



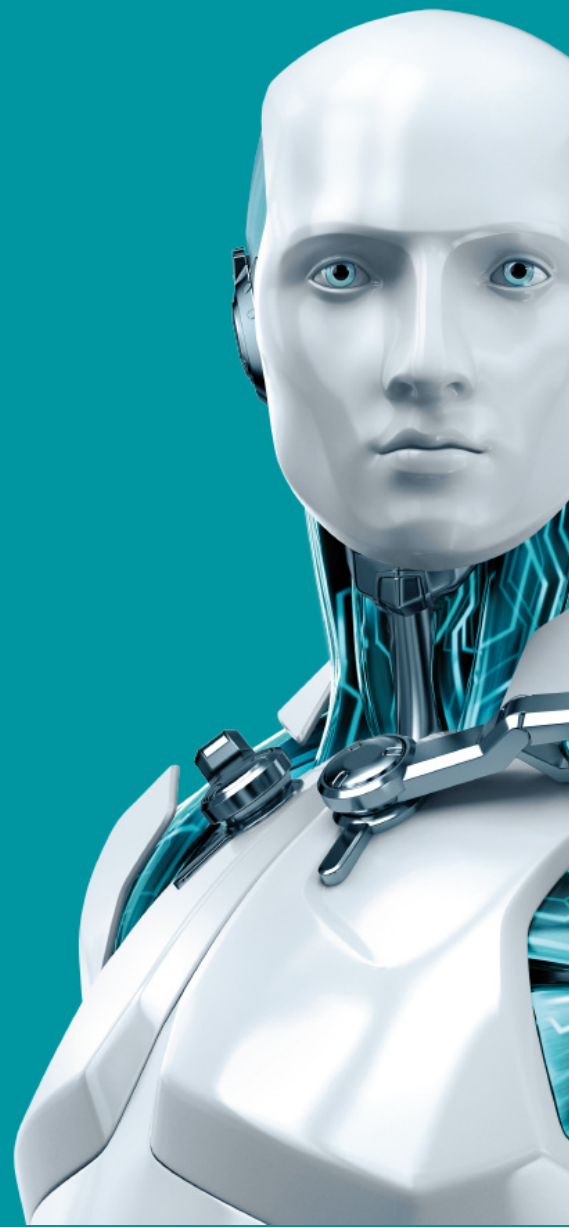
# NOD32<sup>®</sup> ANTIVIRUS

## Guide de l'utilisateur

(version 11.0 et ultérieures)

Microsoft<sup>®</sup> Windows<sup>®</sup> 10 / 8.1 / 8 / 7 / Vista / Home Server 2011

[Cliquez ici pour télécharger la dernière version de ce document.](#)



## ESET NOD32 ANTIVIRUS

**Copyright ©2017 de ESET, spol. s r. o.**

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

Pour plus d'informations, visitez [www.eset.com/fr](http://www.eset.com/fr).

Tous droits réservés. Aucune partie de cette documentation ne peut être reproduite, stockée dans un système d'archivage ou transmise sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement, numérisation ou autre, sans l'autorisation écrite de l'auteur.

ESET, spol. s r. o. se réserve le droit de modifier les applications décrites sans préavis.

Assistance clientèle internationale : [www.eset.com/support](http://www.eset.com/support)

RÉV. 06/09/2017

# Table des matières

<b>1. ESET NOD32 Antivirus.....</b>	<b>5</b>
1.1 Nouveautés de cette version.....	6
1.2 Quel produit est installé sur mon ordinateur ?.....	6
1.3 Configuration système.....	7
1.4 Prévention.....	7
<b>2. Installation.....</b>	<b>9</b>
2.1 Live installer.....	9
2.2 Installation hors connexion.....	10
2.2.1 Entrer une clé de licence.....	11
2.2.2 Utiliser le Gestionnaire de licences.....	12
2.2.3 Paramètres avancés.....	12
2.3 Problèmes d'installation courants.....	12
2.4 Activation du produit.....	13
2.5 Saisie de la clé de licence.....	13
2.6 Mise à niveau vers une nouvelle version.....	14
2.7 Première analyse après l'installation.....	14
<b>3. Guide du débutant.....</b>	<b>15</b>
3.1 Fenêtre principale de l'application.....	15
3.2 Mises à jour.....	17
<b>4. Utilisation d'ESET NOD32 Antivirus .....</b>	<b>19</b>
4.1 Protection de l'ordinateur.....	20
4.1.1 Antivirus.....	21
4.1.1.1 Protection en temps réel du système de fichiers.....	22
4.1.1.1.1 Autres paramètres ThreatSense.....	23
4.1.1.1.2 Niveaux de nettoyage.....	23
4.1.1.1.3 Quand faut-il modifier la configuration de la protection en temps réel.....	24
4.1.1.1.4 Vérification de la protection en temps réel.....	24
4.1.1.1.5 Que faire si la protection en temps réel ne fonctionne pas ?.....	24
4.1.1.2 Analyse d'ordinateur.....	25
4.1.1.2.1 Lanceur d'analyses personnalisées.....	26
4.1.1.2.2 Progression de l'analyse.....	27
4.1.1.2.3 Profils d'analyse.....	28
4.1.1.2.4 Journal d'analyse de l'ordinateur.....	28
4.1.1.3 Analyse en cas d'inactivité.....	28
4.1.1.4 Analyse au démarrage.....	29
4.1.1.4.1 Vérification automatique des fichiers de démarrage.....	29
4.1.1.5 Exclusions.....	29
4.1.1.6 Paramètres ThreatSense.....	31
4.1.1.6.1 Nettoyage.....	35
4.1.1.6.2 Extensions de fichier exclues de l'analyse.....	36
4.1.1.7 Une infiltration est détectée.....	36
4.1.1.8 Protection des documents.....	38
4.1.2 Supports amovibles.....	38
4.1.3 Contrôle de périphérique.....	39
4.1.3.1 Éditeur de règles de contrôle de périphérique.....	40
4.1.3.2 Ajout de règles de contrôle de périphérique.....	41
4.1.4 Système de détection d'intrusion au niveau de l'hôte (HIPS).....	42
4.1.4.1 Configuration avancée.....	45
4.1.4.2 Fenêtre interactive HIPS.....	45
4.1.4.3 Comportement de rançongiciel potentiel détecté.....	46
4.1.5 Mode joueur.....	46
<b>4.2 Protection Internet.....</b>	<b>47</b>
4.2.1 Protection de l'accès Web.....	48
4.2.1.1 General.....	49
4.2.1.2 Protocoles Web.....	49
4.2.1.3 Gestion d'adresse URL.....	49
4.2.2 Protection du client de messagerie.....	50
4.2.2.1 Clients de messagerie.....	50
4.2.2.2 Protocoles de messagerie.....	51
4.2.2.3 Alertes et notifications.....	52
4.2.2.4 Intégration aux clients de messagerie.....	53
4.2.2.4.1 Configuration de la protection du client de messagerie.....	53
4.2.2.5 Filtre POP3, POP3S.....	54
4.2.3 Filtrage des protocoles.....	54
4.2.3.1 Web et clients de messagerie.....	55
4.2.3.2 Applications exclues.....	55
4.2.3.3 Adresses IP exclues.....	56
4.2.3.3.1 Ajouter une adresse IPv4.....	56
4.2.3.3.2 Ajouter une adresse IPv6.....	56
4.2.3.4 SSL/TLS.....	57
4.2.3.4.1 Certificats.....	58
4.2.3.4.1.1 Trafic réseau chiffré.....	58
4.2.3.4.2 Liste des certificats connus.....	58
4.2.3.4.3 Liste des applications filtrées par le protocole SSL/TLS.....	59
4.2.4 Protection antihameçonnage.....	60
<b>4.3 Mise à jour du programme.....</b>	<b>61</b>
4.3.1 Mise à jour les paramètres.....	63
4.3.1.1 Profils de mise à jour.....	64
4.3.1.2 Configuration avancée des mises à jour.....	65
4.3.1.2.1 Mode de mise à jour.....	65
4.3.1.2.2 Proxy HTTP.....	65
4.3.2 Annulation des mises à jour.....	66
4.3.3 Comment créer des tâches de mise à jour.....	67
<b>4.4 Outils.....</b>	<b>68</b>
4.4.1 Outils dans ESET NOD32 Antivirus.....	68
4.4.1.1 Fichiers journaux.....	69
4.4.1.1.1 Fichiers journaux.....	70
4.4.1.2 Processus en cours.....	72
4.4.1.3 Statistiques de protection.....	73
4.4.1.4 Surveiller l'activité.....	74
4.4.1.5 ESET SysInspector.....	75
4.4.1.6 Planificateur.....	75
4.4.1.7 Outil de nettoyage système.....	77
4.4.1.8 ESET SysRescue.....	77
4.4.1.9 ESET LiveGrid®.....	78

4.4.1.9.1	Fichiers suspects .....	79	6.2.3	ESET LiveGrid® .....	115
4.4.1.10	Quarantaine .....	79	6.2.4	Bloqueur d'exploit Java .....	115
4.4.1.11	Serveur proxy .....	80	6.2.5	Protection contre les attaques basées sur des scripts .....	115
4.4.1.12	Notifications par e-mail .....	81	6.2.6	Protection antirançongiciels .....	116
4.4.1.12.1	Format des messages .....	82	<b>6.3</b>	<b>Courrier électronique .....</b>	<b>116</b>
4.4.1.13	Sélectionner un échantillon pour analyse .....	83	6.3.1	Publicités .....	116
4.4.1.14	Microsoft Windows® update .....	83	6.3.2	Canulars .....	117
4.4.1.15	ESET CMD .....	84	6.3.3	Hameçonnage .....	117
<b>4.5</b>	<b>Interface utilisateur .....</b>	<b>85</b>	<b>7</b>	<b>Questions fréquentes .....</b>	<b>118</b>
4.5.1	Éléments de l'interface utilisateur .....	85	<b>7.1</b>	<b>Comment mise à jour ESET NOD32</b>	
4.5.2	Alertes et notifications .....	86		<b>Antivirus .....</b>	<b>118</b>
4.5.2.1	Configuration avancée .....	88	<b>7.2</b>	<b>Comment éliminer un virus de mon PC .....</b>	<b>118</b>
4.5.3	Configuration de l'accès .....	88	<b>7.3</b>	<b>Comment créer une tâche dans le</b>	
4.5.4	Menu du programme .....	89		<b>Planificateur .....</b>	<b>119</b>
<b>5</b>	<b>Utilisateur chevronné .....</b>	<b>91</b>	<b>7.4</b>	<b>Comment programmer une analyse</b>	
<b>5.1</b>	<b>Profils .....</b>	<b>91</b>		<b>hebdomadaire de l'ordinateur .....</b>	<b>119</b>
<b>5.2</b>	<b>Raccourcis clavier .....</b>	<b>91</b>			
<b>5.3</b>	<b>Diagnostics .....</b>	<b>92</b>			
<b>5.4</b>	<b>Importer et exporter les paramètres .....</b>	<b>92</b>			
<b>5.5</b>	<b>ESET SysInspector .....</b>	<b>93</b>			
5.5.1	Présentation de ESET SysInspector .....	93			
5.5.1.1	Démarrer ESET SysInspector .....	94			
5.5.2	Interface utilisateur et utilisation de l'application .....	94			
5.5.2.1	Contrôles du programme .....	94			
5.5.2.2	Navigation dans ESET SysInspector .....	96			
5.5.2.2.1	Raccourcis clavier .....	98			
5.5.2.3	Comparer .....	99			
5.5.3	Paramètres de la ligne de commande .....	100			
5.5.4	Script de service .....	101			
5.5.4.1	Création d'un script de service .....	101			
5.5.4.2	Structure du script de service .....	101			
5.5.4.3	Exécution des scripts de service .....	104			
5.5.5	FAQ .....	105			
5.5.6	ESET SysInspector en tant que partie de ESET NOD32				
	Antivirus .....	106			
<b>5.6</b>	<b>Ligne de commande .....</b>	<b>107</b>			
<b>6</b>	<b>Glossaire .....</b>	<b>109</b>			
<b>6.1</b>	<b>Types d'infiltrations .....</b>	<b>109</b>			
6.1.1	Virus .....	109			
6.1.2	Vers .....	109			
6.1.3	Chevaux de Troie .....	110			
6.1.4	Rootkits .....	110			
6.1.5	Logiciels publicitaires .....	110			
6.1.6	Logiciels espions .....	111			
6.1.7	Compresseurs .....	111			
6.1.8	Applications potentiellement dangereuses .....	111			
6.1.9	Applications potentiellement indésirables .....	112			
<b>6.2</b>	<b>Technologie ESET .....</b>	<b>114</b>			
6.2.1	Bloqueur d'exploit .....	114			
6.2.2	Scanner de mémoire avancé .....	115			



# 1. ESET NOD32 Antivirus

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

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

## Fonctionnalités et avantages

<b>Nouvelle interface utilisateur</b>	L'interface utilisateur de la version 10 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. <b>L'aide en ligne</b> est désormais intégrée dans ESET NOD32 Antivirus et propose automatiquement des contenus de support mis à jour.
<b>Antivirus et antispyware</b>	Détecte et supprime de manière proactive un grand nombre de virus, vers, chevaux de Troie et rootkits, connus et inconnus. La technologie d' <b>heuristique avancée</b> 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 <b>protection de l'accès Web</b> et l' <b>antihameçonnage</b> surveillent les communications entre les navigateurs Internet et les serveurs distants (y compris SSL). La <b>protection du client de messagerie</b> contrôle les communications par courrier électronique reçues via les protocoles POP3(S) et IMAP(S).
<b>Mises à jour régulières</b>	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.
<b>ESET LiveGrid® (Évaluation de la réputation effectuée par le service de Cloud)</b>	Vous pouvez vous informer de la réputation des processus et des fichiers en cours d'exécution à partir de ESET NOD32 Antivirus.
<b>Contrôle de périphérique</b>	Analyse automatiquement toutes les clés USB, cartes mémoire et CD/DVD. Bloque les supports amovibles selon le type de support, le fabricant, la taille et d'autres attributs.
<b>Fonctionnalité HIPS (Host Intrusion Prevention System)</b>	Vous pouvez personnaliser le comportement du système de manière plus poussée : spécifier des règles pour le registre système, activer les processus et les programmes et optimiser votre niveau de sécurité.
<b>Mode joueur</b>	Diffère toutes les fenêtres contextuelle, les mises à jour ou les autres activités intensives du système pour économiser les ressources système au bénéfice du jeu et d'autres activités en plein écran.

Il est nécessaire d'activer une licence pour pouvoir utiliser les fonctionnalités de ESET NOD32 Antivirus. Il est recommandé de renouveler votre licence plusieurs semaines avant l'expiration de celle d'ESET NOD32 Antivirus.

## 1.1 Nouveautés de cette version

La nouvelle version d'ESET NOD32 Antivirus offre les améliorations suivantes :

- **Protection contre les attaques basées sur des scripts** : vous protège de manière proactive contre les attaques basées sur des scripts dynamiques et les vecteurs d'attaque qui ne sont pas traditionnels. Pour plus d'informations, cliquez [ici](#).
- **Performances optimales et faible impact sur le système** : cette version a été conçue pour que les ressources système soient utilisées efficacement, afin que vous puissiez tirer parti des performances de votre ordinateur tout en le protégeant contre de nouveaux types de menace.
- **Comptabilité avec Windows 10** : ESET prend entièrement en charge Microsoft Windows 10.
- **JAWS** : ESET NOD32 Antivirus prend en charge JAWS, le lecteur d'écran le plus utilisé.
- **Analyse par glisser-déposer** : vous pouvez analyser manuellement un fichier ou un dossier en le déplaçant vers la zone marquée.
- ESET NOD32 Antivirus vous informe lorsque vous vous connectez à un réseau sans fil sans protection ou à un réseau avec une faible protection.

Pour obtenir plus d'informations sur les nouvelles fonctionnalités d'ESET NOD32 Antivirus, veuillez consulter l'article de la base de connaissances ESET suivant :

[Nouveautés de cette version 10 des produits ESET pour les particuliers](#)

## 1.2 Quel produit est installé sur mon ordinateur ?

ESET offre plusieurs couches de sécurité à l'aide de nouveaux produits qui vont d'une solution antivirus puissante et rapide à une solution de sécurité tout en un, avec une empreinte minimale sur le système :

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

Pour déterminer quel produit est installé sur votre ordinateur, ouvrez la fenêtre principale du programme (voir l'[article de la base de connaissances](#)). Le nom du produit apparaît en haut de la fenêtre (titre).

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

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Antivirus	✓	✓	✓
Antispyware	✓	✓	✓
Bloqueur d'exploit	✓	✓	✓
Protection contre les attaques basées sur des scripts	✓	✓	✓
Antihameçonnage	✓	✓	✓
Protection de l'accès Web	✓	✓	✓
HIPS (incluant la protection antiransomware)	✓	✓	✓
Antispam		✓	✓
Pare-feu		✓	✓
Surveillance des périphériques connectés au réseau domestique		✓	✓

Protection de la Webcam		✓	✓
Protection contre les attaques réseau		✓	✓
Protection anti-botnet		✓	✓
Protection des transactions bancaires		✓	✓
Contrôle parental		✓	✓
Antivol		✓	✓
ESET Password Manager			✓
ESET Secure Data			✓

#### REMARQUE

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

## 1.3 Configuration système

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

### Processeurs pris en charge

Intel® ou AMD x86 - x64

### Systèmes d'exploitation pris en charge

Microsoft® Windows® 10

Microsoft® Windows® 8.1

Microsoft® Windows® 8

Microsoft® Windows® 7

Microsoft® Windows® Vista

Microsoft® Windows® Home Server 2011, version 64 bits

## 1.4 Prévention

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

### Mise à jour régulièrement

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

### Télécharger les patches de sécurité

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

## **Sauvegarder les données importantes**

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

## **Rechercher régulièrement les virus sur votre ordinateur**

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

## **Suivre les règles de sécurité de base**

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

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

## 2. Installation

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

- [Live installer](#) peut être téléchargé à partir du site Web d'ESET. Le package d'installation est universel et s'applique à toutes les langues (choisissez la langue souhaitée). Live installer lui-même est un fichier de petite taille ; les fichiers supplémentaires nécessaires à l'installation de ESET NOD32 Antivirus sont téléchargés automatiquement.
- [Installation hors connexion](#) – Ce type d'installation est utilisé lorsque l'installation s'effectue à partir d'un CD/DVD du produit. Dans ce cas, on utilise un fichier .exe qui est plus volumineux que le fichier Live installer et qui ne nécessite pas de connexion à Internet ou de fichiers supplémentaires pour réaliser l'installation.

### ! IMPORTANT

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

### 2.1 Live installer

Après avoir téléchargé le programme d'installation *Live installer*, double-cliquez sur le fichier d'installation et suivez les instructions indiquées dans la fenêtre du programme d'installation.

### ! IMPORTANT

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



Sélectionnez la langue souhaitée dans le menu déroulant, puis cliquez sur **Continuer**. Attendez un instant, le temps de télécharger les fichiers d'installation.

Après avoir accepté le **contrat de licence de l'utilisateur final**, vous êtes invité à configurer **ESET LiveGrid®** et la **détection des applications potentiellement indésirables**. [ESET LiveGrid®](#) veille à ce qu'ESET soit immédiatement et sans cesse informé des nouvelles menaces pour la protection des clients. Le système permet de soumettre les nouvelles menaces au laboratoire de recherche ESET, où elles sont analysées, traitées, puis ajoutées au moteur de détection.

Par défaut, l'option **Activer le système de commentaires ESET LiveGrid® (recommandé)** est sélectionnée et cette fonction est donc activée.

L'étape suivante de l'installation consiste à configurer la détection des applications potentiellement indésirables. Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais peuvent avoir une incidence négative sur le comportement du système d'exploitation. Reportez-vous au chapitre [Applications potentiellement indésirables](#) pour plus d'informations.

Cliquez sur **Installer** pour lancer le processus d'installation. Cette opération peut prendre quelques minutes. Cliquez sur **Terminer** pour compléter la configuration du produit et commencer l'activation.

#### **i REMARQUE**

Si vous disposez d'une licence vous permettant d'installer d'autres versions d'un produit, vous pouvez sélectionner ce produit selon vos préférences. Pour plus d'informations sur les fonctionnalités de chaque produit, cliquez [ici](#).

## **2.2 Installation hors connexion**

Lancez le programme (.exe) d'installation hors connexion ; l'assistant d'installation vous guide tout au long du processus de configuration.



Sélectionnez la langue souhaitée dans le menu déroulant, puis cliquez sur **Continuer**. Attendez un instant, le temps de télécharger les fichiers d'installation.

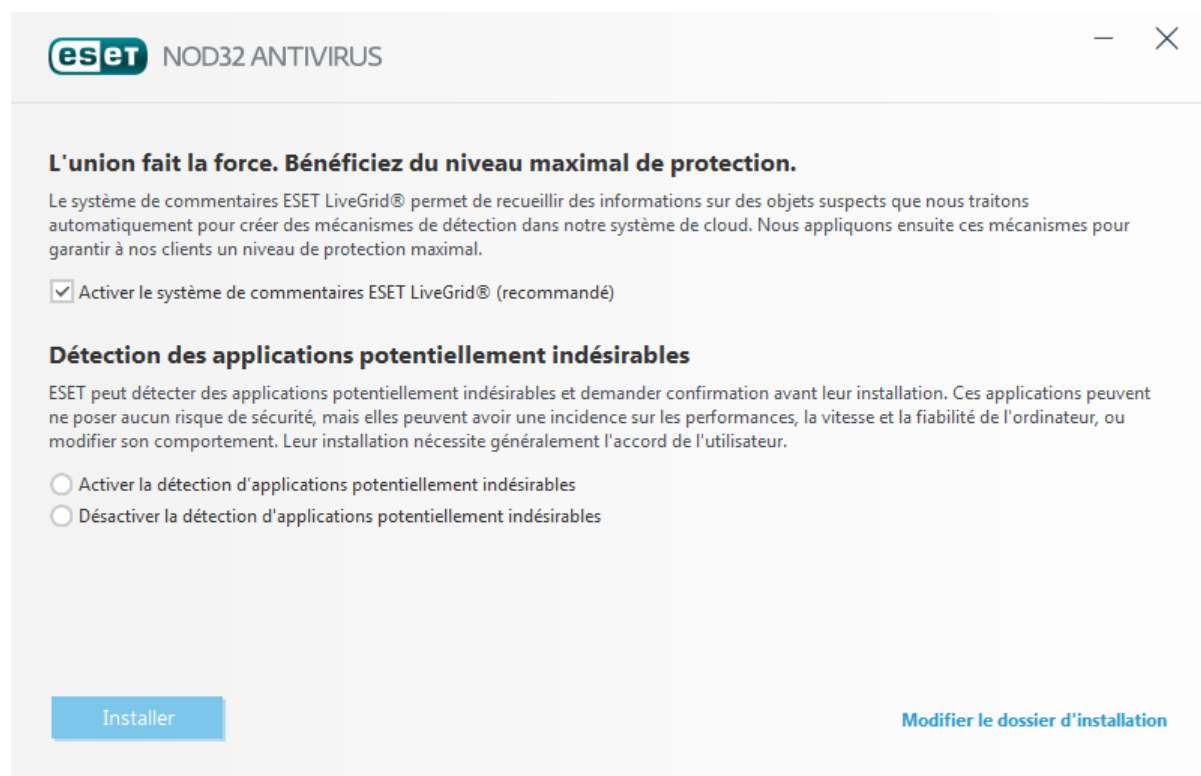
Après avoir accepté le **contrat de licence de l'utilisateur final**, vous êtes invité à [entrer une clé de licence](#) ou [utiliser le Gestionnaire de licences](#).

Si vous ne disposez pas encore d'une licence, sélectionnez **Essai gratuit** pour tester le produit ESET pendant une période limitée ou sélectionnez **Acheter une licence**. Vous pouvez aussi sélectionner **Ignorer l'activation** pour continuer l'installation sans activer de licence. Vous devrez entrer une clé de licence ultérieurement.

### 2.2.1 Entrer une clé de licence

The Setup Wizard select the product to install according to your license key and display the product name during installation. To view a list products your license can be used to activate, click **Change product**. For more information about the features in each specific product, click [here](#).

Click **Continue** and select your preferred settings for **ESET LiveGrid®** and **detection of potentially unwanted applications**. **ESET LiveGrid®** helps ensure that ESET is immediately and continuously informed about new threats in order to protect our customers. Le système permet de soumettre les nouvelles menaces au laboratoire de recherche ESET, où elles sont analysées, traitées, puis ajoutées au moteur de détection. Les **applications potentiellement indésirables** ne sont pas nécessairement malveillantes, mais peuvent avoir une incidence négative sur le comportement du système d'exploitation. Reportez-vous au chapitre [Applications potentiellement indésirables](#) pour plus d'informations.



The screenshot shows the ESET NOD32 ANTIVIRUS installation window. The title bar includes the ESET logo and the text "NOD32 ANTIVIRUS". The main content area has a header "L'union fait la force. Bénéficiez du niveau maximal de protection." followed by a paragraph explaining the ESET LiveGrid system. Below this, there is a checkbox labeled "Activer le système de commentaires ESET LiveGrid® (recommandé)" which is checked. Another section titled "Détection des applications potentiellement indésirables" explains that ESET can detect such applications and asks for confirmation before installation. Below this, there are two radio buttons: "Activer la détection d'applications potentiellement indésirables" (selected) and "Désactiver la détection d'applications potentiellement indésirables". At the bottom left is a blue "Installer" button, and at the bottom right is a link "Modifier le dossier d'installation".

Cliquez sur **Installer** pour lancer le processus d'installation. Cette opération peut prendre quelques minutes. Click **Done** to complete product setup and begin the activation process.

#### **i** REMARQUE

If you have a license that allows you select between products, you can install a product according to your preferences. For more information about the features in each specific product, click [here](#).

For more instructions about installation steps, **ESET LiveGrid®** and **Detection of potentially unwanted applications**, follow the instructions in the [“Live installer”](#) section.

### 2.2.2 Utiliser le Gestionnaire de licences

After selecting **Use License Manager** you will be asked for your my.eset.com credentials in a new window. Enter your my.eset.com credentials and click **Sign in** to use a license in License Manager. Sélectionnez une licence pour l'activation, puis cliquez sur **Continuer**. ESET NOD32 Antivirus est activé.

#### REMARQUE

If you do not have a my.eset.com account yet, register by clicking the **Create account** button.

#### REMARQUE

Si vous avez oublié votre mot de passe, cliquez sur **J'ai oublié mon mot de passe** et suivez la procédure indiquée sur la page Web vers laquelle vous êtes redirigé.

ESET License Manager vous permet de gérer toutes vos licences ESET. You can easily renew, upgrade or extend your license and see the important license details. Entrez tout d'abord votre clé de licence. After that, you will see the product, associated device, the number of available seats and the expiration date. You can deactivate or rename specific devices. Lorsque vous cliquez sur **Étendre**, vous êtes redirigé vers un magasin en ligne où vous pouvez confirmer votre achat et acquérir le renouvellement.

If you want to upgrade your license (for example from ESET NOD32 Antivirus to ESET Smart Security Premium) or would like to install an ESET security product on another device, you will be redirected to the online store to complete the purchase.

In ESET License Manager you can also add different licenses, download products to your devices or share licenses through email.

### 2.2.3 Paramètres avancés

Après avoir sélectionné **Modifier le dossier d'installation**, vous serez invité à sélectionner un emplacement d'installation. Par défaut, le système installe le programme dans le répertoire suivant :

*C:\Program Files\ESET\ESET NOD32 Antivirus\*

Cliquez sur **Parcourir** pour changer d'emplacement (non recommandé).

Pour effectuer les étapes d'installation suivantes, **ESET LiveGrid®** et **Détection des applications potentiellement indésirables**, suivez les instructions de la section Live Installer (voir [Live installer](#)).

Pour terminer l'installation, cliquez sur **Continuer**, puis sur **Installer**.

## 2.3 Problèmes d'installation courants

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




## 2.4 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 du mode de distribution (CD/DVD, page Web ESET, etc.) :


- Si vous disposez d'une version du produit vendue dans une boîte, activez votre produit à l'aide d'une **clé de licence**. Cette clé de licence se trouve généralement à l'intérieur ou au dos de l'emballage du produit. Vous devez entrer la clé de licence exactement comme elle est indiquée. Clé de licence : chaîne unique au format XXXX-XXXX-XXXX-XXXX ou XXXX-XXXXXXXXX qui sert à identifier le propriétaire de la licence et à activer la licence.
- Si vous souhaitez évaluer ESET NOD32 Antivirus avant d'en faire l'acquisition, sélectionnez **Licence d'essai gratuit**. Indiquez votre adresse électronique et le pays dans lequel vous résidez pour activer ESET NOD32 Antivirus pendant une période limitée. Votre licence de test sera envoyée à cette adresse. Les licences d'essai ne peuvent être activées qu'une seule fois par client.
- Si vous n'avez pas de licence et souhaitez en acheter une, cliquez sur Acheter une licence. Cette opération vous redirigera vers le site Web de votre distributeur ESET local.

### Je possède une licence



#### Entrer une clé de licence

Utilisez une licence que vous avez achetée en ligne ou en magasin.



#### Utiliser le Gestionnaire de licences

Connectez-vous à [my.eset.com](https://my.eset.com) et procédez à l'activation à l'aide d'une licence que vous avez ajoutée au Gestionnaire de licences.

### Je souhaite acheter une nouvelle licence



#### Acheter une licence

Achetez une nouvelle licence pour ce produit ou d'autres produits ESET.

