. Cette configuration n'est affichée que si la gestion des vulnérabilités et des correctifs est activée dans votre environnement (activée dans ESET PROTECT).

Activer la journalisation avancée du filtrage Internet – Enregistrez tous les événements qui se produisent dans le filtrage web. Les développeurs peuvent ainsi diagnostiquer et résoudre les problèmes liés au filtrage web.

Les fichiers journaux sont situés dans *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Assistance technique

Lorsque vous contactez l'assistance technique ESET dans ESET Endpoint Security, vous pouvez envoyer les données de configuration système. Sélectionnez **Toujours soumettre** dans le menu déroulant **Soumettre les données de configuration système** pour soumettre automatiquement les données. Vous pouvez également sélectionner **Demander avant soumission** pour que le système vous demande si vous souhaitez soumettre effectivement les données.

Connectivité

Dans des réseaux spécifiques, les communications entre votre ordinateur et Internet peuvent s'effectuer par l'intermédiaire d'un serveur proxy. Si vous utilisez un serveur proxy, vous devez définir les paramètres ci-après. Sinon, ESET Endpoint Security et ses modules ne peuvent pas être mis à jour automatiquement. Dans ESET Endpoint Security, la configuration du serveur proxy est disponible dans deux sections différentes des Configurations avancées.

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

Pour spécifier les paramètres globaux du serveur proxy, activez **Utiliser un serveur proxy** et saisissez l'adresse du **serveur proxy** avec le numéro de **port** du serveur proxy.

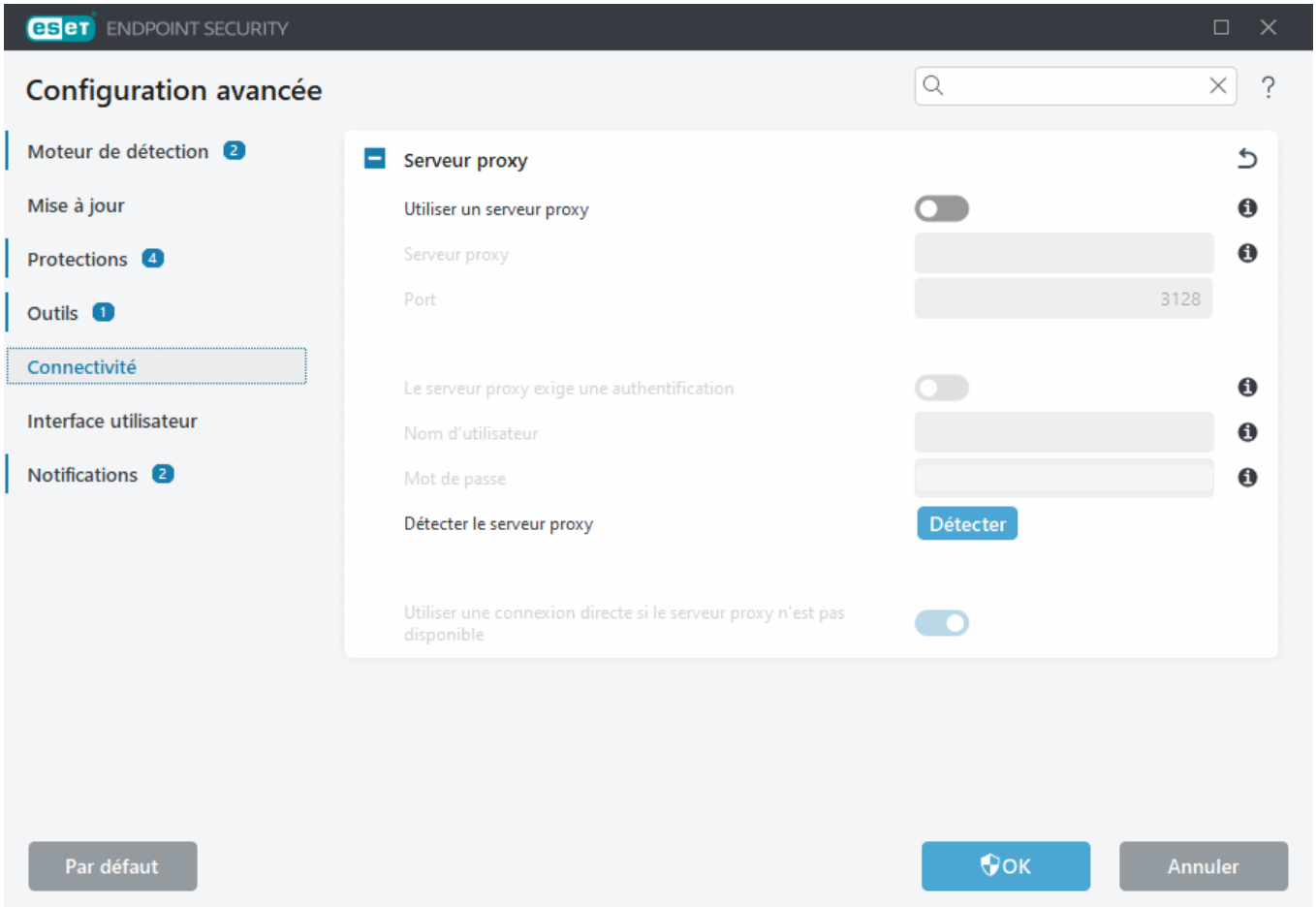
Si les communications avec le serveur proxy exigent une authentification, sélectionnez **Le serveur proxy nécessite une authentification** et entrez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants. Cliquez sur **Détecter** pour détecter et renseigner automatiquement les paramètres du serveur proxy. Pour trouver les paramètres de proxy dans votre système d'exploitation, appuyez sur les touches de raccourci **Windows + I**,

puis cliquez sur **Réseau et Internet** > **Proxy**. ESET Endpoint Security copiera les paramètres spécifiés dans les options internet pour Internet Explorer ou Google Chrome.

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

Utiliser une connexion directe si le proxy HTTP n'est pas disponible – Si ESET Endpoint Security est configuré pour se connecter via le proxy et que ce dernier est injoignable, ESET Endpoint Security ignore le proxy et communique directement avec les serveurs ESET.

Les paramètres du serveur proxy peuvent également configurés dans Configurations avancées > **Mise à jour** > **Profils** > **Mises à jour** > **Options de connexion** en sélectionnant **Connexion via un serveur proxy** dans le menu déroulant **Mode proxy**. Cette configuration ne s'applique qu'aux mises à jour et est recommandée pour les ordinateurs portables recevant des mises à jour de modules à partir de sites distants. Pour plus d'informations, consultez Configuration avancée des mises à jour.



Interface utilisateur

Pour configurer le comportement de l'interface utilisateur graphique (GUI) du programme, ouvrez Configurations avancées > **Interface utilisateur**.

Vous pouvez ajuster l'apparence du programme et les effets dans l'écran des configurations avancées Éléments de l'interface utilisateur.

Afin de bénéficier de la sécurité maximum de votre logiciel de sécurité, vous pouvez empêcher toute

désinstallation ou modification non autorisée en protégeant les paramètres par un mot de passe à l'aide de l'outil Configuration de l'accès.

> Pour configurer le comportement des notifications système, des alertes de détection et des états d'application, consultez la section Notifications.

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 Security (utilise pour les environnements administrés).

Éléments de l'interface utilisateur

La configuration de l'interface utilisateur d'ESET Endpoint Security peut être modifiée de manière à adapter l'environnement de travail à vos besoins. Ces options de configuration sont accessibles dans **Configuration avancée** (F5) > **Interface utilisateur** > **Éléments de l'interface utilisateur**.

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.

> Une fois le mode de démarrage Minimal sélectionné et l'ordinateur redémarré, les notifications s'affichent, mais pas l'interface graphique. Pour rétablir le mode complet, exécutez l'interface utilisateur graphique dans le menu Démarrer, **Tous les programmes** > **ESET** > ESET Endpoint Security (en tant qu'administrateur). Vous pouvez également effectuer cette opération via ESET PROTECT On-Prem à l'aide d'une politique.

Mode couleur – Sélectionnez le modèle de couleur de l'interface utilisateur graphique ESET Endpoint Security dans le menu déroulant :

- **Identique à la couleur système** – Le modèle de couleurs d'ESET Endpoint Security est défini selon les paramètres du système d'exploitation.
- **Sombre** – ESET Endpoint Security aura un modèle de couleurs foncées (mode sombre).
- **Clair** – ESET Endpoint Security aura un modèle de couleurs clairs standard.

> Vous pouvez également sélectionner le modèle de couleurs de l'interface utilisateur graphique d'ESET Endpoint Security dans le coin supérieur droit de la fenêtre principale du programme.

Pour désactiver l'écran de démarrage de ESET Endpoint Security, désactivez **Afficher l'écran de démarrage**.

Pour qu'ESET Endpoint Security émette un signal sonore en cas d'événement important lors d'une analyse, par exemple lorsqu'une menace est découverte ou lorsque l'analyse est terminée, sélectionnez **Utiliser un signal sonore**.

Intégrer dans le menu contextuel – Intègre les options ESET Endpoint Security dans le menu contextuel.

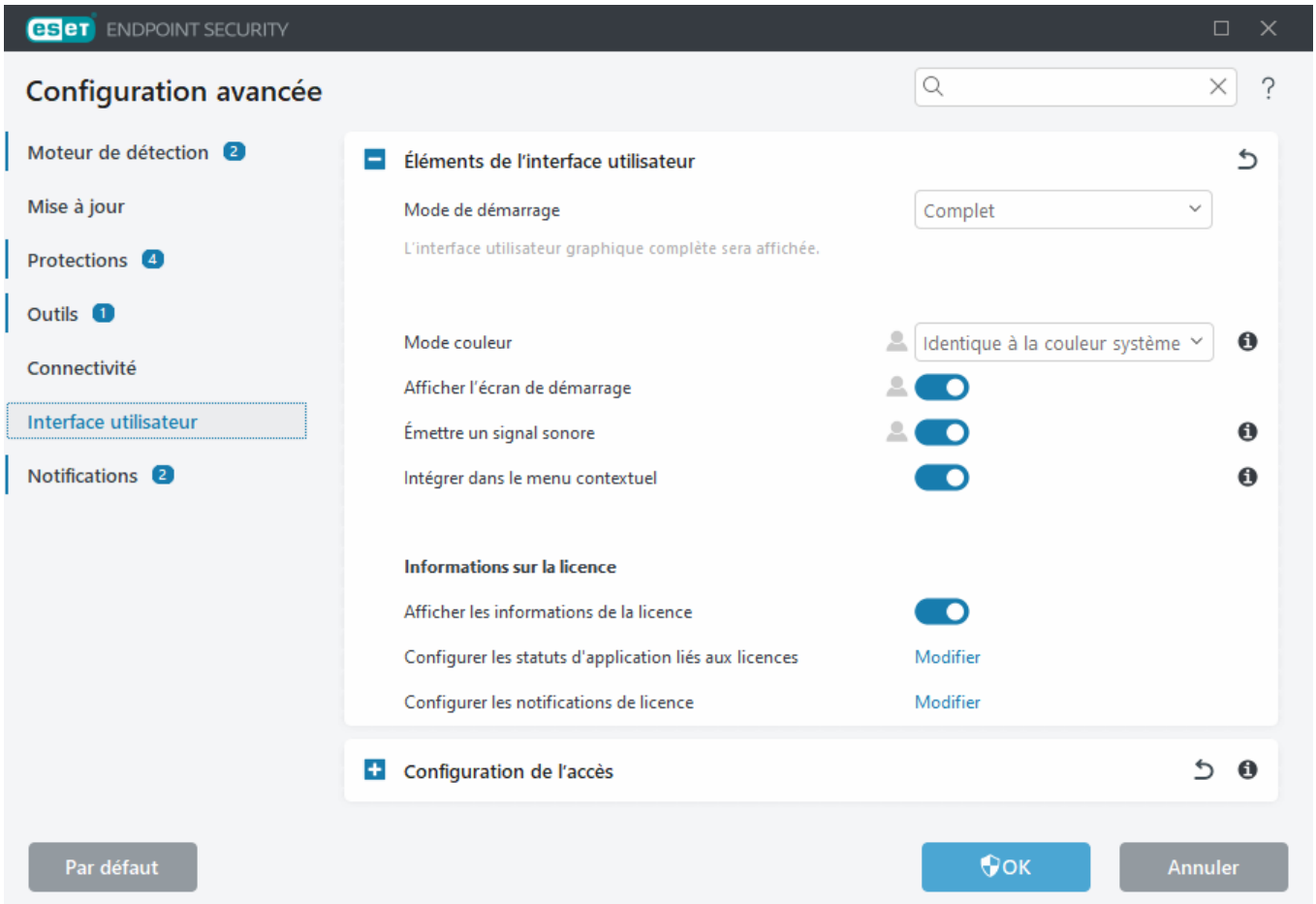
Informations sur la licence

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**.

Configurer les statuts d'application liés aux licences—Ouvre la liste desstatuts d'application liés aux licences.

Configurer les notifications de licence : ouvre la liste des notifications liées aux licences.

> Les paramètres d'informations sur la licence sont appliqués mais ne sont pas accessibles pour ESET Endpoint Security activé à l'aide d'une licence MSP.



Configuration de l'accès

Les paramètres de ESET Endpoint Security constituent une partie essentielle de votre stratégie de sécurité. Des modifications non autorisées peuvent mettre en danger la stabilité et la protection de votre système. Pour éviter des modifications non autorisées, les paramètres de la configuration d'ESET Endpoint Security peuvent être

protégés par mot de passe. La configuration de l'accès peut être définie dans Configurations avancées > **Interface utilisateur** > **Configuration de l'accès**.

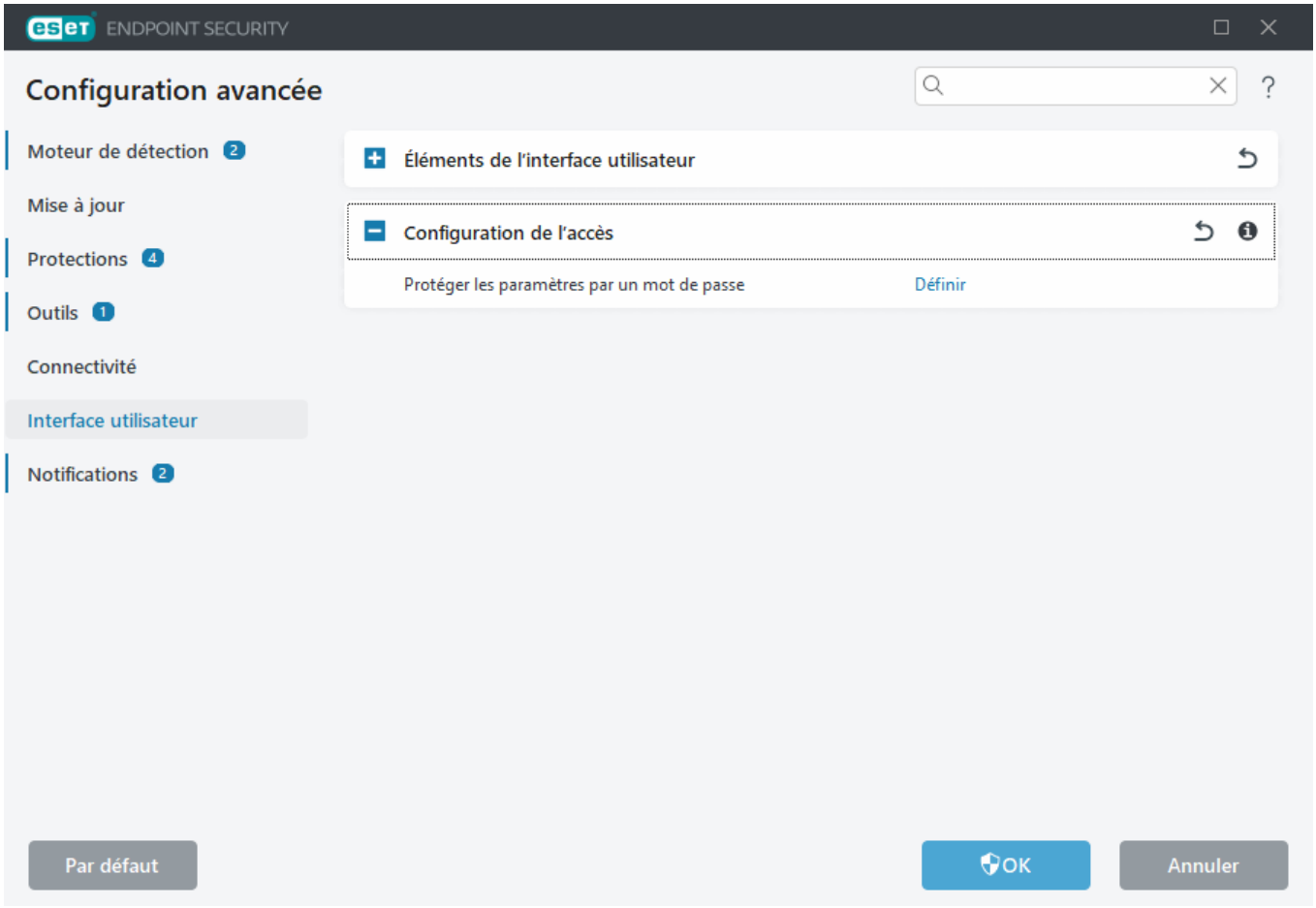
Pour définir un mot de passe afin de protéger les paramètres de configuration et empêcher la désinstallation d'ESET Endpoint Security, cliquez sur **Définir** en regard de l'option **Protéger les paramètres par un mot de passe**.

Pour changer votre mot de passe, cliquez sur **Modifier le mot de passe** en regard de l'option **Protéger les paramètres par mot de passe**.

Pour supprimer votre mot de passe, cliquez sur **Supprimer** en regard de l'option **Protéger les paramètres par mot de passe**.

Environnements gérés

L'administrateur peut créer une politique de façon à protéger les configurations de ESET Endpoint Security par mot de passe sur les ordinateurs clients connectés. Pour créer une politique, consultez Configurations protégées par mot de passe.



Mot de passe des configurations avancées

Pour protéger les configurations avancées d'ESET Endpoint Security et éviter toute modification non autorisée, saisissez le nouveau mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**. Cliquez sur **OK**.

Environnements gérés

L'administrateur peut créer une politique de façon à protéger les configurations de ESET Endpoint Security 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 Security.

Si vous avez oublié votre mot de passe, consultez l'article Déverrouiller le mot de passe de paramètres dans les produits ESET Endpoint.

Pour récupérer votre clé de licence ESET perdue, la date d'expiration de votre licence ou d'autres informations sur votre licence pour ESET Endpoint Security, consultez l'article J'ai perdu mes nom d'utilisateur et mot de passe/clé de licence..

Mot de passe

Pour éviter des modifications non autorisées, les paramètres de la configuration d'ESET Endpoint Security peuvent être protégés par mot de passe.

Mode sans échec

Si l'interface graphique d'ESET Endpoint Security est lancée en mode sans échec, une boîte de dialogue s'affiche, indiquant que l'application va s'exécuter en mode sans échec. Étant donné que tous les programmes sont limités dans ce mode, il n'est pas possible d'ouvrir l'interface graphique d'ESET Endpoint Security comme dans le mode standard.

La fenêtre affichée vous permettra de lancer une analyse de l'ordinateur. Si vous souhaitez vérifier l'absence de code malveillant sur l'ordinateur, sélectionnez l'option **Oui**.

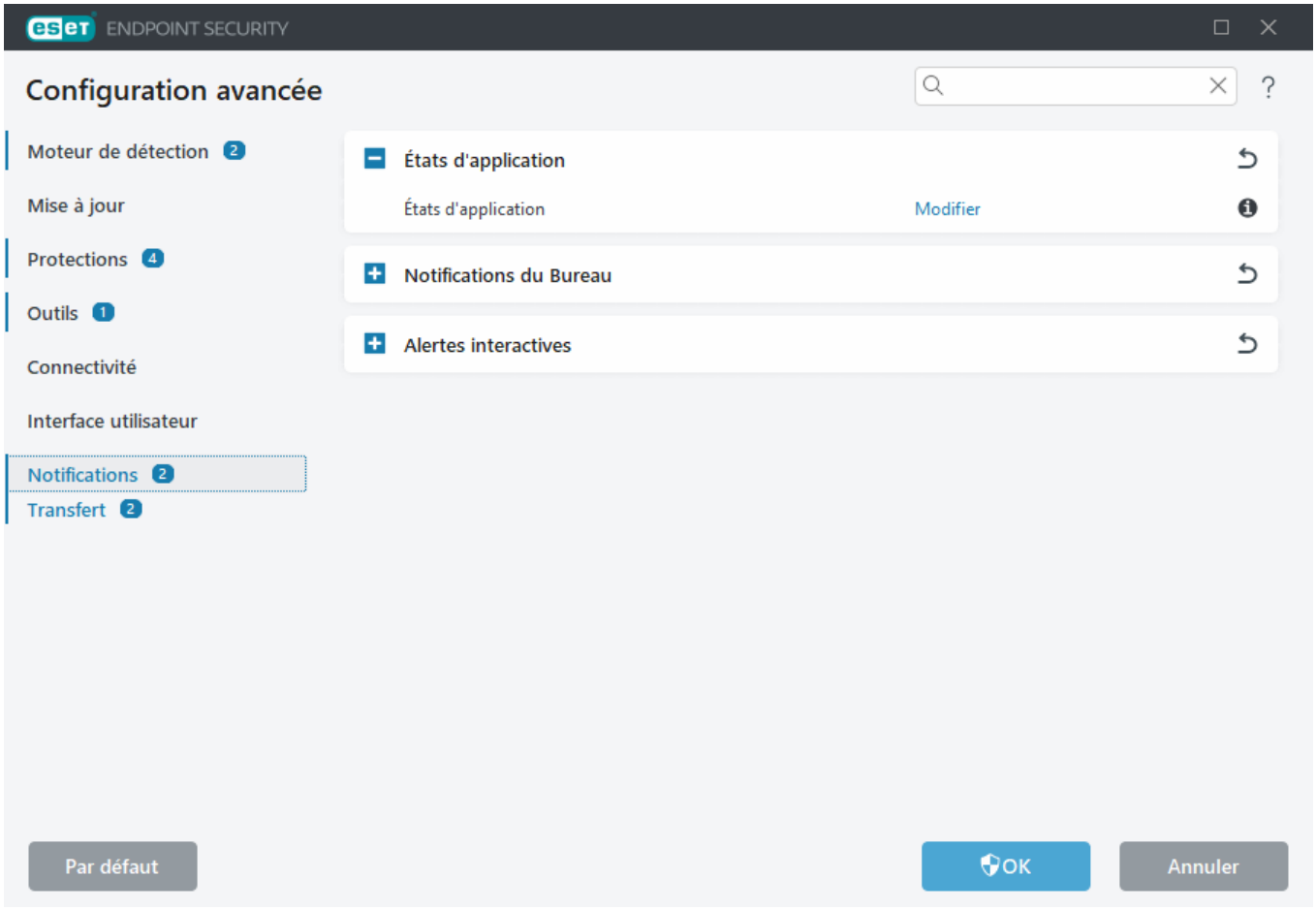
L'analyse est alors lancée dans une fenêtre séparée, avec les mêmes paramètres que ceux du profil d'analyse de l'ordinateur par défaut créé après l'installation d'ESET Endpoint Security.

Sélectionnez l'option **Non** pour fermer la boîte de dialogue ; ESET Endpoint Security n'effectue aucune opération.

Notifications

Pour gérer les notifications d'ESET Endpoint Security, ouvrez Configurations avancées > **Notifications**. Vous pouvez configurer les types de notifications suivants :

- États d'application : notifications affichées dans la section d'accueil de la fenêtre principale du programme.
- Notifications du Bureau : petites notifications en regard de la barre des tâches système.
- Alertes interactives : fenêtres d'alerte et boîtes de message qui nécessitent une interaction de l'utilisateur.
- Transfert (notifications par e-mail) : sont envoyées à l'adresse e-mail indiquée.
- Personnalisation des notifications : permet d'ajouter un message personnalisé à une notification du bureau, par exemple.



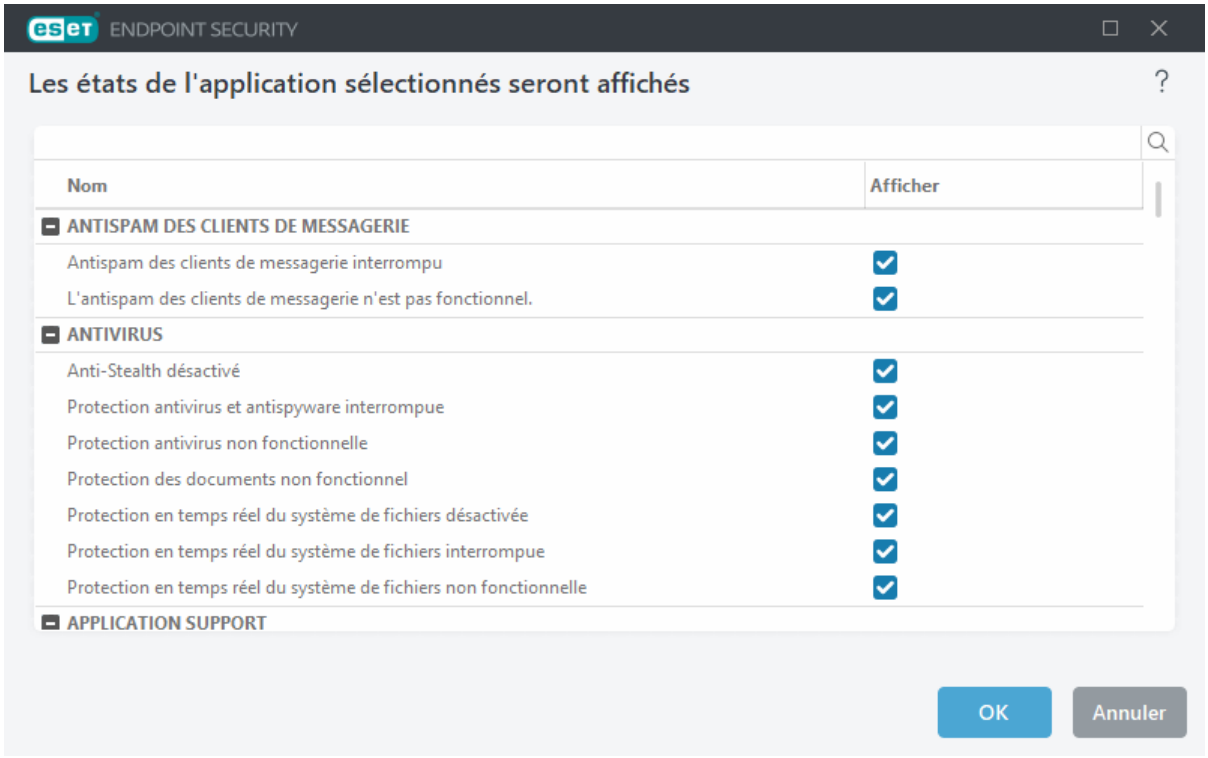
États d'application

États d'application : cliquez sur **Modifier** pour sélectionner les états d'application qui seront affichés dans la section d'accueil de la fenêtre principale du programme.

États d'application

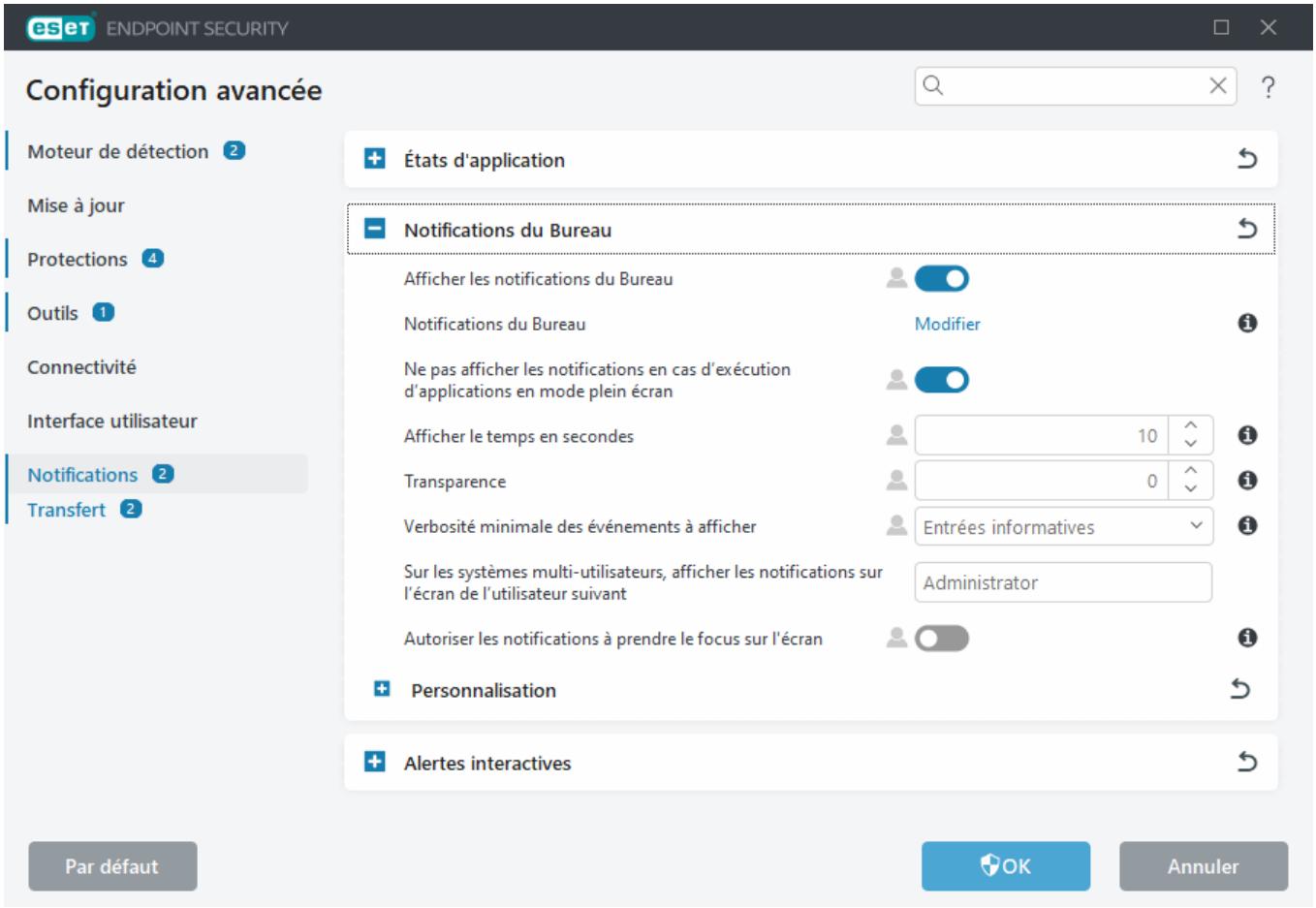
Pour configurer quels états d'application seront affichés (lorsque vous suspendez la protection antivirus et antispyware ou activez le mode de présentation, par exemple), ouvrez les Configurations avancées > **Notifications**, puis cliquez sur **Modifier** en regard de l'option **États d'application**.

Un état d'application est également affiché si votre produit n'est pas activé ou si votre licence est arrivée à expiration. Cette configuration peut être modifiée par le biais des politiques d'ESET PROTECT On-Prem.



Notifications du Bureau

Une notification du bureau est une petite fenêtre de notification située à côté de la barre des tâches système. Par défaut, elle est configurée pour s'afficher pendant 10 secondes et disparaître lentement. C'est la méthode principale utilisée par ESET Endpoint Security 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.



Afficher les notifications sur le Bureau : il est recommandé de laisser cette option activée afin que le produit puisse vous informer lorsqu'un nouvel événement se produit.

Notifications du Bureau : cliquez sur **Modifier** pour activer ou désactiver des Notifications du Bureau spécifiques.

Ne pas afficher les notifications en cas d'exécution d'applications en mode plein écran : supprime toutes les notifications qui ne sont pas interactives lors de l'exécution d'applications en mode plein écran.

Délai d'attente en secondes – Définissez la durée de visibilité de la notification. La valeur doit être entre 3 et 30 secondes.

Transparence – Définissez le pourcentage de transparence de la notification. La plage prise en charge est comprise entre 0 (pas de transparence) et 80 (transparence très élevée).

Verbosité minimale des événements à afficher – Définissez le niveau de gravité de départ des notifications affichées. Dans le menu déroulant, sélectionnez l'une des options suivantes :

- **Diagnostic** – Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** – Enregistre tous les messages d'information (les événements réseau non standard, par exemple), y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissements** – Enregistre les erreurs critiques et les messages d'avertissement (par exemple, l'échec d'une mise à jour).
- **Erreurs** – Enregistre les erreurs (la protection des documents n'a pas démarré) et les erreurs critiques.
- **Critique** – 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 – Permet au compte sélectionné de recevoir des notifications sur le Bureau. Par exemple, si vous n'utilisez pas le compte Administrateur, saisissez le nom complet du compte pour que les notifications du Bureau s'affichent pour ce compte. Seul un compte d'utilisateur peut recevoir les notifications sur le Bureau.