## 2.5 Saisie de la clé de licence

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

## 2.6 Mise à niveau vers une nouvelle version

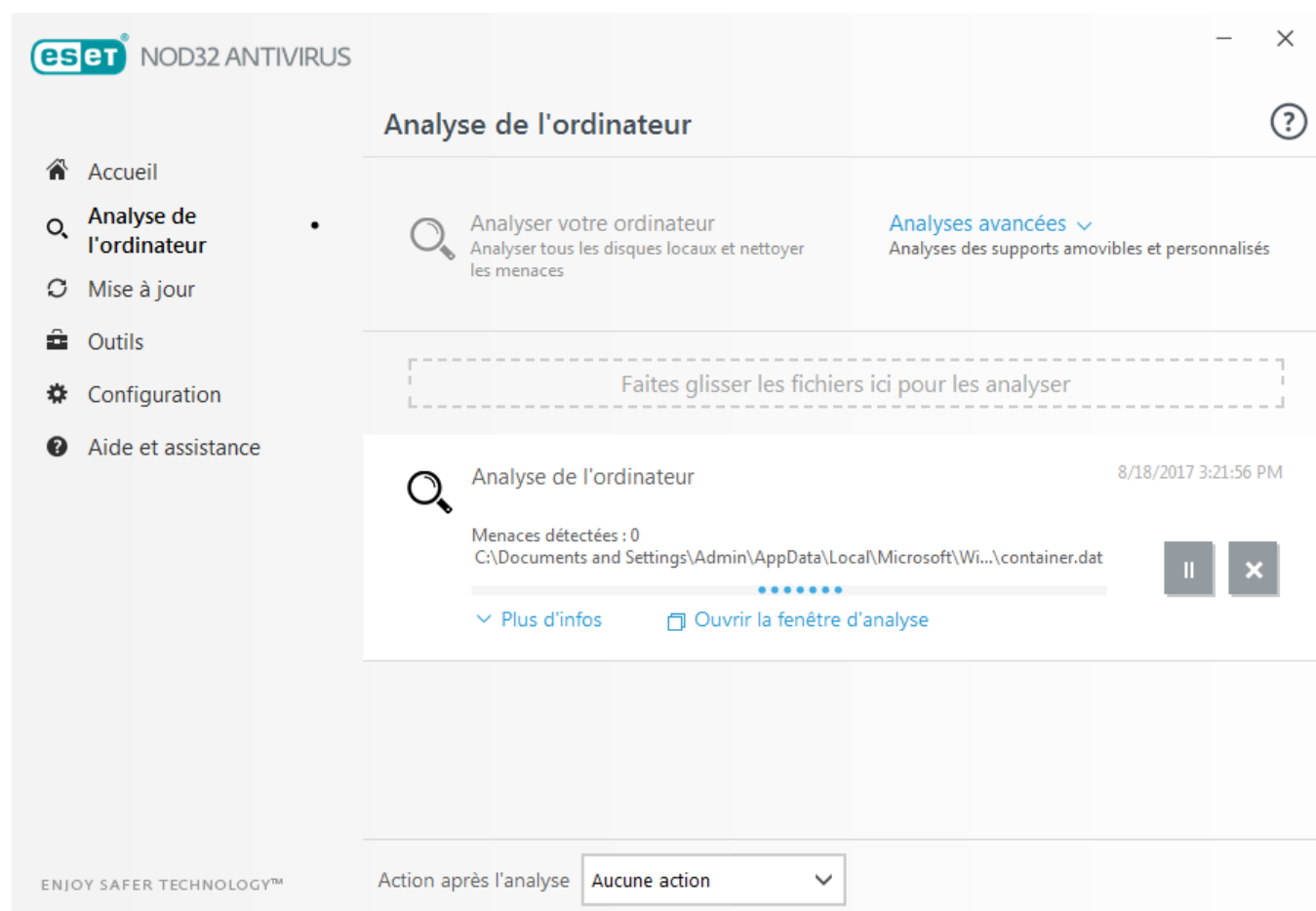
Les nouvelles versions d'ESET NOD32 Antivirus offrent des améliorations ou apportent des solutions aux problèmes que les mises à jour automatiques des modules ne peuvent pas résoudre. La mise à niveau vers une nouvelle version peut s'effectuer de différentes manières :

1. Automatiquement, par l'intermédiaire d'une mise à jour du programme.  
Les mises à niveau du programme sont distribuées à tous les utilisateurs et peuvent avoir un impact sur certaines configurations système. Elles sont par conséquent mises à disposition après de longues périodes de test afin que leur fonctionnement 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.
2. Manuellement, en cliquant dans la fenêtre principale du programme sur **Rechercher des mises à jour** dans la section **Mettre à jour**.
3. Manuellement, en téléchargeant la nouvelle version et en l'installant sur l'installation précédente.

## 2.7 Première analyse après l'installation

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

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



## 3. Guide du débutant

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

### 3.1 Fenêtre principale de l'application

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

Voici une description des options disponibles dans le menu principal :

**Accueil** – Fournit des informations sur l'état de protection d'ESET NOD32 Antivirus.

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

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

**Outils** – Permet d'accéder aux fichiers journaux, aux statistiques de protection, à la surveillance de l'activité, aux processus en cours, au planificateur, à ESET SysInspector et à ESET SysRescue.

**Configuration** – Sélectionnez cette option pour régler le niveau de sécurité de votre ordinateur, d'Internet.

**Aide et assistance** – Permet d'accéder aux fichiers d'aide, à la [base de connaissances ESET](#), au site d'ESET et aux liens nécessaires à l'envoi d'une requête d'assistance.




La section **Accueil** contient des informations importantes sur le niveau de protection actuel de votre ordinateur. La fenêtre d'état affiche les fonctionnalités utilisées fréquemment dans ESET NOD32 Antivirus. La date d'expiration du programme et les informations sur la dernière mise à jour figurent également ici.

✓ L'icône verte et l'état vert **Protection maximale** indiquent que la protection maximale est assurée.


## Que faire lorsque le programme ne fonctionne pas correctement ?

Si un module de protection actif fonctionne correctement, l'icône d'état de la protection est verte. Une icône représentant un point d'exclamation rouge ou orange indique que la protection maximale n'est pas garantie. Des informations supplémentaires sur l'état de protection de chaque module, ainsi que des suggestions de solution permettant de restaurer la protection complète, sont affichées dans l'**Accueil**. Pour changer l'état des différents modules, cliquez sur **Configuration**, puis sur le module souhaité.



 L'icône rouge et l'état rouge « La protection maximale n'est pas assurée » signalent des problèmes critiques. Cet état peut être affiché pour différentes raisons, par exemple :

- **Produit non activé** : vous pouvez activer ESET NOD32 Antivirus depuis l'**Accueil** en cliquant sur **Activer le produit** ou sur **Acheter maintenant** sous l'état de la protection.
- **Le moteur de détection n'est plus à jour** – Cette erreur apparaît après plusieurs tentatives infructueuses de mise à jour de la base des signatures de virus. Nous vous conseillons de vérifier les paramètres de mise à jour. Cette erreur provient généralement de l'entrée incorrecte de [données d'authentification](#) ou de la configuration incorrecte des [paramètres de connexion](#).
- **Protection antivirus et antispyware désactivée** : vous pouvez réactiver la protection antivirus et antispyware en cliquant sur **Activer la protection antivirus et antispyware**.
- **Licence arrivée à expiration** : cette information est indiquée par l'icône d'état de protection qui devient rouge. Le programme ne peut plus effectuer de mise à jour après expiration de la licence. Suivez les instructions de la fenêtre d'alerte pour renouveler la licence.

 L'icône orange indique une protection limitée. Par exemple, il peut s'agir d'un problème de mise à jour ou de l'imminence de l'expiration de votre licence.

Cet état peut être affiché pour différentes raisons :

- **Mode joueur activé** : l'activation du [mode joueur](#) représente un risque potentiel pour la sécurité. L'activation de cette fonctionnalité désactive toutes les fenêtres contextuelles et arrête toutes les tâches planifiées.

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

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

## 3.2 Mises à jour

La mise à jour du moteur de détection et celle des composants du programme sont des opérations importantes pour la protection de votre système contre les attaques des codes malveillants. Il convient donc d'apporter une grande attention à leur configuration et à leur fonctionnement. Dans le menu principal, cliquez sur **Mise à jour**, puis sur **Mise à jour maintenant** pour rechercher toute nouvelle mise à jour du moteur de détection.

Si la clé de licence n'a pas été saisie lors de l'activation de ESET NOD32 Antivirus, vous êtes invité à l'indiquer à cette étape.

**eset** NOD32 ANTIVIRUS

### Mise à jour

✓	<b>ESET NOD32 Antivirus</b> Version actuelle :	11.0.113.1
✓	Dernière mise à jour : Dernière recherche de mises à jour :	8/18/2017 3:15:35 PM 8/18/2017 3:15:35 PM

[Afficher tous les modules](#)

ENJOY SAFER TECHNOLOGY™

Rechercher des mises à jour

La fenêtre Configuration avancée (cliquez sur **Configuration** dans le menu principal et sur **Configuration avancée**, ou appuyez sur la touche **F5** de votre clavier) comporte d'autres options de mise à jour. Pour configurer les options avancées de mise à jour telles que le mode de mise à jour, l'accès au serveur proxy et les connexions LAN, cliquez sur un onglet particulier de la fenêtre **Mise à jour**.

Configuration avancée

ANTIVIRUS 2

MISE À JOUR 2

INTERNET ET MESSAGERIE 3

CONTRÔLE DE PÉRIPHÉRIQUE 1

OUTILS

INTERFACE UTILISATEUR

+

GÉNÉRAL

-

PROFILS

Liste des profils

Modifier

MODIFIER LE PROFIL

Sélectionner le profil à modifier

Mon profil

-

GÉNÉRAL

Type de mise à jour

Mise à jour régulière

Désactiver la notification de réussite de la mise à jour

☒

+

MODE DE MISE À JOUR

+

PROXY HTTP

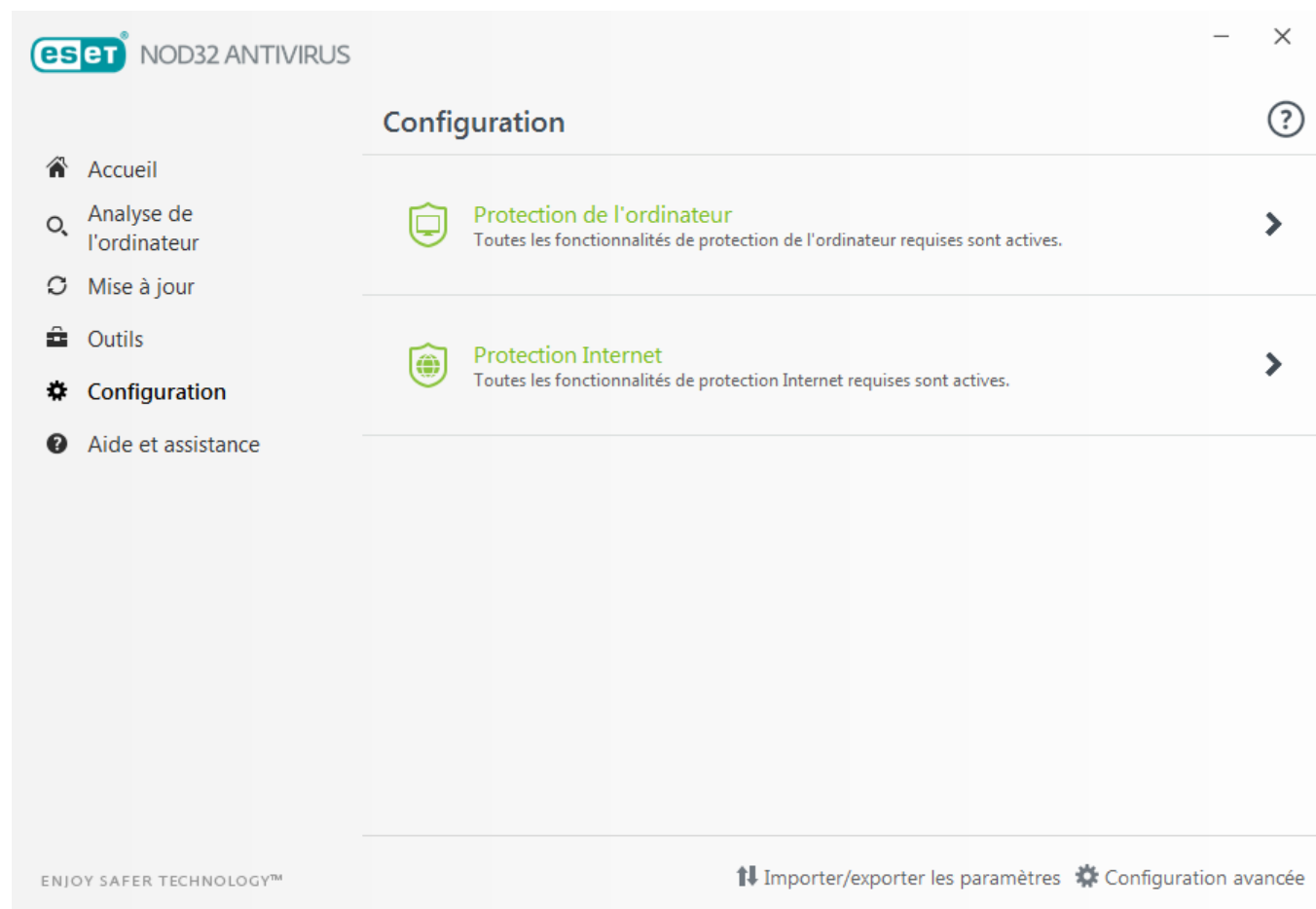
Par défaut

OK

Annuler

## 4. Utilisation d'ESET NOD32 Antivirus

Les options de configuration ESET NOD32 Antivirus permettent de régler les niveaux de protection de votre ordinateur.



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



**Protection de l'ordinateur**



**Protection Internet**

Cliquez sur un composant pour régler les paramètres avancés du module de protection correspondant.

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

- **Protection en temps réel du système de fichiers** – Tous les fichiers ouverts, créés ou exécutés sur l'ordinateur sont analysés pour y rechercher la présence éventuelle de code malveillant.
- **HIPS** – Le système [HIPS](#) surveille les événements dans le système d'exploitation et réagit en fonction d'un ensemble de règles personnalisées.
- **Mode joueur** – Active ou désactive le [mode joueur](#). Vous recevez un message d'avertissement (risque potentiel de sécurité) et la fenêtre principale devient orange lorsque le mode joueur est activé.

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

- **Protection de l'accès Web** – Si cette option est activée, tout le trafic HTTP ou HTTPS est analysé afin d'y rechercher des codes malveillants.
- **Protection du client de messagerie** – Contrôle les communications reçues via les protocoles POP3 et IMAP.
- **Protection anti-hameçonnage** – Filtre les sites Web soupçonnés de distribuer du contenu visant à manipuler les utilisateurs en vue de leur faire envoyer des informations confidentielles.



Pour réactiver un composant de sécurité désactivé, cliquez sur  pour qu'une coche verte  apparaisse.

## REMARQUE

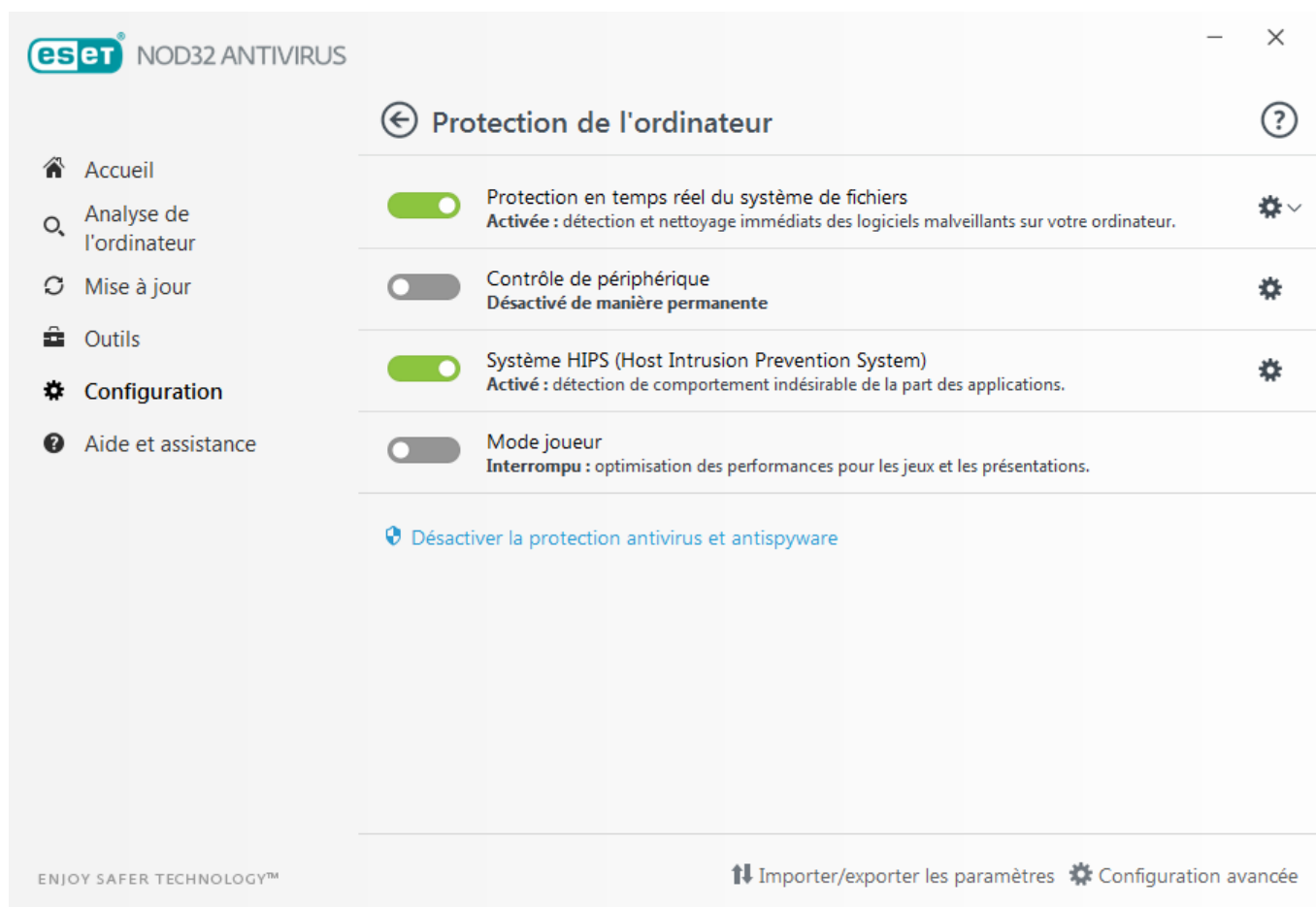
lorsque vous désactivez la protection à l'aide de cette méthode, tous les modules de protection désactivés sont activés au redémarrage de l'ordinateur.

D'autres options sont disponibles au bas de la fenêtre de configuration. Utilisez le lien **Configuration avancée** 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**.

## 4.1 Protection de l'ordinateur

Cliquez sur Protection de l'ordinateur pour voir une présentation de tous les modules de protection. Pour désactiver temporairement des modules, cliquez sur . Notez que cela pourrait abaisser le niveau de protection de l'ordinateur. Cliquez sur  à côté d'un module de protection pour accéder aux paramètres avancés de ce module.

Cliquez sur  > **Modifier les exclusions** en regard de **Protection en temps réel du système de fichiers** pour ouvrir la fenêtre de configuration [Exclusion](#) qui permet d'exclure des fichiers et des dossiers de l'analyse.



**Interrompre la protection antivirus et antispyware jusqu'au redémarrage** – Désactive tous les modules de protection antivirus et antispyware. Lorsque vous désactivez la protection, une fenêtre s'ouvre dans laquelle vous pouvez déterminer la durée pendant laquelle la protection est désactivée en sélectionnant une valeur dans le menu déroulant **Intervalle**. Cliquez sur **Appliquer** pour confirmer.



### 4.1.1 Antivirus

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

The screenshot shows the 'Configuration avancée' (Advanced Configuration) window for the Windows Security Antivirus module. The left sidebar lists various security features: ANTIVIRUS (2), MISE À JOUR (2), INTERNET ET MESSAGERIE (3), CONTRÔLE DE PÉRIPHÉRIQUE (1), OUTILS, and INTERFACE UTILISATEUR. The main pane is titled 'GÉNÉRAL' (General) and contains three sections: 'OPTION DU MOTEUR D'ANALYSE' (Analysis Engine Options), 'ANTI-STEALTH', and 'EXCLUSIONS'. In the 'OPTION DU MOTEUR D'ANALYSE' section, there are four toggle switches: 'Activer la détection d'applications potentiellement indésirables' (disabled), 'Activer la détection d'applications potentiellement dangereuses' (disabled), 'Activer la détection des applications suspectes' (checked), and 'Activer l'analyse initiale' (disabled). The 'ANTI-STEALTH' section has one toggle switch: 'Activer la technologie Anti-Stealth' (checked). The 'EXCLUSIONS' section shows 'Chemins d'accès à exclure de l'analyse' (Paths to exclude from analysis) with a 'Modifier' (Modify) link. At the bottom, there are three buttons: 'Par défaut' (Default), 'OK', and 'Annuler' (Cancel).

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

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

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

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

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

#### 4.1.1.1 Protection en temps réel du système de fichiers

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

The screenshot shows the 'Configuration avancée' window for 'Protection en temps réel du système de fichiers'. The left sidebar lists various security features: ANTIVIRUS (2), MISE À JOUR (2), INTERNET ET MESSAGERIE (3), CONTRÔLE DE PÉRIPHÉRIQUE (1), OUTILS, and INTERFACE UTILISATEUR. The main area is divided into sections: GÉNÉRAL, SUPPORTS À ANALYSER, ANALYSER QUAND, and PARAMÈTRES THREATSENSE. In the GÉNÉRAL section, 'Lancement automatique de la Protection en temps réel du système de fichiers' is checked. The SUPPORTS À ANALYSER section shows 'Lecteurs locaux', 'Périphériques amovibles', and 'Lecteurs réseau' all checked. The ANALYSER QUAND section shows 'Ouverture de fichier', 'Création de fichier', 'Exécution de fichier', and 'Accès aux périphériques amovibles' all checked. At the bottom, there are buttons for 'Par défaut', 'OK', and 'Annuler'.

Configuration avancée	
<b>ANTIVIRUS 2</b>	
<b>Protection en temps réel du système de fichiers</b>	
Analyse de l'ordinateur à la demande	
Analyse en cas d'inactivité	
Analyse au démarrage	
Périphériques amovibles	
Protection des documents	
<b>HIPS 3</b>	
<b>MISE À JOUR 2</b>	
<b>INTERNET ET MESSAGERIE 3</b>	
<b>CONTRÔLE DE PÉRIPHÉRIQUE 1</b>	
<b>OUTILS</b>	
<b>INTERFACE UTILISATEUR</b>	
<b>GÉNÉRAL</b>	
Lancement automatique de la Protection en temps réel du système de fichiers	<input checked="" type="checkbox"/>
<b>SUPPORTS À ANALYSER</b>	
Lecteurs locaux	<input checked="" type="checkbox"/>
Périphériques amovibles	<input checked="" type="checkbox"/>
Lecteurs réseau	<input checked="" type="checkbox"/>
<b>ANALYSER QUAND</b>	
Ouverture de fichier	<input checked="" type="checkbox"/>
Création de fichier	<input checked="" type="checkbox"/>
Exécution de fichier	<input checked="" type="checkbox"/>
Accès aux périphériques amovibles	<input checked="" type="checkbox"/>
<b>PARAMÈTRES THREATSENSE</b>	
Par défaut	
OK	
Annuler	

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

#### Supports à analyser

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

**Lecteurs locaux** – Contrôle tous les disques durs système.

**Supports amovibles** – Contrôle les CD/DVD, les périphériques USB, les périphériques Bluetooth, etc.

**Lecteurs réseau** – Analyse tous les lecteurs mappés.

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

#### Analyser quand

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

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

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

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

#### 4.1.1.1.1 Autres paramètres ThreatSense

##### Autres paramètres ThreatSense pour les fichiers nouveaux et les fichiers modifiés

La probabilité d'infection de fichiers nouveaux ou modifiés est comparativement supérieure à celles de fichiers existants. Pour cette raison, le programme vérifie ces fichiers avec d'autres paramètres d'analyse. ESET NOD32 Antivirus utilise l'heuristique avancée qui détecte les nouvelles menaces avant la mise à disposition de la mise à jour du moteur de détection avec les méthodes d'analyse basées sur les signatures. Outre les nouveaux fichiers, l'analyse porte également sur les **archives auto-extractibles** (.sfx) et les **fichiers exécutables compressés** (en interne). Par défaut, les archives sont analysées jusqu'au dixième niveau d'imbrication et sont contrôlées indépendamment de leur taille réelle. Pour modifier les paramètres d'analyse d'archive, désactivez **Paramètres d'analyse d'archive par défaut**.

##### Autres paramètres ThreatSense pour les fichiers exécutés

**Heuristique avancée à l'exécution du fichier** – Par défaut, l'[heuristique avancée](#) est utilisée lorsque des fichiers sont exécutés. Lorsque ce paramètre est activé, il est fortement recommandé de conserver les options [Optimisation intelligente](#) et ESET LiveGrid® activées pour limiter l'impact sur les performances système.

**Heuristique avancée lors de l'exécution de fichiers à partir de périphériques amovibles** – L'heuristique avancée émule le code dans un environnement virtuel et évalue son comportement avant qu'il ne soit autorisé à s'exécuter à partir d'un support amovible.

#### 4.1.1.1.2 Niveaux de nettoyage

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

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

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


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

#### **AVERTISSEMENT**

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

#### **4.1.1.1.3 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 d'ESET NOD32 Antivirus, tous les paramètres sont optimisés pour garantir le niveau maximum de système de sécurité aux utilisateurs. Pour rétablir les paramètres par défaut, cliquez sur  en regard de chaque onglet dans la fenêtre (**Configuration avancée > Antivirus > Protection du système de fichiers en temps réel**).

#### **4.1.1.1.4 Vérification de la protection en temps réel**

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

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

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

##### **La protection en temps réel est désactivée**

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

Si la protection en temps réel ne se lance pas au démarrage du système, c'est probablement parce que l'option **Lancer automatiquement la protection en temps réel du système de fichiers** est désactivée. Pour vérifier que cette option est activée, accédez à **Configuration avancée (F5)** et cliquez sur **Antivirus > 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 **Lancer automatiquement la protection en temps réel du système de fichiers** est activé), le problème peut provenir de conflits avec d'autres programmes. Afin d'obtenir une assistance pour résoudre ce problème, veuillez contacter le service client d'ESET.

#### 4.1.1.2 Analyse d'ordinateur

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

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

##### 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. Elle 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.

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

##### Analyse personnalisée

L'analyse personnalisée vous permet de spécifier des paramètres d'analyse tels que les cibles et les méthodes 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.

Reportez-vous au chapitre sur la [progression de l'analyse](#) pour plus d'informations sur le processus d'analyse.

#### REMARQUE

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

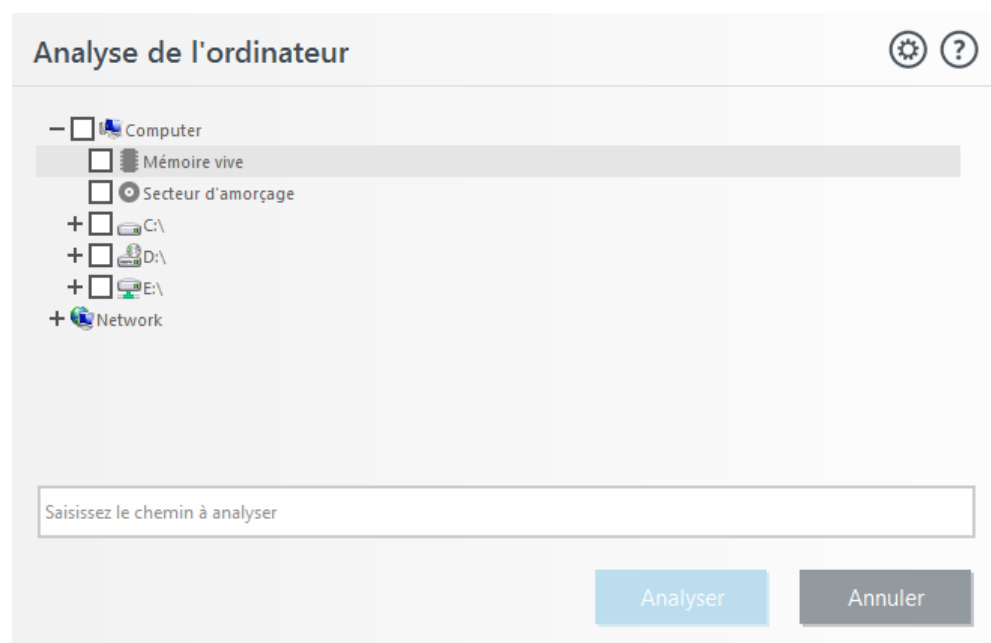
#### 4.1.1.2.1 Lanceur d'analyses personnalisées

Vous pouvez utiliser une analyse personnalisée pour analyser des parties spécifiques d'un disque plutôt que le disque entier. Pour ce faire, cliquez sur **Analyse de l'ordinateur > Analyse personnalisée**, puis sélectionnez une option dans le menu déroulant **Cibles à analyser** ou sélectionnez des cibles spécifiques dans la structure (arborescence) des dossiers.

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.
- **Lecteurs locaux** – Permet de sélectionner tous les disques durs du système.
- **Lecteurs réseau** – Analyse tous les lecteurs réseau mappés.
- **Aucune sélection** – Annule toutes les sélections.

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



Vous pouvez configurer les paramètres de nettoyage de l'analyse dans **Configuration avancée > Antivirus > Analyse de l'ordinateur à la demande > Paramètres ThreatSense > Nettoyage**. Pour effectuer une analyse sans action de nettoyage, 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 choisir un profil à utiliser lors de l'analyse de cibles spécifiques dans le menu déroulant **Profil d'analyse**. Le profil par défaut est **Analyse intelligente**. Il existe deux autres profils d'analyse prédéfinis nommés **Analyse approfondie** et **Analyse via le menu contextuel**. Ces profils d'analyse utilisent différents [paramètres ThreatSense](#). Cliquez sur **Configuration...** pour configurer un profil d'analyse personnalisé. Les options de profil d'analyse sont décrites dans la section **Autre** des [Paramètres ThreatSense](#).

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

**Analyser en tant qu'administrateur** vous permet d'exécuter l'analyse sous le compte administrateur. 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.

#### REMARQUE

Une fois une analyse terminée, vous pouvez consulter le journal d'analyse de l'ordinateur en cliquant sur [Afficher le journal](#).