Autoriser les notifications à prendre le focus sur l'écran – Les notifications prendront le focus sur l'écran et seront accessibles à l'aide de Alt+Tab.

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.

Détections

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 détection** pour utiliser des messages de notification personnalisés.

Boîte de dialogue - Notifications du Bureau

Pour régler la visibilité des notifications du Bureau (affichées en bas à droite de l'écran), ouvrez les Configurations avancées > **Notifications** > **Notifications du Bureau**. Cliquez sur **Modifier** en regard de **Notifications du Bureau**, puis cochez la case **Afficher sur le Bureau** appropriée.

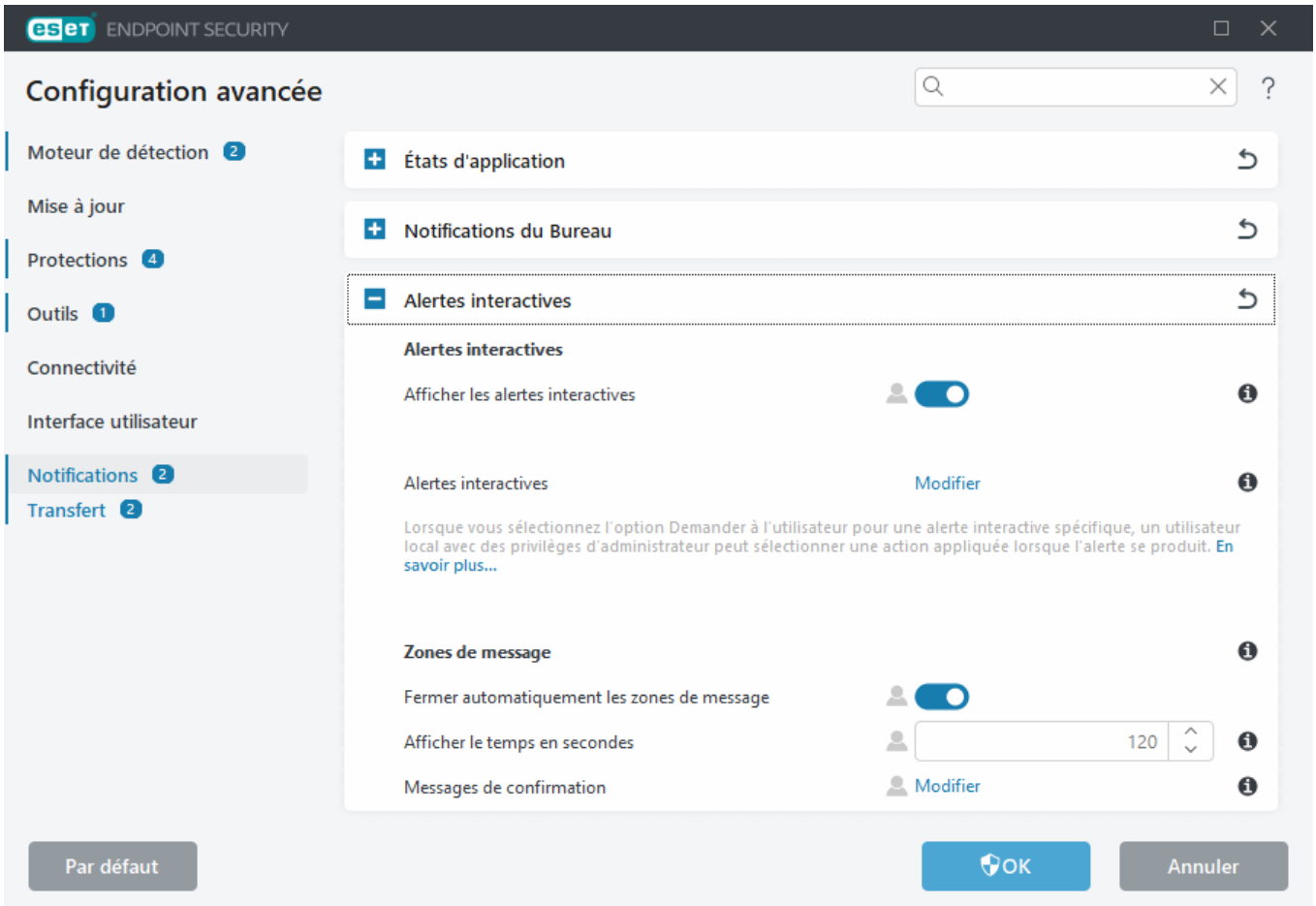
Si vous souhaitez configurer les notifications **Fichier analysé** et **Fichier non analysé** pendant l'utilisation d'ESET LiveGuard, la protection proactive doit être définie sur **Bloquer l'exécution jusqu'à la réception du résultat de l'analyse**.

Alertes interactives

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
- Fichier bloqué en raison de l'analyse

La section **Alertes interactives** dans Configurations avancées > **Notifications** vous permet de configurer la manière dont ESET Endpoint Security traite les boîtes de message et les alertes interactives pour les détections pour lesquelles une décision doit être prise par un utilisateur (par exemple, un site web d'hameçonnage potentiel).



Alertes interactives

Lorsque l'option **Afficher les alertes interactives** est désactivée, toutes les fenêtres et les boîtes de dialogue dans le navigateur sont masquées, ce qui ne convient qu'à un nombre limité de situations particulières.

- 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.

Alertes interactives – Cliquez sur **Modifier** pour sélectionner les alertes interactives à afficher.

Zones de message

Pour fermer automatiquement les boîtes de message après un certain délai, sélectionnez **Fermer automatiquement les zones de message**. Si les fenêtres d'alerte ne sont pas fermées manuellement, le système les ferme automatiquement une fois le laps de temps écoulé.

Délai d'attente en secondes – Définit la durée de visibilité de l'alerte. La valeur doit être entre 10 et 999 secondes.

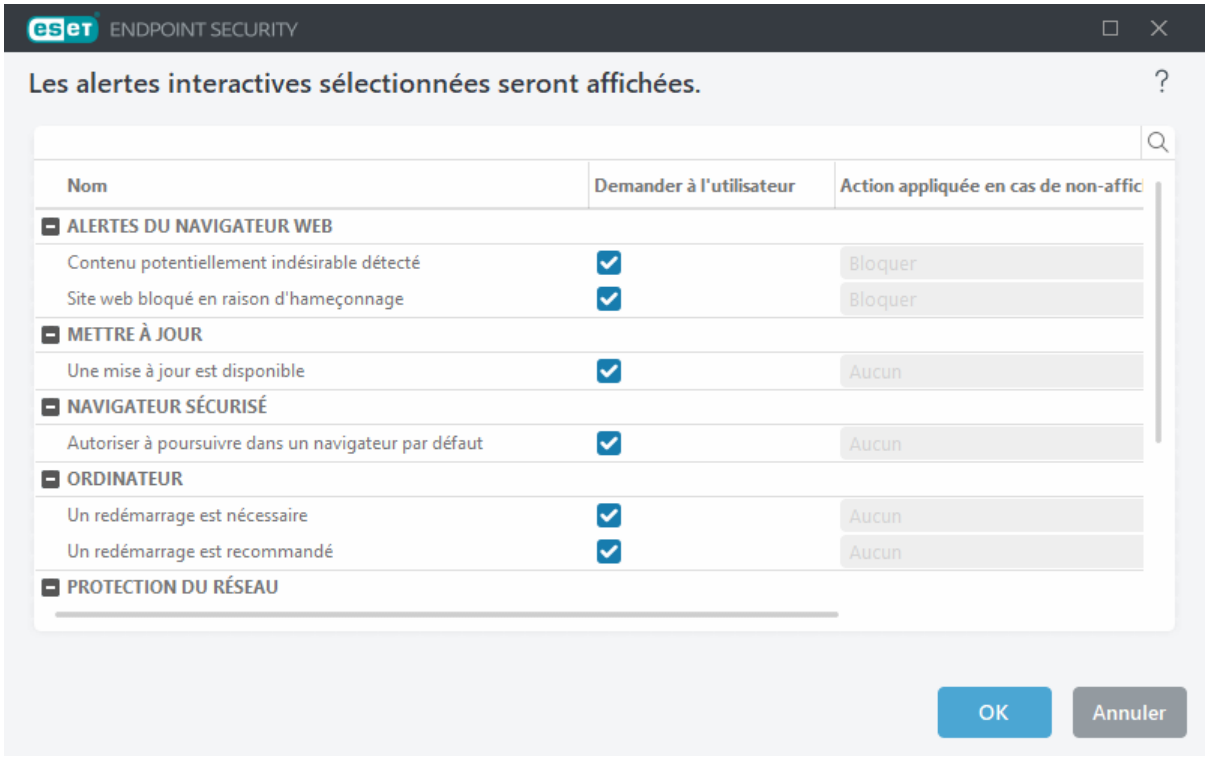
Messages de confirmation – Cliquez sur **Modifier** pour afficher une liste de messages de confirmation que vous pouvez choisir d'afficher ou non.

Liste des alertes interactives

Cette section décrit plusieurs fenêtres d'alerte interactives qu'ESET Endpoint Security affichera avant toute action.

Pour régler le comportement des alertes interactives configurables, ouvrez Configurations avancées > **Notifications** > **Alertes interactives**, puis cliquez sur **Modifier** en regard de **Alertes interactives**.

> 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.



Recherchez dans les autres sections de l'aide une fenêtre d'alerte interactive spécifique :

Supports amovibles

- Nouvel appareil détecté

Navigateur sécurisé

- Autoriser à poursuivre dans un navigateur par défaut

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 ESET PROTECT On-Prem.
- Communications réseau bloquées
- Menace réseau bloquée

Alertes du navigateur web

- Contenu potentiellement indésirable détecté
- Site web bloqué en raison d'hameçonnage

Ordinateur

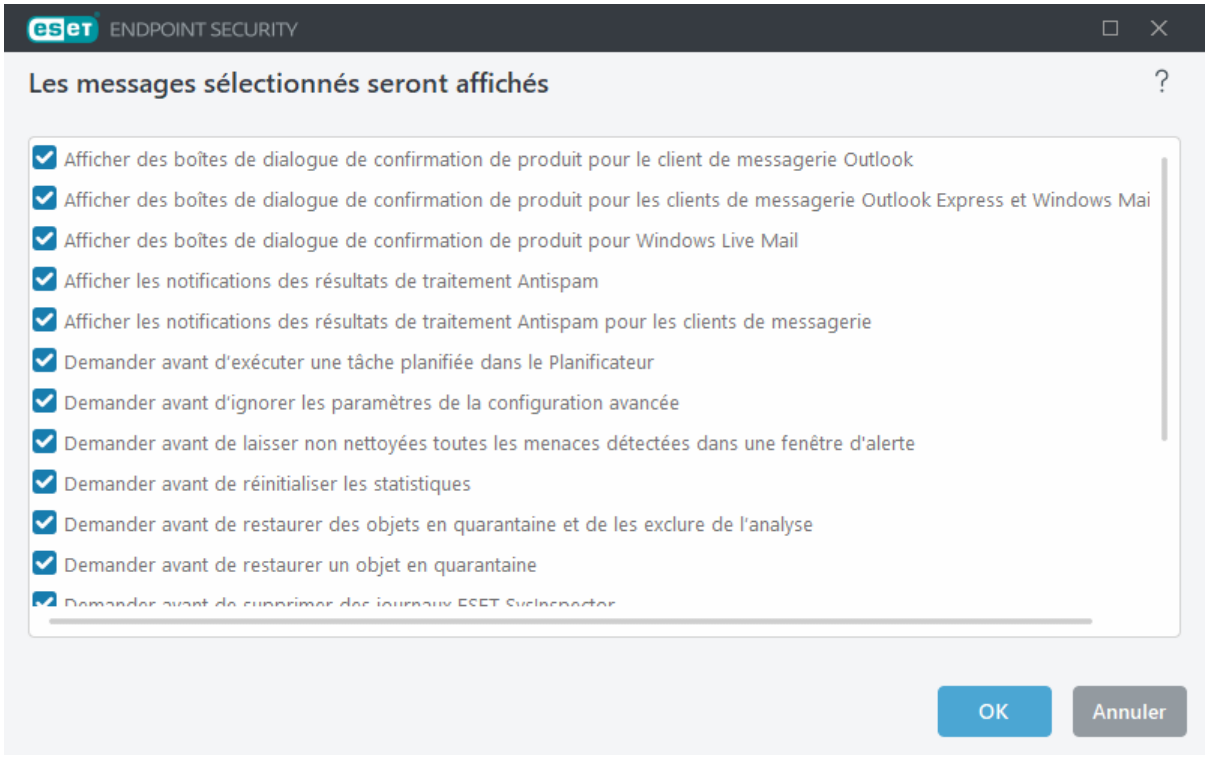
La présence de ces alertes modifiera la couleur de l'interface utilisateur :

- Redémarrer l'ordinateur (requis)
- Redémarrer l'ordinateur (recommandé)

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 Configurations avancées > **Notifications** > **Alertes interactives**, puis cliquez sur **Modifier** en regard de **Messages de confirmation**.



Cette boîte de dialogue contient les messages de confirmation qu'ESET Endpoint Security affiche avant l'exécution de toute action. Activez ou désactivez la case à cocher en regard de chaque message de confirmation pour l'activer ou non.

Découvrez la fonctionnalité spécifique liée aux messages de confirmation :

- Demander avant de supprimer les journaux ESET SysInspector
- Demander avant de supprimer tous les journaux ESET SysInspector
- Demander avant de supprimer un objet de quarantaine
- Demander avant d'ignorer les paramètres de la configuration avancée
- Demander avant de laisser non nettoyées toutes les menaces détectées dans une fenêtre d'alerte
- Demander avant de supprimer une entrée d'un journal
- Demander avant de supprimer une tâche planifiée dans le Planificateur
- Demander avant de supprimer toutes les entrées de journal
- Demander avant de réinitialiser les statistiques
- Demander avant de restaurer un objet en quarantaine
- Demander avant de restaurer des objets en quarantaine et de les exclure de l'analyse
- Demander avant d'exécuter une tâche planifiée dans le Planificateur
- Afficher les notifications des résultats de traitement Antispam
- Afficher les notifications des résultats de traitement Antispam pour les clients de messagerie
- Afficher des boîtes de dialogue de confirmation de produit pour les clients de messagerie Outlook Express et Windows Mail

- Afficher des boîtes de dialogue de confirmation de produit pour Windows Live Mail
- Afficher des boîtes de dialogue de confirmation de produit pour le client de messagerie Outlook

Erreur de conflit de paramètres avancés

Cette erreur peut se produire si un composant (par exemple le système HIPS ou le pare-feu) et un utilisateur créent simultanément les règles en mode interactif ou d'apprentissage.

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 mode d'apprentissage du Pare-feu ESET. En savoir plus sur le système HIPS et les modes de filtrage HIPS.

Autoriser à poursuivre dans un navigateur par défaut

Une alerte interactive spécifique ne s'affiche que lorsqu'une erreur se produit lors du démarrage du Navigateur sécurisé.

Redémarrage nécessaire

Un redémarrage de l'ordinateur est nécessaire après la mise à niveau d'ESET Endpoint Security vers une nouvelle version ou l'application de correctifs aux applications via la gestion des vulnérabilités et des correctifs. Les nouvelles versions d'ESET Endpoint Security offrent des améliorations ou apportent des solutions aux problèmes que les mises à jour automatiques des modules de programme ne peuvent pas résoudre.

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

Pour désactiver les alertes « Redémarrage requis » ou « Redémarrage recommandé », procédez comme suit :

1. Ouvrez **Configurations avancées** (F5) > **Notifications** > **Alertes interactives**.
2. Cliquez sur **Modifier** en regard de **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 Security, 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

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

Cliquez sur **Redémarrer maintenant** pour redémarrer votre ordinateur. Si vous envisagez de redémarrer votre ordinateur ultérieurement, cliquez sur **Me le rappeler ultérieurement**. Vous pourrez redémarrer manuellement

votre ordinateur dans la section **État de la protection** de la fenêtre principale du programme.

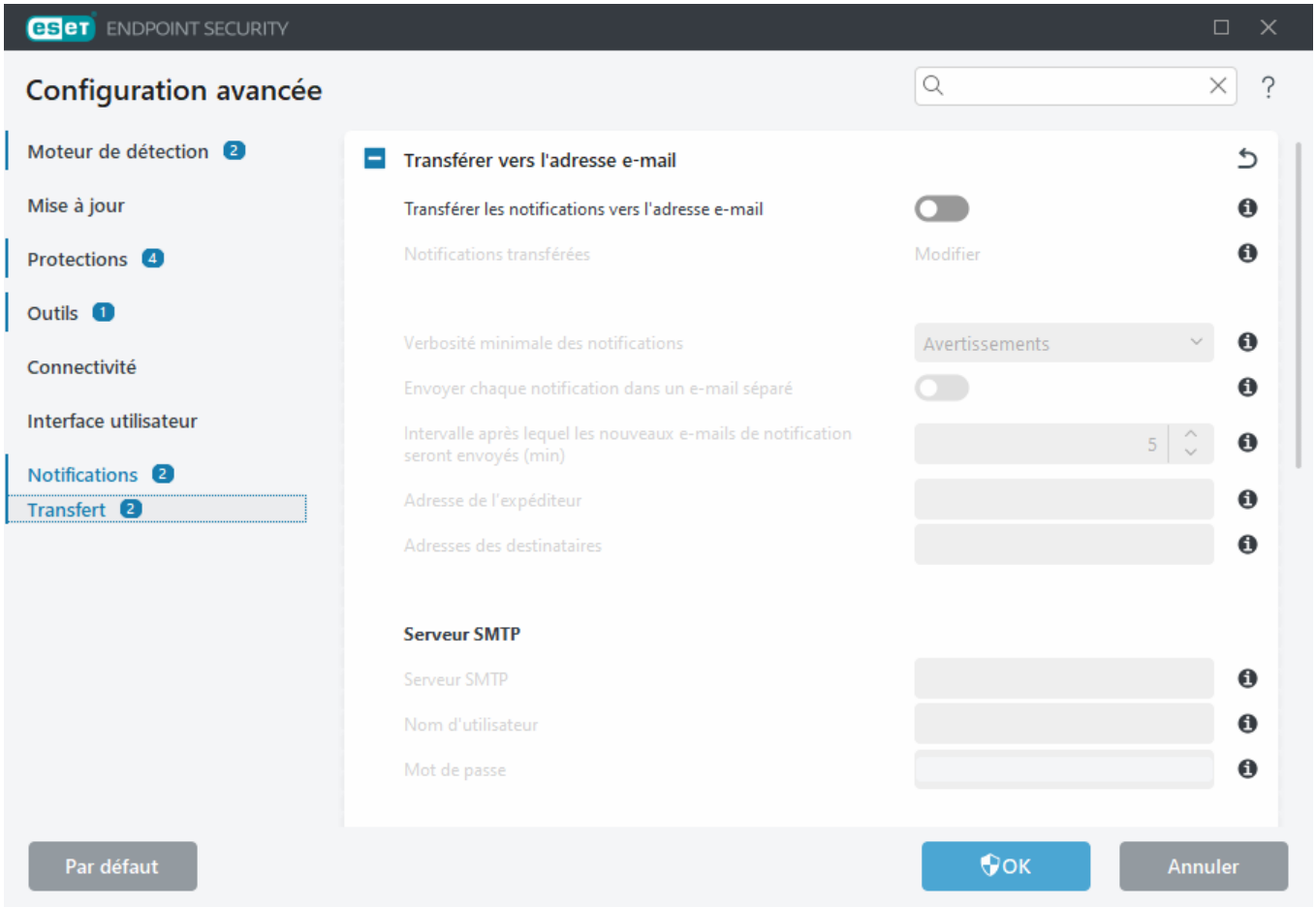
Pour désactiver les alertes « Redémarrage requis » ou « Redémarrage recommandé », procédez comme suit :

1. Ouvrez **Configurations avancées** (F5) > **Notifications** > **Alertes interactives**.
2. Cliquez sur **Modifier** en regard de **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 Security, 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**.

Transfert

ESET Endpoint Security peut automatiquement envoyer des e-mails de notification si un événement avec le niveau de verbosité sélectionné se produit. Dans la section Configurations avancées > **Notifications** > **Transfert** > **Transférer les notifications vers l'adresse e-mail**, activez **Transférer les notifications vers l'adresse e-mail** pour activer les notifications par e-mail.

Notifications transférées – Sélectionnez quelles notifications du Bureau sont transférées vers l'adresse e-mail.



Dans le menu déroulant **Verbosité minimale des notifications**, vous pouvez sélectionner le niveau de gravité de départ des notifications à envoyer.

- **Diagnostic** – Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** – Enregistre tous les messages d'information (les événements réseau non standard, par exemple), y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissements** – Enregistre les erreurs critiques et les messages d'avertissement (par exemple, l'échec d'une mise à jour).
- **Erreurs** – Enregistre les erreurs (la protection des documents n'a pas démarré) et les erreurs critiques.
- **Critique** – Enregistre uniquement les erreurs critiques (erreur de démarrage de la protection antivirus ou menace détectée, par exemple).

Envoyer chaque notification dans un e-mail séparé – Lorsque cette option est activée, le destinataire recevra un nouvel e-mail pour chaque notification. Cela peut se traduire par la réception de nombreux e-mails dans une courte période.

Intervalle après lequel les nouveaux e-mails de notification seront envoyés (min) – Intervalle en minutes après lequel de nouvelles notifications seront envoyées par e-mail. Si vous définissez cette valeur sur 0, les notifications sont envoyées immédiatement.

Adresse de l'expéditeur – Définit l'adresse de l'expéditeur qui apparaît dans l'en-tête des notifications.

Adresses des destinataires – Définit les adresses des destinataires qui apparaissent dans l'en-tête des notifications. Plusieurs valeurs sont prises en charge. Utilisez un point-virgule comme séparateur.

Serveur SMTP

Serveur SMTP – Serveur SMTP utilisé pour envoyer des notifications (*smtp.fournisseur.com:587*, le port prédéfini est le port 25).

> Les serveurs SMTP avec chiffrement TLS sont pris en charge par ESET Endpoint Security.

Nom d'utilisateur et mot de passe – Si le serveur SMTP exige une authentification, ces champs doivent être remplis avec un nom d'utilisateur et un mot de passe valides donnant accès au serveur SMTP.

Adresse de l'expéditeur – Ce champ spécifie l'adresse de l'expéditeur qui apparaît dans l'en-tête des notifications.

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.

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.

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. Ils sont rétablis dans l'état qu'ils auraient après une nouvelle installation.

Consultez également Importer et exporter les paramètres.

Rétablir tous les paramètres de la section actuelle

Cliquez sur la flèche courbée pour rétablir les paramètres par défaut définis par ESET de tous les paramètres de la section actuelle.

Notez que les modifications apportées après avoir cliqué sur **Rétablir les paramètres par défaut** sont perdues.

Rétablir le contenu des tables – Lorsque cette option est activée, les tâches ou les profils ajoutés automatiquement ou manuellement sont perdus.

Consultez également Importer et exporter les paramètres.

Erreur lors de l’enregistrement de la configuration

Ce message d'erreur indique que, à la suite d'une erreur, les paramètres n'ont pas été enregistrés correctement.

Cela signifie généralement que l'utilisateur qui a tenté de modifier les paramètres du programme :

- possède des droits d'accès insuffisants ou ne dispose pas des privilèges nécessaires du système d'exploitation pour modifier les fichiers de configuration et le registre du système.
  > Pour apporter les modifications souhaitées, l'administrateur système doit se connecter.
- a récemment activé le mode d'apprentissage dans HIPS ou le pare-feu et a tenté d'apporter des modifications aux Configurations avancées.
  > Pour enregistrer la configuration et éviter tout conflit de configuration, fermez les Configurations avancées sans procéder à l'enregistrement et réessayez d'apporter les modifications souhaitées.

Sinon, il est également possible que le programme ne fonctionne plus correctement, qu'il soit endommagé et qu'il doive donc être réinstallé.

Analyseur de ligne de commande

Le module antivirus d'ESET Endpoint Security peut être lancé depuis la ligne de commande, manuellement (avec la commande « ecls ») ou au moyen d'un fichier de commandes (« bat »).

Utilisation de l’analyseur de ligne de commande ESET :

```
ecls [OPTIONS..] FILES..
```

Les paramètres suivants peuvent être utilisés lors de l'exécution de l'analyseur à la demande, à partir de la ligne de commande :

Options

/base-dir=DOSSIER	charger les modules depuis le DOSSIER
/quar-dir=DOSSIER	DOSSIER de quarantaine
/exclude=MASK	exclure les fichiers correspondant à MASQUE de l'analyse
/subdir	analyser les sous-dossiers (valeur par défaut)
/no-subdir	ne pas analyser les sous-dossiers
/max-subdir-level=NIVEAU	sous-niveau maximal de sous-dossiers dans les dossiers à analyser
/symlink	suivre les liens symboliques (valeur par défaut)
/no-symlink	ignorer les liens symboliques
/ads	analyser ADS (valeur par défaut)
/no-ads	ne pas analyser ADS
/log-file=FICHIER	journaliser les résultats dans un FICHIER
/log-rewrite	écraser le fichier de résultats (valeur par défaut – append)
/log-console	journaliser les résultats sur la console (valeur par défaut)
/no-log-console	ne pas journaliser les résultats sur la console
/log-all	journaliser également les fichiers nettoyés

/no-log-all	ne pas journaliser les fichiers nettoyés (valeur par défaut)
/aind	afficher l'indicateur d'activité
/auto	analyser et nettoyer automatiquement tous les disques locaux

Options de l'analyseur

/files	analyser les fichiers (valeur par défaut)
/no-files	ne pas analyser les fichiers
/memory	analyser la mémoire
/boots	analyser les secteurs d'amorçage
/no-boots	ne pas analyser les secteurs d'amorçage (valeur par défaut)
/arch	analyser les archives (valeur par défaut)
/no-arch	ne pas analyser les archives
/max-obj-size=TAILLE	analyser uniquement les fichiers plus petits que TAILLE Mo (valeur par défaut 0 = illimité)
/max-arch-level=NIVEAU	sous-niveau maximal d'archives à analyser dans les archives (archives imbriquées)
/scan-timeout=LIMITE	analyser les archives pendant un maximum de LIMITE secondes
/max-arch-size=TAILLE	n'analyser les fichiers contenus dans une archive que s'ils sont plus petits que TAILLE (valeur par défaut 0 = illimité)
/max-sfx-size=TAILLE	n'analyser les fichiers d'une archive auto-extractible que s'ils sont plus petits que TAILLE Mo (valeur par défaut 0 = illimité)
/mail	analyser les fichiers des courriers électroniques (valeur par défaut)
/no-mail	ne pas analyser les fichiers des courriers électroniques
/mailbox	analyser les boîtes aux lettres (valeur par défaut)
/no-mailbox	ne pas analyser les boîtes aux lettres
/sfx	analyser les archives auto-extractibles (valeur par défaut)
/no-sfx	ne pas analyser les archives auto-extractibles
/rtp	analyser les fichiers exécutables compressés par un compresseur d'exécutables (valeur par défaut)
/no-rtp	ne pas analyser les fichiers exécutables compressés
/unsafe	rechercher les applications potentiellement dangereuses
/no-unsafe	ne pas rechercher les applications potentiellement dangereuses (valeur par défaut)
/unwanted	rechercher les applications potentiellement indésirables
/no-unwanted	ne pas rechercher les applications potentiellement indésirables (valeur par défaut)
/suspicious	rechercher les applications suspectes (valeur par défaut)
/no-suspicious	ne pas rechercher les applications suspectes
/pattern	utiliser les signatures (valeur par défaut)
/no-pattern	ne pas utiliser les signatures
/heur	activer l'heuristique (valeur par défaut)
/no-heur	désactiver l'heuristique
/adv-heur	activer l'heuristique avancée (valeur par défaut)
/no-adv-heur	désactiver l'heuristique avancée

/ext-exclude=EXTENSIONS	exclure de l'analyse les EXTENSIONS de fichier délimitées par deux-points
/clean-mode=MODE	utiliser le MODE de nettoyage pour les objets infectés Les options disponibles sont les suivantes : • `none` (par défaut) – Aucun nettoyage automatique ne se produit. • `standard` – ecls.exe tente automatiquement de nettoyer ou de supprimer les fichiers infectés. • `nettoyage strict` – ecls.exe tente automatiquement de nettoyer ou de supprimer les fichiers infectés sans intervention de l'utilisateur (vous ne recevez pas d'invite avant la suppression des fichiers). • `nettoyage rigoureux` – ecls.exe supprime les fichiers sans tenter de les nettoyer, quel que soit leur type. • `suppression` – ecls.exe supprime les fichiers sans tenter de les nettoyer, mais s'abstient de supprimer les fichiers sensibles tels que les fichiers système de Windows.
/quarantine	copier les fichiers infectés (si nettoyés) vers Quarantaine (complète l'action effectuée lors du nettoyage)
/no-quarantine	ne pas copier les fichiers infectés vers Quarantaine

Options générales

/help	afficher l'aide et quitter
/version	afficher les informations de version et quitter
/preserve-time	conserver la date et l'heure du dernier accès

Codes de sortie

0	aucune menace détectée
1	menace détectée et nettoyée
10	certains fichiers n'ont pas pu être analysés (peuvent être des menaces)
50	menace détectée
100	erreur

Un code sortie supérieur à 100 signale un fichier non analysé qui est potentiellement infecté.

Questions fréquentes

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

- Comment mise à jour ESET Endpoint Security
- Comment activer ESET Endpoint Security
- ESET Endpoint Security a détecté une menace
- Comment éliminer un virus de mon PC
- Comment autoriser la communication pour une certaine application
- Comment créer une tâche dans le Planificateur
- Comment programmer une analyse hebdomadaire de l'ordinateur

- Comment gérer les notifications et les alertes interactives
- Comment connecter mon produit à ESET PROTECT On-Prem
  - Utilisation du mode de remplacement
  - Comment appliquer une politique recommandée pour ESET Endpoint Security
- Comment configurer un miroir
- Comment effectuer une mise à niveau vers Windows 10 avec ESET Endpoint Security
- 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 Security

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

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

- Procédure de désinstallation d'ESET Endpoint Security
- Meilleures pratiques pour se protéger contre les logiciels malveillants Filecoder (ransomwares)
- FAQ sur ESET Endpoint Security et ESET Endpoint Antivirus
- 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.

FAQ sur les mises à jour automatiques

> ⚠ Pour plus d'informations sur les mises à jour du produit ESET Endpoint Security, consultez cet article de la base de connaissances ESET :
> • Quels sont les différents types de versions et de mises à jour des produits ESET ?

Les ordinateurs seront-ils mis à jour automatiquement ? La mise à jour est-elle téléchargée avant ou après le redémarrage ?

Le téléchargement a lieu avant le redémarrage, et les fichiers mis à jour sont également préparés à ce stade. Après le redémarrage, les fichiers mis à jour sont encore préparés uniquement en vue de leur utilisation, et la version actuellement installée offre une protection ininterrompue. Les modifications sont appliquées après le prochain démarrage du ESET Endpoint Security.

Je possède environ 3 000 ordinateurs. Tous les ordinateurs téléchargeront-ils les mises à jour en même temps ? Puis-je utiliser un proxy pour les mises à jour automatiques pour autant d'ordinateurs ?

ESET propose l'outil Mirror Tool et des solutions de proxy pour les réseaux de plus grande taille afin que les mises à jour ne soient téléchargées qu'une seule fois depuis Internet et ensuite distribuées localement. Les mises à jour sont plus petites ; leur taille est généralement de 5 à 10 Mo. ESET limitera en outre les mises à jour pendant les premières semaines de disponibilité. Par conséquent, tous les clients ne lanceront pas le téléchargement

simultanément lorsqu'ils seront connectés directement aux serveurs ESET.

Puis-je décider du nombre ou de la nature des ordinateurs qui seront mis à jour automatiquement ? Je ne veux pas effectuer de téléchargement pour plus de dix ordinateurs par heure, ou je souhaite seulement mettre à jour dix ordinateurs pour l'instant et un autre ordinateur après quelques jours.

Les environnements gérés ont une politique de mise à jour automatique où vous pouvez spécifier la version la plus récente souhaitée. Les caractères génériques (par exemple, 9.0.2032.*) sont également pris en charge. Pour plus d'informations, consultez le chapitre sur les mises à jour automatiques de l'aide en ligne d'ESET PROTECT On-Prem ou ESET PROTECT. Malheureusement, aucune autre option permettant de limiter les mises à jour automatiques n'est disponible pour le moment. Vous pouvez attribuer plusieurs politiques pour plusieurs groupes.

Les mises à jour automatiques sont-elles configurées uniquement par une politique ? Puis-je simplement désactiver la politique si je ne veux pas qu'un produit ESET soit mis à jour ?

S'il existe un correctif de sécurité et de stabilité pour le produit ESET Endpoint, ce dernier sera mis à jour même si les mises à jour automatiques sont désactivées, conformément aux conditions définies dans le Contrat de licence de l'utilisateur final applicable. ESET utilise des correctifs de sécurité et de stabilité pour résoudre des problèmes critiques et assurer une sécurité et une stabilité maximales pour votre produit ESET.