#### 4.1.1.2.2 Progression de l'analyse

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

##### REMARQUE

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

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

**Cible** – Nom de l'élément analysé et emplacement.

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

**Interrompre** – Interrompt une analyse.

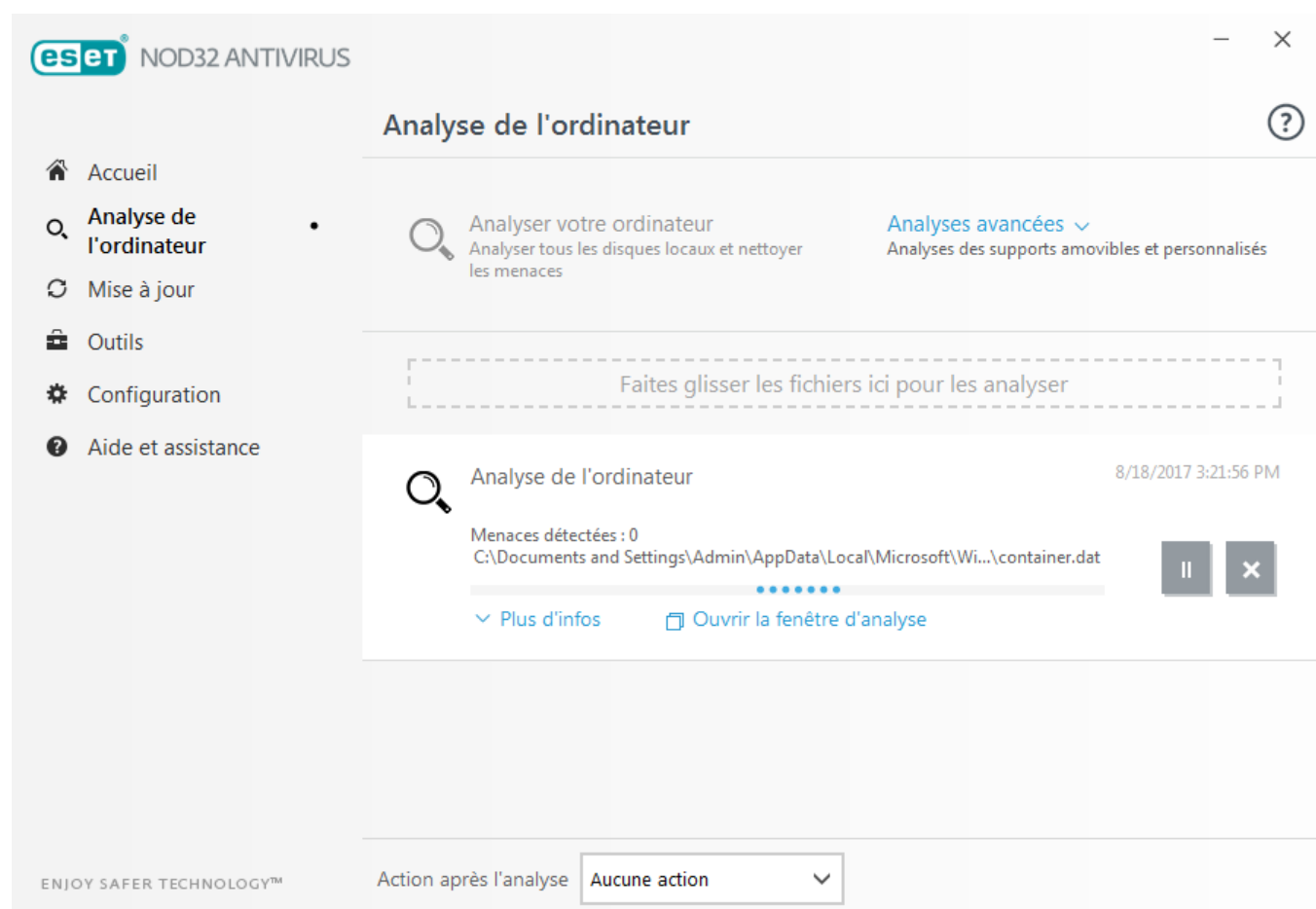
**Reprendre** – Cette option est visible lorsque l'analyse est interrompue. Cliquez sur **Reprendre** pour poursuivre l'analyse.

**Arrêter** – Met fin à l'analyse.

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

##### REMARQUE

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 intelligente** ou sur **Analyse personnalisée**.



**Action après l'analyse** – Active un arrêt, un redémarrage ou une mise en veille planifiée à la fin de l'analyse de l'ordinateur. Une fois l'analyse terminée, une boîte de dialogue de confirmation d'arrêt s'ouvre pendant 60 secondes.

#### 4.1.1.2.3 Profils d'analyse

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

Pour créer un profil, ouvrez la fenêtre Configuration avancée (F5) et cliquez sur **Antivirus > Analyse de l'ordinateur à la demande > Général > Liste des profils**. La fenêtre **Gestionnaire de profils** dispose du menu déroulant **Profil sélectionné** contenant les profils d'analyse existants, ainsi qu'une option permettant de créer un profil. Pour plus d'informations sur la création d'un profil d'analyse correspondant à vos besoins, reportez-vous à la section [ThreatSenseConfiguration du moteur](#) ; vous y trouverez une description de chaque paramètre de configuration de l'analyse.

#### REMARQUE

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

#### 4.1.1.2.4 Journal d'analyse de l'ordinateur

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

- Heure de fin
- Durée totale de l'analyse
- Nombre de menaces détectées
- Nombre d'objets analysés
- Disque, dossiers et fichiers analysés
- Date et heure de l'analyse
- Version du moteur de détection

#### 4.1.1.3 Analyse en cas d'inactivité

Cliquez sur le commutateur en regard de l'option **Activer l'analyse en cas d'inactivité** dans **Configuration avancée > Antivirus > Analyse en cas d'inactivité > Général** pour autoriser des analyses automatiques du système lorsque l'ordinateur n'est pas utilisé.

Par défaut, l'analyse d'inactivité n'est pas exécutée lorsque l'ordinateur (portable) fonctionne sur batterie. Vous pouvez remplacer ce paramètre par la fonctionnalité **Exécuter même si l'ordinateur est alimenté par batterie**.

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

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

- Économiseur d'écran
- Ordinateur verrouillé
- Utilisateur déconnecté

Cliquez sur [Paramètres ThreatSense](#) pour modifier les paramètres d'analyse (par exemple, les méthodes de détection) pour l'analyse en cas d'inactivité.



#### 4.1.1.4 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 (reportez-vous à la section suivante pour plus de détails).

Pour des instructions détaillées sur la création et à la gestion de tâches planifiées, voir [Création de nouvelles tâches](#).

##### 4.1.1.4.1 Vérification automatique des fichiers de démarrage

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

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

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

Il existe en outre deux groupes spécifiques :

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

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

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

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

##### 4.1.1.5 Exclusions

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

Pour exclure un objet de l'analyse :

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

Vous pouvez utiliser des caractères génériques pour indiquer un groupe de fichiers. Un point d'interrogation (?)

représente un seul caractère variable tandis qu'un astérisque (\*) représente une chaîne variable de zéro caractère ou plus.

## Exemples

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

Chemin d'accès	Menace
C:\Recovery\*.*	

### REMARQUE

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

## Colonnes

**Chemin** – Chemin d'accès aux fichiers et dossiers exclus.

**Menace** – Si le nom d'une menace figure à côté d'un fichier exclu, cela signifie que ce fichier n'est exclu que pour cette menace, mais qu'il n'est pas exclu complètement. Si le fichier est infecté ultérieurement par un autre logiciel malveillant, il est détecté par le module antivirus. Ce type d'exclusion ne peut être utilisé que pour certains types d'infiltrations. Il peut être créé soit dans la fenêtre des alertes de menaces qui signale l'infiltration (cliquez sur **Afficher les options avancées** et sélectionnez **Exclure de la détection**), soit dans **Outils > Quarantaine** et **Restaurer et exclure de la détection** dans le menu contextuel.

## Éléments de commande

**Ajouter** – Exclut les objets de la détection.

**Modifier** – Permet de modifier des entrées sélectionnées.

**Supprimer** – Supprime les entrées sélectionnées.

#### 4.1.1.6 Paramètres ThreatSense

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

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

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

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

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

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

#### Objets à analyser

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

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

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

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

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

**Archives auto-extractibles** – Les archives auto-extractibles (SFX) sont des archives qui sont extraites automatiquement.

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

## Options d'analyse

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

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

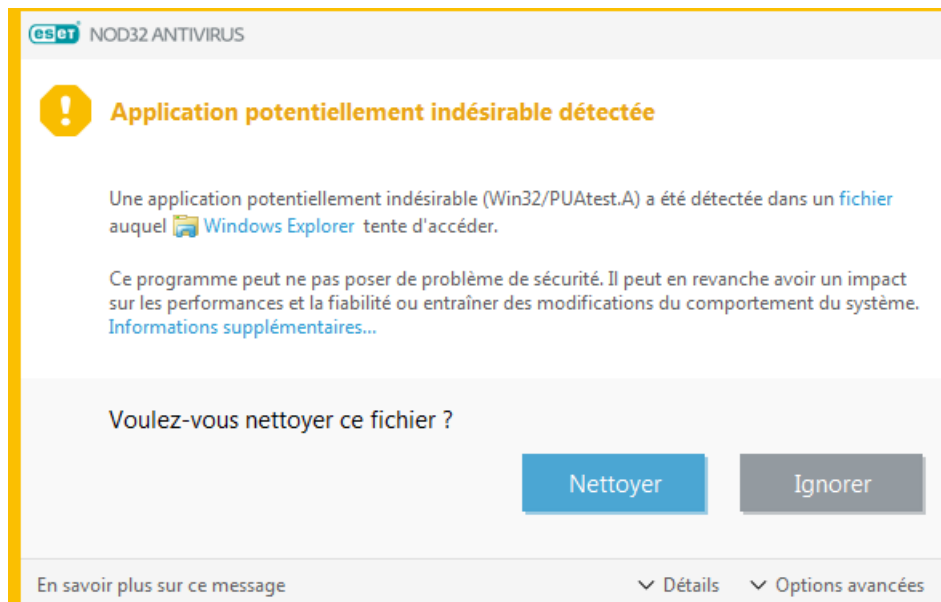
**Heuristique avancée/Signatures ADN** – La méthode heuristique avancée utilise un algorithme heuristique unique développé par ESET, optimisé pour la détection des vers d'ordinateur et des chevaux de Troie, et écrit dans un langage de programmation de haut niveau. L'utilisation de la méthode heuristique 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).

Une application potentiellement indésirable est un programme qui contient un logiciel publicitaire, qui installe des barres d'outils ou dont les objectifs ne sont pas clairs. Dans certains cas, un utilisateur peut estimer que les avantages offerts par une application potentiellement indésirable dépassent de loin les risques. Pour cette raison, ESET classe les applications de ce type dans une catégorie à faible risque par rapport aux autres types de logiciels malveillants (chevaux de Troie ou vers, par exemple).

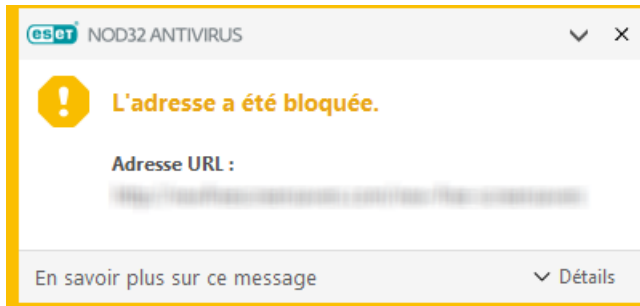
## Avertissement - Menace potentielle détectée

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

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



Si une application potentiellement indésirable est détectée et si elle ne peut pas être nettoyée, la notification **L'adresse a été bloquée** s'affiche. Pour plus d'informations sur cet événement, accédez à **Outils > Fichiers journaux > Sites Web filtrés** dans le menu principal.



## Applications potentiellement indésirables - Paramètres

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



### AVERTISSEMENT

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

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

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

# Configuration avancée

x
?

ANTIVIRUS 2

Protection en temps réel du système de fichiers

Analyse de l'ordinateur à la demande

Analyse en cas d'inactivité

Analyse au démarrage

Périphériques amovibles

Protection des documents

HIPS 3

MISE À JOUR 2

INTERNET ET MESSAGERIE 3

CONTRÔLE DE PÉRIPHÉRIQUE 1

OUTILS

INTERFACE UTILISATEUR

GÉNÉRAL

OPTION DU MOTEUR D'ANALYSE

Activer la détection d'applications potentiellement indésirables

☐
x
i

Activer la détection d'applications potentiellement dangereuses

☐
x
i

Activer la détection des applications suspectes

☒
i

Activer l'analyse initiale

☐
x
i

ANTI-STEALTH

Activer la technologie Anti-Stealth

☒
i

EXCLUSIONS

Chemin d'accès à exclure de l'analyse

Modifier

i

Par défaut

OK

Annuler

## Applications potentiellement indésirables - Wrappers logiciels

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

Consultez cet [article de la base de connaissances ESET](#) pour obtenir une version mise à jour de cette page d'aide.

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

Les paramètres de nettoyage déterminent le comportement de l'analyseur lors du nettoyage des fichiers infectés. Il existe [3 niveaux de nettoyage](#).

## Exclusions

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

## Autre

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

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

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

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

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

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

## **– Limites**

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

### **Paramètres d'objet**

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

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

### **Configuration de l'analyse d'archive**

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

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

## **i REMARQUE**

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

### **4.1.1.6.1 Nettoyage**

Les paramètres de nettoyage déterminent le comportement de l'analyseur lors du nettoyage des fichiers infectés. Il existe [3 niveaux de nettoyage](#).

#### 4.1.1.6.2 Extensions de fichier exclues de l'analyse

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

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

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

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

Vous pouvez utiliser le symbole ? (point d'interrogation). Le symbole le point d'interrogation symbolise n'importe quel caractère.

#### REMARQUE

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

#### 4.1.1.7 Une infiltration est détectée

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

##### Comportement standard

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

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

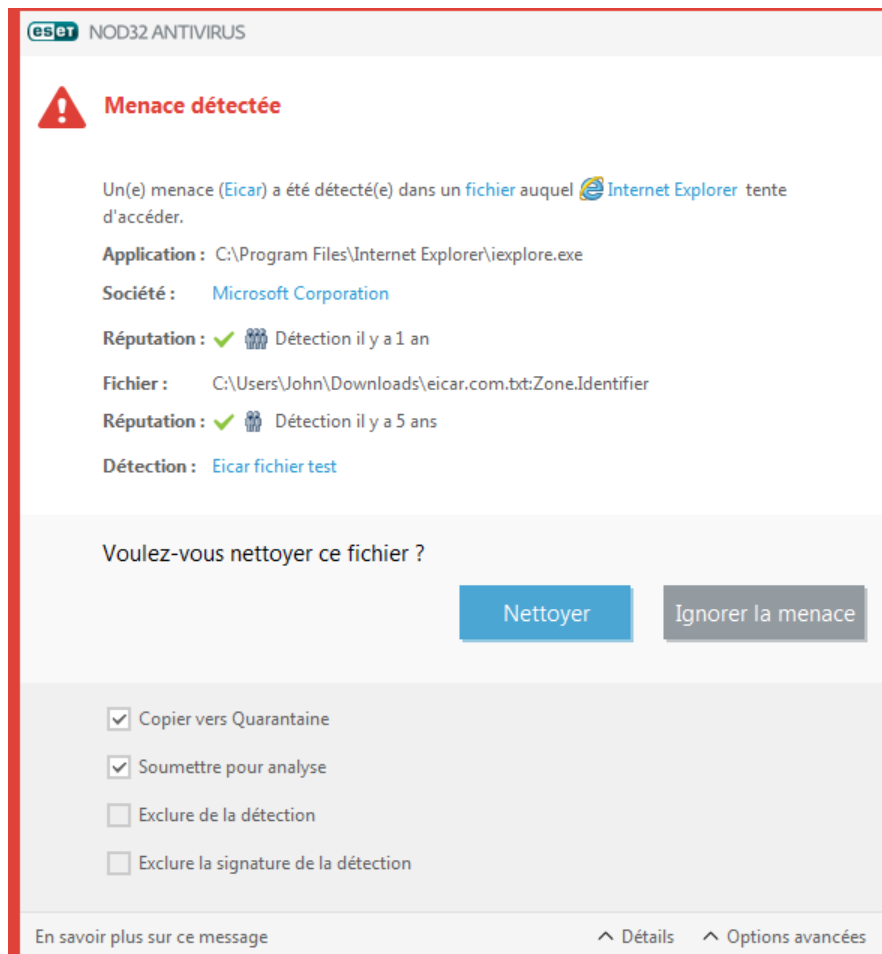
Chaque fonction utilise le niveau de nettoyage standard et tente de nettoyer le fichier et de le déplacer en [Quarantaine](#) ou met fin à la connexion. Une fenêtre de notification s'affiche dans la zone de notification, dans l'angle inférieur droit de l'écran. Pour plus d'informations sur les niveaux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





## Nettoyage et suppression

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



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

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

## Menaces multiples

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

## Suppression de fichiers dans les archives

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

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

- Ouvrez ESET NOD32 Antivirus et cliquez sur Analyse de l'ordinateur
- Cliquez sur **Analyse intelligente** (pour plus d'informations, reportez-vous à la section [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.

#### 4.1.1.8 Protection des documents

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

Pour activer la protection des documents, ouvrez la fenêtre **Configuration avancée** (press F5) > **Antivirus** > **Protection des documents**, puis cliquez sur le commutateur **Intégrer dans le système**.

##### REMARQUE

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

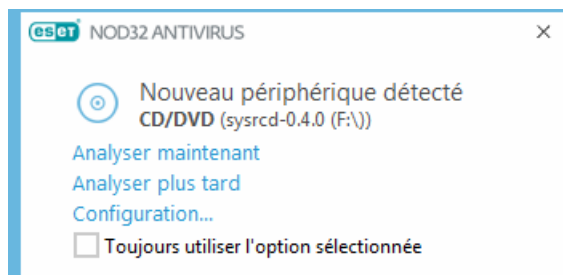
#### 4.1.2 Supports amovibles

ESET NOD32 Antivirus permet d'analyser automatiquement les supports amovibles (CD/DVD/USB...). Ce module permet d'analyser un support inséré. Cela peut être utile si l'administrateur souhaite empêcher les utilisateurs d'utiliser des supports amovibles avec du contenu non sollicité.

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

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

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



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

**Analyser ultérieurement** – L'analyse du support amovible est reportée.

**Configuration** – Ouvre la boîte de dialogue Configuration avancée.

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

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

#### 4.1.3 Contrôle de périphérique

##### Contrôle de périphérique

ESET NOD32 Antivirus permet un contrôle automatique des périphériques (CD/DVD/USB/...). Ce module permet de bloquer ou d'ajuster les filtres étendus/autorisations, et de définir les autorisations des utilisateurs à accéder à un périphérique et à l'utiliser. Ce procédé peut être utile si l'administrateur souhaite empêcher l'utilisation de périphériques avec du contenu non sollicité.

##### Périphériques externes pris en charge :

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

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

Si vous activez l'option **Intégrer au système**, la fonctionnalité de contrôle de périphérique est activée dans ESET NOD32 Antivirus ; vous devrez redémarrer votre ordinateur pour que cette modification soit prise en compte. Une fois le contrôle de périphérique activé, les **règles** deviennent actives, ce qui vous permet d'ouvrir la fenêtre [Éditeur de règles](#).

##### REMARQUE

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

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

##### Protection de la Webcam

Si vous cliquez sur le commutateur en regard de l'option **Intégrer dans le système**, la fonctionnalité Protection de la Webcam est activée dans ESET NOD32 Antivirus. Une fois la protection de la Webcam activée, les **règles** deviennent actives, ce qui vous permet d'ouvrir la fenêtre [Éditeur de règles](#).

### 4.1.3.1 Éditeur de règles de contrôle de périphérique

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

Nom	Activé	Type	Description	Action	Utilisateurs	Gravité
Block USB for User	<input checked="" type="checkbox"/>	Stockage disque	Fournisseur "Ga...	Bloquer	Tout	Toujours
Rule	<input checked="" type="checkbox"/>	Périphérique Blu...		Lire/Écrire	Tout	Toujours

Ajouter Modifier Copier Supprimer Renseigner

OK Annuler

Des périphériques spécifiques peuvent être autorisés ou bloqués par utilisateur ou groupe d'utilisateurs et basés sur des paramètres de périphériques supplémentaires qui peuvent être spécifiés dans la configuration des règles. La liste des règles contient plusieurs descriptions de la règle, telles que le nom, le type de périphérique externe, l'action à exécuter après la connexion d'un périphérique externe à l'ordinateur et le niveau de gravité d'après le journal.

Cliquez sur **Ajouter** ou **Modifier** pour gérer une règle. Cliquez sur **Copier** pour créer une règle à l'aide d'options prédéfinies utilisées pour une autre règle sélectionnée. Les chaînes XML qui s'affichent lorsque vous cliquez sur une règle peuvent être copiées dans le Presse-papiers ou aider les administrateurs système à exporter/importer ces données et à les utiliser, par exemple dans ESET Remote Administrator.

En appuyant sur CTRL et en cliquant, vous pouvez sélectionner plusieurs règles et appliquer des actions à toutes les règles sélectionnées (par exemple les supprimer ou les déplacer dans la liste). La case à cocher **Activé** permet d'activer ou de désactiver la règle ; elle peut être utile si vous ne voulez pas supprimer la règle de façon définitive.

Le contrôle s'effectue par des règles triées en fonction de leur priorité, les règles de priorité supérieure au-dessus.

Les entrées de journaux peuvent être affichées dans la fenêtre principale de ESET NOD32 Antivirus dans **Outils > Fichiers journaux**.

Le journal du contrôle de périphérique enregistre toutes les occurrences où le contrôle de périphérique est déclenché.

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

### 4.1.3.2 Ajout de règles de contrôle de périphérique

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

Modifier la règle ?

Nom: Block USB for User

Règle activée: ☒

Type de périphérique: Stockage disque

Action: Bloquer

Type de critère: Périphérique

Fournisseur: Games Company, Inc.

Modèle: basic

Série: 0x4322600934

Niveau de verbosité: Toujours

Liste des utilisateurs: [Modifier](#)

OK

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

#### Type de périphérique

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

#### Action

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

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

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

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

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

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

#### REMARQUE

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

#### REMARQUE

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

### Niveau de verbosité

ESET NOD32 Antivirus enregistre tous les événements importants dans un journal, accessible directement à partir du menu du programme. Cliquez sur **Outils > Fichiers journaux**, puis sélectionnez **Contrôle de périphérique** dans le menu déroulant **Journaliser**.

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

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

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

#### REMARQUE

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

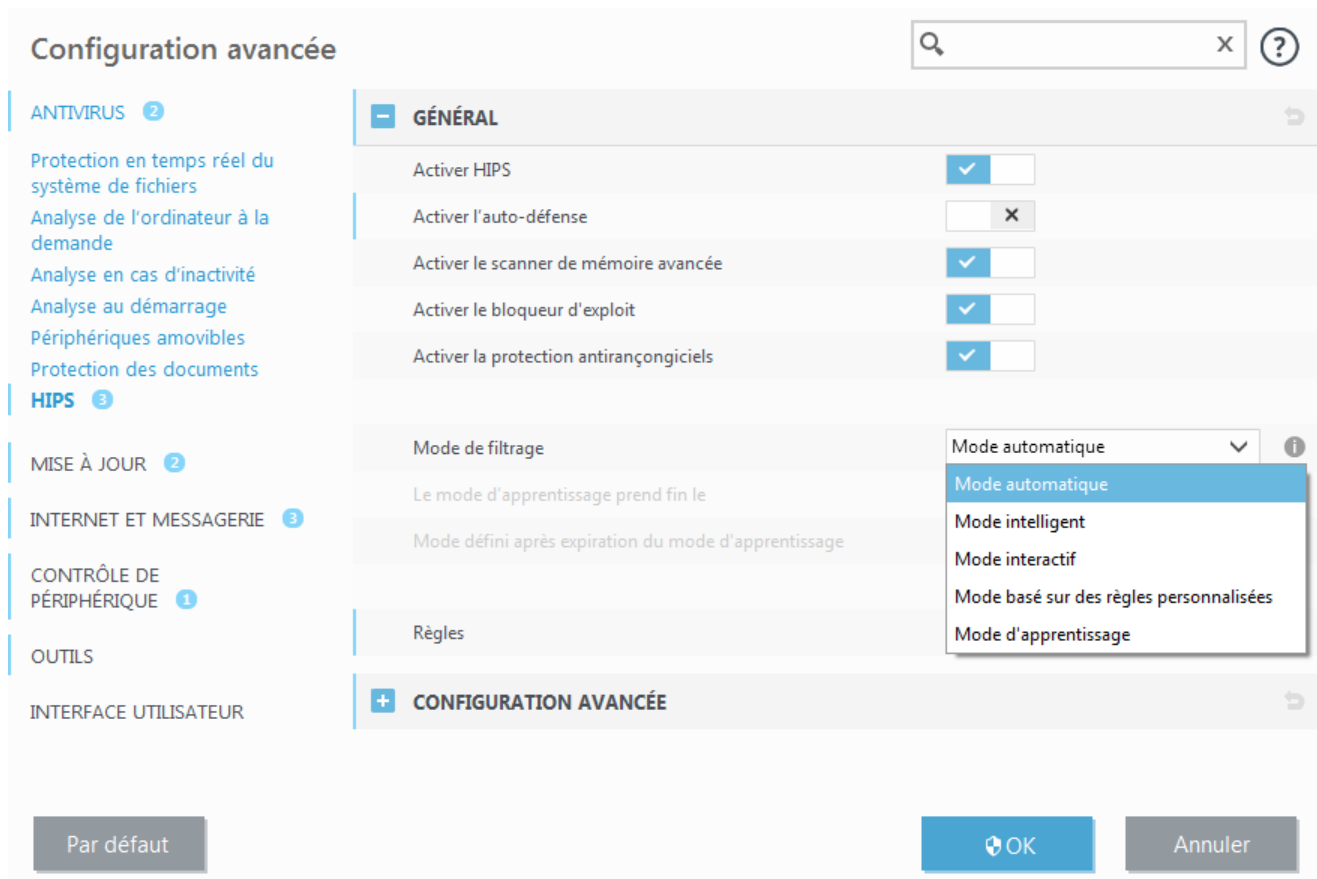
### 4.1.4 Système de détection d'intrusion au niveau de l'hôte (HIPS)

#### AVERTISSEMENT

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

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

Les paramètres HIPS sont disponibles dans **Configuration avancée (F5) > Antivirus > HIPS > Général**. L'état du système HIPS (activé/désactivé) est indiqué dans la fenêtre principale du programme ESET NOD32 Antivirus, dans la section **Configuration > Protection de l'ordinateur**.



ESET NOD32 Antivirus utilise la technologie intégrée **Auto-défense** pour empêcher les logiciels malveillants d'endommager ou de désactiver la protection antivirus et antispyware ; vous avez la garantie que votre système est protégé en permanence. Il est nécessaire de redémarrer Windows pour désactiver le système HIPS ou Auto-défense.

**Service protégé** – Active la protection du noyau (Windows 8.1, 10).

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

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

La **protection antiransomware** 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 LiveGrid. Consultez [ici](#) d'autres informations sur ce type de protection.

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

**Mode automatique** – Les opérations sont autorisées, à l'exception de celles bloquées par des règles prédéfinies qui protègent votre système.

**Mode 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 règles personnalisées** – Les opérations sont bloquées.

**Mode d'apprentissage** – Les opérations sont autorisées et une règle est créée après chaque opération. Les règles créées dans ce mode peuvent être affichées dans l'éditeur de règles, mais leur niveau de priorité est inférieur à celui des règles créées manuellement ou en mode automatique. Lorsque vous sélectionnez l'option Mode d'apprentissage dans le menu déroulant Mode de filtrage HIPS, le paramètre **Le mode d'apprentissage prend fin le**

devient disponible. Sélectionnez la durée du mode d'apprentissage. La durée maximale est de 14 jours. Lorsque la durée spécifiée est arrivée à son terme, vous êtes invité à modifier les règles créées par HIPS en mode d'apprentissage. Vous pouvez également choisir un autre mode de filtrage ou continuer à utiliser le mode d'apprentissage.

**Mode défini après expiration du mode d'apprentissage** – Sélectionnez le mode de filtrage qui sera utilisé après expiration du mode d'apprentissage.

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 des règles pour ouvrir la fenêtre de gestion des règles HIPS. La fenêtre des règles HIPS permet de sélectionner, d'ajouter, de modifier ou de supprimer des règles.

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

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

Paramètres de règle HIPS

Nom de la règle

Exemple

Action

Autoriser

Opérations affectant

Fichiers

X

Applications

✓

Entrées du Registre

X

Activé

✓

Niveau de verbosité

Aucune

Avertir l'utilisateur

✓

Précédent

Suivant

Annuler



#### 4.1.4.1 Configuration avancée

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

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

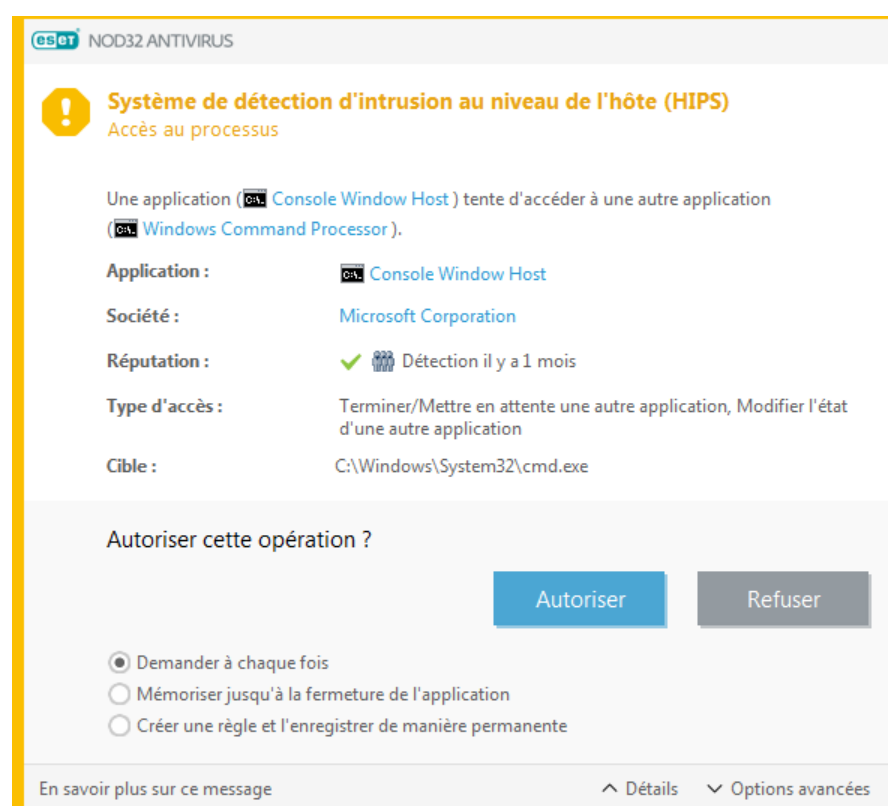
**Consigner toutes les opérations bloquées** – Toutes les opérations bloquées sont inscrites dans le journal HIPS.

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

Veuillez vous reporter à notre [base de connaissance](#) pour une version mise à jour de cette page d'aide.

#### 4.1.4.2 Fenêtre interactive HIPS

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

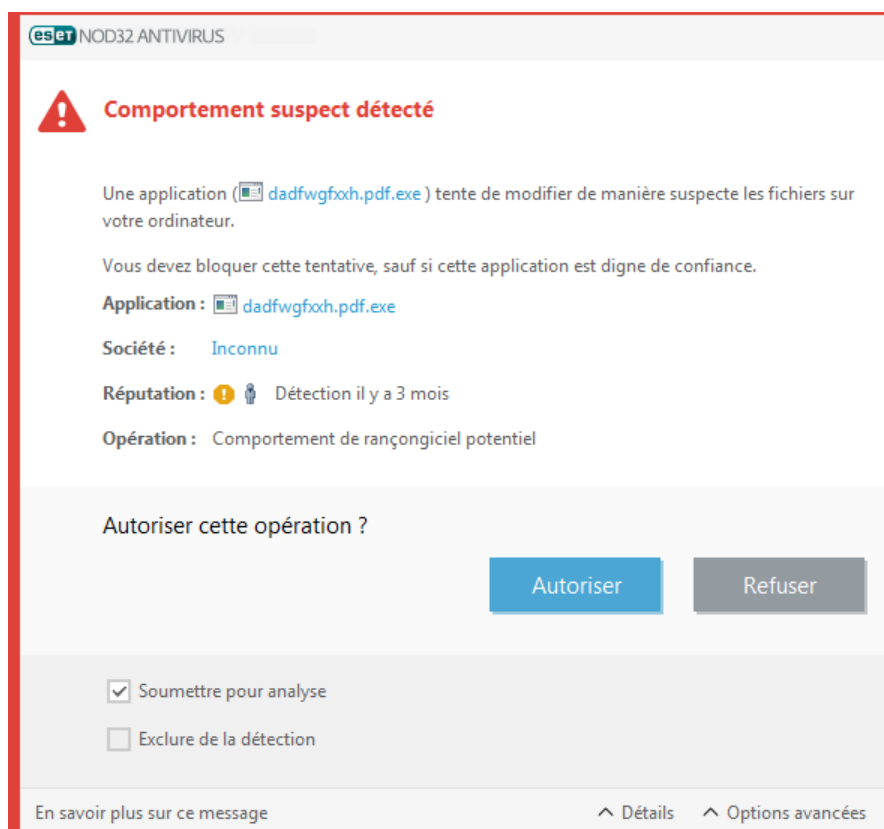


La boîte de dialogue permet de créer une règle en fonction de toute nouvelle action détectée par le système HIPS, puis de définir les conditions dans lesquelles autoriser ou refuser cette action. Pour définir les paramètres exacts, cliquez sur **Détails**. Les règles créées de cette manière sont équivalentes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

**Mémoriser 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.

#### 4.1.4.3 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.





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

#### ! IMPORTANT

Pour que la protection contre les rançongiciels fonctionne correctement, ESET Live Grid doit être activé.

#### 4.1.5 Mode joueur

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

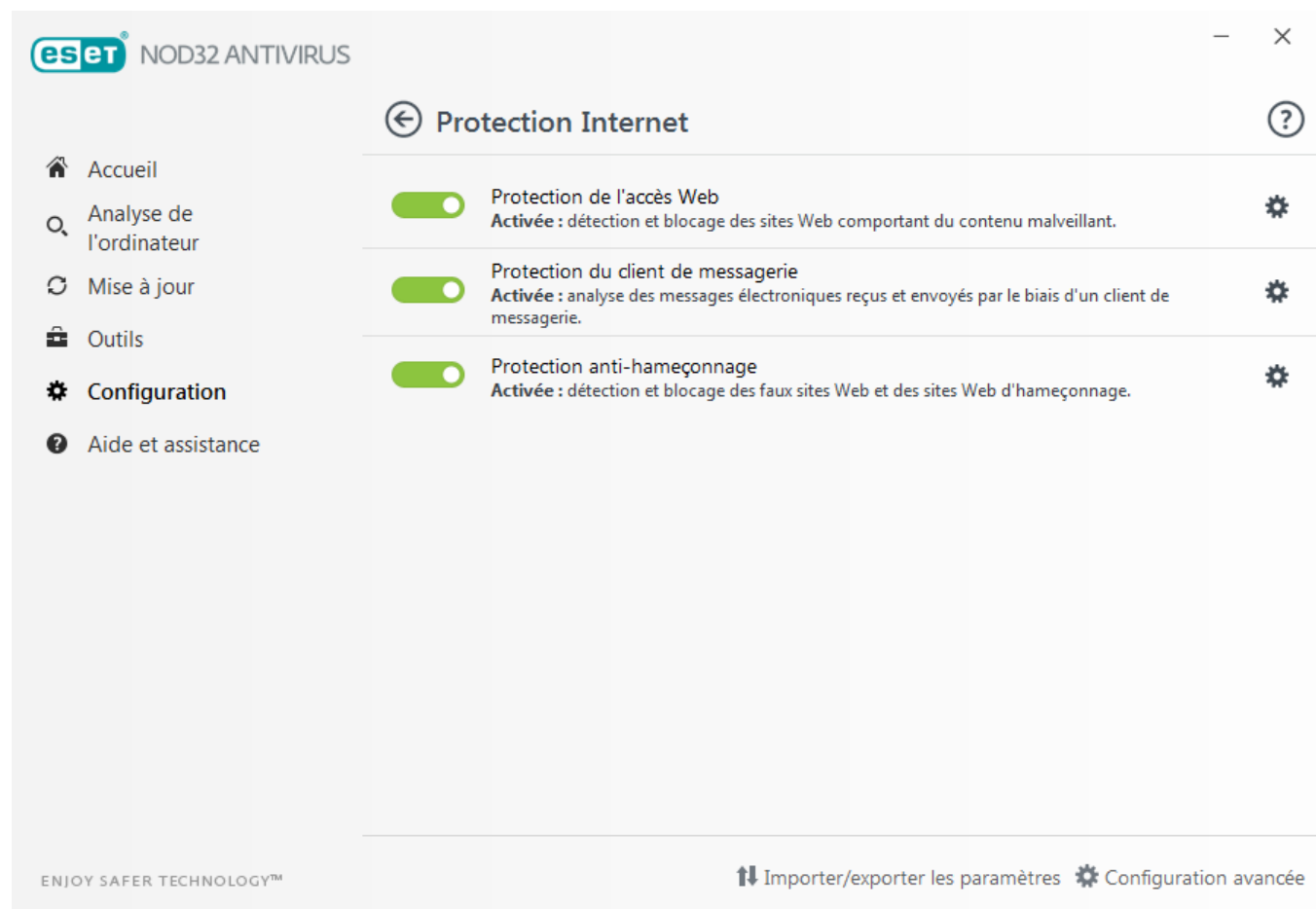
Vous pouvez activer ou désactiver le mode joueur dans la fenêtre principale du programme en cliquant sur **Configuration > Protection de l'ordinateur**, puis  ou  à côté de **Mode joueur**. L'activation du mode joueur constitue un risque potentiel pour la sécurité. C'est la raison pour laquelle l'icône d'état de la protection située dans la barre des tâches devient orange et affiche un symbole d'avertissement. Ce symbole apparaît également dans la fenêtre principale du programme, où **Mode joueur activé** apparaît en orange.

Activez l'option **Activer le mode joueur automatiquement lors de l'exécution d'applications en mode plein écran** dans **Configuration avancée (F5) > Outils** pour que le mode joueur démarre dès que vous lancez une application en mode plein écran et s'arrête lorsque vous quittez l'application.


Activez l'option **Désactiver automatiquement le mode joueur après** pour définir une durée après laquelle le mode joueur est automatiquement désactivé.

## 4.2 Protection Internet

La configuration Internet et messagerie est accessible dans le volet **Configuration** en cliquant sur **Protection Internet**. Elle permet d'accéder à des paramètres plus détaillés du programme.




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

Cliquez sur  pour ouvrir les paramètres de protection Web/messagerie/antihameçonnage dans la configuration avancée.

La **protection du client de messagerie** offre le contrôle de la communication par courrier électronique effectuée via les protocoles POP3 et IMAP. ESET NOD32 Antivirus utilise le plugin de votre client de messagerie pour contrôler toutes les communications échangées avec le client de messagerie (POP3, MAPI, IMAP, HTTP).

La **protection antihameçonnage** 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.

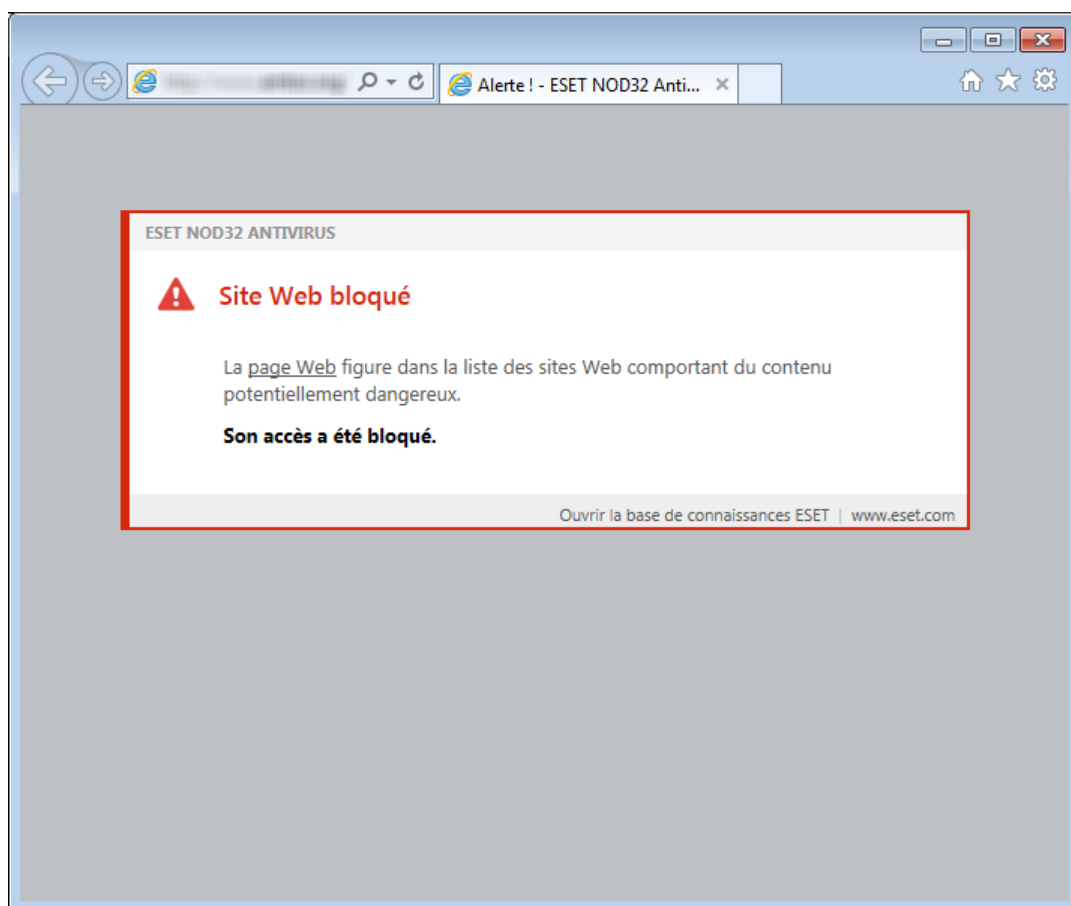
Vous pouvez désactiver temporairement le module de protection Wem/messagerie/antihameçonnage en cliquant sur .

### 4.2.1 Protection de l'accès Web

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

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

Nous vous recommandons vivement d'activer l'option de protection de l'accès au Web. Cette option est accessible à partir de la fenêtre principale de ESET NOD32 Antivirus en accédant à **Configuration > Protection Internet > Protection de l'accès Web**.



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

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

#### 4.2.1.1 General

**Activer la protection de l'accès Web** – Lorsque cette option est désactivée, la protection de l'accès Web et la protection anti-hameçonnage ne sont pas assurées.

**Activer l'analyse avancée des scripts de navigateur** – Lorsque cette option est activée, tous les programmes JavaScript exécutés par les navigateurs Internet sont vérifiés par l'analyse antivirus.

#### REMARQUE

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

#### 4.2.1.2 Protocoles Web

Par défaut, ESET NOD32 Antivirus est configuré pour contrôler le protocole HTTP utilisé par la plupart des navigateurs Internet.

##### Configuration du scanner HTTP

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

##### Configuration du scanner HTTPS

ESET NOD32 Antivirus prend également en charge le contrôle de protocole HTTPS. Les communications HTTPS utilisent un canal chiffré pour transférer des informations entre un serveur et un client. ESET NOD32 Antivirus contrôle les communications à l'aide des protocoles SSL (Secure Socket Layer) et TLS (Transport Layer Security). Le programme analyse uniquement le trafic sur les ports définis dans **Ports utilisés par le protocole HTTPS**, quelle que soit la version du système d'exploitation.

La communication chiffrée n'est pas vérifiée. Pour activer l'analyse de la communication chiffrée et afficher la configuration de l'analyseur, accédez à l'option [SSL/TLS](#) dans la section Configuration avancée, cliquez sur **Internet et messagerie** > **SSL/TLS** et activez l'option **Activer le filtrage du protocole SSL/TLS**.

#### 4.2.1.3 Gestion d'adresse URL

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

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

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

Si vous ajoutez une adresse URL à la **liste des adresses exclues du filtrage**, l'adresse est exclue de l'analyse. Vous pouvez également autoriser ou bloquer certaines adresses en les ajoutant à la **liste des adresses autorisées** ou à la **liste des adresses bloquées**.

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

Vous ne pouvez pas utiliser le symbole « \* » (astérisque) et le caractère « ? » (point d'interrogation) dans les listes. L'astérisque remplace n'importe quelle chaîne de caractères, tandis que le point d'interrogation remplace n'importe quel caractère. Soyez particulièrement prudent dans la définition des adresses exclues, car la liste ne doit contenir que des adresses fiables et sûres. De la même manière, veillez à employer correctement les symboles « \* » et « ? » dans cette liste. Reportez-vous à Ajout d'un masque de domaine/d'adresse HTTP pour déterminer comment faire

correspondre un domaine complet avec tous ses sous-domaines en toute sécurité. Pour activer une liste, sélectionnez l'option **Liste active**. Si vous souhaitez être averti lors de la saisie d'une adresse figurant dans la liste actuelle, sélectionnez l'option **Notifier lors de l'application**.

#### **i** REMARQUE

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

Liste d'adresses

Nom de la liste	Types d'adresses	Description de la liste
Liste des adresses autorisées	Autorisées	
Liste des adresses bloquées	Bloquées	
Liste des adresses exclues de la vérification	Exclues de la vérification	

Ajouter

Modifier

Supprimer

Ajouter un caractère générique (\*) à la liste des adresses bloquées pour bloquer toutes les URL, à l'exception de celles incluses dans une liste d'adresses autorisées.

OK

Annuler

### 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.

## 4.2.2 Protection du client de messagerie

### 4.2.2.1 Clients de messagerie

L'intégration d'ESET NOD32 Antivirus à votre client de messagerie augmente le niveau de protection active contre les codes malveillants dans les messages électroniques. Si votre client de messagerie est pris en charge, l'intégration peut être activée dans ESET NOD32 Antivirus. Une fois le produit intégré à votre client de messagerie, la barre d'outils d'ESET NOD32 Antivirus est insérée directement dans le client de messagerie (la barre d'outils pour les nouvelles versions de Windows Live Mail n'est pas insérée), ce qui permet une protection plus efficace des messages. Les paramètres d'intégration sont situés dans **Configuration avancée (F5) > Internet et messagerie > Protection du client de messagerie > Clients de messagerie**.

### Intégration aux clients de messagerie

Les clients de messagerie actuellement pris en charge sont Microsoft Outlook, Outlook Express, Windows Mail et Windows Live Mail. Ce module fonctionne comme un plugin pour ces programmes. L'avantage principal du

plugin réside dans le fait qu'il est indépendant du protocole utilisé. Lorsqu'un client de messagerie reçoit un message chiffré, il le déchiffre et l'envoie au scanner de virus. Pour obtenir la liste complète des clients de messagerie pris en charge, avec leur version, reportez-vous à [cet article de la base de connaissances ESET](#).

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

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

### Email à analyser

**Activer la protection de la messagerie par les plug-ins clients** – Lorsque la protection du client de messagerie par le client de messagerie est désactivée, la protection du client de messagerie par filtrage des protocoles est toujours activée.

**Courrier reçu** – Active/désactive la vérification des messages reçus.

**Courrier envoyé** – Active/désactive la vérification des messages envoyés.

**Courrier lu** – Active/désactive la vérification des messages lus.

### Action à exécuter sur le courrier électronique infecté

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

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

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

**Déplacer les courriers vers le dossier** – Les courriers infectés sont automatiquement placés dans le dossier spécifié.

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

**Répéter l'analyse après mise à jour** – Active/désactive la répétition de l'analyse après la mise à jour du moteur de détection.

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

### REMARQUE

Il est recommandé d'activer les options **Activer la protection de la messagerie par les plug-ins clients** et **Activer la protection de la messagerie par filtrage des protocoles**. Ces paramètres sont situés dans Configuration avancée (F5) > Internet et messagerie > Protection du client de messagerie > Protocoles de messagerie.

#### 4.2.2.2 Protocoles de messagerie

Les protocoles IMAP et POP3 sont les plus répandus pour la réception de courriers électroniques dans les applications clientes de messagerie. Le protocole IMAP (Internet Message Access Protocol) est un autre protocole Internet qui permet de récupérer les courriers électroniques. Le protocole IMAP présente un certain nombre d'avantages sur le protocole POP3 : par exemple, plusieurs clients peuvent se connecter simultanément à la même boîte aux lettres et tenir à jour les informations sur l'état du message (s'il a été lu, supprimé, ou encore si une réponse a été envoyée). ESET NOD32 Antivirus fournit une protection pour ces protocoles, quel que soit le client de messagerie utilisé et sans reconfiguration nécessaire du client de messagerie.

Le module de protection assurant cette vérification est automatiquement lancé au démarrage du système et reste ensuite actif en mémoire. Le contrôle de protocole IMAP est effectué automatiquement sans qu'il soit nécessaire de reconfigurer le client de messagerie. Par défaut, toutes les communications sur le port 143 sont analysées, mais vous pouvez y ajouter d'autres ports de communication au besoin. Les différents numéros de ports doivent être séparés par une virgule.

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

**Activer la protection de la messagerie par le filtrage de protocoles** : permet la vérification des protocoles de messagerie.

Dans Windows Vista et versions ultérieures, les protocoles IMAP et POP3 sont automatiquement détectés et analysés sur tous les ports. Dans Windows XP, seuls les **ports utilisés par le protocole IMAP/POP3** configurés sont analysés pour toutes les applications. Tous les ports sont analysés pour les applications signalées en tant que [Internet et clients de messagerie](#).

ESET NOD32 Antivirus prend également en charge l'analyse des protocoles IMAPS et POP3S qui utilisent un canal chiffré pour transférer des informations entre un serveur et un client. ESET NOD32 Antivirus contrôle la communication à l'aide des protocoles SSL (Secure Socket Layer) et TLS (Transport Layer Security). Le programme analyse uniquement le trafic sur les ports définis dans **Ports utilisés par le protocole IMAPS/POP3S**, quelle que soit la version du système d'exploitation.

La communication chiffrée n'est pas vérifiée. Pour activer l'analyse de la communication chiffrée et afficher la configuration de l'analyseur, accédez à l'option [SSL/TLS](#) dans la section Configuration avancée, cliquez sur **Internet et messagerie > SSL/TLS** et activez l'option **Activer le filtrage du protocole SSL/TLS**.

Configuration avancée

ANTIVIRUS 2

MISE À JOUR 2

INTERNET ET MESSAGERIE 3

Protection du client de messagerie 4

Protection de l'accès Web

Protection anti-hameçonnage

CONTRÔLE DE PÉRIPHÉRIQUE 1

OUTILS

INTERFACE UTILISATEUR

+ CLIENTS DE MESSAGERIE

- PROTOCOLES DE MESSAGERIE

Activer la protection de messagerie par le filtrage de protocoles ☒

CONFIGURATION DU MOTEUR D'ANALYSE IMAP

Activer le contrôle de protocole IMAP ☒

CONFIGURATION DU MOTEUR D'ANALYSE IMAPS

Activer le contrôle IMAPS ☒

Ports utilisés par le protocole IMAPS 585, 993

CONFIGURATION DU MOTEUR D'ANALYSE POP3

Activer le contrôle de protocole POP3 ☒

CONFIGURATION DU MOTEUR D'ANALYSE POP3S

Par défaut OK Annuler

#### 4.2.2.3 Alertes et notifications

La protection de la messagerie permet de contrôler les communications reçues via les protocoles POP3 et IMAP. ESET NOD32 Antivirus utilise le plugin pour Microsoft Outlook et d'autres clients de messagerie pour contrôler toutes les communications impliquant le client de messagerie (POP3, MAPI, IMAP, HTTP). Lorsqu'il examine les messages entrants, le programme utilise toutes les méthodes d'analyse avancées comprises dans le moteur d'analyse ThreatSense. Autrement dit, la détection des programmes malveillants s'effectue avant la comparaison avec le moteur de détection. L'analyse des communications via le protocole POP3 et IMAP est indépendante du client de messagerie utilisé.

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



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

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

**Ajouter une note à l'objet des messages infectés envoyés** – Désactivez cette option si vous ne souhaitez pas que la protection de la messagerie ajoute un avertissement de virus dans l'objet d'un message infecté. Cette fonctionnalité permet tout simplement de filtrer les courriers infectés en fonction de son objet (s'il est pris en charge par le programme de messagerie). Elle permet aussi d'augmenter la crédibilité du destinataire. En cas de détection d'une infiltration, elle fournit des informations précieuses sur le niveau de menace d'un message ou d'un expéditeur.

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

#### 4.2.2.4 Intégration aux clients de messagerie

L'intégration d'ESET NOD32 Antivirus aux clients de messagerie augmente le niveau de protection active contre les codes malveillants dans les messages électroniques. Si votre client de messagerie est pris en charge, l'intégration peut être activée dans ESET NOD32 Antivirus. Lorsque l'intégration est activée, la barre d'outils ESET NOD32 Antivirus est insérée directement dans le client de messagerie, ce qui permet de protéger les messages plus efficacement. Les paramètres d'intégration sont accessibles dans **Configuration > Configuration avancée > Internet et messagerie > Protection du client de messagerie > Clients de messagerie**.

Les clients de messagerie actuellement pris en charge sont Microsoft Outlook, Outlook Express, Windows Mail et Windows Live Mail. Pour obtenir une liste complète des clients de messagerie pris en charge, avec leur version, reportez-vous à cet article de la [base de connaissances ESET](#).

Cochez la case à côté de **Désactiver la vérification au changement de contenu de la boîte de réception** si vous constatez un ralentissement du système lors de l'utilisation du client de messagerie. Ce cas de figure peut survenir lors de la récupération d'un e-mail à partir du magasin Kerio Outlook Connector.

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

##### 4.2.2.4.1 Configuration de la protection du client de messagerie

Le module de protection de la messagerie électronique prend en charge les clients de messagerie suivants : Microsoft Outlook, Outlook Express, Windows Mail et Windows Live Mail. Ce module fonctionne comme un module plugin pour ces programmes. L'avantage principal du plugin réside dans le fait qu'il est indépendant du protocole utilisé. Lorsqu'un client de messagerie reçoit un message chiffré, il le déchiffre et l'envoie à l'analyseur de virus.

#### 4.2.2.5 Filtre POP3, POP3S

Le protocole POP3 est le protocole le plus répandu pour la réception de messages dans un client de messagerie. ESET NOD32 Antivirus protège ce protocole, quel que soit le client de messagerie utilisé.

Le module de protection qui assure ce contrôle est automatiquement lancé au démarrage du système d'exploitation et reste ensuite actif en mémoire. Pour que le module fonctionne correctement, assurez-vous qu'il est activé. Le contrôle POP3 s'effectue automatiquement sans qu'il faille reconfigurer le client de messagerie. Par défaut, toute communication sur le port 110 est soumise à une analyse, mais d'autres ports de communication peuvent être ajoutés au besoin. Les différents numéros de ports doivent être séparés par une virgule.

La communication chiffrée n'est pas vérifiée. Pour activer l'analyse de la communication chiffrée et afficher la configuration de l'analyseur, accédez à l'option [SSL/TLS](#) dans la section Configuration avancée, cliquez sur **Internet et messagerie** > **SSL/TLS** et activez l'option **Activer le filtrage du protocole SSL/TLS**.

Dans cette section, vous pouvez configurer le contrôle des protocoles POP3 et POP3S.

**Activer le contrôle du courrier électronique** – Si cette option est activée, les codes malveillants sont recherchés dans tout le trafic POP3.

**Ports utilisés par le protocole POP3S** – Liste des ports utilisés par le protocole POP3 (110 par défaut).

ESET NOD32 Antivirus prend également en charge le contrôle du protocole POP3S. Ce type de communication utilise un canal chiffré pour transférer des informations entre un serveur et un client. ESET NOD32 Antivirus contrôle les communications à l'aide des méthodes de chiffrement SSL (Secure Socket Layer) et TLS (Transport Layer Security).

**Ne pas utiliser de contrôle de protocole POP3S** – Les communications chiffrées ne sont pas vérifiées.

**Utiliser le contrôle de protocole POP3S pour les ports sélectionnés** – Activez cette option pour ne permettre le contrôle POP3S que pour les ports définis dans **Ports utilisés par le protocole POP3S**.

**Ports utilisés par le protocole POP3S** – Liste des ports POP3S à contrôler (995 par défaut).

#### 4.2.3 Filtrage des protocoles

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

**Activer le filtrage du contenu des protocoles d'application** : cette option peut être utilisée pour désactiver le filtrage des protocoles. Notez que la plupart des composants d'ESET NOD32 Antivirus (protection de l'accès Web, protection des protocoles de messagerie, protection anti-hameçonnage, filtrage Internet) dépendent de ce filtrage et ne fonctionneront pas sans celui-ci.

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

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

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

### 4.2.3.1 Web et clients de messagerie

#### REMARQUE

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

À cause du nombre considérable de codes malveillants circulant sur Internet, la sécurisation de la navigation sur Internet est un aspect très important de la protection des ordinateurs. Les vulnérabilités des navigateurs Internet et les liens frauduleux contribuent à faciliter l'accès imperceptible au système par des codes malveillants. C'est pourquoi ESET NOD32 Antivirus se concentre sur la sécurité des navigateurs Internet. Chaque application accédant au réseau peut être marquée comme étant un navigateur Internet. La case à cocher a deux états possibles :

- **Désélectionnée** – La communication des applications est filtrée uniquement pour les ports spécifiés.
- **Sélectionnée** – La communication est toujours filtrée (même si un autre port est défini).

### 4.2.3.2 Applications exclues

Pour exclure du filtrage de contenu la communication de certaines applications sensibles au réseau, sélectionnez ces applications dans la liste. Les communications HTTP/POP3/IMAP liées aux adresses sélectionnées ne font pas l'objet d'une détection des menaces. Il est recommandé d'utiliser cette option uniquement pour les applications qui ne fonctionnent pas correctement lorsque leur communication est vérifiée.

L'exécution des applications et des services est disponible automatiquement. Cliquez sur **Ajouter** pour sélectionner manuellement une application qui ne figure pas dans la liste des filtres de protocole.

Applications exclues

C:\WINDOWS\SYSTEM32\SVCHOST.EXE  
C:\WINDOWS\MICROSOFT.NET\FRAMEWORK\V4.0.30319\MSCORSVW.EXE  
C:\WINDOWS\MICROSOFT.NET\FRAMEWORK64\V4.0.30319\MSCORSVW.EXE  
C:\Windows\System32\svchost.exe

Ajouter

Modifier

Supprimer

OK

Annuler

### 4.2.3.3 Adresses IP exclues

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

Cliquez sur **Ajouter** pour exclure une adresse/une plage d'adresses/un sous-réseau IP d'un point distant qui ne figure pas dans la liste des filtrages de protocole.

Cliquez sur **Supprimer** pour supprimer les entrées sélectionnées de la liste.

Adresses IP exclues

10.1.2.3  
10.2.1.1-10.2.1.10  
192.168.1.0/255.255.255.0  
fe80::b434:b801:e878:5975  
2001:21:420::/64

Ajouter Modifier Supprimer

OK Annuler

#### 4.2.3.3.1 Ajouter une adresse IPv4

Cette option permet d'ajouter une adresse IP/une plage d'adresses/un sous-réseau d'un point distant auquel une règle est appliquée. Internet Protocol version 4 est l'ancienne version, mais il est toujours largement utilisé.

**Adresse unique** – Ajoute l'adresse IP d'un ordinateur auquel appliquer la règle (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) à laquelle la règle doit être appliquée (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 réseau du préfixe *192.168.1.0/24*, ce qui signifie que la plage d'adresses est comprise entre *192.168.1.1 à 192.168.1.254*.

#### 4.2.3.3.2 Ajouter une adresse IPv6

Cette option permet d'ajouter une adresse IPv6/un sous-réseau d'un point distant pour lequel la règle est appliquée. Il s'agit de la version la plus récente du protocole Internet et elle remplacera la version 4 plus ancienne.

**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*).

#### 4.2.3.4 SSL/TLS

ESET NOD32 Antivirus est capable de rechercher les menaces dans les communications qui utilisent le protocole SSL. Vous pouvez utiliser plusieurs modes d'analyse pour examiner les communications SSL protégées à l'aide de certificats approuvés, de certificats inconnus ou de certificats exclus de la vérification des communications SSL protégées.

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

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

**Mode automatique** : ce mode par défaut n'analyse que les applications appropriées telles que les navigateurs Web et les clients de messagerie. Vous pouvez l'ignorer en sélectionnant les applications dont les communications seront analysées.

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

**Mode de stratégie** : 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.

**Liste des applications filtrées par le protocole SSL** : permet de personnaliser le comportement d'ESET NOD32 Antivirus pour des applications spécifiques.

**Liste des certificats connus** : permet de personnaliser le comportement d'ESET NOD32 Antivirus pour des certificats SSL spécifiques.

**Exclure les communications protégées à l'aide de certificats de validation étendue** : lorsque cette option est activée, la communication avec ce type de certificat SSL est exclue de la vérification. Les certificats SSL de validation étendue garantissent que vous consultez vraiment votre site Web et non un faux site dont l'apparence est strictement identique à celle du vôtre (c'est le cas des sites de hameçonnage).

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

#### Certificat racine

**Ajouter le certificat racine aux navigateurs connus** : pour que la communication SSL fonctionne correctement dans les navigateurs/clients de messagerie, il est essentiel d'ajouter le certificat racine pour ESET à la liste des certificats racines connus (éditeurs). Lorsque cette option est activée, ESET NOD32 Antivirus ajoute automatiquement le certificat racine d'ESET aux navigateurs connus (Opera et Firefox par exemple). Pour les navigateurs utilisant le magasin de certification système, le certificat est ajouté automatiquement (Internet Explorer par exemple).

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

#### Validité du certificat

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

**toute communication utilisant le certificat** pour mettre toujours fin aux connexions chiffrées aux sites avec des certificats non vérifiés.