Vous pouvez affecter une politique de mise à jour automatique à n'importe quel groupe d'endpoints, quelle que soit leur configuration actuelle de mise à jour automatique. Dans les environnements non gérés, l'utilisateur peut configurer localement les mises à jour automatiques dans l'écran de configurations avancées d'un produit ESET Endpoint.

Que se passe-t-il si je configure une politique pour utiliser la plus ancienne version disponible ? ESET mettra-t-il mes produits à jour, même dans ce cas ?

Les correctifs et les correctifs critiques (mises à jour de sécurité et de stabilité) sont des catégories de mise à jour légèrement différentes. Les correctifs réguliers sont affectés aux mises à jour automatiques avec une priorité standard lorsque les paramètres de l'utilisateur sont acceptés. Les correctifs critiques sont appliqués en priorité, quels que soient les paramètres de l'utilisateur.

Comment les mises à jour fonctionnement-elles dans les scénarios hors ligne ? Quand les utilisateurs utilisent-ils le répertoire hors ligne ?

Le répertoire hors ligne contient également des fichiers .dup et .fup. La section du répertoire doit être téléchargée par l'outil Miroir (Mirror Tool), et non par la mise à jour du module. Pour plus d'informations, consultez la rubrique Répertoire hors ligne de l'aide en ligne d'ESET PROTECT On-Prem.

Comment les produits ESET savent-ils qu'une mise à jour est nécessaire ? Depuis le répertoire ? Des données sont-elles envoyées aux serveurs ? Si ESET prévoit d'effectuer une mise à jour un mois après la publication d'une version, les serveurs ESET peuvent-ils gérer une publication mondiale ?

Les produits ESET téléchargent des mises à jour automatiques depuis le répertoire. Les serveurs peuvent les prendre en charge car les mises à jour critiques ne font que quelques kilo-octets. ESET n'applique pas de limitation de bande passante aux mises à jour critiques sur les serveurs du répertoire. Il existe toutefois une option qui permet de limiter la bande passante sur les serveurs si les mises à jour automatiques sont plus volumineuses. Le tableau suivant contient des exemples de taille de correctifs dans le cas d'une mise à jour automatique différentielle :

Version précédente	Nouvelle version	Taille
9.0.2032.2	9.0.2032.6	420 Ko
8.1.2037.2	9.0.2032.2	6.5 Mo
8.0.2028.0	9.0.2032.2	11.5 Mo

Si une mise à jour automatique différentielle échoue, il est possible que le produit ESET lance une mise à jour complète. Il s'agit toujours d'une mise à jour automatique avec un fonctionnement garanti, mais un fichier .fup (plus volumineux) est téléchargé à la place d'un fichier .dup. Pour la version 9.0.2032.2, la taille du fichier est de 27 Mo. Un tel scénario est toutefois rare.

La mise à jour d'ESET Endpoint Security sera-t-elle publiée avec une limitation de bande passante ? Si c'est le cas, combien de temps la mise à jour sera-t-elle limitée après sa publication ?

ESET applique une limitation de bande passante aux mises à jour pendant les premières semaines après la publication d'une nouvelle version afin de réduire la charge sur les serveurs et de distribuer la nouvelle version de manière uniforme.

Les mises à jour automatiques vont devenir l'une des principales méthodes de mise à niveau. Comment cela fonctionnera-t-il ?

ESET souhaite avoir le plus grand nombre possible de clients utilisant les mises à jour automatiques. Il est difficile de prendre en charge un si grand nombre d'anciennes versions. La fonctionnalité de mise à jour automatique fonctionne de manière simple : des fichiers .dup sont téléchargés lors de la première vérification de la mise à jour du module. Pendant la procédure de mise à jour, le produit est entièrement fonctionnel et protège l'ordinateur. La nouvelle version est activée après un redémarrage. Dans ESET PROTECT On-Prem (côté serveur), vous pourrez utiliser une politique pour spécifier la version la plus récente vers laquelle vous voulez effectuer la mise à jour ou employer des caractères génériques. Pour plus d'informations, consultez le chapitre sur les mises à jour automatiques de l'aide en ligne d'ESET PROTECT On-Prem ou ESET PROTECT.

Est-il exact que les mises à jour automatiques fonctionnent en 1/10 ? J'utilise actuellement ESET Endpoint Security 8.0.2028.1. Vers quelle version le produit sera-t-il mis à jour si les mises à jour automatiques sont exécutées ?

La mise à jour des produits à l'aide d'une mise à jour automatique peut être retardée en raison de la limitation de bande passante des serveurs de répertoire. Si une mise à jour de produit est publiée avec une limitation de bande passante, les vérifications de mise à jour automatique peuvent ne pas la recevoir immédiatement. Si la mise à jour est considérée comme sûre et stable, la limitation peut être réduite ou supprimée complètement afin que tous les clients restants reçoivent la mise à jour.

La limitation de bande passante est une procédure dont la durée peut être différente pour chaque mise à jour. Elle varie en fonction du nombre de clients qui demandent la mise à jour, du trafic sur nos serveurs et d'autres facteurs. Cette procédure est en constante évolution et des modifications sont apportées en permanence.

Quand les mises à jour automatiques seront-elles exécutées si je démarre un ordinateur à 8 h 45 et que je l'éteins à 17 h ?

Les mises à jour automatiques démarreront lors de la prochaine mise à jour du module, au maximum une fois toutes les 24 heures.

Quand la prochaine mise à jour sera-t-elle exécutée si l'ordinateur s'éteint pendant que les mises à jour automatiques sont en cours ?

La mise à jour sera exécutée lors de la prochaine fenêtre de mise à jour planifiée. Il existe un mécanisme de sécurité robuste pour la procédure de mise à jour automatique (anciennement uPCU). Après le téléchargement de la mise à jour et le redémarrage de l'ordinateur, les fichiers mis à jour sont encore préparés en vue de leur utilisation, et la version actuellement installée offre une protection ininterrompue. Les modifications sont appliquées après le prochain démarrage du produit ESET Endpoint.

Comment puis-je lancer les mises à jour automatiques immédiatement sans attendre une connexion régulière toutes les 24 heures ? Existe-t-il un autre moyen de cliquer sur Rechercher des mises à jour ?

Vous ne pouvez commencer la procédure de mise à jour automatique manuellement que lorsque vous ouvrez la fenêtre principale du programme et que vous cliquez sur **Mise à jour** > **Rechercher des mises à jour**. Toutes les autres façons de lancer les mises à jour de modules reflètent la politique de 24 heures du planificateur de mise à jour automatique. Vous ne pouvez pas lancer à distance un téléchargement de mise à jour automatique. Cette fonctionnalité sera ajoutée à l'avenir.

Comment mettre à jour ESET Endpoint Security

Les mises à jour de module ESET Endpoint Security peuvent être effectuées 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 les mises à niveau de produits, consultez Mise à niveau vers une nouvelle version.

Comment éliminer un virus de mon PC

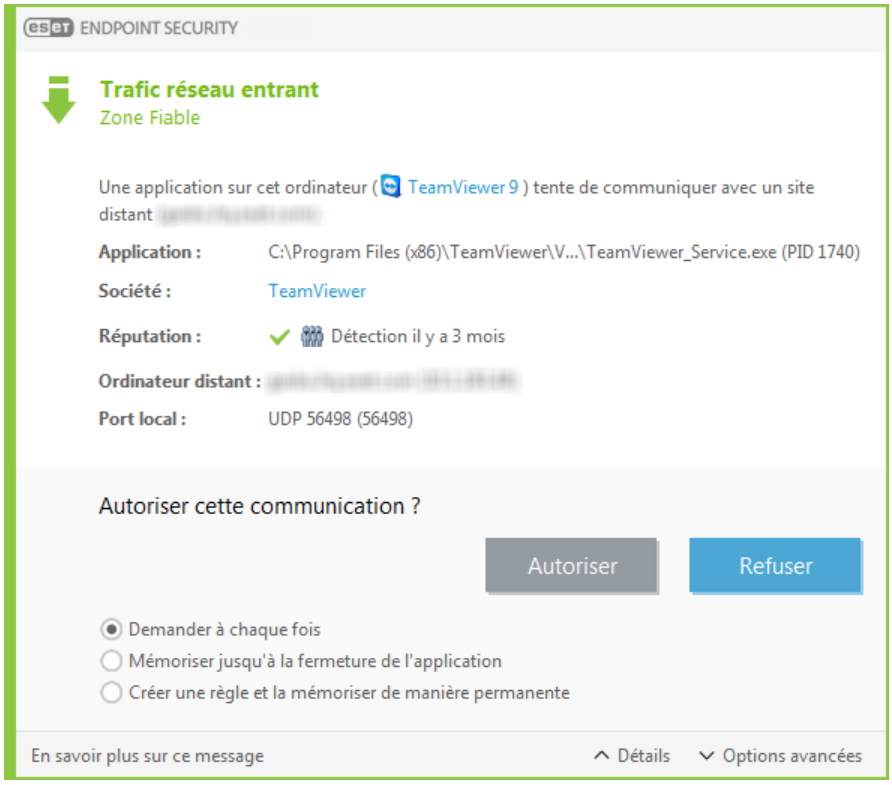
Si votre ordinateur montre des signes d'infection par un logiciel malveillant (ralentissement, blocages fréquents, par exemple), nous recommandons d'effectuer les opérations suivantes :

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 autoriser la communication pour une certaine application

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



Vous pouvez créer des règles de pare-feu pour les applications avant leur détection par ESET Endpoint Security dans la fenêtre Configuration du pare-feu. Pour ce faire, ouvrez la fenêtre principale du programme, cliquez sur **Configuration** > **Réseau** > **Pare-feu**, cliquez sur l'icône représentant un engrenage > **Configurer** > **Avancé** > **Règles** > **Modifier**.

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

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

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 une tâche** 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 Security à ESET PROTECT On-Prem

Lorsque ESET Endpoint Security est installé sur votre ordinateur et que vous souhaitez vous connecter via ESET PROTECT On-Prem, 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 ESET PROTECT On-Prem 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 Security

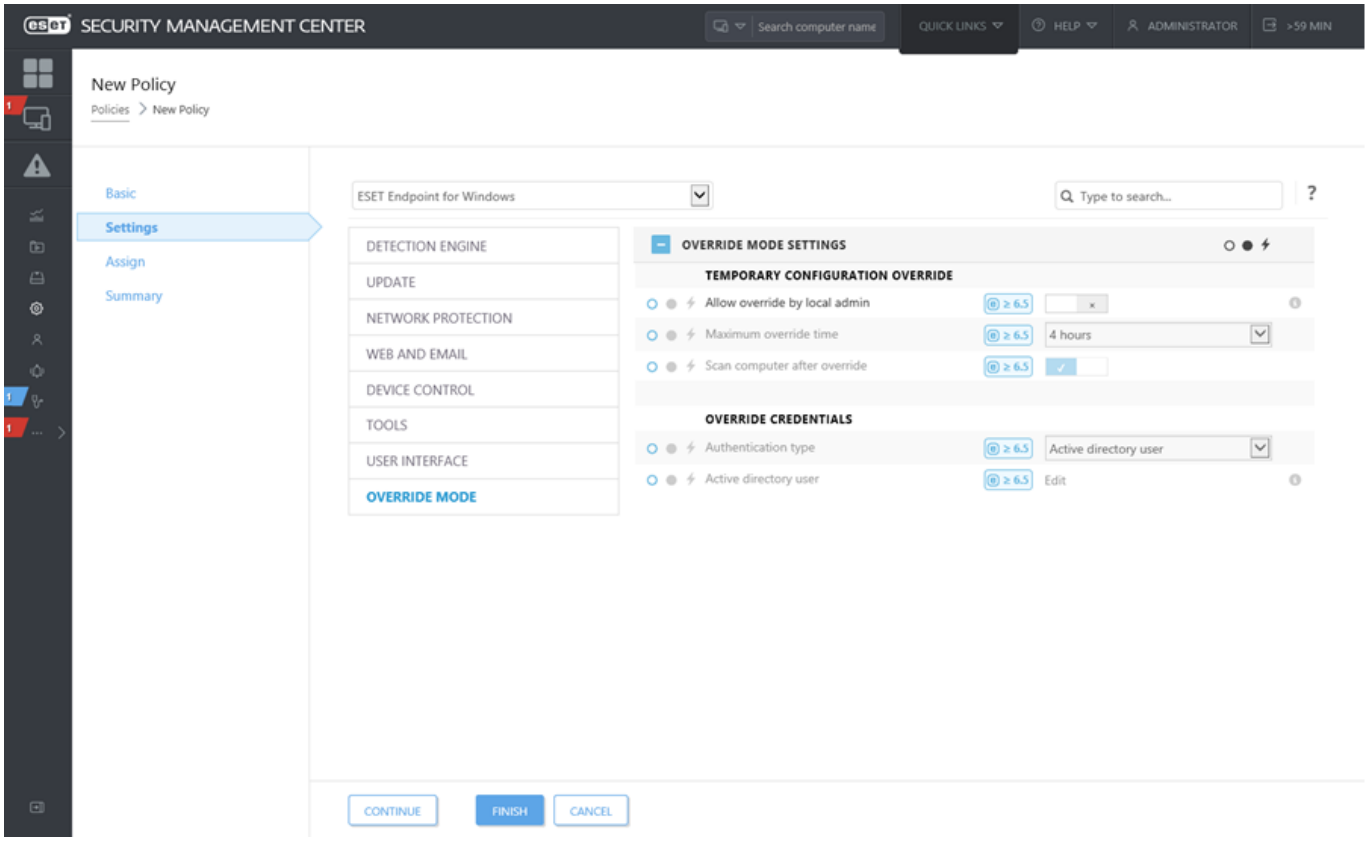
Utilisation du mode de remplacement

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.

⚠ Le mode de remplacement ne peut pas être arrêté à partir de la console web ESET PROTECT On-Prem Web Console lorsqu'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 Security.
L'authentification de groupe Active Directory est prise en charge.

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.



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 ESET PROTECT On-Prem 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 ESET PROTECT On-Prem 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 politique de remplacement lorsqu'elle n'est plus utile.

Comment appliquer une politique recommandée pour ESET Endpoint Security

Après avoir connecté ESET Endpoint Security à ESET PROTECT On-Prem, il est conseillé d'appliquer une politique recommandée ou personnalisée.

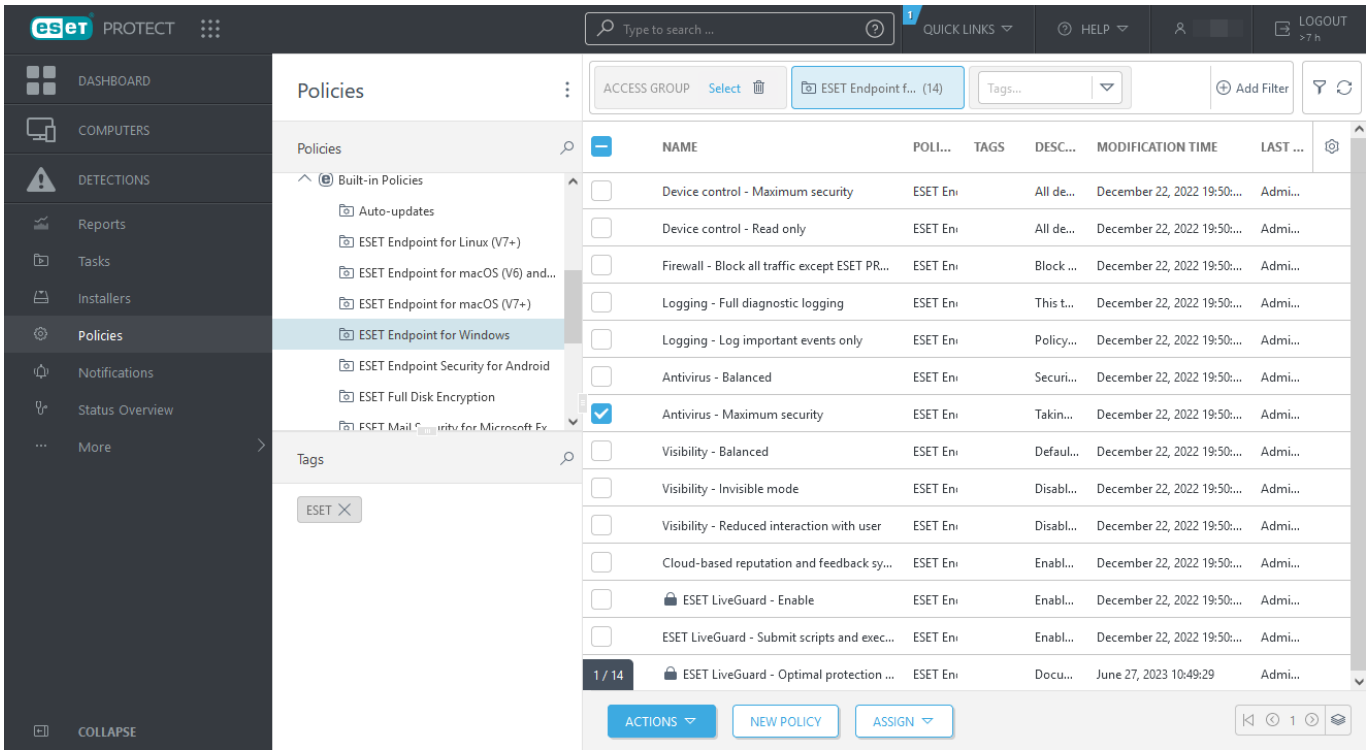
Il existe plusieurs politiques intégrées pour ESET Endpoint Security :

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 ESET PROTECT On-Prem et ESET Inspect	Bloquez l'ensemble du trafic, à l'exception des connexions à ESET PROTECT On-Prem et ESET Inspect 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 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.
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 Security installé sur vos postes de travail, procédez comme suit :

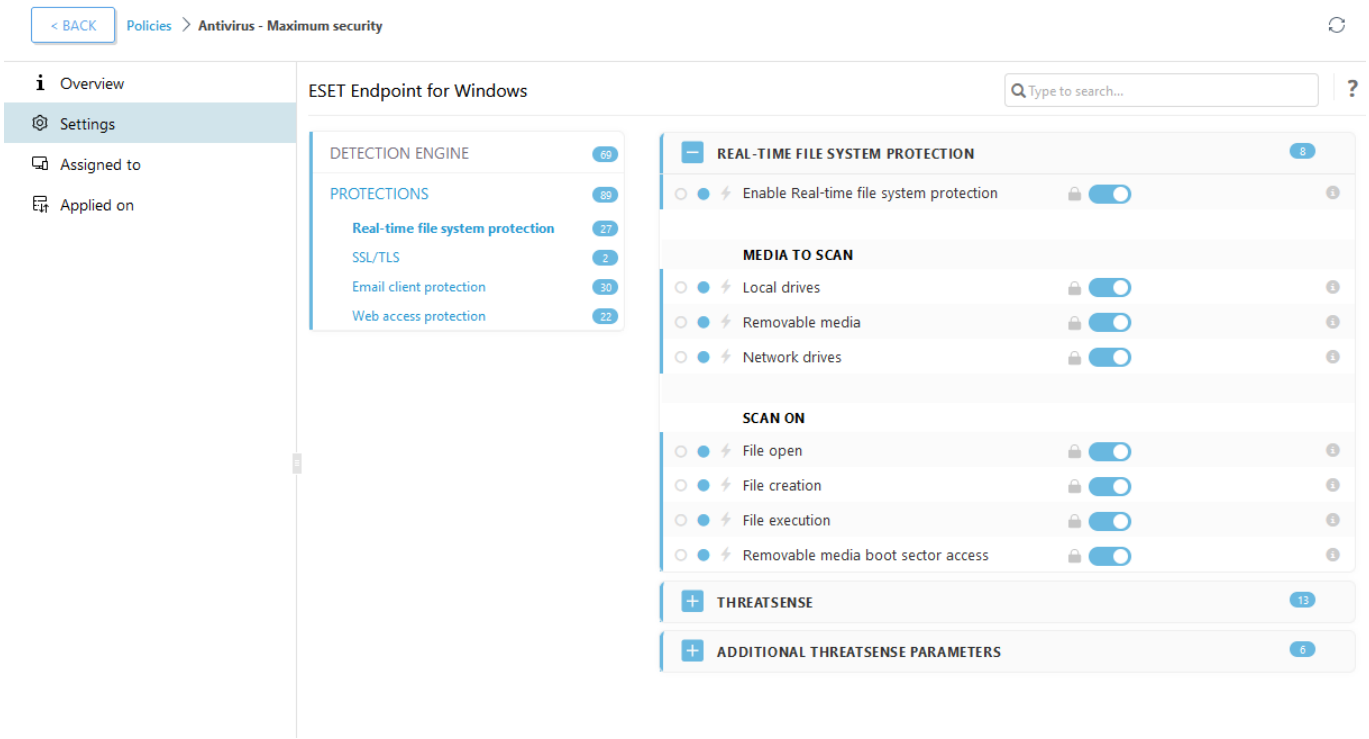
> Les articles suivants de la base de connaissances ESET peuvent être disponibles uniquement en anglais : Appliquer une politique recommandée ou prédéfinie pour ESET Endpoint Security à l'aide d'ESET PROTECT On-Prem

1. Ouvrez la console ESET PROTECT On-Prem 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 ESET PROTECT On-Prem



Comment configurer un miroir

ESET Endpoint Security 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 Antivirus ou ESET Endpoint Security.

Le miroir de mise à jour crée des copies des fichiers de mise à jour qui peuvent être utilisées pour mettre à jour les postes de travail qui exécutent la même génération du produit ESET Endpoint Security pour Windows. (Par exemple, ESET Endpoint Security pour Windows version 10.x crée des fichiers de mise à jour uniquement pour la version 10.x d'ESET Endpoint Antivirus pour Windows et ESET Endpoint Security pour Windows.)

Configuration d'ESET Endpoint Security 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
- Mise à jour à partir du miroir

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.

Si vous ne souhaitez pas fournir de mises à jour de module via le serveur HTTP interne, désactivez **Activer le serveur HTTP**.

Comment effectuer une mise à niveau vers Windows 10 avec ESET Endpoint Security

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.

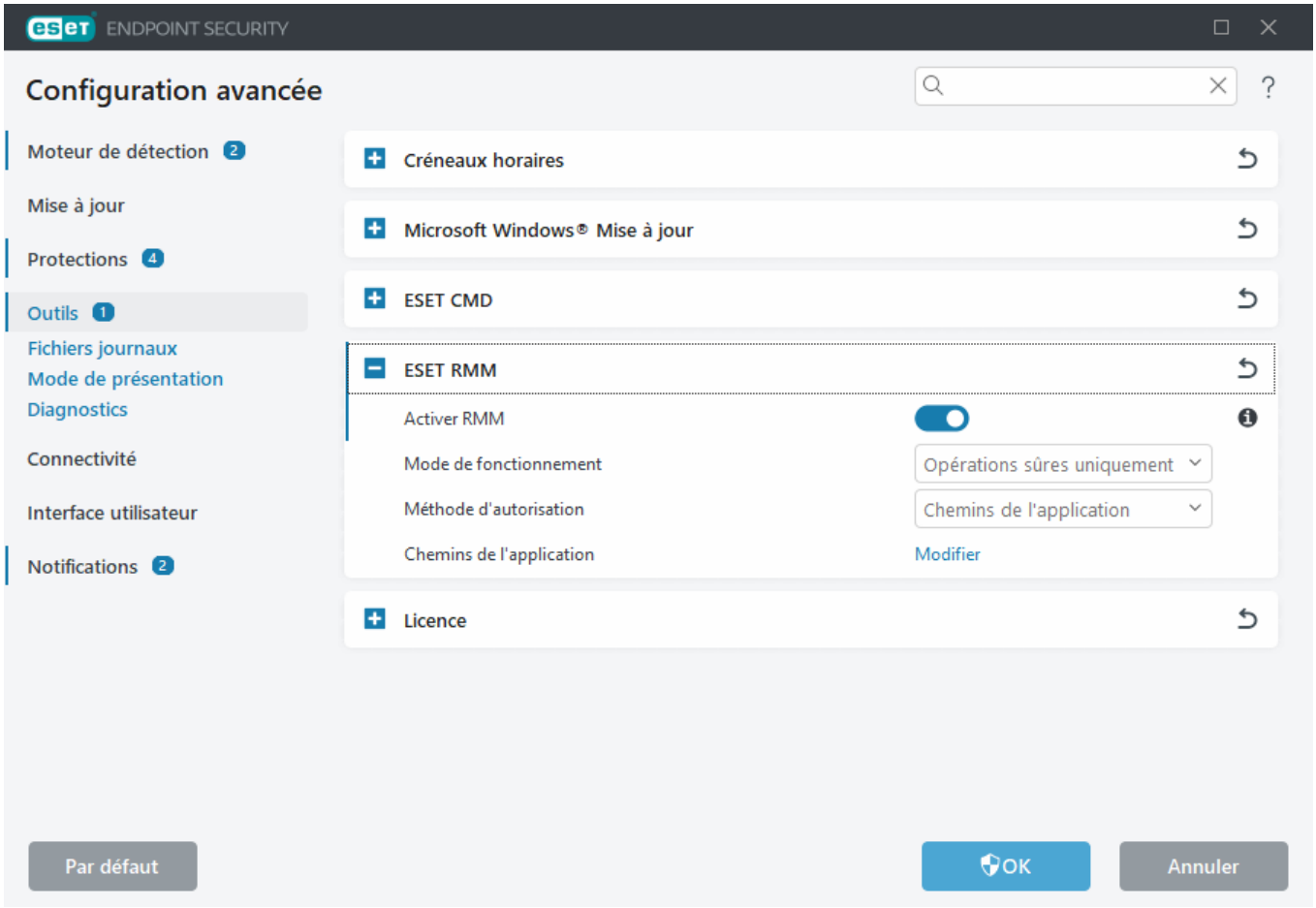
Autres versions linguistiques :

Si vous recherchez une autre version linguistique du produit ESET Endpoint, consultez notre page de téléchargement.

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 Security peut être géré par RMM à partir de la version 6.6.2028.0.



Par défaut, ESET RMM est désactivé. Pour activer ESET RMM, ouvrez Configurations avancées > **Outils** > **ESET RMM**, puis activez le bouton bascule en regard de l'option **Activer RMM**.

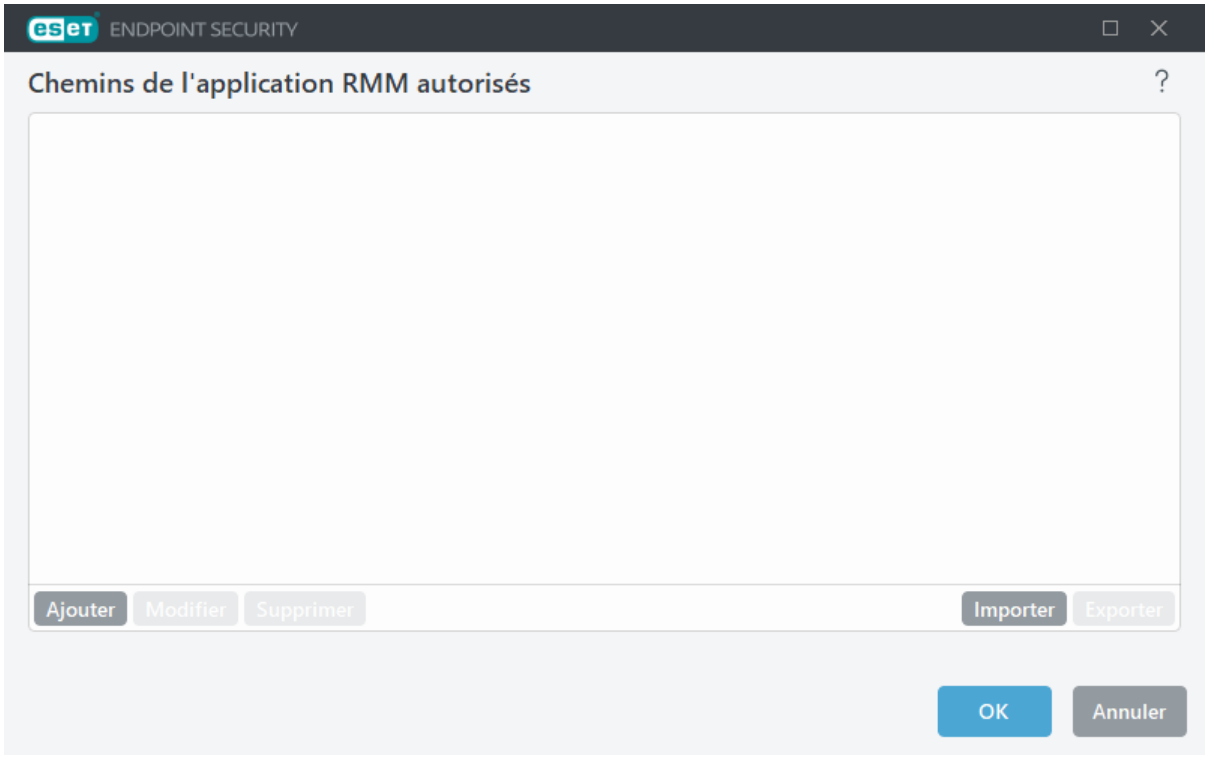
Mode de fonctionnement : sélectionnez **Opérations sûres uniquement** si vous souhaitez activer l'interface RMM pour les opérations sûres et en lecture seule. Sélectionnez **Toutes les opérations** si vous souhaitez activer l'interface RMM pour toutes les opérations.

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**.

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 Security 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.

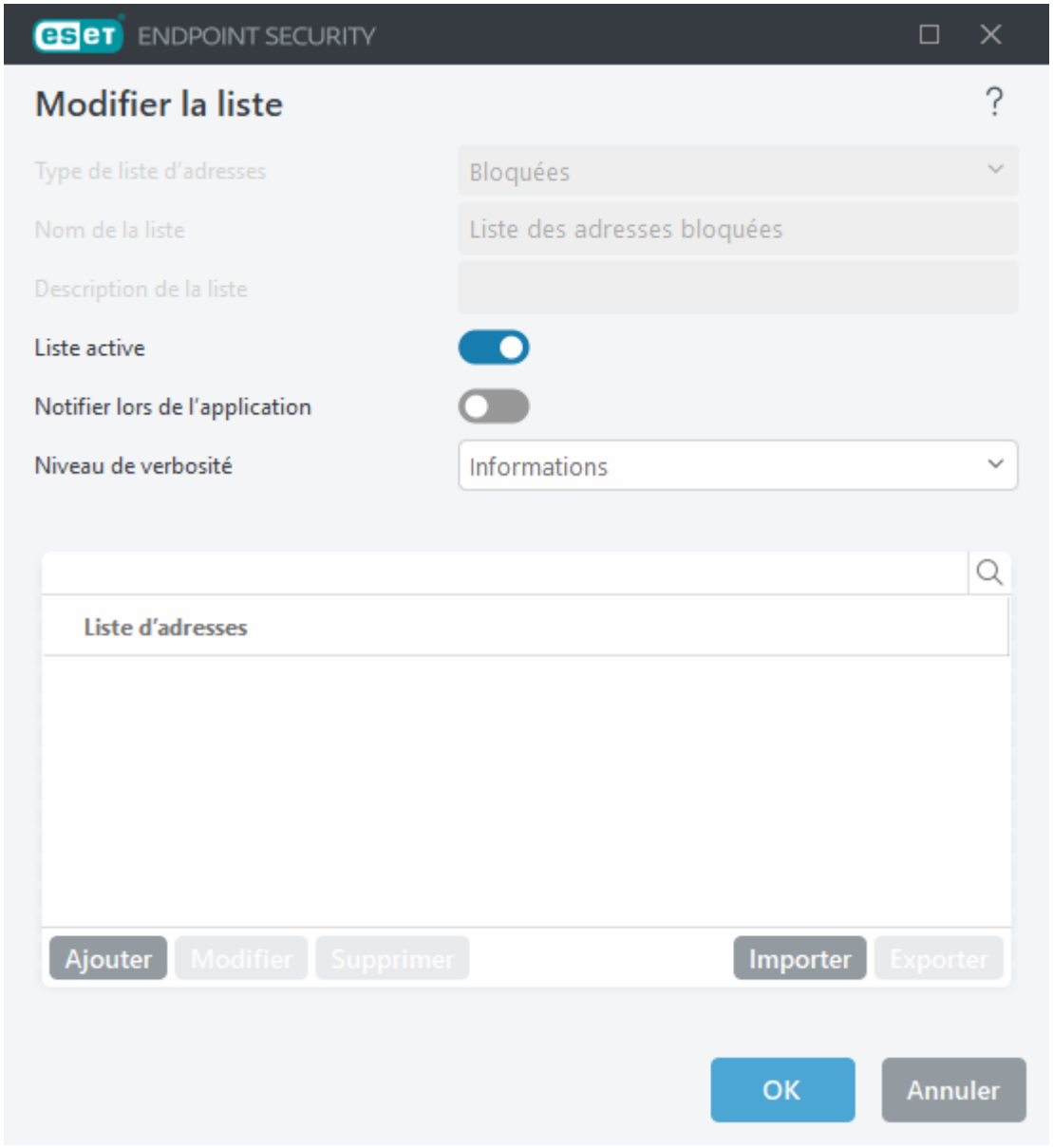
Blocage du téléchargement de types de fichiers

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 sur **Ajouter** pour créer/modifier 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. ESET PROTECT On-Prem peut collecter des enregistrements avec le niveau de verbosité **Avertissement**.