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

#### 4.2.3.4.1 Certificats

Pour que la communication SSL fonctionne correctement dans les navigateurs/clients de messagerie, il est essentiel d'ajouter le certificat racine pour ESET à la liste des certificats racines connus (éditeurs). **Ajouter le certificat racine aux navigateurs connus** doit être activé. Activez cette option pour ajouter automatiquement le certificat racine d'ESET aux navigateurs connus (Opera et Firefox par exemple). Pour les navigateurs utilisant le magasin de certification système (Internet Explorer par exemple), le certificat est ajouté automatiquement. Pour appliquer le certificat à des navigateurs non pris en charge, cliquez sur **Afficher le certificat > Détails > Copier dans un fichier...**, puis importez-le manuellement dans le navigateur.

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

Vous pouvez sélectionner **Bloquer toute communication utilisant le certificat** pour toujours mettre fin à la connexion chiffrée au site utilisant le certificat non vérifié.

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

##### 4.2.3.4.1.1 Trafic réseau chiffré

Si l'ordinateur est configuré pour l'analyse du protocole SSL, la boîte de dialogue vous invitant à choisir une action peut s'afficher en cas de tentative d'établissement d'une communication chiffrée (à l'aide d'un certificat inconnu).

La boîte de dialogue contient les informations suivantes :

- Nom de l'application ayant établi la communication
- Nom du certificat utilisé
- Action à exécuter : analyser ou non la communication chiffrée et mémoriser ou non l'action pour l'application et le certificat

Si le certificat ne figure pas dans le magasin TRCA, il est considéré comme non fiable.

##### 4.2.3.4.2 Liste des certificats connus

La **liste des certificats connus** peut être utilisée pour personnaliser le comportement d'ESET NOD32 Antivirus pour des certificats SSL spécifiques et mémoriser les actions choisies en cas de sélection de l'option **Mode interactif** dans **Mode de filtrage de protocole SSL/TLS**. La liste peut être affichée et modifiée dans **Configuration avancée (F5) > Internet et messagerie > SSL/TLS > Liste des certificats connus**.

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

#### Colonnes

**Nom** : nom du certificat.

**Émetteur du certificat** : nom du créateur du certificat.

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

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

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

#### Éléments de commande

**Ajouter** – 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.

#### 4.2.3.4.3 Liste des applications filtrées par le protocole SSL/TLS

La **liste des applications filtrées SSL/TSL** peut être utilisée pour personnaliser le comportement d'ESET NOD32 Antivirus pour des applications spécifiques et mémoriser les actions choisies en cas de sélection de l'option **Mode interactif** dans **Mode de filtrage de protocole SSL/TLS**. La liste peut être affichée et modifiée dans **Configuration avancée** (F5) > **Internet et messagerie** > **SSL/TLS** > **Liste des applications filtrées SSL/TLS**.

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

#### Colonnes

**Application** – Nom de l'application.

**Action d'analyse** – Sélectionnez **Analyser** ou **Ignorer** pour analyser ou ignorer la communication. Sélectionnez **Automatique** pour effectuer une analyse en mode automatique et demander quelle action entreprendre en mode interactif. Sélectionnez **Demander** pour demander toujours à l'utilisateur quelle action effectuer.

#### Éléments de commande

**Ajouter** – Ajoute une application filtrée.

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

**Supprimer** – Sélectionnez le certificat à supprimer, puis cliquez sur **Supprimer**.

**OK/Annuler** – Cliquez sur **OK** si vous souhaitez enregistrer les modifications. Sinon, cliquez sur **Annuler** pour quitter sans enregistrer.

#### 4.2.4 Protection antihameçonnage

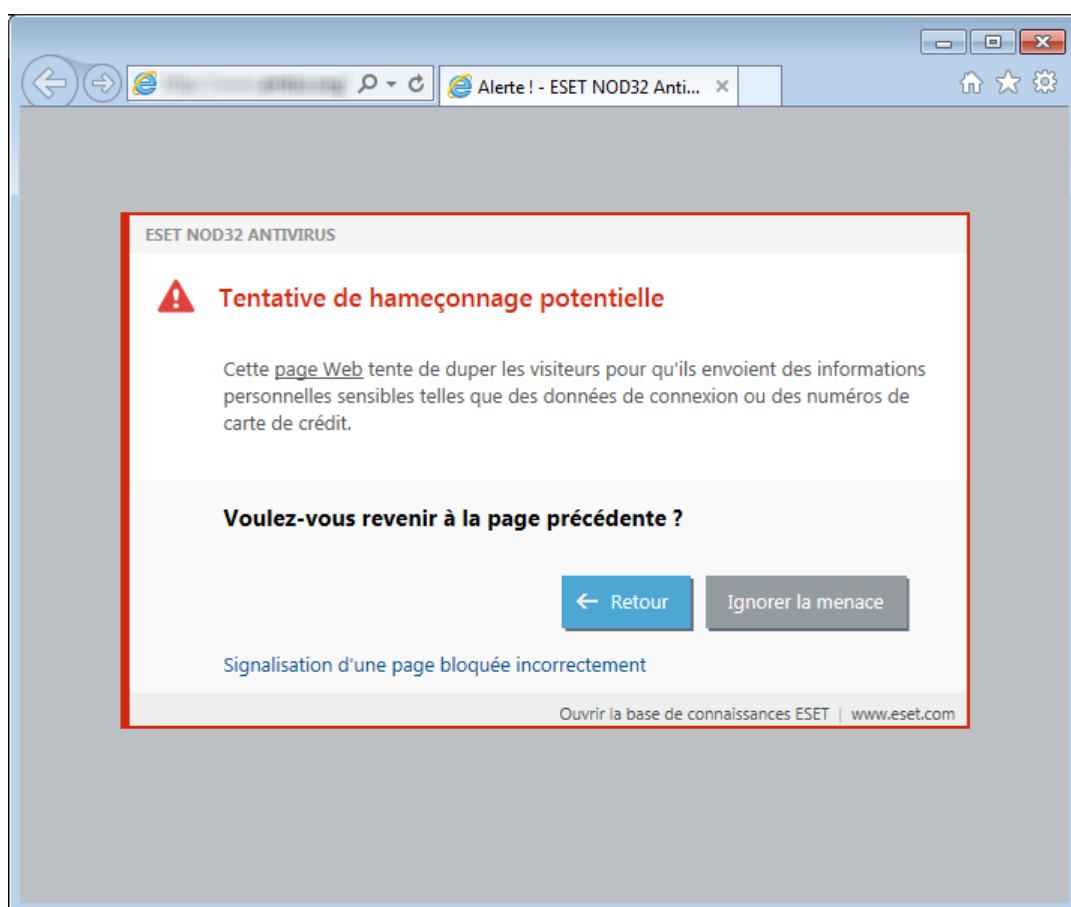
Le terme d'hameçonnage (phishing en anglais) désigne une activité frauduleuse utilisant des techniques de piratage psychologique qui consistent à manipuler les utilisateurs pour obtenir des informations confidentielles. L'hameçonnage est souvent utilisé pour accéder à des données sensibles, telles que numéros de comptes bancaires, codes secrets, etc. Pour en savoir plus sur cette activité, reportez-vous au [glossaire](#). ESET NOD32 Antivirus assure une protection antihameçonnage qui permet de bloquer les pages Web connues présentant ce type de contenu.

Nous vous recommandons fortement d'activer l'antihameçonnage dans ESET NOD32 Antivirus. Pour ce faire, accédez à **Configuration avancée** (F5), puis à **Internet et messagerie** > **Protection antihameçonnage**.

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

##### Accès à un site Web d'hameçonnage

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



##### REMARQUE

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

##### Signalement d'un site de hameçonnage

Le lien [Signaler](#) vous permet de signaler un site Web de hameçonnage/malveillant à ESET pour analyse.

##### REMARQUE

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



- le site Web n'est pas du tout détecté,
- le site Web est, à tort, détecté comme une menace. Dans ce cas, vous pouvez [signaler une page bloquée incorrectement](#).

Vous pouvez également soumettre le site Web par e-mail. Envoyez votre message à l'adresse [samples@eset.com](mailto:samples@eset.com). Veuillez à utiliser un objet descriptif et à indiquer 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.).

### 4.3 Mise à jour du programme

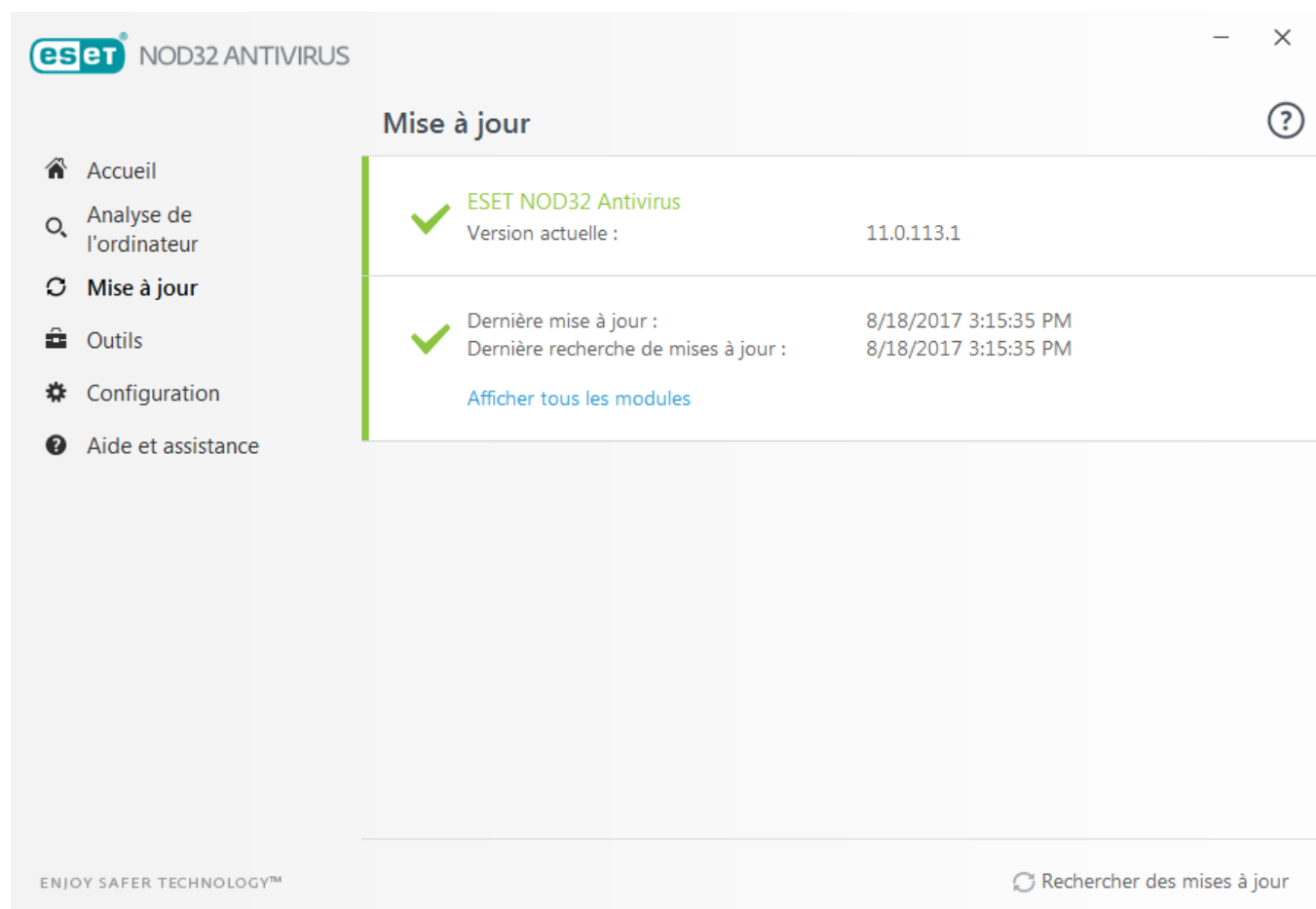
La mise à jour régulière d'ESET NOD32 Antivirus est la meilleure méthode pour assurer le niveau maximum de sécurité à votre ordinateur. Le module de mise à jour veille à ce que les modules du programme et les composants système soient toujours à jour.

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

En plus des 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 leur configuration 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 pouvez entrer votre clé de licence pour activer le produit lors de la mise à jour afin d'accéder aux serveurs de mise à jour ESET.

#### REMARQUE

la clé de licence est fournie dans un courrier électronique par ESET après l'achat d'ESET NOD32 Antivirus.




**eset** NOD32 ANTIVIRUS

**Mise à jour** ⓘ

✓	<b>ESET NOD32 Antivirus</b> Version actuelle :	11.0.113.1
✓	Dernière mise à jour : Dernière recherche de mises à jour :	8/18/2017 3:15:35 PM 8/18/2017 3:15:35 PM

[Afficher tous les modules](#)

ENJOY SAFER TECHNOLOGY™

 Rechercher des mises à jour

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

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

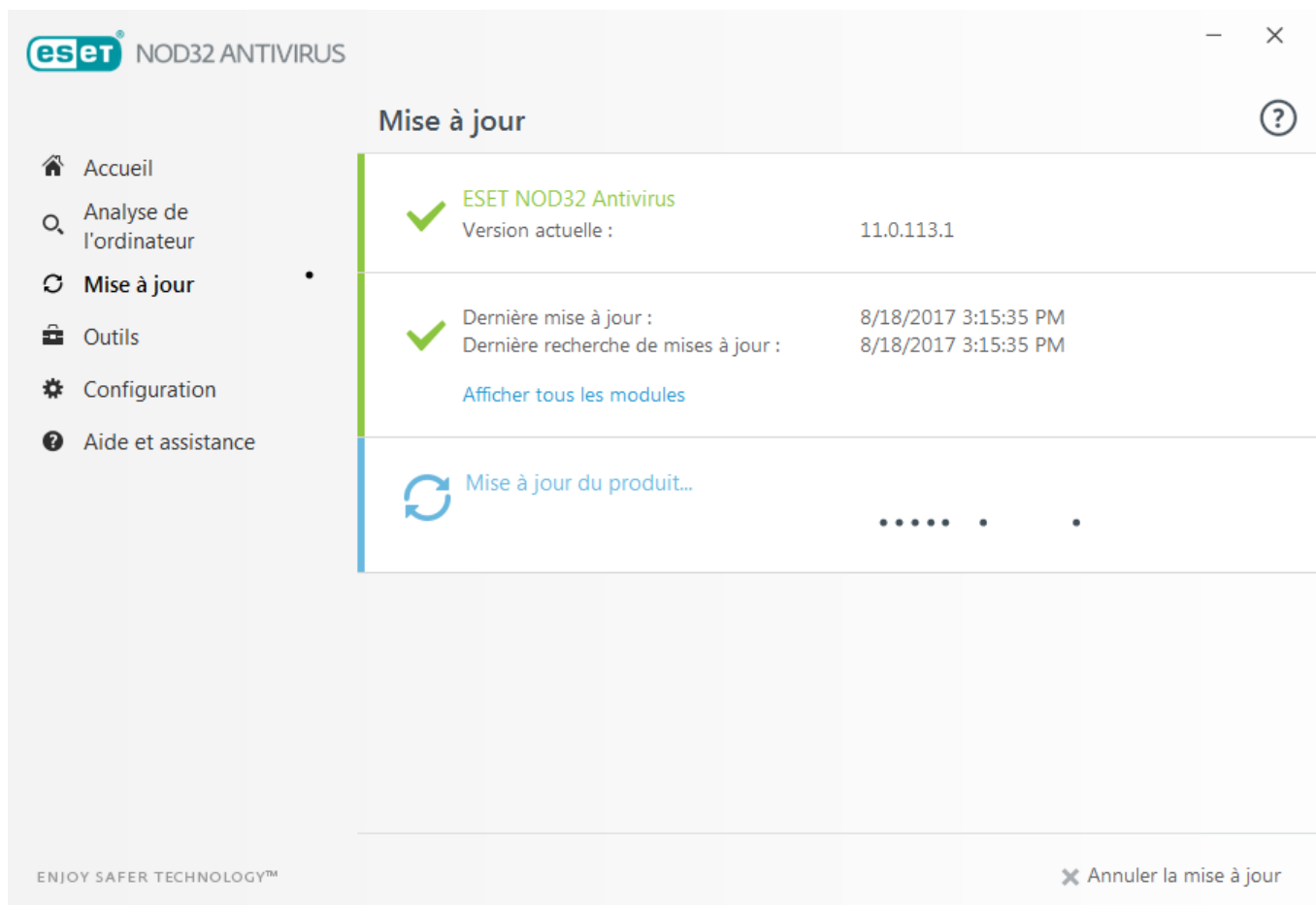
**Dernière recherche de mises à jour** – Indique la date de la dernière recherche de mises à jour.

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

Cliquez sur **Vérifier les mises à jour** pour détecter la plus récente version disponible d'ESET NOD32 Antivirus.

### Processus de mise à jour

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



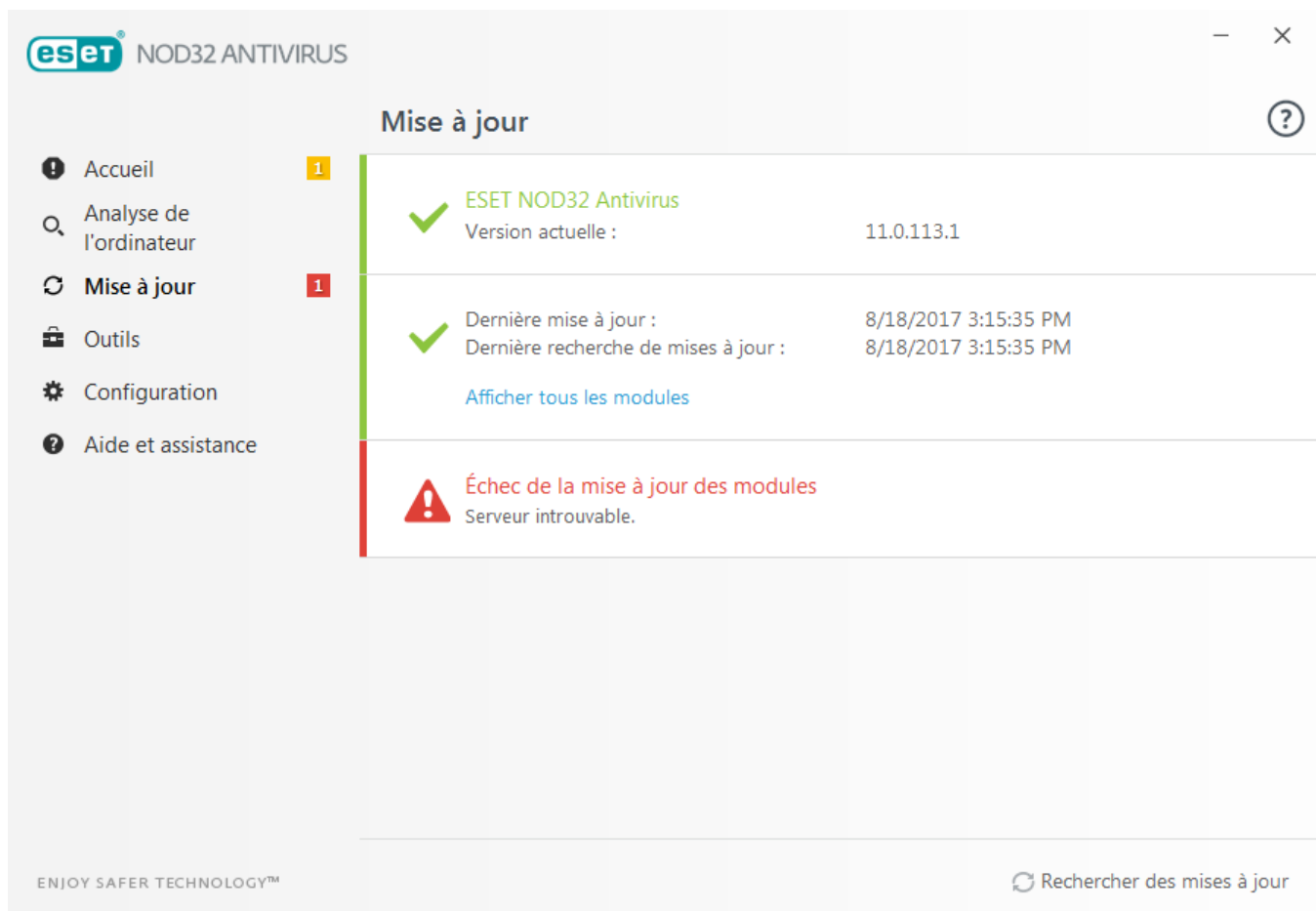
### ! IMPORTANT

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 dès que possible.

La notification précédente concerne les deux messages suivants sur les mises à jour infructueuses :

1. **Licence non valide** – La clé de licence n'a pas été correctement saisie lors de la configuration des mises à jour. Nous vous recommandons de vérifier vos données d'authentification. La fenêtre Configuration avancée (cliquez sur **Configuration** dans le menu principal et sur **Configuration avancée**, ou appuyez sur la touche **F5** de votre clavier) comporte d'autres options de mise à jour. Dans le menu principal, cliquez sur **Aide et assistance** > **Modifier la licence** pour saisir une nouvelle clé de licence.
2. **Une erreur s'est produite pendant le téléchargement des fichiers de mise à jour** – Cette erreur peut être due à des [paramètres de connexion Internet](#) incorrects. Nous vous recommandons de vérifier votre connectivité à Internet (en ouvrant un site Web dans votre navigateur). Si le site Web ne s'ouvre pas, cela est probablement dû

au fait qu'aucune connexion à Internet n'est établie ou que votre ordinateur a des problèmes de connectivité. Consultez votre fournisseur de services Internet si vous n'avez pas de connexion Internet active.



#### REMARQUE

Pour plus d'informations, consultez cet [article de la base de connaissances ESET](#).

### 4.3.1 Mise à jour les paramètres

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

#### — Général

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

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

#### Restaurer

Si vous pensez qu'une mise à jour de la base de virus ou des modules du programme est instable ou corrompue, vous pouvez restaurer la version précédente et désactiver les mises à jour pendant une période donnée. D'un autre côté, il est aussi possible d'activer les mises à jour précédemment désactivées si vous les avez reportées pour une durée indéterminée.

ESET NOD32 Antivirus enregistre des instantanés du moteur de détection et de modules du programme à utiliser avec la fonctionnalité de *restauration*. Pour permettre la création d'instantanés de la base de virus, conservez le bouton bascule **Créer des instantanés des fichiers de mise à jour** activé. Le champ **Nombre d'instantanés stockés localement** définit le nombre d'instantanés de la base de virus stockés.

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

**Configuration avancée**

ANTIVIRUS 2

MISE À JOUR 2

INTERNET ET MESSAGERIE 3

CONTRÔLE DE PÉRIPHÉRIQUE 1

OUTILS

INTERFACE UTILISATEUR

**+ GÉNÉRAL**

**- PROFILS**

Liste des profils [Modifier](#)

**MODIFIER LE PROFIL**

Sélectionner le profil à modifier Mon profil

**+ GÉNÉRAL**

Type de mise à jour Mise à jour régulière

Désactiver la notification de réussite de la mise à jour ☒

**+ MODE DE MISE À JOUR**

**+ PROXY HTTP**

Par défaut OK Annuler

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

#### **- General**

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.

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

#### **4.3.1.1 Profils de mise à jour**

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

Le menu déroulant **Profil de mise à jour** 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**.

### 4.3.1.2 Configuration avancée des mises à jour

Les options de configuration avancée de mise à jour englobent la configuration des options **Mode de mise à jour** et **Proxy HTTP**.

#### 4.3.1.2.1 Mode de mise à jour

L'onglet **Mode de mise à jour** contient les options concernant la mise à jour régulière du programme. Ces paramètres permettent de prédéfinir le comportement du programme lorsque de nouvelles mises à jour du moteur de détection ou des composants du programme sont disponibles.

Les mises à jour des composants du programme comprennent de nouvelles fonctionnalités ou apportent des modifications aux fonctionnalités des versions précédentes et font partie des mises à jour régulières (moteur de détection). Le redémarrage de l'ordinateur peut être nécessaire après la mise à jour des composants du programme.

Les paramètres suivants sont disponibles :

**Mise à jour de l'application** – Lorsque cette option est activée, la mise à niveau de chaque composant de programme est effectuée automatiquement et en silence, sans mise à niveau du produit complet.

**Activer la mise à jour manuelle du composant du programme** – Cette option est désactivée par défaut. Lorsqu'elle est activée et qu'une nouvelle version d'ESET NOD32 Antivirus est disponible, vous pouvez rechercher la présence de mises à jour dans le volet **Mise à jour et installer** la nouvelle version.

**Demander avant de télécharger une mise à jour** – Lorsque cette option est activée, une notification est affichée et vous devez confirmer l'installation de toute mise à jour disponible.

**Demander si un fichier de mise à jour a une taille supérieure à (Ko)** – Si la taille du fichier de mise à jour est supérieure à celle spécifiée, une notification s'affiche et vous devez confirmer l'installation de toute mise à jour disponible.

#### 4.3.1.2.2 Proxy HTTP

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

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

Sélectionnez l'option **Utiliser les paramètres globaux de serveur proxy** pour utiliser les options de configuration de serveur proxy déjà indiquées dans la branche **Outils > Serveur proxy** de la configuration avancée complète.

Sélectionnez **Ne pas utiliser de serveur proxy** pour indiquer qu'aucun serveur proxy ne sera utilisé pour la mise à jour d'ESET NOD32 Antivirus.

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

- Un autre serveur proxy que celui défini dans **Outils > Serveur proxy** est utilisé pour mettre à jour ESET NOD32 Antivirus. Dans cette configuration, les informations du nouveau proxy doivent être spécifiées adresse du **serveur proxy**, **port** de communication (3128 par défaut) et **nom d'utilisateur** et **mot de passe** du serveur proxy, si nécessaire).
- Les paramètres de serveur proxy ne sont pas définis globalement, mais ESET NOD32 Antivirus se connecte à un serveur proxy pour les mises à jour.
- Votre ordinateur est connecté à Internet par l'intermédiaire d'un serveur proxy. Les paramètres sont pris dans Internet Explorer pendant l'installation du programme, mais s'ils sont modifiés (par exemple en cas de changement de fournisseur de services Internet), vérifiez que les paramètres du proxy HTTP 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.

#### **i REMARQUE**

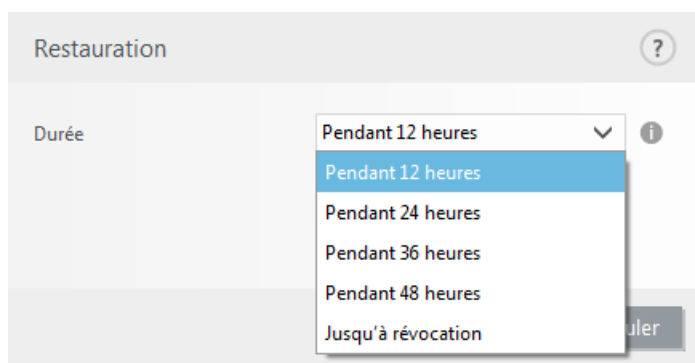
Les champs **Nom d'utilisateur** et **Mot de passe** de cette section sont propres au serveur proxy. Ne renseignez ces champs que si un nom d'utilisateur et un mot de passe sont nécessaires pour accéder au serveur proxy. Ces champs ne sont pas ceux du mot de passe et nom d'utilisateur d'ESET NOD32 Antivirus et ne doivent être renseignés que si vous savez que vous avez besoin d'un mot de passe pour accéder à Internet via un serveur proxy.

### **4.3.2 Annulation des mises à jour**

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

ESET NOD32 Antivirus enregistre des instantanés du moteur de détection et de modules du programme à utiliser avec la fonctionnalité de *restauration*. Pour permettre la création d'instantanés du moteur de détection, ne décochez pas la case **Créer des instantanés des fichiers de mise à jour**. Le champ **Nombre d'instantanés stockés localement** définit le nombre d'instantanés du moteur de détection stockés.

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



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

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 base 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.

# Configuration avancée

x
?

ANTIVIRUS 2

MISE À JOUR 2

INTERNET ET MESSAGERIE 3

CONTRÔLE DE PÉRIPHÉRIQUE 1

OUTILS

INTERFACE UTILISATEUR

GÉNÉRAL

Profil de mise à jour

Mon profil

▼

i

Effacer le cache de mise à jour

Effacer

i

RESTAURATION

Créer des instantanés des modules

✓

i

Nombre d'instantanés stockés localement

2

▲ ▼

i

Restaurer les modules précédents

Restaurer

PROFILS

Par défaut

OK

Annuler

## REMARQUE

Admettons que le numéro 6871 correspond au moteur de détection le plus récent. Les moteurs de détection 6870 et 6868 sont stockés sous forme d'instantanés. Notez que la base numéro 6869 n'est pas disponible parce que l'ordinateur était éteint et qu'une mise à jour plus récente a été mise à disposition avant que 6869 ait été téléchargée, par exemple. Si le champ **Nombre d'instantanés stockés localement** est défini sur 2 et que vous cliquez sur **Restaurer**, le moteur de détection (y compris les modules du programme) sera restauré à la version numéro 6868. Ce processus peut prendre un certain temps. Vérifiez si le moteur de détection est bien retourné à une version antérieure dans la fenêtre principale de ESET NOD32 Antivirus dans la section [Mise à jour](#).

### 4.3.3 Comment créer des tâches de mise à jour

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

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

- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion d'accès à distance**
- **Mise à jour automatique après connexion de l'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](#).

67

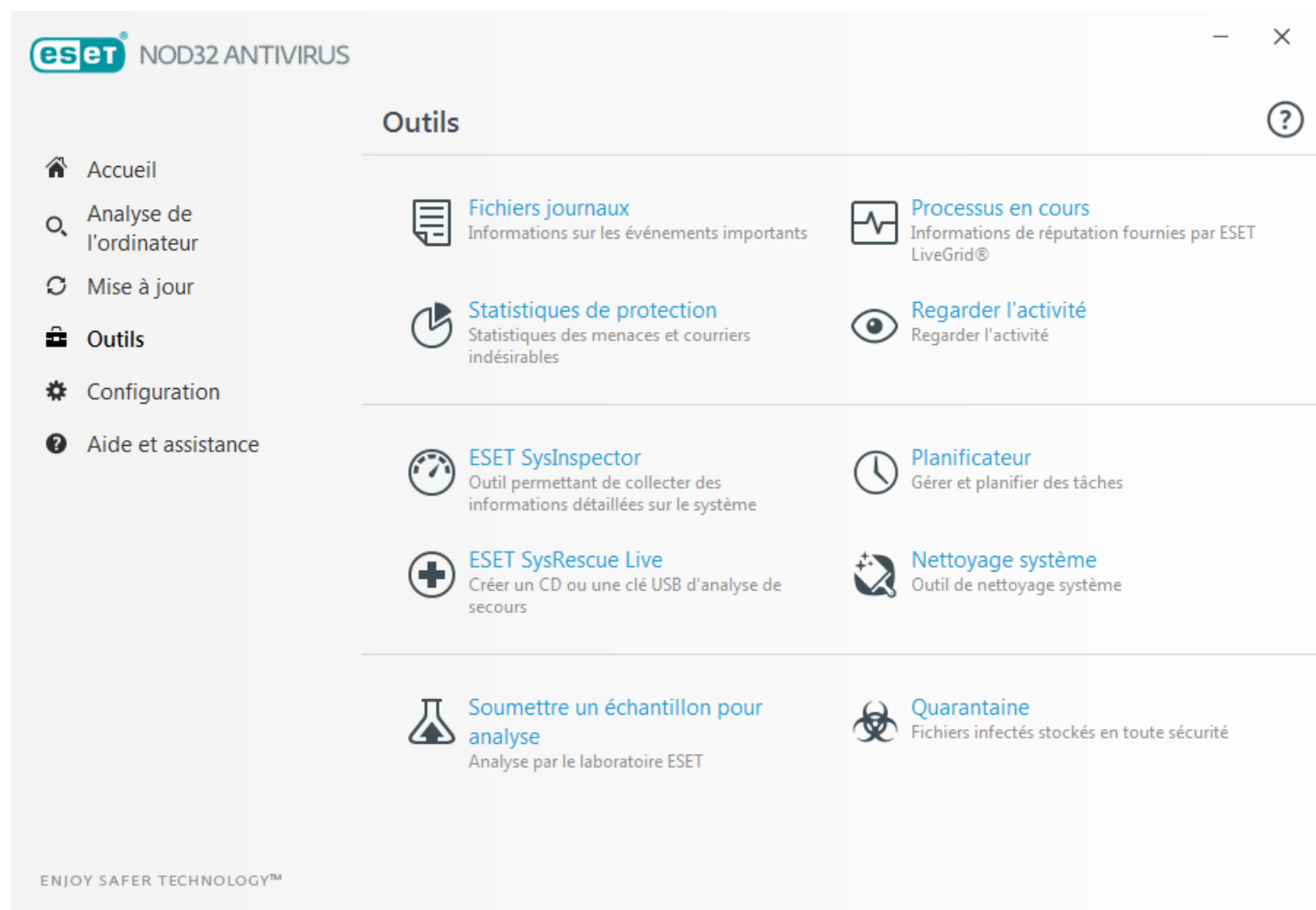
## 4.4 Outils

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

Cliquez sur [Autres outils](#) pour afficher d'autres outils afin de protéger votre ordinateur.

### 4.4.1 Outils dans ESET NOD32 Antivirus

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





Ce menu comprend les éléments suivants :



[Fichiers journaux](#)



[Statistiques de protection](#)



[Surveiller l'activité](#)



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



[ESET SysInspector](#)



[ESET SysRescue Live](#) – Vous redirige vers la page ESET SysRescue Live à partir de laquelle vous pouvez télécharger l'image d'ESET SysRescue Live ou Live CD/USB Creator pour les systèmes d'exploitation Microsoft Windows.



[Planificateur](#)



[Outils de nettoyage système](#) – Permet de restaurer un état utilisable de l'ordinateur après le nettoyage de la menace.



[Soumettre un échantillon pour analyse](#) – Permet de soumettre un fichier suspect pour analyse au laboratoire d'ESET. La boîte de dialogue qui s'affiche lorsque vous cliquez sur cette option est décrite dans la section.



[Quarantaine](#)

#### **i REMARQUE**

ESET SysRescue peut ne pas être disponible pour Windows 8 dans les versions antérieures des produits de sécurité d'ESET. Dans ce cas, nous vous recommandons de mettre à niveau votre produit ou de créer un disque ESET SysRescue en utilisant une autre version de Microsoft Windows.

#### **4.4.1.1 Fichiers journaux**

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

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

- **Menaces détectées** – le journal des menaces contient des informations sur les infiltrations détectées par ESET NOD32 Antivirus. Ces informations comprennent l'heure de détection, le nom de l'infiltration, l'emplacement, l'action exécutée et le nom de l'utilisateur connecté au moment où l'infiltration a été détectée. Double-cliquez sur une entrée du journal pour afficher son contenu dans une fenêtre distincte.
- **Événements** – Toutes les actions importantes exécutées par ESET NOD32 Antivirus sont enregistrées dans le journal des événements. Le journal des événements contient des informations sur les événements qui se sont produits dans le programme. Il permet aux administrateurs système et aux utilisateurs de résoudre des problèmes. Les informations qu'il contient peuvent aider à trouver une solution à un problème qui s'est produit dans le programme.
- **Analyse de l'ordinateur** – Cette fenêtre affiche toutes les analyses effectuées, qu'elles soient manuelles ou planifiées. Chaque ligne correspond à un seul contrôle d'ordinateur. Double-cliquez sur une entrée pour afficher les détails de l'analyse correspondante.

- **HIPS** – Contient des entrées de règles [HIPS](#) spécifiques qui ont été marquées pour enregistrement. Le protocole affiche l'application qui a déclenché l'opération, le résultat (si la règle a été autorisée ou bloquée), ainsi que le nom de la règle.
- **Sites Web filtrés** – Cette liste est utile pour afficher la liste des sites Web bloqués par la [Protection de l'accès Web](#). Chaque journal comprend l'heure, l'adresse URL, l'utilisateur et l'application ayant créé une connexion à un site Web en particulier.
- **Contrôle de périphérique** – Contient des enregistrements des supports amovibles ou périphériques qui ont été connectés à l'ordinateur. Seuls les périphériques auxquels correspond une règle de contrôle seront enregistrés dans le fichier journal. Si la règle ne correspond pas à un périphérique connecté, aucune entrée de journal ne sera créée pour un périphérique connecté. Des détails figurent également tels que le type de périphérique, le numéro de série, le nom du fournisseur et la taille du support (le cas échéant).

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

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

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

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

#### 4.4.1.1.1 Fichiers journaux

La configuration de la consignation d'ESET NOD32 Antivirus est accessible à partir de la fenêtre principale du programme. Cliquez sur **Configuration > Accéder à la configuration avancée... > Outils > Fichiers journaux**. La section des fichiers journaux permet de définir la manière dont les journaux sont gérés. Le programme supprime automatiquement les anciens fichiers journaux pour gagner de l'espace disque. Les options suivantes peuvent être spécifiées pour les fichiers journaux :

**Verbosité minimale des journaux** – Spécifie le niveau minimum de verbosité des événements à consigner.

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

Les entrées des journaux plus anciennes que le nombre de jours spécifiés dans le champ **Supprimer automatiquement les entrées plus anciennes que (jours)** seront automatiquement supprimées.

**Optimiser automatiquement les fichiers journaux** – Si cette option est activée, les fichiers journaux sont automatiquement défragmentés si le pourcentage est supérieur à la valeur spécifiée dans le champ **Si le nombre d'entrées inutilisées dépasse (%)**.

Cliquez sur **Optimiser** pour démarrer la défragmentation des fichiers journaux. Au cours de ce processus, toutes les entrées vides du journal sont supprimées, ce qui améliore les performances et accélère le traitement des journaux. Cette amélioration se constate notamment si les journaux comportent un grand nombre d'entrées.

L'option **Activer le protocole texte** permet d'activer le stockage des journaux dans un autre format de fichier séparé des [fichiers journaux](#) :

- **Répertoire cible** – Répertoire dans lequel les fichiers journaux sont stockés (s'applique uniquement aux formats texte/CSV). Chaque section de journal dispose de son propre fichier avec un nom de fichier prédéfini (par exemple *virlog.txt* pour la section **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.

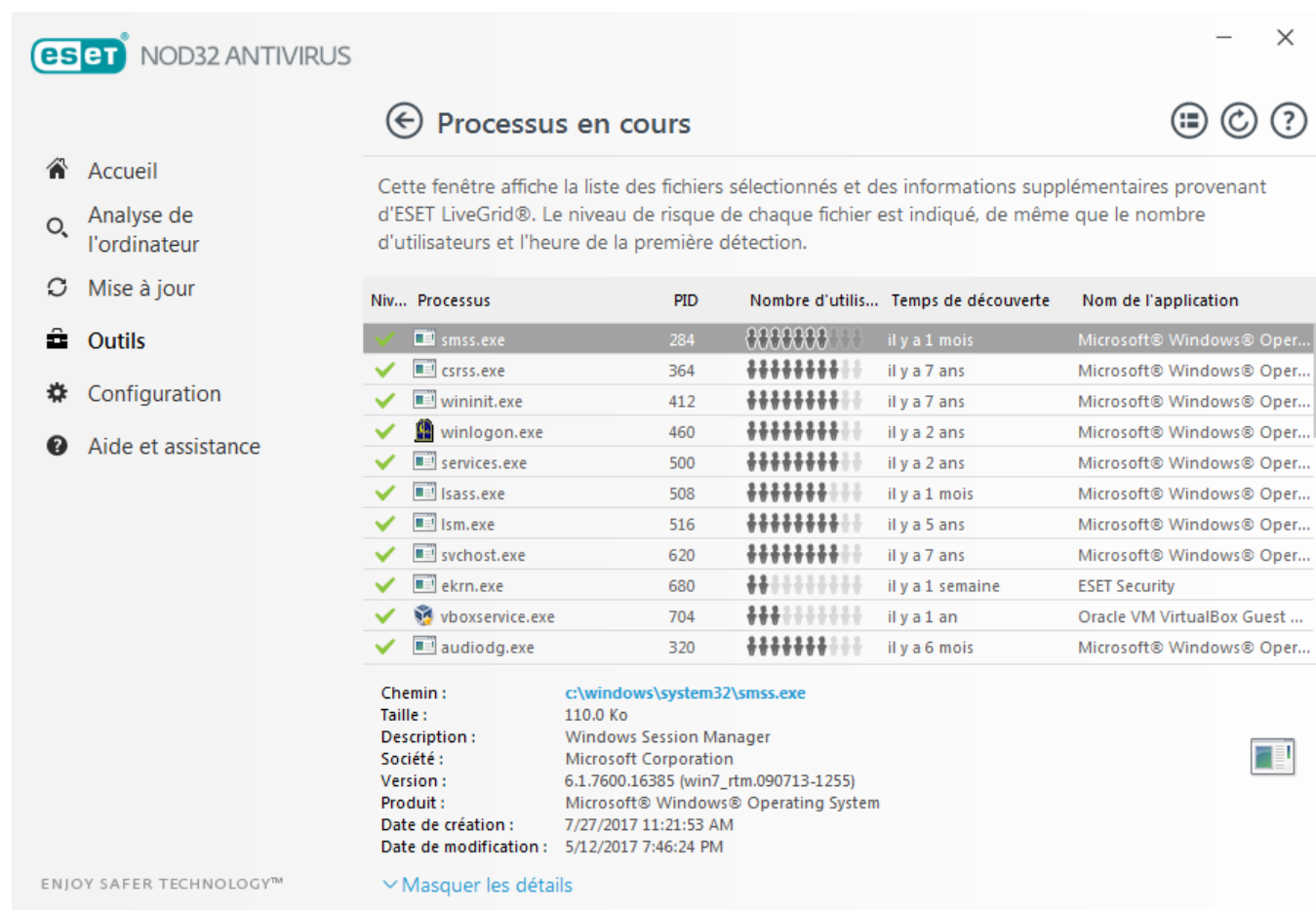
**Supprimer tous les fichiers journaux** – Efface tous les fichiers journaux sélectionnés dans le menu déroulant **Type**. Une notification indiquant la suppression des journaux s'affiche.

#### **i REMARQUE**

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 l'article de la [base de connaissances ESET](#).

#### 4.4.1.2 Processus en cours

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



**Processus en cours**

Cette fenêtre affiche la liste des fichiers sélectionnés et des informations supplémentaires provenant d'ESET LiveGrid®. Le niveau de risque de chaque fichier est indiqué, de même que le nombre d'utilisateurs et l'heure de la première détection.

Niv...	Processus	PID	Nombre d'utilis...	Temps de découverte	Nom de l'application
✓	smss.exe	284	00000000	il y a 1 mois	Microsoft® Windows® Oper...
✓	csrss.exe	364	00000000	il y a 7 ans	Microsoft® Windows® Oper...
✓	wininit.exe	412	00000000	il y a 7 ans	Microsoft® Windows® Oper...
✓	winlogon.exe	460	00000000	il y a 2 ans	Microsoft® Windows® Oper...
✓	services.exe	500	00000000	il y a 2 ans	Microsoft® Windows® Oper...
✓	lsass.exe	508	00000000	il y a 1 mois	Microsoft® Windows® Oper...
✓	lsmd.exe	516	00000000	il y a 5 ans	Microsoft® Windows® Oper...
✓	svchost.exe	620	00000000	il y a 7 ans	Microsoft® Windows® Oper...
✓	ekrn.exe	680	00000000	il y a 1 semaine	ESET Security
✓	vboxservice.exe	704	00000000	il y a 1 an	Oracle VM VirtualBox Guest ...
✓	audiodg.exe	320	00000000	il y a 6 mois	Microsoft® Windows® Oper...

**Détails de smss.exe :**

- Chemin : c:\windows\system32\smss.exe
- Taille : 110,0 Ko
- Description : Windows Session Manager
- Société : Microsoft Corporation
- Version : 6.1.7600.16385 (win7\_rtm.090713-1255)
- Produit : Microsoft® Windows® Operating System
- Date de création : 7/27/2017 11:21:53 AM
- Date de modification : 5/12/2017 7:46:24 PM

[Masquer les détails](#)

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

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

#### REMARQUE

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

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

**Nombre d'utilisateurs** – Nombre d'utilisateurs utilisant une application donnée. Ces informations sont collectées par la technologie ThreatSense.

**Temps de découverte** – Durée écoulée depuis la détection de l'application par la technologie ThreatSense.

#### REMARQUE

Une application marquée **Inconnu (orange)** n'est pas nécessairement un logiciel malveillant. Il s'agit généralement d'une nouvelle application. Si ce fichier vous semble toutefois suspect, vous pouvez [le soumettre](#)

[pour analyse](#) au laboratoire de recherche ESET. S'il s'avère être une application malveillante, sa détection sera intégrée à une prochaine mise à jour.

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

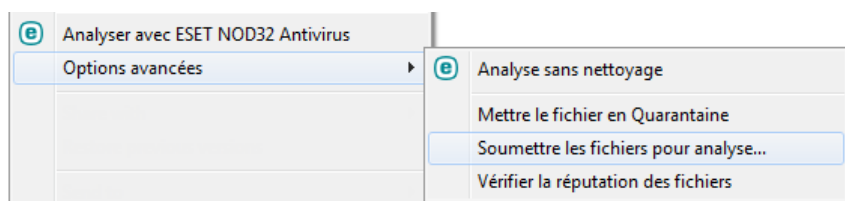
**Ouvrir dans une nouvelle fenêtre** – Les informations concernant les processus en cours d'exécution s'affichent dans une nouvelle fenêtre.

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

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

#### REMARQUE

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



#### 4.4.1.3 Statistiques de protection

Pour afficher un graphique des données statistiques relatives aux modules de protection d'ESET NOD32 Antivirus, cliquez sur **Outils > Statistiques**. Dans le menu déroulant **Statistiques**, sélectionnez le module de protection souhaité pour afficher le graphique et la légende correspondants. Si vous faites glisser le pointeur de la souris sur un élément de la légende, seules les données correspondant à cet élément sont représentées dans le graphique.

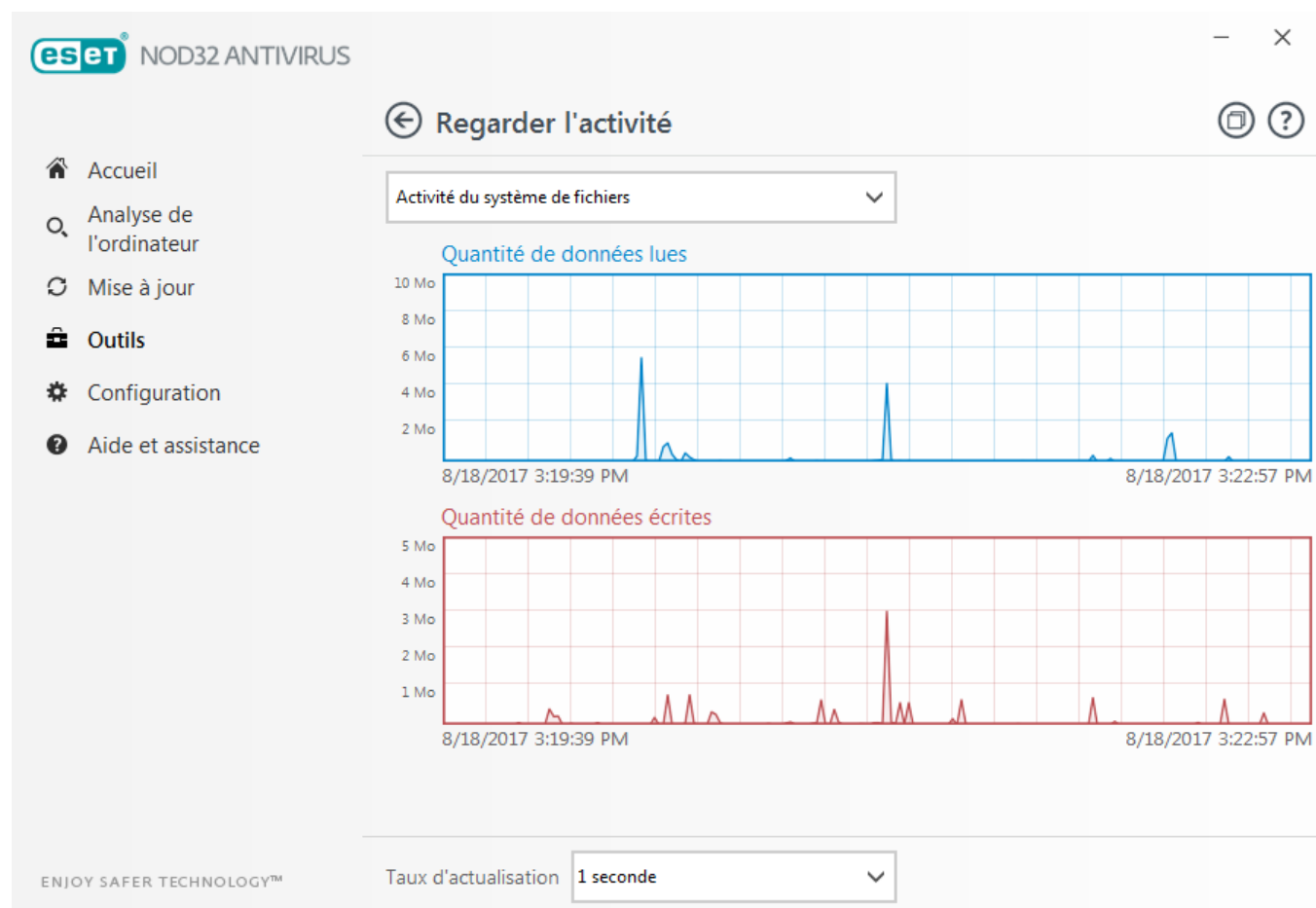
Les graphiques statistiques suivants sont disponibles :

- **Protection antivirus et antispyware** – Affiche le nombre d'objets infectés et nettoyés.
- **Protection du système de fichiers** – Affiche uniquement les objets lus ou écrits dans le système de fichiers.
- **Protection du client de messagerie** – Affiche uniquement les objets envoyés ou reçus par les clients de messagerie.
- **Protection de l'accès Web et antihameçonnage** – Affiche uniquement les objets téléchargés par des navigateurs Web.

Sous les graphiques statistiques, vous pouvez voir le nombre total d'objets analysés, le dernier objet analysé et l'horodatage des statistiques. Cliquez sur **Réinitialiser** pour supprimer toutes les informations statistiques.

#### 4.4.1.4 Surveiller l'activité

Pour voir l'**activité actuelle du système de fichiers** sous forme graphique, cliquez sur **Outils > Regarder l'activité**. Au bas du graphique figure une chronologie qui enregistre en temps réel l'activité du système de fichiers sur la base de l'intervalle sélectionné. Pour modifier l'intervalle, effectuez une sélection dans le menu déroulant **Taux d'actualisation**.



Les options disponibles sont les suivantes :

- **Étape : 1 seconde** – Le graphique est actualisé toutes les secondes et la chronologie couvre les 10 dernières minutes.
- **Étape : 1 minute (24 dernières heures)** – Le graphique est actualisé toutes les minutes et la chronologie couvre les 24 dernières heures.
- **Pas : 1 heure (dernier mois)** – Le graphique est actualisé toutes les heures et la chronologie couvre le dernier mois.
- **Étape : 1 heure (mois sélectionné)** – Le graphique est actualisé toutes les heures et la chronologie couvre les X mois sélectionnés.

L'axe vertical **Graphique d'activité du système de fichiers** représente les données lues (en bleu) et les données écrites (en rouge). Les deux valeurs sont exprimées en Ko (kilo-octets)/Mo/Go. Si vous faites glisser le curseur de la souris sur les données lues ou écrites dans la légende sous le graphique, celui-ci n'affiche que les données relatives à ce type d'activité.

#### 4.4.1.5 ESET SysInspector

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

La fenêtre SysInspector affiche les informations suivantes relatives aux journaux créés :

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

Les actions disponibles sont les suivantes :

- **Afficher** – Ouvre le journal créé. Vous pouvez également cliquer avec le bouton droit sur un fichier journal, puis sélectionner **Afficher** dans le menu contextuel.
- **Comparer** – Compare deux journaux existants.
- **Créer...** – Crée un journal. Patientez jusqu'à ce qu'ESET SysInspector ait terminé (l'état du journal s'affiche en tant que créé) avant d'accéder au journal.
- **Supprimer** – Supprime les journaux sélectionnés de la liste.

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

- **Afficher** – Ouvre le journal sélectionné dans ESET SysInspector (équivalent à double-cliquer sur un journal).
- **Comparer** – Compare deux journaux existants.
- **Créer...** – Crée un journal. Patientez jusqu'à ce qu'ESET SysInspector ait terminé (l'état du journal s'affiche en tant que créé) avant d'accéder au journal.
- **Supprimer** – Supprime 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.

#### 4.4.1.6 Planificateur

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

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

Il sert à planifier les tâches suivantes : la mise à jour des modules, l'analyse, le contrôle des fichiers de démarrage du système et la maintenance des journaux. Vous pouvez ajouter ou supprimer des tâches dans la fenêtre principale du planificateur (cliquez sur **Ajouter...** 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 d'accès à distance**
- **Mise à jour automatique après connexion de l'utilisateur**
- **Recherche régulière de la dernière version du produit** (voir [Mode de mise à jour](#))
- **Vérification automatique des fichiers de démarrage** (après l'ouverture de session de l'utilisateur)
- **Vérification des fichiers de démarrage** (après la mise à jour réussie du moteur de détection)

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

### Ajout d'une nouvelle tâche

1. Cliquez sur **Ajouter une tâche** dans la partie inférieure de la fenêtre.
2. Entrez le nom de la tâche.
3. Sélectionnez la tâche souhaitée dans le menu déroulant :
  - **Exécuter une application externe** – Permet de programmer l'exécution d'une application externe.
  - **Maintenance des journaux** – Les fichiers journaux contiennent également des éléments provenant d'enregistrements supprimés. Cette tâche optimise régulièrement les entrées des fichiers journaux pour garantir leur efficacité.
  - **Contrôle des fichiers de démarrage du système** – Vérifie les fichiers autorisés à s'exécuter au démarrage du système ou lors de l'ouverture de session de l'utilisateur.
  - **Analyse de l'ordinateur** – Crée un instantané [ESET SysInspector](#) de l'ordinateur et collecte des informations détaillées sur les composants système (pilotes, applications) et évalue le niveau de risque de chacun de ces composants.
  - **Analyse de l'ordinateur à la demande** – Effectue une analyse des fichiers et des dossiers de votre ordinateur.
  - **Mise à jour** – Planifie une tâche de mise à jour en mettant à jour les modules.
4. Activez le bouton bascule **Activé** si vous souhaitez activer la tâche (vous pouvez le faire ultérieurement en activant/désactivant la case à cocher correspondante dans la liste des tâches planifiées). Cliquez ensuite sur **Suivant** et sélectionnez une des options de planification :
  - **Une fois** – La tâche est exécutée à la date et à l'heure prédéfinies.
  - **Plusieurs fois** – La tâche est exécutée aux intervalles indiqués.
  - **Quotidiennement** – La tâche est exécutée tous les jours à l'heure définie.
  - **Chaque semaine** – La tâche est exécutée à l'heure et au jour prédéfinis.
  - **Déclenchée par un événement** – La tâche est exécutée après un événement particulier.
5. Sélectionnez **Ignorer la tâche en cas d'alimentation par batterie** pour diminuer les ressources système lorsque l'ordinateur portable fonctionne sur batterie. Cette tâche est exécutée à l'heure et au jour spécifiées dans les champs **Exécution de tâche**. Si la tâche n'a pas pu être exécutée au moment défini, vous pouvez désigner le moment auquel elle doit être réexécutée :
  - **À la prochaine heure planifiée**
  - **Dès que possible**
  - **Immédiatement, si la durée écoulée depuis la dernière exécution dépasse la valeur spécifiée** (l'intervalle peut être spécifié dans la zone de liste déroulante **Durée écoulée depuis la dernière exécution**.)

Pour examiner une tâche planifiée, cliquez sur **Afficher les détails des tâches**.



Aperçu des tâches planifiées?

Nom de la tâche

Maintenance des journaux

Type de tâche

Maintenance des journaux

Exécuter la tâche

La tâche sera exécutée chaque jour à 3:00:00 AM.

Action à entreprendre si la tâche n'a pas été exécutée à l'heure spécifiée

Dès que possible

OK

#### 4.4.1.7 Outil de nettoyage système

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

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

- lorsqu'une menace est détectée ;
- lorsqu'un utilisateur clique sur **Réinitialiser**.

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

##### **i** REMARQUE

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

#### 4.4.1.8 ESET SysRescue

ESET SysRescue est un utilitaire qui permet de créer un disque amorçable contenant une des solutions ESET Security : ESET NOD32 Antivirus, <%ESET\_INTERNET\_SECURITY%>, ESET Smart Security, <%ESET\_SMART\_SECURITY\_PREMIUM%> ou l'un des produits orientés serveur. Le principal avantage d'ESET SysRescue réside dans le fait que la solution ESET Security est exécutée indépendamment du système d'exploitation hôte, tout en ayant un accès direct au disque et au système de fichiers. Il est par conséquent possible de supprimer les infiltrations qui ne pourraient normalement pas être supprimées, par exemple lorsque le système d'exploitation est en cours d'exécution.

#### 4.4.1.9 ESET LiveGrid®

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® vous permet de réagir immédiatement aux besoins de nos clients et à ESET de répondre aux dernières menaces. Pour en savoir plus sur ESET LiveGrid®, consultez le [glossaire](#).

Un utilisateur peut s'informer 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®. Deux options sont possibles :

1. Vous pouvez choisir de ne pas activer ESET LiveGrid®. Vous ne perdez rien de la fonctionnalité du logiciel, mais ESET NOD32 Antivirus peut répondre dans certains cas plus rapidement aux nouvelles menaces que la mise à jour du moteur de détection lorsque l'option ESET Live Grid est activée.
2. Vous pouvez configurer ESET LiveGrid® afin d'envoyer des informations anonymes qui concernent les nouvelles menaces et indiquent l'endroit où se trouve le code dangereux. Ce fichier peut être envoyé à ESET pour une analyse détaillée. En étudiant ces menaces, ESET améliore ses capacités à détecter les menaces.

Le système ESET 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 NOD32 Antivirus est configuré pour demander une confirmation avant de soumettre les fichiers suspects au laboratoire d'ESET pour une analyse détaillée. Les fichiers ayant une extension définie (.doc ou .xls par exemple) sont toujours exclus. Vous pouvez également ajouter d'autres extensions si vous ou votre entreprise souhaitez éviter d'envoyer certains fichiers.

Le menu de configuration ESET LiveGrid® propose différentes options permettant d'activer et de désactiver ESET LiveGrid®. Ce système sert à soumettre les fichiers suspects aux laboratoires d'ESET et à fournir des informations statistiques anonymes. Cette option est accessible depuis la fenêtre Configuration avancée en cliquant sur **Outils > ESET LiveGrid®**.

**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.

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

**Soumettre les fichiers** – Les fichiers suspects ressemblant à des menaces et/ou des fichiers aux caractéristiques ou au comportement inhabituels peuvent être envoyés pour analyse à ESET.

Sélectionnez **Activer la journalisation** pour créer un journal d'événements permettant d'enregistrer les soumissions des fichiers et des informations statistiques. Il permettra de consigner les fichiers ou statistiques envoyés dans le [Journal des événements](#).

**Adresse de contact (facultative)** – Votre adresse électronique peut être incluse avec les fichiers suspects. Nous pourrions 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.

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

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.

#### 4.4.1.9.1 Fichiers suspects

Si vous trouvez un fichier suspect, vous pouvez le soumettre au laboratoire de recherche ESET pour analyse. S'il s'agit d'une application malveillante, sa détection est ajoutée à la prochaine mise à jour de la base des signatures de virus.

**Filtre d'exclusion** – Cette option permet d'exclure certains fichiers/dossiers de la soumission. Les fichiers de la liste ne seront jamais envoyés aux laboratoires de recherche ESET pour analyse, même s'ils contiennent un code suspect. 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 les plus ordinaires sont exclus par défaut (.doc, etc.). Vous pouvez ajouter des fichiers à la liste des fichiers exclus si vous le souhaitez.