Le niveau de détail de la consignation des informations et avertissements n'est disponible que pour les règles qui contiennent au moins deux composants sans caractère générique dans le domaine. Par exemple :
- *.domain.com/*
- *www.domain.com/*



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://example.com/file.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 **/*.zip* 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 Security

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

En vigueur à compter du 19 octobre 2021.

IMPORTANT : Veuillez lire soigneusement les termes et conditions d'application du produit stipulés ci-dessous avant de télécharger, d'installer, de copier ou d'utiliser le produit. **EN TÉLÉCHARGEANT, INSTALLANT, COPIANT OU UTILISANT LE LOGICIEL, VOUS ACCEPTEZ CES TERMES ET CONDITIONS ET RECONNAISSEZ AVOIR PRIS CONNAISSANCE DE LA POLITIQUE DE CONFIDENTIALITÉ.**

Contrat de licence de l'utilisateur final

Selon les termes du présent Contrat de Licence pour l'Utilisateur Final (« Contrat ») signé par et entre ESET, spol. s r. o., dont le siège social se situe au Einsteinova 24, 85101 Bratislava, Slovak Republic, inscrite au Registre du Commerce du tribunal de Bratislava I. Section Sro, Insertion No 3586/B, numéro d'inscription des entreprises : 31333532 (« ESET » ou « Fournisseur ») et vous, personne physique ou morale, (« vous » ou « Utilisateur Final »), vous êtes autorisé à utiliser le Logiciel défini à l'article 1 du présent Contrat. Dans le cadre des modalités indiquées ci-dessous, le Logiciel défini à l'article 1 du présent Contrat peut être enregistré sur un support de données, envoyé par courrier électronique, téléchargé sur Internet, téléchargé à partir de serveurs du Fournisseur ou obtenu à partir d'autres sources.

CE DOCUMENT N'EST PAS UN CONTRAT D'ACHAT, MAIS UN ACCORD LIÉ AUX DROITS DE L'UTILISATEUR FINAL. Le

Fournisseur reste le propriétaire de la copie du Logiciel et du support physique fourni dans l'emballage commercial, et de toutes les copies du Logiciel que l'Utilisateur Final est autorisé à faire dans le cadre du présent Contrat.

En cliquant sur « J'accepte » ou « J'accepte... » lorsque vous téléchargez, installez, copiez ou utilisez le Logiciel, vous acceptez les termes et conditions du présent Contrat et reconnaissez avoir pris connaissance de la Politique de confidentialité. Si vous n'êtes pas d'accord avec tous les termes et conditions du présent Contrat et/ou de la Politique de confidentialité, cliquez immédiatement sur l'option d'annulation, annulez le téléchargement ou l'installation, détruisez ou renvoyez le Logiciel, le support d'installation, la documentation connexe et une facture au Fournisseur ou à l'endroit où vous avez obtenu le Logiciel.

VOUS RECONNAISSEZ QUE VOTRE UTILISATION DU LOGICIEL INDIQUE QUE VOUS AVEZ LU ET COMPRIS LE PRÉSENT CONTRAT ET ACCEPTÉ D'EN RESPECTER LES TERMES ET CONDITIONS.

1. **Logiciel.** Dans le cadre du présent Contrat, le terme « Logiciel » désigne : (i) le programme informatique et tous ses composants ; (ii) le contenu des disques, des CD-ROM, des DVD, des courriers électroniques et de leurs pièces jointes, ou de tout autre support auquel le présent Contrat est attaché, dont le formulaire de code objet fourni sur un support de données, par courrier électronique ou téléchargé par le biais d'Internet ; (iii) tous documents explicatifs écrits et toute documentation relative au Logiciel, en particulier, toute description du Logiciel, ses caractéristiques, description des propriétés, description de l'utilisation, description de l'interface du système d'exploitation sur lequel le Logiciel est utilisé, guide d'installation ou d'utilisation du Logiciel ou description de l'utilisation correcte du Logiciel (« Documentation ») ; (iv) les copies du Logiciel, les correctifs d'erreurs du Logiciel, les ajouts au Logiciel, ses extensions, ses versions modifiées et les mises à jour des parties du Logiciel, si elles sont fournies, au titre desquels le Fournisseur vous octroie la Licence conformément à l'article 3 du présent Contrat. Le Logiciel est fourni exclusivement sous la forme d'un code objet exécutable.

2. **Installation, Ordinateur et Clé de licence**. Le Logiciel fourni sur un support de données, envoyé par courrier électronique, téléchargé à partir d'Internet ou de serveurs du Fournisseur ou obtenu à partir d'autres sources nécessite une installation. Vous devez installer le Logiciel sur un Ordinateur correctement configuré, qui doit au moins satisfaire les exigences spécifiées dans la Documentation. La méthode d'installation est décrite dans la Documentation. L'Ordinateur sur lequel le Logiciel sera installé doit être exempt de tout programme ou matériel susceptible de nuire au bon fonctionnement du Logiciel. Le terme Ordinateur désigne le matériel, notamment les ordinateurs personnels, ordinateurs portables, postes de travail, ordinateurs de poche, smartphones, appareils électroniques portatifs ou autres appareils électroniques, pour lequel le Logiciel a été conçu et sur lequel il sera installé et/ou utilisé. Le terme Clé de licence désigne la séquence unique de symboles, lettres, chiffres ou signes spéciaux fournie à l'Utilisateur Final afin d'autoriser l'utilisation légale du Logiciel, de sa version spécifique ou de l'extension de la durée de la Licence conformément au présent Contrat.

3. **Licence**. Sous réserve que vous ayez accepté les termes du présent Contrat et que vous respectiez tous les termes et conditions stipulés dans le présent Contrat, le Fournisseur vous accorde les droits suivants (« Licence ») :

a) **Installation et utilisation.** Vous détenez un droit non exclusif et non transférable d'installer le Logiciel sur le disque dur d'un ordinateur ou sur un support similaire de stockage permanent de données, d'installer et de stocker le Logiciel dans la mémoire d'un système informatique et d'exécuter, de stocker et d'afficher le Logiciel.

b) **Précision du nombre de licences.** Le droit d'utiliser le Logiciel est lié au nombre d'Utilisateurs Finaux. On entend par « Utilisateur Final » : (i) l'installation du Logiciel sur un seul système informatique, ou (ii) si l'étendue de la Licence est liée au nombre de boîtes aux lettres, un Utilisateur Final désigne un utilisateur d'ordinateur qui reçoit un courrier électronique par le biais d'un client de messagerie. Si le client de messagerie accepte du courrier électronique et le distribue automatiquement par la suite à plusieurs utilisateurs, le nombre d'Utilisateurs Finaux doit être déterminé en fonction du nombre réel d'utilisateurs auxquels le courrier

électronique est distribué. Si un serveur de messagerie joue le rôle de passerelle de courriel, le nombre d'Utilisateurs Finaux est égal au nombre de serveurs de messagerie pour lesquels la passerelle fournit des services. Si un certain nombre d'adresses de messagerie sont affectées à un seul et même utilisateur (par l'intermédiaire d'alias) et que ce dernier les accepte et si les courriels ne sont pas distribués automatiquement du côté du client à d'autres utilisateurs, la Licence n'est requise que pour un seul ordinateur. Vous ne devez pas utiliser la même Licence au même moment sur plusieurs ordinateurs. L'Utilisateur Final n'est autorisé à saisir la Clé de licence du Logiciel que dans la mesure où il a le droit d'utiliser le Logiciel conformément à la limite découlant du nombre de licences accordées par le Fournisseur. La Clé de licence est confidentielle. Vous ne devez pas partager la Licence avec des tiers ni autoriser des tiers à utiliser la Clé de licence, sauf si le présent Contrat ou le Fournisseur le permet. Si votre Clé de licence est endommagée, informez-en immédiatement le Fournisseur.

c) **Home/Business Edition.** Une version Home Edition du Logiciel doit être utilisée exclusivement dans des environnements privés et/ou non commerciaux, pour un usage domestique et familial uniquement. Une version Business Edition du Logiciel est requise pour l'utiliser dans un environnement commercial ainsi que pour utiliser le Logiciel sur des serveurs de messagerie, relais de messagerie, passerelles de messagerie ou passerelles Internet.

d) **Durée de la Licence.** Le droit d'utiliser le Logiciel est limité dans le temps.

e) **Logiciel acheté à un fabricant d'équipement informatique.** Les logiciels classés comme achetés à un fabricant d'équipement informatique sont limités à l'ordinateur avec lequel vous les avez obtenus. Elle ne peut pas être transférée à un autre ordinateur.

f) **Version d'évaluation ou non destinée à la revente.** Un Logiciel classé comme non destiné à la revente ou comme version d'évaluation ne peut pas être vendu et ne doit être utilisé qu'aux fins de démonstration ou d'évaluation des caractéristiques du Logiciel.

g) **Résiliation de la Licence.** La Licence expire automatiquement à la fin de la période pour laquelle elle a été accordée. Si vous ne respectez pas les dispositions du présent Contrat, le Fournisseur est en droit de mettre fin au Contrat, sans renoncer à tout droit ou recours juridique ouvert au Fournisseur dans de tels cas. En cas d'annulation du présent Contrat, vous devez immédiatement supprimer, détruire ou renvoyer à vos frais le Logiciel et toutes les copies de sauvegarde à ESET ou à l'endroit où vous avez obtenu le Logiciel. Lors de la résiliation de la Licence, le Fournisseur est en droit de mettre fin au droit de l'Utilisateur final à l'utilisation des fonctions du Logiciel, qui nécessitent une connexion aux serveurs du Fournisseur ou à des serveurs tiers.

4. **Fonctions avec des exigences en matière de connexion Internet et de collecte de données.** Pour fonctionner correctement, le Logiciel nécessite une connexion Internet et doit se connecter à intervalles réguliers aux serveurs du Fournisseur ou à des serveurs tiers et collecter des données en conformité avec la Politique de confidentialité. Une connexion Internet et une collecte de données sont requises pour les fonctions suivantes du Logiciel :

a) **Mises à jour du Logiciel.** Le Fournisseur est autorisé de temps à autre à publier des mises à jour ou des mises à niveau du Logiciel (« Mises à jour »), mais n'en a pas l'obligation. Cette fonction est activée dans la configuration standard du Logiciel ; les Mises à jour sont donc installées automatiquement, sauf si l'Utilisateur Final a désactivé l'installation automatique des Mises à jour. Pour la mise à disposition de Mises à jour, une vérification de l'authenticité de la Licence est requise. Elle comprend notamment la collecte d'informations sur l'Ordinateur et/ou la plate-forme sur lesquels le Logiciel est installé, en conformité avec la Politique de confidentialité.

La fourniture des mises à jour peut être soumise à la Politique de fin de vie (« Politique de fin de vie »), qui est disponible à l'adresse suivante : https://go.eset.com/eol_business. Aucune mise à jour ne sera fournie après que le Logiciel ou l'une de ses fonctionnalités ait atteint la date de fin de vie telle que définie dans la Politique de fin de vie.

b) **Réacheminement des infiltrations et des données au Fournisseur.** Le Logiciel contient des fonctions qui collectent des échantillons de virus, d'autres programmes informatiques également nuisibles et d'objets

problématiques, suspects, potentiellement indésirables ou dangereux tels que des fichiers, des URL, des paquets IP et des trames Ethernet (« Infiltrations »), puis les envoient au Fournisseur, en incluant, sans s'y limiter, des informations sur le processus d'installation, l'Ordinateur ou la plateforme hébergeant le Logiciel et des informations sur les opérations et fonctions du Logiciel (« Informations »). Les Informations et les Infiltrations sont susceptibles de contenir des données (y compris des données personnelles obtenues par hasard ou accidentellement) concernant l'Utilisateur final et/ou d'autres usagers de l'ordinateur sur lequel le Logiciel est installé et les fichiers affectés par les Infiltrations et les métadonnées associées.

Les informations et les infiltrations peuvent être collectées pat les fonctions suivantes du Logiciel :

i. La fonction Système de réputation LiveGrid collecte et envoie les hachages unidirectionnelles liés aux Infiltrations au Fournisseur. Cette fonction est activée dans les paramètres standard du Logiciel.

ii. La fonction Système de commentaires LiveGrid collecte et envoie les Infiltrations avec les Informations et les métadonnées associées au Fournisseur. Cette fonction peut être activée par l'Utilisateur Final pendant le processus d'installation du Logiciel.

Le Fournisseur utilisera les Informations et Infiltrations reçues uniquement pour effectuer des analyses et des recherches sur les Infiltrations et améliorer le Logiciel et la vérification de l'authenticité de la Licence. Il prendra en outre les mesures adéquates afin de protéger les Infiltrations et Informations reçues. Si vous activez cette fonction du Logiciel, les Infiltrations et Informations peuvent être collectées et traitées par le Fournisseur, comme stipulé dans la Politique de confidentialité et conformément aux réglementations en vigueur. Vous pouvez désactiver ces fonctions à tout moment.

Aux fins du présent Contrat, il est nécessaire de collecter, traiter et stocker des données permettant au Fournisseur de vous identifier conformément à la Politique de confidentialité. Vous acceptez que le Fournisseur vérifie à l'aide de ses propres moyens si vous utilisez le Logiciel conformément aux dispositions du présent Contrat. Vous reconnaissez qu'aux fins du présent Contrat, il est nécessaire que vos données soient transférées pendant les communications entre le Logiciel et les systèmes informatiques du Fournisseur ou de ceux de ses partenaires commerciaux, dans le cadre du réseau de distribution et de support du Fournisseur, afin de garantir les fonctionnalités du Logiciel, l'autorisation d'utiliser le Logiciel et la protection des droits du Fournisseur.

Après la conclusion du présent Contrat, le Fournisseur et ses partenaires commerciaux, dans le cadre du réseau de distribution et de support du Fournisseur, sont autorisés à transférer, à traiter et à stocker des données essentielles vous identifiant, aux fins de facturation, d'exécution du présent Contrat et de transmission de notifications sur votre Ordinateur.

Des informations détaillées sur la vie privée, la protection des données personnelles et Vos droits en tant que personne concernée figurent dans la Politique de confidentialité, disponible sur le site Web du Fournisseur et directement accessible à partir de l'installation. Vous pouvez également la consulter depuis la section d'aide du Logiciel.

5. **Exercice des droits de l'Utilisateur Final**. Vous devez exercer les droits de l'Utilisateur Final en personne ou par l'intermédiaire de vos employés. Vous n'êtes autorisé à utiliser le Logiciel que pour assurer la sécurité de vos opérations et protéger les Ordinateurs ou systèmes informatiques pour lesquels vous avez obtenu une Licence.

6. **Restrictions des droits.** Vous ne pouvez pas copier, distribuer, extraire des composants ou créer des travaux dérivés basés sur le Logiciel. Vous devez respecter les restrictions suivantes lorsque vous utilisez le Logiciel :

a) Vous pouvez effectuer une copie de sauvegarde archivée du Logiciel sur un support de stockage permanent, à condition que cette copie de sauvegarde archivée ne soit pas installée ni utilisée sur un autre ordinateur. Toutes les autres copies que vous pourriez faire du Logiciel seront considérées comme une violation du présent Contrat.

b) Vous n’êtes pas autorisé à utiliser, modifier, traduire, reproduire ou transférer les droits d’utilisation du Logiciel ou des copies du Logiciel d’aucune manière autre que celles prévues dans le présent Contrat.

c) Vous ne pouvez pas vendre, concéder en sous-licence, louer à bail ou louer le Logiciel ou utiliser le Logiciel pour offrir des services commerciaux.

d) Vous ne pouvez pas rétroconcevoir, décompiler ou désassembler le Logiciel ni tenter de toute autre façon de découvrir le code source du Logiciel, sauf dans la mesure où cette restriction est expressément interdite par la loi.

e) Vous acceptez de n’utiliser le Logiciel que de façon conforme à toutes les lois applicables de la juridiction dans laquelle vous utilisez le Logiciel, notamment les restrictions applicables relatives aux droits d’auteur et aux droits de propriété intellectuelle.

f) Vous acceptez de n'utiliser le Logiciel et ses fonctions que de façon à ne pas entraver la possibilité des autres Utilisateurs Finaux à accéder à ces services. Le Fournisseur se réserve le droit de limiter l'étendue des services fournis à chacun des Utilisateurs Finaux, pour permettre l'utilisation des services au plus grand nombre possible d'Utilisateurs Finaux. Le fait de limiter l'étendue des services implique aussi la résiliation totale de la possibilité d'utiliser toute fonction du Logiciel ainsi que la suppression des Données et des informations présentes sur les serveurs du Fournisseur ou sur des serveurs tiers, qui sont afférentes à une fonction particulière du Logiciel.

g) Vous acceptez de ne pas exercer d'activités impliquant l'utilisation de la Clé de licence, qui soit contraire aux termes du présent Contrat, ou conduisant à fournir la Clé de licence à toute personne n'étant pas autorisée à utiliser le logiciel (comme le transfert d'une Clé de licence utilisée ou non utilisée ou la distribution de Clés de licence dupliquées ou générées ou l'utilisation du Logiciel suite à l'emploi d'une Clé de licence obtenue d'une source autre que le Fournisseur).