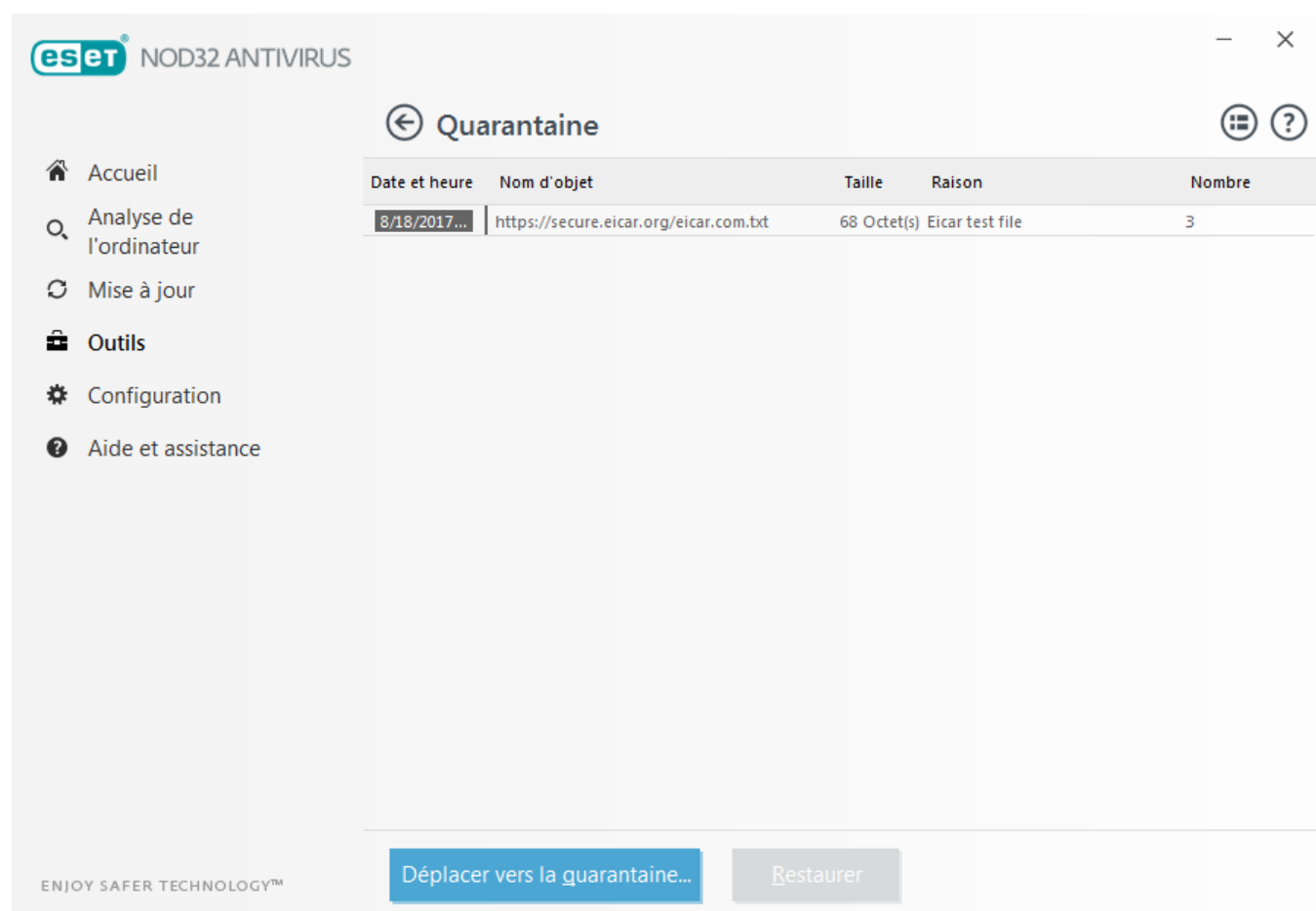
**Adresse de contact (facultative)** – Votre adresse électronique peut être incluse avec les fichiers suspects. Nous pourrions l'utiliser pour vous contacter si des informations complémentaires sont nécessaires pour l'analyse. Notez que vous ne recevrez pas de réponse d'ESET, sauf si des informations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

Sélectionnez **Activer la journalisation** pour créer un journal d'événements permettant d'enregistrer les soumissions des fichiers et des informations statistiques. Il permettra de consigner les fichiers ou statistiques envoyés dans le [Journal des événements](#).

#### 4.4.1.10 Quarantaine

La principale fonction de la quarantaine est de stocker les fichiers infectés en toute sécurité. Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer ou s'ils sont détectés erronément par ESET NOD32 Antivirus.

Vous pouvez choisir de mettre n'importe quel fichier en quarantaine. Cette action est conseillée si un fichier se comporte de façon suspecte, mais n'a pas été détecté par l'analyseur antivirus. Les fichiers en quarantaine peuvent être soumis pour analyse au laboratoire de recherche d'ESET.



The screenshot shows the ESET NOD32 Antivirus Quarantine window. The window has a sidebar on the left with navigation options: Accueil, Analyse de l'ordinateur, Mise à jour, Outils, Configuration, and Aide et assistance. The main area is titled 'Quarantaine' and contains a table with the following data:

Date et heure	Nom d'objet	Taille	Raison	Nombre
8/18/2017...	https://secure.eicar.org/eicar.com.txt	68 Octet(s)	Eicar test file	3

At the bottom of the window, there are two buttons: 'Déplacer vers la quarantaine...' and 'Restaurer'.

Les fichiers du dossier de quarantaine peuvent être visualisés dans un tableau qui affiche la date et l'heure de mise en quarantaine, le chemin d'accès à l'emplacement d'origine du fichier infecté, sa taille en octets, la raison (par

exemple, objet ajouté par l'utilisateur) et le nombre de menaces (s'il s'agit d'une archive contenant plusieurs infiltrations par exemple).

### Mise en quarantaine de fichiers

ESET NOD32 Antivirus met automatiquement en quarantaine les fichiers supprimés (si vous n'avez pas annulé cette option dans la fenêtre d'alerte). Au besoin, vous pouvez mettre manuellement en quarantaine tout fichier suspect en cliquant sur le bouton **Quarantaine....** Dans ce cas, le fichier d'origine n'est pas supprimé de son emplacement initial. Il est également possible d'utiliser le menu contextuel à cette fin : cliquez avec le bouton droit dans la fenêtre **Quarantaine** et sélectionnez l'option **Quarantaine...**

### Restauration depuis la quarantaine

Les fichiers mis en quarantaine peuvent aussi être restaurés à leur emplacement d'origine. Pour ce faire, utilisez la fonctionnalité **Restaurer** du menu contextuel après avoir cliqué avec le bouton droit sur un fichier dans la fenêtre de quarantaine. Si un fichier est marqué comme application potentiellement indésirable, l'option **Restaurer et exclure de l'analyse** est activée. Pour en savoir plus sur ce type d'application, consultez le [glossaire](#). 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.

**Suppression d'un élément en quarantaine** – Cliquez avec le bouton droit sur un élément donné, puis sélectionnez **Supprimer l'élément en quarantaine**. Vous pouvez également sélectionner l'élément à supprimer, puis appuyer sur **Suppr** sur votre clavier. Vous pouvez aussi sélectionner plusieurs éléments et les supprimer simultanément.

#### REMARQUE

si le programme place en quarantaine, par erreur, un fichier inoffensif, il convient de le restaurer, de l'[exclure de l'analyse](#) et de l'envoyer au service d'assistance d'ESET.

### 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, envoyez ce fichier au laboratoire d'ESET. Pour soumettre un fichier mis en quarantaine, cliquez avec le bouton droit sur le fichier et sélectionnez l'option **Soumettre un échantillon pour analyse** dans le menu contextuel.

#### 4.4.1.11 Serveur proxy

Dans les grands réseaux locaux, les communications entre votre ordinateur et Internet peuvent s'effectuer par l'intermédiaire d'un serveur proxy. Lorsque cette configuration est utilisée, les paramètres suivants doivent être définis. Dans le cas contraire, le programme ne pourra pas se mettre à jour automatiquement. Dans ESET NOD32 Antivirus, il est possible de configurer le serveur proxy à partir de deux sections différentes de la configuration avancée complète.

Tout d'abord, les paramètres de serveur proxy peuvent être configurés dans **Configuration avancée**, depuis **Outils > Serveur proxy**. La spécification du serveur proxy à ce niveau définit les paramètres de serveur proxy globaux pour l'intégralité d'ESET NOD32 Antivirus. Les paramètres définis ici seront utilisés par tous les modules qui requièrent une connexion à Internet.

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

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

#### REMARQUE

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

**Utiliser une connexion directe si le proxy HTTP n'est pas disponible** – Si un produit est configuré pour utiliser le proxy HTTP et que ce dernier est injoignable, le produit ignore le proxy et communique directement avec les serveurs ESET.

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

#### 4.4.1.12 Notifications par e-mail

ESET NOD32 Antivirus peut automatiquement envoyer des courriers électroniques de notification si un événement avec le niveau de verbosité sélectionné se produit. Activez l'option **Envoyer des notifications d'événement par e-mail** pour activer les notifications par e-mail.

#### Serveur SMTP

**Serveur SMTP** – Serveur SMTP utilisé pour envoyer des notifications (*smtp.fournisseur.com:587*, le port prédéfini est le port 25).

##### REMARQUE

les serveurs SMTP avec chiffrement TLS sont pris en charge par ESET NOD32 Antivirus.

**Nom d'utilisateur et mot de passe** – Si le serveur SMTP exige une authentification, ces champs doivent être remplis avec un nom d'utilisateur et un mot de passe valides donnant accès au serveur SMTP.

**Adresse de l'expéditeur** – Ce champ spécifie l'adresse de l'expéditeur qui apparaît dans l'en-tête des notifications.

**Adresse du destinataire** – Ce champ spécifie l'adresse du destinataire qui apparaît dans l'en-tête des notifications.

Dans le menu déroulant **Verbosité minimale des notifications**, vous pouvez sélectionner le niveau de gravité de départ des notifications à envoyer.

- **Diagnostic** – Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** – Enregistre tous les messages d'information (les événements réseau non standard, par exemple), y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Avertissements** – Enregistre les erreurs critiques et les messages d'avertissement (Anti-Stealth ne s'exécute pas correctement ou une mise à jour a échoué).
- **Erreurs** – Enregistre les erreurs (la protection des documents n'a pas démarré) et les erreurs critiques.
- **Critique** – Consigne uniquement les erreurs critiques (erreur de démarrage de la protection antivirus ou système infecté.).

**Activer TLS** – Permet d'activer l'envoi de messages d'alerte et de notification pris en charge par le chiffrement TLS.

**Intervalle après lequel les nouveaux e-mails de notification seront envoyés (min)** – Intervalle en minutes après lequel de nouvelles notifications seront envoyées par e-mail. Si vous définissez cette valeur sur 0, les notifications sont envoyées immédiatement.

**Envoyer chaque notification dans un e-mail séparé** – Lorsque cette option est activée, le destinataire recevra un nouvel e-mail pour chaque notification spécifique. Cela peut se traduire par la réception d'un nombre important d'e-mails dans une courte période de temps.

## Format des messages

**Format des messages d'événement** – Format des messages d'événement qui s'affichent sur les ordinateurs distants.

**Format des messages d'avertissement de menace** – Messages d'alerte et de notification de menace dont le format par défaut est prédéfini. Il est déconseillé de modifier ce format. Toutefois, dans certaines circonstances (par exemple, si vous avez un système automatisé de traitement des messages), vous serez peut-être amené à modifier le format des messages.

**Jeu de caractères** – Convertit un courrier électronique en codage ANSI sur la base des paramètres régionaux de Windows (windows-1250, par exemple), Unicode (UTF-8), ACSII 7 bits ("à" sera remplacé par "a" et un symbole inconnu par "?", par exemple) ou japonais (ISO-2022-JP).

**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).

### 4.4.1.12.1 Format des messages

Vous pouvez ici définir le format des messages d'événement qui s'affichent sur les ordinateurs distants.

Les messages d'alerte et de notification de menace utilisent un format par défaut 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.

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
- **%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.

**Utiliser les caractères alphabétiques locaux** – Convertit le message électronique au codage ANSI sur la base des paramètres régionaux de Windows (par ex. windows-1250). Si vous ne sélectionnez pas cette option, le message est converti et codé au format ACSII 7 bits (ainsi, « á » est remplacé par « a » et un symbole inconnu par un « ? »).

**Utiliser l'encodage des caractères locaux** – Le message électronique source est codé au format Quoted-printable (QP) qui utilise les caractères ASCII et peut correctement transmettre les caractères spéciaux par e-mail au format 8 bits (áéíóú).

#### 4.4.1.13 Sélectionner un échantillon pour analyse

La boîte de dialogue de soumission de fichiers permet d'envoyer un fichier ou un site à ESET pour analyse ; elle est accessible depuis **Outils > Soumettre un échantillon pour analyse**. Si vous trouvez sur votre ordinateur un fichier dont le comportement est suspect, vous pouvez le soumettre au laboratoire de recherche d'ESET pour analyse. Si le fichier s'avère être une application malveillante, sa détection sera intégrée à une prochaine mise à jour.

Vous pouvez également soumettre le fichier par e-mail. Si vous préférez, compressez le ou les fichiers à l'aide de WinRAR/ZIP, protégez l'archive à l'aide du mot de passe « infected » et envoyez-la à [samples@eset.com](mailto:samples@eset.com). Veillez à utiliser un objet descriptif et indiquez le plus d'informations possible sur le fichier (notez par exemple le site Internet à partir duquel vous l'avez téléchargé).

##### REMARQUE

avant de soumettre un fichier à ESET, assurez-vous qu'il répond à au moins l'un des critères suivants :

- le fichier n'est pas du tout détecté
- le fichier est détecté à tort comme une menace

Vous ne recevrez pas de réponse, excepté si des informations complémentaires sont nécessaires à l'analyse.

Sélectionnez dans le menu déroulant **Motif de soumission du fichier** 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. L'échantillon peut être **envoyé de façon anonyme**. 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.

#### 4.4.1.14 Microsoft Windows® update

La fonctionnalité Windows Update est un élément important de la protection des utilisateurs contre les logiciels malveillants. C'est pourquoi il est essentiel d'installer les mises à jour de Microsoft Windows dès qu'elles sont disponibles. ESET NOD32 Antivirus vous informe des mises à jour manquantes en fonction du niveau que vous spécifiez. 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.

#### 4.4.1.15 ESET CMD

Il s'agit d'une fonctionnalité qui permet d'utiliser des commandes `ecmd` avancées. Elle vous offre la possibilité d'exporter et d'importer des paramètres à l'aide d'une ligne de commande (`ecmd.exe`). Auparavant, Il n'était possible d'exporter et d'importer des paramètres que dans l'[interface utilisateur graphique](#). La configuration de <%PN%> 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** : utilise la protection par mot de passe. Lorsque vous importez une configuration depuis un fichier `.xml`, ce dernier doit être signé (reportez-vous à la section relative à la signature d'un fichier de configuration `.xml` plus bas). Cette méthode d'autorisation vérifie le mot de passe pendant l'importation de la configuration pour vérifier qu'il correspond à celui spécifié dans la [configuration de l'accès](#). Si la configuration de l'accès n'est pas activée, que le mot de passe ne correspond pas ou que le fichier `.xml` n'est pas signé, la configuration n'est pas importée.

Une fois qu'ESET CMD est activé, vous pouvez commencer à utiliser la ligne de commande pour exporter/importer la configuration de <%PN%>. Vous pouvez le faire manuellement ou créer un script pour l'automatisation.

#### ! IMPORTANT

Pour utiliser les commandes `ecmd` avancées, vous devez les exécuter avec des privilèges d'administrateur ou ouvrir une invite de commandes Windows (`cmd`) à l'aide de la commande **Exécuter en tant qu'administrateur**. Si vous ne procédez pas ainsi, le message **Error executing command**. s'affiche. Le dossier de destination doit aussi exister lors de l'exportation de la configuration.

#### i REMARQUE

Les commandes `ecmd` ne peuvent être exécutées que localement. L'exécution d'une tâche client **Exécuter une commande** à l'aide d'ERA ne fonctionnera pas.

#### ✓ EXEMPLE

Commande d'exportation des paramètres :

```
ecmd /getcfg c:\config\settings.xml
```

Commande d'importation des paramètres :

```
ecmd /setcfg c:\config\settings.xml
```

Signature du fichier de configuration `.xml` :

1. Téléchargez **XmlSignTool** à partir de la [page de téléchargement des outils et des utilitaires ESET](#), puis extrayez-le. Cet outil a été spécifiquement développé pour signer les fichiers de configuration `.xml` eset.
2. Ouvrez une invite de commandes Windows en utilisant **Exécuter en tant qu'administrateur**.
3. Accédez à l'emplacement de `XmlSignTool.exe`.
4. Exécutez une commande pour signer le fichier de configuration `.xml` : `XmlSignTool <chemin_fichier_xml>`
5. Lorsque l'utilitaire `XmlSignTool` vous le demande, 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 <%PN%> avec ESET CMD à l'aide de la méthode d'autorisation du mot de passe de configuration avancée.



## AVERTISSEMENT

Il n'est pas recommandé d'activer ESET CMD sans autorisation, car cela permet l'importation de configuration non signée. Définissez le mot de passe dans **Configuration avancée > Interface utilisateur > Configuration de l'accès** pour empêcher toute modification non autorisée par les utilisateurs.

## 4.5 Interface utilisateur

La section **Interface utilisateur** permet de configurer le comportement de l'interface utilisateur graphique du programme (GUI).

Grâce à l'outil [Graphiques](#), vous pouvez ajuster l'apparence du programme et l'utilisation des effets.

En configurant [Alertes et notifications](#), vous pouvez modifier le comportement des alertes concernant les menaces détectées et les notifications système. Ces alertes peuvent être personnalisées en fonction de vos besoins.

Afin de bénéficier de la sécurité maximum de votre logiciel de sécurité, vous pouvez empêcher toute modification non autorisée en protégeant les paramètres par un mot de passe à l'aide de l'outil [Configuration de l'accès](#).

### 4.5.1 Éléments de l'interface utilisateur

La configuration de l'interface utilisateur d'ESET NOD32 Antivirus peut être modifiée de manière à adapter l'environnement de travail à vos besoins. Ces options de configuration sont accessibles depuis la branche **Interface utilisateur > Éléments de l'interface utilisateur** de l'arborescence de la configuration avancée ESET NOD32 Antivirus.

Pour désactiver l'écran de démarrage de ESET NOD32 Antivirus, désactivez **Afficher l'écran de démarrage**.

Pour qu'ESET NOD32 Antivirus émette un signal sonore en cas d'événement important lors d'une analyse, par exemple lorsqu'une menace est découverte ou lorsque l'analyse est terminée, sélectionnez **Utiliser un signal sonore**.

**Intégrer dans le menu contextuel** – Intègre les options ESET NOD32 Antivirus dans le menu contextuel.

#### États

**États d'application** – Cliquez sur le bouton **Modifier** pour gérer (désactiver) les états affichés dans le volet **État de la protection** du menu principal.

## Configuration avancée

ANTIVIRUS 2

MISE À JOUR 2

INTERNET ET MESSAGERIE 3

CONTRÔLE DE PÉRIPHÉRIQUE 1

OUTILS

INTERFACE UTILISATEUR

ÉLÉMENTS DE L'INTERFACE UTILISATEUR

Afficher l'écran de démarrage

☒
☐

?

Émettre un signal sonore

☒
☐

?

Intégrer dans le menu contextuel

☒
☐

?

ÉTATS

États d'application

Modifier

?

ALERTES ET NOTIFICATIONS

CONFIGURATION DE L'ACCÈS

Par défaut

OK

Annuler

### 4.5.2 Alertes et notifications

La section **Alertes et notifications** sous **Interface utilisateur** vous permet de configurer la manière dont ESET NOD32 Antivirus traite les alertes de menace et les notifications système (par exemple, les messages indiquant une mise à jour réussie). Vous pouvez également configurer l'heure d'affichage et la transparence des notifications dans la barre d'état système (cela ne s'applique qu'aux systèmes prenant en charge ces notifications).

## Configuration avancée

ANTIVIRUS 2

MISE À JOUR 2

INTERNET ET MESSAGERIE 3

CONTRÔLE DE PÉRIPHÉRIQUE 1

OUTILS

INTERFACE UTILISATEUR

ÉLÉMENTS DE L'INTERFACE UTILISATEUR

ALERTES ET NOTIFICATIONS

FENÊTRES D'ALERTE

Afficher les alertes

☒
☐

?

MESSAGES INTÉGRÉS AU PRODUIT

Afficher les messages publicitaires ESET

☐
☒

?

NOTIFICATIONS DU BUREAU

Afficher les notifications sur le Bureau

☒
☐

?

Ne pas afficher les notifications en cas d'exécution d'applications en mode plein écran

☒
☐

?

Durée

10

?

Transparence

20

?

Verbosité minimale des événements à afficher

Entrées informatives

?

Sur les systèmes multi-utilisateurs, afficher les notifications sur

Administrator

?

Par défaut

OK

Annuler

86

## Fenêtres d'alerte

Lorsque l'option **Afficher les alertes** est désactivée, aucune fenêtre d'alerte ne s'affiche, ce qui ne convient qu'à un nombre limité de situations particulières. Nous recommandons à la majorité des utilisateurs de conserver l'option par défaut (activée).

## Messages intégrés au produit

**Afficher les messages marketing** – Les messages intégrés au produit ont été conçus pour informer les utilisateurs des actualités et autres communications d'ESET. Désactivez cette option si vous ne souhaitez pas recevoir des messages marketing.

## Notifications du Bureau

Les notifications sur le bureau et les info-bulles sont fournies à titre d'information uniquement et n'exigent aucune interaction avec l'utilisateur. Elles s'affichent dans la partie système de la barre d'état, dans l'angle inférieur droit de l'écran. Pour activer l'affichage des notifications sur le bureau, activez l'option **Afficher les notifications sur le bureau**.

Activez l'option **Ne pas afficher les notifications en cas d'exécution d'applications en mode plein écran** pour supprimer toutes les notifications non interactives. D'autres options détaillées (la durée d'affichage des notifications et la transparence de la fenêtre) peuvent être modifiées en dessous.

Le menu déroulant **Verbosité minimale des événements à afficher** permet de sélectionner le niveau de gravité des alertes et notifications à afficher. Les options disponibles sont les suivantes :

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

La dernière fonctionnalité de cette section permet de configurer la destination des notifications dans un environnement multi-utilisateur. Le champ **Sur les systèmes multi-utilisateurs, afficher les notifications sur l'écran de l'utilisateur suivant** indique l'utilisateur qui recevra les notifications système et autres notifications lorsque le système autorise la connexion simultanée de plusieurs utilisateurs. Normalement, il doit s'agir de l'administrateur système ou de l'administrateur réseau. Cette option est particulièrement utile pour les serveurs Terminal Server, à condition que toutes les notifications système soient envoyées à l'administrateur.

## Zones de message

Pour fermer automatiquement les fenêtres d'alerte après un certain délai, sélectionnez **Fermer automatiquement les zones de message**. Si les fenêtres d'alerte ne sont pas fermées manuellement, le système les ferme automatiquement une fois le laps de temps écoulé.

**Messages de confirmation** – Affiche une liste de messages de confirmation que vous pouvez choisir d'afficher ou non.

### 4.5.2.1 Configuration avancée

Dans le menu déroulant **Verbosité minimale des événements à afficher**, vous pouvez sélectionner le niveau de gravité de démarrage des alertes et notifications à afficher.

- **Diagnostic** – Consigne toutes les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.
- **Entrées informatives** – Enregistre tous les messages d'information, 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** – Consigne les erreurs du type « *Erreur de téléchargement du fichier* » et erreurs critiques.
- **Critique** – Répertorie toutes les erreurs critiques (erreur de démarrage de la protection antivirus, etc...).

La dernière fonctionnalité de cette section permet de configurer la destination des notifications dans un environnement multi-utilisateur. Le champ **Sur les systèmes multi-utilisateurs, afficher les notifications sur l'écran de l'utilisateur suivant** indique l'utilisateur qui recevra les notifications système et autres notifications lorsque le système autorise la connexion simultanée de plusieurs utilisateurs. Normalement, il doit s'agir de l'administrateur système ou de l'administrateur réseau. Cette option est particulièrement utile pour les serveurs Terminal Server, à condition que toutes les notifications système soient envoyées à l'administrateur.

### 4.5.3 Configuration de l'accès

Les paramètres de ESET NOD32 Antivirus constituent une partie essentielle de votre stratégie de sécurité. Des modifications non autorisées peuvent mettre en danger la stabilité et la protection de votre système. Pour éviter des modifications non autorisées, les paramètres de la configuration d'ESET NOD32 Antivirus peuvent être protégés par mot de passe.

**Configuration avancée** [Rechercher] [x] [?]

- ANTIVIRUS 2
- MISE À JOUR 2
- INTERNET ET MESSAGERIE 3
- CONTRÔLE DE PÉRIPHÉRIQUE 1
- OUTILS
- INTERFACE UTILISATEUR**

**ÉLÉMENTS DE L'INTERFACE UTILISATEUR**

**ALERTES ET NOTIFICATIONS**

**CONFIGURATION DE L'ACCÈS**

Protéger les paramètres par un mot de passe [Champ de mot de passe] [x]

Définir le mot de passe [Définir]

Demander des droits d'administrateur complets pour des comptes Administrateur limités [✓]

[Par défaut] [OK] [Annuler]

**Protéger les paramètres par un mot de passe** : indiquez les paramètres du mot de passe. Cliquez sur cette option pour ouvrir la fenêtre Configuration du mot de passe.

Pour définir ou modifier un mot de passe visant à protéger les paramètres de configuration, cliquez sur **Définir**.


**Demander des droits d'administrateur complets pour des comptes administrateur limités** : sélectionnez cette option pour inviter l'utilisateur actuel (s'il ne possède pas les autorisations d'administrateur) à saisir un nom et un

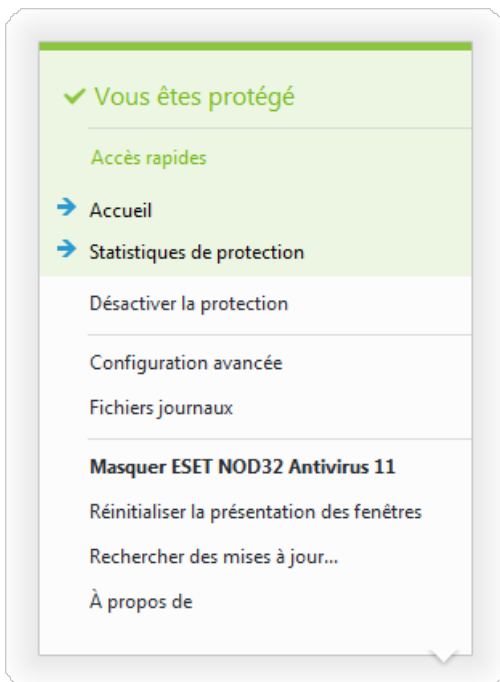
mot de passe d'administrateur lors de la modification de certains paramètres du système (semblable au contrôle UAC (User Account Control) dans Windows Vista et Windows 7). Elles portent également sur la désactivation des modules de protection. Sous les systèmes Windows XP qui ne prennent pas en charge le contrôle UAC, les utilisateurs pourront utiliser l'option **Demander des droits d'administrateur (système sans prise en charge UAC)**.

Pour Windows XP uniquement :

**Demander des droits d'administrateur (système sans prise en charge UAC)** : activez cette option pour qu'ESET NOD32 Antivirus demande des informations d'identification d'administrateur.

#### 4.5.4 Menu du programme

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.



**Liens rapides** – Affiche les parties les plus utilisées de ESET NOD32 Antivirus. Vous pouvez y accéder rapidement depuis le menu du programme.

**Désactiver la protection** – Affiche la boîte de dialogue de confirmation qui désactive la [protection antivirus et antispyware](#) ; cette dernière protège le système des attaques malveillantes en contrôlant les fichiers et les communications par messagerie et Internet.

Le menu déroulant **Intervalle** indique la durée pendant laquelle la protection antivirus et antispyware est désactivée.



#### Désactiver la protection en temps réel ?

La désactivation de la protection en temps réel, même pour une courte période, est dangereuse et rend votre ordinateur vulnérable aux virus et autres menaces.

Interrompre pendant 10 ... ▼

 Appliquer

Annuler

**Configuration avancée** – Sélectionnez cette option pour afficher l'arborescence **Configuration avancée**. Vous pouvez également ouvrir Configuration avancée en appuyant par exemple sur la touche F5 ou en sélectionnant **Configuration > Configuration avancée**.

**Fichiers journaux** – Les [fichiers journaux](#) contiennent les événements importants qui se sont produits et fournissent un aperçu des menaces détectées.

**Masquer ESET NOD32 Antivirus** – Masque la fenêtre ESET NOD32 Antivirus.

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

**Rechercher des mises à jour** – Commence la mise à jour du moteur de détection (précédemment appelé « base de signatures des virus ») afin de garantir un niveau optimal de protection contre les codes malveillants.

**À propos** – Les informations système fournissent des détails sur la version installée d'ESET NOD32 Antivirus et sur les modules installés. Vous y trouverez aussi la date d'expiration de la licence ainsi que des informations sur le système d'exploitation et les ressources du système.

## 5. Utilisateur chevronné

### 5.1 Profils

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

#### Analyse d'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 la fenêtre Configuration avancée (F5) et cliquez sur **Antivirus > Analyse de l'ordinateur à la demande > Général > Liste des profils**. La fenêtre **Gestionnaire de profils** dispose du menu déroulant **Profil sélectionné** contenant les profils d'analyse existants, ainsi qu'une option permettant de créer un profil. Pour plus d'informations sur la création d'un profil d'analyse correspondant à vos besoins, reportez-vous à la section [ThreatSense Configuration du moteur](#) ; vous y trouverez une description de chaque paramètre de configuration de l'analyse.

#### REMARQUE

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

#### Mise à jour

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

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

**Profil 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.

### 5.2 Raccourcis clavier

Pour simplifier la navigation dans votre produit ESET, vous pouvez utiliser les raccourcis clavier suivants :

F1	ouvre les pages d'aide
F5	ouvre la boîte de dialogue Configuration avancée
Haut/Bas	navigation dans les différents composants du produit
-	réduit les nœuds de l'arborescence Configuration avancée
TAB	déplace le curseur dans une fenêtre
Échap	ferme la boîte de dialogue active

## 5.3 Diagnostics

Le diagnostic fournit un fichier d'image mémoire en cas de défaillance d'une application lors des processus ESET (par exemple *ekrn*). Dès qu'une application présente une défaillance, un fichier d'image mémoire est généré. Ce fichier permet aux développeurs de déboguer et de résoudre différents problèmes ESET NOD32 Antivirus. 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** (valeur par défaut) pour désactiver cette fonctionnalité.
- **Mini** – 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.

**Activer la journalisation avancée du filtrage des protocoles** – Enregistrez toutes les données qui passent par le moteur de filtrage des protocoles au format PCAP. Les développeurs peuvent ainsi diagnostiquer et résoudre les problèmes liés au filtrage des protocoles.

**Activer la journalisation avancée du moteur de mise à jour** – Enregistrez tous les événements qui se produisent pendant le processus de mise à jour. Les développeurs peuvent ainsi diagnostiquer et résoudre les problèmes liés au moteur de mise à jour.

Les fichiers journaux sont disponibles dans le dossier suivant :

*C:\ProgramData\ESET\ESET NOD32 Antivirus\Diagnostics\* dans Windows Vista et versions ultérieures ou *C:\Documents and Settings\All Users\...* dans les versions antérieures de Windows.