7. **Droit d’auteur**. Le Logiciel et tous les droits inclus, notamment les droits d’auteur et les droits de propriété intellectuelle sont la propriété d’ESET et/ou de ses concédants de licence. ESET est protégée par les dispositions des traités internationaux et par toutes les lois nationales applicables dans le pays où le Logiciel est utilisé. La structure, l’organisation et le code du Logiciel sont des secrets commerciaux importants et des informations confidentielles appartenant à ESET et/ou à ses concédants de licence. Vous n’êtes pas autorisé à copier le Logiciel, sauf dans les exceptions précisées en 6 (a). Toutes les copies que vous êtes autorisé à faire en vertu du présent Contrat doivent contenir les mentions relatives aux droits d’auteur et de propriété qui apparaissent sur le Logiciel. Si vous rétroconcevez, décompilez ou désassemblez le Logiciel ou tentez de toute autre façon de découvrir le code source du Logiciel, en violation des dispositions du présent Contrat, vous acceptez que les données ainsi obtenues doivent être automatiquement et irrévocablement transférées au Fournisseur dans leur totalité, dès que de telles données sont connues, indépendamment des droits du Fournisseur relativement à la violation du présent Contrat.

8. **Réservation de droits**. Le Fournisseur se réserve tous les droits sur le Logiciel, à l’exception des droits qui vous sont expressément garantis en vertu des termes du présent Contrat en tant qu’Utilisateur final du Logiciel.

9. **Versions multilingues, logiciel sur plusieurs supports, copies multiples**. Si le Logiciel est utilisé sur plusieurs plateformes et en plusieurs langues, ou si vous recevez plusieurs copies du Logiciel, vous ne pouvez utiliser le Logiciel que pour le nombre de systèmes informatiques ou de versions pour lesquels vous avez obtenu une Licence. Vous ne pouvez pas vendre, louer à bail, louer, concéder en sous-licence, prêter ou transférer des versions ou des copies du Logiciel que vous n’utilisez pas.

10. **Début et fin du Contrat.** Ce Contrat entre en vigueur à partir du jour où vous en acceptez les modalités. Vous pouvez résilier ce Contrat à tout moment en désinstallant de façon permanente, détruisant et renvoyant, à vos frais, le Logiciel, toutes les copies de sauvegarde et toute la documentation associée remise par le Fournisseur ou ses partenaires commerciaux. Votre droit d'utiliser le Logiciel et l'une de ses fonctionnalités peut être soumis à la Politique de fin de vie. Lorsque le logiciel ou l'une de ses fonctionnalités atteint la date de fin de vie définie dans la

Politique de fin de vie, votre droit d'utiliser le logiciel prend fin. Quelle que soit la façon dont ce Contrat se termine, les dispositions énoncées aux articles 7, 8, 11, 13, 19 et 21 continuent de s'appliquer pour une durée illimitée.

11. **DÉCLARATIONS DE L'UTILISATEUR FINAL**. EN TANT QU'UTILISATEUR FINAL, VOUS RECONNAISSEZ QUE LE LOGICIEL EST FOURNI « EN L'ÉTAT », SANS AUCUNE GARANTIE D'AUCUNE SORTE, QU'ELLE SOIT EXPRESSE OU IMPLICITE, DANS LA LIMITE PRÉVUE PAR LA LOI APPLICABLE. NI LE FOURNISSEUR, NI SES CONCÉDANTS DE LICENCE, NI SES FILIALES, NI LES DÉTENTEURS DE DROIT D'AUTEUR NE FONT UNE QUELCONQUE DÉCLARATION OU N'ACCORDENT DE GARANTIE EXPRESSE OU IMPLICITE QUELCONQUE, NOTAMMENT DES GARANTIES DE VENTE, DE CONFORMITÉ À UN OBJECTIF PARTICULIER OU SUR LE FAIT QUE LE LOGICIEL NE PORTE PAS ATTEINTE À DES BREVETS, DROITS D'AUTEURS, MARQUES OU AUTRES DROITS DÉTENUS PAR UN TIERS. NI LE FOURNISSEUR NI AUCUN AUTRE TIERS NE GARANTIT QUE LES FONCTIONS DU LOGICIEL RÉPONDRONT À VOS ATTENTES OU QUE LE FONCTIONNEMENT DU LOGICIEL SERA CONTINU ET EXEMPT D'ERREURS. VOUS ASSUMEZ L'ENTIÈRE RESPONSABILITÉ ET LES RISQUES LIÉS AU CHOIX DU LOGICIEL POUR L'OBTENTION DES RÉSULTATS ESCOMPTÉS ET POUR L'INSTALLATION, L'UTILISATION ET LES RÉSULTATS OBTENUS.

12. **Aucune obligation supplémentaire**. À l'exception des obligations mentionnées explicitement dans le présent Contrat, aucune obligation supplémentaire n'est imposée au Fournisseur et à ses concédants de licence.

13. **LIMITATION DE GARANTIE**. DANS LA LIMITE MAXIMALE PRÉVUE PAR LES LOIS APPLICABLES, LE FOURNISSEUR, SES EMPLOYÉS OU SES CONCÉDANTS DE LICENCE NE SERONT EN AUCUN CAS TENUS POUR RESPONSABLES D'UNE QUELCONQUE PERTE DE PROFIT, REVENUS, VENTES, DONNÉES, OU DES FRAIS D'OBTENTION DE BIENS OU SERVICES DE SUBSTITUTION, DE DOMMAGE MATÉRIEL, DOMMAGE PHYSIQUE, INTERRUPTION D'ACTIVITÉ, PERTE DE DONNÉES COMMERCIALES, OU DE TOUT DOMMAGE DIRECT, INDIRECT, FORTUIT, ÉCONOMIQUE, DE GARANTIE, PUNITIF, SPÉCIAL OU CORRÉLATIF, QUELLE QU'EN SOIT LA CAUSE ET QUE CE DOMMAGE DÉCOULE D'UNE RESPONSABILITÉ CONTRACTUELLE, DÉLICTUELLE OU D'UNE NÉGLIGENCE OU DE TOUTE AUTRE THÉORIE DE RESPONSABILITÉ, LIÉE À L'INSTALLATION, À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISER LE LOGICIEL, MÊME SI LE FOURNISSEUR OU SES CONCÉDANTS DE LICENCE ONT ÉTÉ AVERTIS DE L'ÉVENTUALITÉ D'UN TEL DOMMAGE. CERTAINS PAYS ET CERTAINES LOIS N'AUTORISANT PAS L'EXCLUSION DE RESPONSABILITÉ, MAIS AUTORISANT LA LIMITATION DE RESPONSABILITÉ, LA RESPONSABILITÉ DU FOURNISSEUR, DE SES EMPLOYÉS OU DE SES CONCÉDANTS DE LICENCE SERA LIMITÉE AU MONTANT QUE VOUS AVEZ PAYÉ POUR LA LICENCE.

14. Aucune disposition du présent Contrat ne porte atteinte aux droits accordés par la loi de toute partie agissant comme client si l'exécution y est contraire.

15. **Assistance technique**. ESET ou des tiers mandatés par ESET fourniront une assistance technique à leur discrétion, sans garantie ni déclaration solennelle. Aucune assistance technique ne sera fournie après que le Logiciel ou l'une de ses fonctionnalités ait atteint la date de fin de vie telle que définie dans la Politique de fin de vie. L'Utilisateur Final devra peut-être sauvegarder toutes les données, logiciels et programmes existants avant que l'assistance technique ne soit fournie. ESET et/ou les tiers mandatés par ESET ne seront en aucun cas tenus responsables d'un quelconque dommage ou d'une quelconque perte de données, de biens, de logiciels ou de matériel, ou d'une quelconque perte de profit en raison de la fourniture de l'assistance technique. ESET et/ou les tiers mandatés par ESET se réservent le droit de décider si l'assistance technique couvre la résolution du problème. ESET se réserve le droit de refuser, de suspendre l'assistance technique ou d'y mettre fin à sa discrétion. Des informations de licence, d'autres informations et des données conformes à la Politique de confidentialité peuvent être requises en vue de fournir une assistance technique.

16. **Transfert de Licence**. Le Logiciel ne peut pas être transféré d'un système informatique à un autre, à moins d'une précision contraire dans les modalités du présent Contrat. L'Utilisateur Final n'est autorisé qu'à transférer de façon définitive la Licence et tous les droits accordés par le présent Contrat à un autre Utilisateur Final avec l'accord du Fournisseur, si cela ne s'oppose pas aux modalités du présent Contrat et dans la mesure où (i) l'Utilisateur Final d'origine ne conserve aucune copie du Logiciel ; (ii) le transfert des droits est direct, c'est-à-dire

qu’il s’effectue directement de l’Utilisateur Final original au nouvel Utilisateur Final ; (iii) le nouvel Utilisateur Final assume tous les droits et devoirs de l’Utilisateur Final d’origine en vertu du présent Contrat ; (iv) l’Utilisateur Final d’origine transmet au nouvel Utilisateur Final toute la documentation permettant de vérifier l’authenticité du Logiciel, conformément à l’article 17.

17. **Vérification de l’authenticité du Logiciel.** L’Utilisateur final peut démontrer son droit d'utiliser le Logiciel de l'une des façons suivantes : (i) au moyen d'un certificat de licence émis par le Fournisseur ou un tiers mandaté par le Fournisseur ; (ii) au moyen d'un contrat de licence écrit, si un tel contrat a été conclu ; (iii) en présentant un courrier électronique envoyé au Fournisseur contenant tous les renseignements sur la licence (nom d'utilisateur et mot de passe). Des informations de licence et des données d'identification de l'Utilisateur Final conformes à la Politique de confidentialité peuvent être requises en vue de vérifier l'authenticité du Logiciel.

18. **Licence pour les pouvoirs publics et le gouvernement des États-Unis**. Le Logiciel est fourni aux pouvoirs publics, y compris le gouvernement des États-Unis, avec les droits de Licence et les restrictions mentionnés dans le présent Contrat.

19. **Conformité aux contrôles à l'exportation**.

a) Vous ne devez en aucun cas, directement ou indirectement, exporter, réexporter, transférer ou mettre le Logiciel à la disposition de quiconque, ou l'utiliser d'une manière ou participer à un acte qui pourrait entraîner ESET ou ses sociétés de holding, ses filiales et les filiales de l'une de ses sociétés de holding, ainsi que les entités contrôlées par ses sociétés de holding (« Sociétés affiliées ») à enfreindre ou faire l'objet des conséquences négatives de l'enfreinte des Lois sur le contrôle à l'exportation, qui comprennent

i. les lois qui contrôlent, limitent ou imposent des exigences en matière de licence pour l'exportation, la réexportation ou le transfert de marchandises, de logiciels, de technologies ou de services, émises ou adoptées par un gouvernement, un état ou un organisme de réglementation des États-Unis d'Amérique, de Singapour, du Royaume-Uni, de l'Union européenne ou de l'un de ses États membres, ou tout pays dans lequel les obligations au titre de l'accord doivent être exécutées, ou dans lequel ESET ou l'une de ses filiales est établie ou mène ses activités et

ii. toute sanction économique, financière, commerciale ou autre, sanction, restriction, embargo, interdiction d'importation ou d'exportation, interdiction de transfert de fonds ou d'actifs ou de prestation de services, ou mesure équivalente imposée par un gouvernement, un État ou un organisme de réglementation des États-Unis d'Amérique, de Singapour, du Royaume-Uni, de l'Union européenne ou de l'un de ses États membres, ou tout pays dans lequel les obligations au titre de l'accord doivent être exécutées, ou dans lequel ESET ou l'une de ses filiales est établie ou mène ses activités.

(les actes juridiques mentionnés aux points i, et ii. ci-dessus étant appelés ensemble « Lois sur le contrôle à l'exportation »).

b) ESET a le droit de suspendre ses obligations en vertu des présentes Conditions ou d'y mettre fin avec effet immédiat dans le cas où :

i. ESET estime raisonnablement que l'Utilisateur a enfreint ou est susceptible d'enfreindre la disposition de l'Article 19 a) du Contrat ; ou

ii. l'Utilisateur final et/ou le Logiciel deviennent soumis aux Lois sur le contrôle à l'exportation et, par conséquent, ESET estime raisonnablement que l'exécution continue de ses obligations en vertu de l'accord pourrait entraîner ESET ou ses affiliés à enfreindre ou faire l'objet des conséquences négatives de l'enfreinte des Lois sur le contrôle à l'exportation.

c) Rien dans le Contrat ne vise, et rien ne doit être interprété comme incitant ou obligeant l'une des parties à agir

ou à s'abstenir d'agir (ou à accepter d'agir ou à s'abstenir d'agir) d'une manière qui soit incompatible, pénalisée ou interdite en vertu de toute loi sur le contrôle à l'exportation applicable.

20. **Avis**. Tous les avis, les renvois du Logiciel et la documentation doivent être adressés à : ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, sans préjudice du droit d'ESET de Vous communiquer toute modification du présent Contrat, des Politiques de confidentialité, de la Politique de fin de vie et de la documentation conformément à l'article 22 du Contrat. ESET peut Vous envoyer des e-mails, des notifications intégrés à l'application via le Logiciel ou publier la communication sur son site web. Vous acceptez de recevoir des communications légales d'ESET sous forme électronique, y compris toute communication sur la modification des Conditions, des Conditions particulières ou des Politiques de confidentialité, toute proposition/acceptation de contrat ou invitation à traiter, avis ou autres communications légales. Ces communications électroniques sont réputées avoir été reçues par écrit, sauf si les lois applicables exigent spécifiquement une autre forme de communication.

21. **Loi applicable**. Le présent Contrat est régi par la loi de la République Slovaque et interprété conformément à celle-ci. L'Utilisateur Final et le Fournisseur conviennent que les principes relatifs aux conflits de la loi applicable et la Convention des Nations Unies sur les contrats pour la Vente internationale de marchandises ne s'appliquent pas. Vous acceptez expressément que le tribunal de Bratislava I. arbitre tout litige ou conflit avec le Fournisseur ou en relation avec votre utilisation du Logiciel, et vous reconnaissez expressément que le tribunal a la juridiction pour de tels litiges ou conflits.

22. **Dispositions générales**. Si une disposition du présent Contrat s'avère nulle et inopposable, cela n'affectera pas la validité des autres dispositions du présent Contrat. Ces dispositions resteront valables et opposables en vertu des conditions stipulées dans le présent Contrat. Le présent Contrat a été signé en anglais. Si une traduction du Contrat est préparée pour des raisons de commodité ou pour toute autre raison, ou en cas de discordance entre les versions linguistiques du présent Contrat, seule la version en langue anglaise fait foi.

ESET se réserve le droit d'apporter des modifications au Logiciel ainsi que de réviser les conditions du présent Contrat, des Annexes, des Addendums, de la Politique de confidentialité, de la Politique de fin de vie et de la Documentation ou toute partie de celle-ci à tout moment en mettant à jour le document approprié (i) pour refléter les modifications apportées au Logiciel ou dans la façon dont ESET mène ses activités, (ii) pour des raisons légales, réglementaires ou de sécurité, ou (iii) pour éviter tout abus ou dommage. Vous serez averti de toute révision du Contrat par e-mail, par le biais d'une notification intégrée à l'application ou par d'autres moyens électroniques. Si vous n'êtes pas d'accord avec les modifications proposées au Contrat, vous pouvez le résilier conformément à l'article 10, dans les 30 jours suivant la réception d'une notification de la modification. À moins que Vous ne résiliez le Contrat dans ce délai, les modifications proposées seront considérées comme acceptées et prendront effet à Votre égard à la date à laquelle vous avez reçu une notification de la modification.

Cela constitue l'intégralité du Contrat entre le Fournisseur et vous en relation avec le Logiciel, et il remplace toute représentation, discussion, entreprise, communication ou publicité antérieure en relation avec le Logiciel.

EULAID: EULA-PRODUCT-LG; 3537.0

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