**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**.

## 5.4 Importer et exporter les paramètres

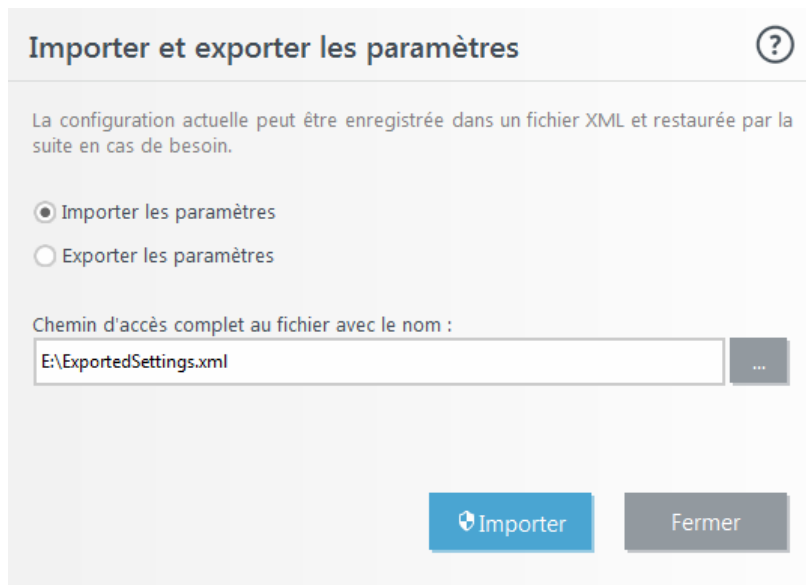
Vous pouvez importer ou exporter votre fichier de configuration .xml ESET NOD32 Antivirus personnalisé à partir du menu **Configuration**.

Ces opérations sont utiles si vous devez sauvegarder la configuration actuelle de ESET NOD32 Antivirus pour l'utiliser ultérieurement. L'option Exporter les paramètres est également pratique pour les utilisateurs qui souhaitent utiliser leur configuration préférée sur plusieurs systèmes. Il leur suffit d'importer un fichier .xml pour transférer ces paramètres.

L'importation d'une configuration est très facile. Dans la fenêtre principale du programme, cliquez sur **Configuration > Importer et exporter les paramètres**, puis sélectionnez **Importer les paramètres**. Saisissez le nom du fichier de configuration ou cliquez sur le bouton ... pour accéder au fichier de configuration à importer.



La procédure d'exportation d'une configuration est très semblable. Dans la fenêtre principale du programme, cliquez sur **Configuration > Importer et exporter les paramètres**. Sélectionnez **Exporter les paramètres** et saisissez le nom de fichier du fichier de configuration (par exemple, *export.xml*). Utilisez le navigateur pour sélectionner un emplacement de votre ordinateur pour enregistrer le fichier de configuration.



#### **i REMARQUE**

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

## **5.5 ESET SysInspector**

### **5.5.1 Présentation de ESET SysInspector**

ESET SysInspector est une application qui inspecte votre ordinateur en profondeur et qui affiche les données obtenues de manière exhaustive. Des informations telles que les pilotes et applications installés, les connexions réseau ou les entrées de registre importantes peuvent vous aider à élucider un comportement suspect du système, qu'il soit dû à une incompatibilité logicielle ou matérielle, ou à une infection par logiciel malveillant.

ESET SysInspector est accessible de deux manières : depuis la version intégrée dans les solutions ESET Security ou par téléchargement gratuit de la version autonome (SysInspector.exe) depuis le site d'ESET. Les deux versions ont les mêmes fonctions et les mêmes contrôles de programme. La seule différence réside dans le mode de gestion des résultats. La version autonome et la version intégrée permettent d'exporter des instantanés du système dans un fichier *.xml* et de les enregistrer sur le disque. Toutefois, la version intégrée permet également de stocker les instantanés système directement dans **Outils > ESET SysInspector** (à l'exception d'ESET Remote Administrator). Pour plus d'informations, consultez la section [ESET SysInspector comme partie de ESET NOD32 Antivirus](#).

Patiencez quelques instants pendant qu'ESET SysInspector analyse votre ordinateur. L'opération peut prendre entre 10 secondes et quelques minutes en fonction de la configuration matérielle, du système d'exploitation et du nombre d'applications installées sur votre ordinateur.

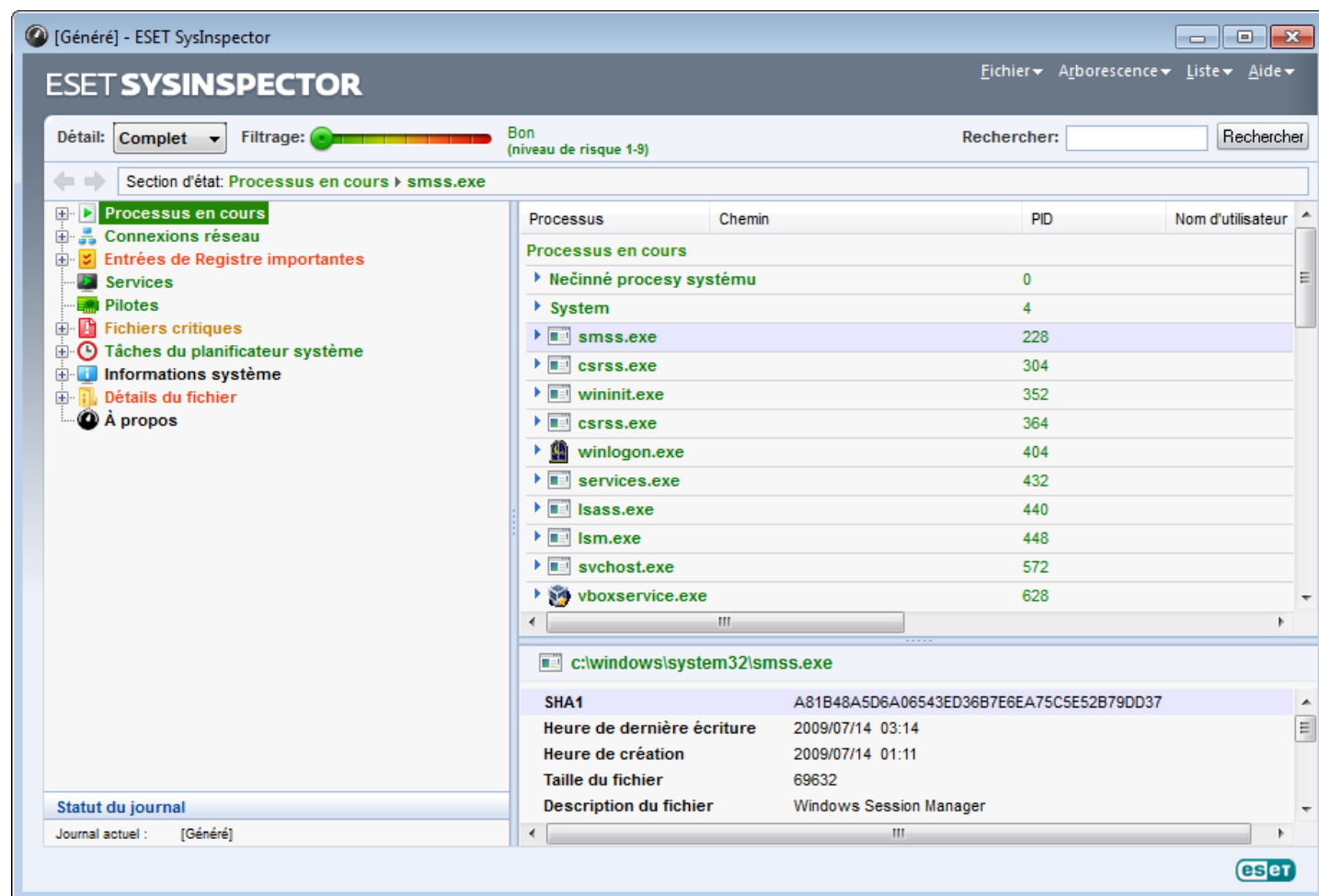
### 5.5.1.1 Démarrer ESET SysInspector.

Pour démarrer ESET SysInspector, il suffit de lancer le fichier exécutable *SysInspector.exe* téléchargé depuis le site d'ESET. Si vous avez déjà installé une des solutions ESET Security, vous pouvez exécuter ESET SysInspector directement à partir du menu Démarrer (cliquez sur **Programmes** > **ESET** > **ESET NOD32 Antivirus**).

Patiencez pendant que l'application vérifie le système. Cette opération peut prendre plusieurs minutes.

### 5.5.2 Interface utilisateur et utilisation de l'application

Pour des raisons de clarté, la fenêtre principale du programme est divisée en quatre principales sections : la section des Contrôles du programme en haut, la fenêtre Navigation à gauche, la fenêtre Description à droite au centre et la fenêtre Détails en bas. La section État du journal reprend les paramètres de base d'un journal (filtre utilisé, type de filtre, le journal est-il le résultat d'une comparaison ?, etc.)



#### 5.5.2.1 Contrôles du programme

Cette section contient la description de tous les contrôles du programme disponible dans ESET SysInspector.

##### Fichier

En cliquant sur **Fichier**, vous pouvez enregistrer l'état actuel du système en vue d'une enquête ultérieure ou ouvrir un journal déjà enregistré. Pour la publication, il est conseillé de créer un journal **approprié pour envoi**. Sous cette forme, le journal omet les informations sensibles (nom d'utilisateur, nom d'ordinateur, nom de domaine, privilèges actuels de l'utilisateur, variables d'environnement, etc.).

**REMARQUE** : vous pouvez ouvrir des rapports enregistrés ESET SysInspector en les faisant glisser et en les déposant dans la fenêtre principale.

## Arborescence

Permet de développer ou de réduire tous les nœuds et d'exporter les sections sélectionnées dans le script de service.

## Liste

Contient les fonctions pour une navigation simplifiée dans le programme et diverses autres fonctions comme l'obtention d'informations en ligne.

## Aide

Contient des informations sur l'application et ses fonctions.

## Détails

Ce paramètre conditionne les informations affichées dans la fenêtre principale, ce qui simplifie leur utilisation. En mode de base, vous avez accès aux informations utilisées pour trouver les solutions aux problèmes communs dans votre système. En mode « Moyen », l'application affiche moins de détails utilisés. En mode « Complet », ESET SysInspector affiche toutes les informations requises pour résoudre des problèmes très particuliers.

## Filtrage

Le filtrage des éléments est particulièrement adapté à la recherche de fichiers suspects ou d'entrées de Registre dans le système. En déplaçant le curseur, vous pouvez filtrer les éléments en fonction de leur niveau de risque. Quand le curseur est en position maximale vers la gauche (niveau de risque 1), tous les éléments sont affichés. En déplaçant le curseur vers la droite, l'application filtre tous les éléments dont le risque est inférieur au niveau de risque actuel et affiche uniquement les éléments plus suspects (dont le niveau est plus élevé que celui affiché). Si le curseur est en position maximale à droite, le programme affiche uniquement les éléments nuisibles connus.

Tous les éléments portant le niveau de risque 6 à 9 peuvent poser un risque pour la sécurité. Si vous n'utilisez pas de solution de sécurité ESET, nous vous conseillons d'analyser votre système à l'aide de [ESET Online Scanner](#) si ESET SysInspector a détecté un élément de ce type. ESET Online Scanner est un service gratuit.

**REMARQUE :** le niveau de risque d'un élément peut être rapidement déterminé en comparant sa couleur à celle du curseur de niveau de risque.

## Comparer

Lors de la comparaison de deux journaux, vous pouvez choisir d'afficher tous les éléments, uniquement les éléments ajoutés, uniquement les éléments supprimés ou uniquement les éléments remplacés.

## Rechercher

La fonction de recherche peut être utilisée pour trouver rapidement un élément en particulier sur la base de son nom ou d'une partie de celui-ci. Les résultats de la recherche sont affichés dans la fenêtre Description.

## Retour



En cliquant sur la flèche arrière ou avant, vous pouvez revenir aux informations affichées précédemment dans la fenêtre Description. Vous pouvez utiliser la touche de retour arrière et la barre d'espace au lieu de cliquer sur la flèche arrière ou avant.

## Section d'état

Affiche le nœud actuel dans la fenêtre Navigation.

**Important :** les éléments surlignés en rouge sont inconnus et c'est la raison pour laquelle l'application les marque comme potentiellement dangereux. Si un élément est rouge, cela ne signifie pas automatiquement que vous pouvez supprimer le fichier. Avant de le supprimer, assurez-vous que les fichiers sont bel et bien dangereux ou qu'ils ne sont pas nécessaires.

### 5.5.2.2 Navigation dans ESET SysInspector

ESET SysInspector répartit divers types d'informations en plusieurs sections élémentaires baptisées nœuds. Le cas échéant, vous pouvez obtenir des détails complémentaires en développant chaque nœud afin d'afficher les sous-nœuds. Pour développer ou réduire un nœud, il suffit de double-cliquer sur son nom ou de cliquer sur  ou sur  en regard du nom du nœud. Quand vous parcourez la structure arborescente des nœuds et des sous-nœuds dans la fenêtre de navigation, vous pouvez voir différents détails pour chaque nœud dans la fenêtre Description. Si vous parcourez les éléments de la fenêtre Description, des détails supplémentaires pour chaque élément peuvent être affichés dans la fenêtre Détails.

Voici les descriptions des principaux nœuds de la fenêtre Navigation et des informations qui s'y rapportent dans les fenêtres Description et Détails.

#### Processus en cours

Ce nœud reprend les informations sur les applications et les processus en cours d'exécution au moment de la création du journal. La fenêtre Détails reprend des détails complémentaires pour chaque processus tels que les bibliothèques dynamiques utilisées par les processus et leur emplacement dans le système, le nom de l'éditeur de l'application, le niveau de risque du fichier, etc.

La fenêtre Détails contient des informations complémentaires sur les éléments sélectionnés dans la fenêtre Description telles que la taille du fichier ou son hachage.

**REMARQUE :** un système d'exploitation contient plusieurs noyaux importants qui fonctionnent en permanence et qui assurent des fonctions élémentaires et vitales pour d'autres applications utilisateur. Dans certains cas, ces processus sont repris dans l'outil ESET SysInspector avec un chemin d'accès au fichier commençant par \??\. Ces symboles garantissent l'optimisation préalable au lancement pour ce processus ; ils ne présentent aucun danger pour le système.

#### Connexions réseau

La fenêtre Description contient la liste des processus et des applications qui communiquent via le réseau à l'aide du protocole sélectionné dans la fenêtre navigation (TCP ou UDP), ainsi que l'adresse distante à laquelle l'application est connectée. Vous pouvez également vérifier les adresses IP des serveurs DNS.

La fenêtre Détails contient des informations complémentaires sur les éléments sélectionnés dans la fenêtre Description telles que la taille du fichier ou son hachage.

#### Entrées de Registre importantes

Contient la liste des entrées de registre sélectionnées qui sont souvent liées à divers problèmes du système telles que celles qui indiquent les applications de démarrage, les objets application d'assistance du navigateur, etc.

La fenêtre Description peut indiquer les fichiers en rapport avec les entrées de Registre particulières. Vous pouvez voir des détails complémentaires dans la fenêtre Détails.

#### Services

La fenêtre Description contient la liste des fichiers enregistrés en tant que services Windows. Vous pouvez consulter la manière dont le service doit démarrer avec des détails spécifiques sur le fichier dans la fenêtre Détails.

#### Pilotes

Liste des pilotes installés sur le système.

#### Fichiers critiques

La fenêtre Description affiche le contenu des fichiers critiques liés au système d'exploitation Microsoft Windows.

#### Tâches système du planificateur

Contient la liste des tâches déclenchées par le planificateur de tâches Windows à une heure/un intervalle spécifiés.

## **Informations système**

Contient des informations détaillées sur le matériel et le logiciel, ainsi que des informations sur les variables d'environnement, les droits de l'utilisateur et les journaux d'événement système définis.

## **Détails du fichier**

Liste des fichiers système importants et des fichiers du dossier Program Files. Des informations complémentaires spécifiques sur les fichiers sont disponibles dans les fenêtres Description et Détails.

## **À propos**

Informations sur la version d'ESET SysInspector et sur la liste des modules de programme.

### 5.5.2.2.1 Raccourcis clavier

Voici les raccourcis clavier disponibles dans ESET SysInspector :

#### Fichier

Ctrl+O	ouvre un journal existant
Ctrl+S	enregistre les journaux créés

#### Générer

Ctrl+G	génère un instantané du statut de l'ordinateur
Ctrl+H	génère un instantané de l'état du système qui pourrait également consigner des informations sensibles

#### Filtrage des éléments

1, O	acceptable, les éléments de niveau de risque 1 à 9 sont affichés
2	acceptable, les éléments de niveau de risque 2 à 9 sont affichés
3	acceptable, les éléments de niveau de risque 3 à 9 sont affichés
4, U	inconnu, les éléments de niveau de risque 4 à 9 sont affichés
5	inconnu, les éléments de niveau de risque 5 à 9 sont affichés
6	inconnu, les éléments de niveau de risque 6 à 9 sont affichés
7, B	risqué, les éléments de niveau de risque 7 à 9 sont affichés
8	risqué, les éléments de niveau de risque 8 à 9 sont affichés
9	risqué, les éléments de niveau de risque 9 sont affichés
-	diminue le niveau de risque
+	augmente le niveau de risque
Ctrl+9	mode de filtrage, niveau égal ou supérieur
Ctrl+0	niveau de filtrage, niveau égal uniquement

#### Afficher

Ctrl+5	afficher par éditeur, tous les éditeurs
Ctrl+6	afficher par éditeur, uniquement Microsoft
Ctrl+7	afficher par éditeur, tous les autres éditeurs
Ctrl+3	appliquer tous les détails
Ctrl+2	afficher les détails moyens
Ctrl+1	affichage de base
Retour	revient une étape en arrière
arrière	
Barre	avance d'une étape
d'espace	
Ctrl+W	développe l'arborescence
Ctrl+Q	réduit l'arborescence

#### Autres commandes

Ctrl+T	va à l'emplacement d'origine de l'élément après la sélection dans les résultats de recherche
Ctrl+P	affiche des informations élémentaires sur un élément
Ctrl+A	affiche des informations complètes sur un élément
Ctrl+C	copie l'arborescence de l'élément
Ctrl+X	copie les éléments
Ctrl+B	trouve des informations sur les fichiers sélectionnés sur Internet
Ctrl+L	ouvre le dossier où se trouve le fichier sélectionné.
Ctrl+R	ouvre l'entrée correspondante dans l'éditeur de registre
Ctrl+Z	copie un chemin d'accès à un fichier (si l'élément est lié à un fichier)
Ctrl+F	passe au champ de recherche
Ctrl+D	ferme les résultats de la recherche
Ctrl+E	exécute le script de service

## Comparaison

Ctrl+Alt+O	ouvre le journal d'origine/de comparaison
Ctrl+Alt+R	annule la comparaison
Ctrl+Alt+1	affiche tous les éléments
Ctrl+Alt+2	affiche uniquement les éléments ajoutés, le journal indiquera les éléments présents dans le journal actuel
Ctrl+Alt+3	affiche uniquement les éléments supprimés, le journal indiquera les éléments présents dans le journal précédent
Ctrl+Alt+4	affiche uniquement les éléments remplacés (fichiers inclus)
Ctrl+Alt+5	affiche uniquement les différences entre les journaux
Ctrl+Alt+C	affiche la comparaison
Ctrl+Alt+N	affiche le journal actuel
Ctrl+Alt+P	ouvre le journal précédent

## Divers

F1	afficher l'aide
Alt+F4	quitter l'application
Alt+Maj+F4	quitter l'application sans demander
Ctrl+I	statistiques du journal

### 5.5.2.3 Comparer

La fonctionnalité Comparer permet de comparer deux journaux. Cette fonctionnalité met en évidence les éléments qui ne sont pas communs aux deux journaux. Ce procédé est utile si vous souhaitez assurer le suivi des modifications dans le système. Vous pourrez peut-être ainsi détecter l'activité d'un code malveillant.

Après son lancement, l'application crée un journal qui apparaît dans une nouvelle fenêtre. Cliquez sur **Fichier > Enregistrer le journal** pour enregistrer le journal dans un fichier. Les fichiers journaux peuvent être ouverts et consultés ultérieurement. Pour ouvrir un journal existant, cliquez sur **Fichier > Ouvrir le journal**. Dans la fenêtre principale de l'application, ESET SysInspector affiche toujours un journal à la fois.

La comparaison de deux journaux permet d'afficher un journal actif et un journal enregistré dans un fichier. Pour comparer des journaux, cliquez sur **Fichier > Comparer les journaux**, puis choisissez **Sélectionner un fichier**. Le journal sélectionné sera comparé au journal actif dans les fenêtres principales de l'application. Le journal des comparaisons n'affiche que les différences entre les deux journaux.

**REMARQUE :** si vous comparez deux fichiers journaux, cliquez sur **Fichier > Enregistrer le journal** et enregistrez-le dans un fichier ZIP. Les deux fichiers sont enregistrés. Si vous ouvrez ce fichier ultérieurement, les journaux qu'il contient seront comparés automatiquement.

En regard des éléments affichés, ESET SysInspector affiche les symboles qui identifient les différences entre les journaux comparés.

Description de tous les symboles qui peuvent être affichés à côté des éléments :

- + nouvelle valeur, absente du journal précédent.
- □ la section de la structure arborescente contient de nouvelles valeurs.
- - valeur supprimée, présente uniquement dans le journal précédent.
- ■ la section de la structure arborescente contient des valeurs supprimées.
- ✎ la valeur/le fichier a été modifié.
- ■ la section de la structure arborescente contient des valeurs/des fichiers modifiés.
- 🟢 le niveau de risque a diminué/il était supérieur dans le journal précédent.
- 🔴 le niveau de risque a augmenté/il était inférieur dans le journal précédent.

La section d'explication affichée dans le coin inférieur gauche décrit tous les symboles et affiche le nom des journaux comparés.

Statut du journal

Journal actuel : SysInspector-WIN-5TAESPU4IF2-110801-1316.xml [Chargé-ZIP]

Journal précédent : SysInspector-WIN-5TAESPU4IF2-110801-1303.xml [Chargé-ZIP]

Comparer : [Résultat de la comparaison]

Comparer la légende des icônes

+ Élément ajouté

- Élément supprimé

↺ Fichier remplacé

↘ L'état a été abaissé

↗ L'état a été élevé

☒ Élément(s) ajouté(s) dans la branche

☐ Élément(s) supprimé(s) de la branche

☐ Élément(s) ajouté(s) ou supprimé(s) dans la branche

☒ Fichier(s) remplacé(s) dans la branche

Les journaux de comparaison peuvent être enregistrés dans un fichier et ouverts plus tard :

### Exemple

Créez un journal reprenant des informations d'origine sur le système et enregistrez-le dans un fichier appelé précédent.xml. Après avoir modifié le système, ouvrez ESET SysInspector et laissez-le créer un nouveau journal. Enregistrez ce journal sous *actuel.xml*.

Pour voir les différences entre ces deux journaux, cliquez sur **Fichier > Comparer les journaux**. Le programme crée un journal de comparaison qui indique les différences entre les journaux.

Un résultat identique peut être obtenu si vous utilisez l'option de ligne de commande suivante :

*SysInspector.exe actuel.xml précédent.xml*

### 5.5.3 Paramètres de la ligne de commande

ESET SysInspector prend en charge la création de rapports via la ligne de commande à l'aide de ces paramètres :

<b>/gen</b>	générer le journal directement à partir de la ligne de commande sans exécuter la GUI
<b>/privacy</b>	générer le journal en omettant les informations sensibles
<b>/zip</b>	enregistrer le journal des résultats dans une archive compressée au format zip
<b>/silent</b>	supprimer la fenêtre de progression durant la génération du journal à partir de la ligne de commande
<b>/blank</b>	lance ESET SysInspector sans générer/charger de journal

### Exemples

Utilisation :

*Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]*

Pour charger un journal en particulier directement dans le navigateur, saisissez : *SysInspector.exe .\clientlog.xml*

Pour générer le journal depuis la ligne de commande, saisissez : *SysInspector.exe /gen=. \mynewlog.xml*

Pour générer un journal qui exclut les informations sensibles directement dans un fichier compressé, saisissez : *SysInspector.exe /gen=. \mynewlog.zip /privacy /zip*

Pour comparer deux fichiers journaux et parcourir leurs différences, saisissez : *SysInspector.exe new.xml old.xml*

**REMARQUE** : si le nom du fichier/du dossier contient un espace, vous devez le saisir entre guillemets.



## 5.5.4 Script de service

Le script de service est un outil qui vise à offrir une aide aux clients qui utilisent ESET SysInspector en leur permettant de supprimer les objets indésirables du système.

Le script de service permet à l'utilisateur d'exporter l'ensemble du journal ESET SysInspector ou des parties sélectionnées uniquement. Après l'exportation, vous pouvez marquer les objets indésirables pour la suppression. Vous pouvez ensuite exécuter le journal modifié pour supprimer les objets marqués.

Le script de service convient aux utilisateurs expérimentés qui connaissent les problèmes des systèmes de diagnostic. Des modifications erronées pourraient endommager le système d'exploitation.

### Exemple

Si vous pensez que votre ordinateur est infecté par un virus qui n'est pas détecté par votre logiciel antivirus, suivez les instructions ci-après :

1. Exécutez ESET SysInspector pour obtenir un nouvel instantané du système.
2. Sélectionnez le premier élément de la section à gauche (dans la structure arborescente), appuyez sur la touche Maj, puis sélectionnez le dernier élément afin de marquer tous les éléments.
3. Cliquez à l'aide du bouton droit sur les objets sélectionnés et sélectionnez **Exporter les sections sélectionnées dans un script de service**.
4. Les objets sélectionnés seront exportés dans un nouveau journal.
5. Il s'agit de l'étape la plus importante de toute la procédure : ouvrez le nouveau journal et remplacez l'attribut + par - pour tous les objets que vous souhaitez supprimer. Veillez à ne marquer aucun objet/fichier important du système d'exploitation.
6. Ouvrez ESET SysInspector, cliquez sur **Fichier > Exécuter le script de service**, puis saisissez le chemin d'accès au script.
7. Cliquez sur **OK** pour lancer le script.

### 5.5.4.1 Création d'un script de service

Pour créer un script, cliquez avec le bouton droit de la souris sur n'importe quel élément de l'arborescence de menus (dans le volet de gauche) dans la fenêtre principale de ESET SysInspector. Dans le menu contextuel, choisissez l'option **Exporter toutes les sections dans un script de service** ou **Exporter les sections sélectionnées dans un script de service**.

**REMARQUE** : il est impossible d'exporter le script de service lorsque deux journaux sont comparés.

### 5.5.4.2 Structure du script de service

La première ligne de l'en-tête du script reprend des informations sur la version du moteur (ev), la version de l'interface utilisateur graphique (gv) et la version du journal (lv). Ces données permettent d'identifier d'éventuelles modifications dans le fichier .xml qui génère le script et d'éviter toute incohérence durant l'exécution. Cette partie du script ne peut être modifiée.

Le reste du fichier est scindé en sections dont les éléments peuvent être modifiés (indique ceux qui seront traités par le script). Pour marquer un élément à traiter, remplacez le caractère « - » qui le précède par « + ». Les sections du script sont séparées par une ligne vide. Chaque section possède un numéro et un titre.

#### 01) Running processes (processus en cours)

Cette section contient la liste de tous les processus en cours d'exécution dans le système. Chaque processus est identifié par son chemin UNC et, ensuite, par son code de hachage CRC16 entre astérisques (\*).

Exemple :

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Dans cet exemple, un processus, à savoir module32.exe, a été sélectionné (marqué par le caractère « + ») ; le processus s'arrêtera à l'exécution du script.

## 02) Loaded modules (modules chargés)

Cette section reprend une liste des modules système en cours d'utilisation :

Exemple :

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbkhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Dans cet exemple, le module khbkhb.dll a été marqué par un « + ». Quand le script est exécuté, il reconnaît les processus qui utilisent ce module en particulier et les arrête.

## 03) TCP connections (connexions TCP)

Cette section contient des informations sur les connexions TCP existantes.

Exemple :

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrm.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Lorsque le script est exécuté, il trouve le propriétaire du socket dans les connexions TCP marquées et arrête le socket, ce qui libère des ressources système.

## 04) UDP endpoints (points de terminaison UDP)

Cette section contient des informations sur les points de terminaison UDP existants.

Exemple :

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Lorsque le script est exécuté, il isole le propriétaire du socket aux points de terminaison UDP marqués et arrête le socket.

## 05) DNS server entries (entrées du serveur DNS)

Cette section contient des informations sur la configuration actuelle du serveur DNS.

Exemple :

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Les entrées du serveur DNS marquées seront supprimées à l'exécution du script.

## 06) Important registry entries (entrées de registre importantes)

Cette section contient des informations relatives aux entrées de registre importantes.

Exemple :

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
  HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Les entrées marquées seront supprimées, réduites à des valeurs de 0 octet ou réinitialisées à leur valeur par défaut lors de l'exécution du script. L'action à appliquer à une entrée en particulier dépendra de la catégorie de l'entrée et de la valeur de la clé dans ce registre en particulier.

## 07) Services (services)

Cette section reprend les services enregistrés dans le système.

Exemple :

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
  startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
  startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
  startup: Manual
[...]
```

Les services marqués et les services dépendants sont arrêtés et désinstallés après l'exécution du script.

## 08) Drivers (pilotes)

Cette section reprend les pilotes installés.

Exemple :

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
  startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\
  \windows\system32\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Lorsque vous exécutez le script, les pilotes sélectionnés seront arrêtés. Notez que certains pilotes ne s'arrêtent pas.

## 09) Critical files (fichiers critiques)

Cette section contient des informations sur les fichiers critiques pour le fonctionnement adéquat du système d'exploitation.

Exemple :

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Les éléments sélectionnés seront soit supprimés, soit restaurés à leur valeur d'origine.

## 10) Tâches planifiées

Cette section contient des informations sur les tâches planifiées.

Exemple :

```
10) Scheduled tasks
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe /c
- c:\users\admin\appdata\local\google\update\googleupdate.exe /ua /installsource
- %windir%\system32\appidpolicyconverter.exe
- %windir%\system32\appidcertstorecheck.exe
- aitagent
[...]
```

### 5.5.4.3 Exécution des scripts de service

Marquez tous les éléments souhaités, puis enregistrez et fermez le script. Exécutez le script modifié directement depuis la fenêtre principale ESET SysInspector en choisissant l'option **Exécuter le script de service** dans le menu Fichier. Lorsque vous ouvrez un script, le programme affiche le message suivant : **Voulez-vous vraiment exécuter le script de service « %Scriptname% » ?** Une fois que vous avez confirmé votre sélection, un autre avertissement peut apparaître pour vous indiquer que le script de service que vous essayez d'exécuter n'a pas été signé. Cliquez sur **Exécuter** pour lancer le script.

Une boîte de dialogue confirme que le script s'est exécuté correctement.

Si le script n'a pu être traité que partiellement, une boîte de dialogue avec le message suivant apparaîtra : **Le script de service n'a été exécuté que partiellement. Voulez-vous afficher le rapport d'erreurs ?** Choisissez **Oui** pour afficher un rapport des erreurs complexe qui reprend les opérations qui n'ont pas été exécutées.

Si le script n'a pas été reconnu, une boîte de dialogue s'affiche avec le message suivant : **Le script de service sélectionné n'est pas signé. L'exécution de scripts sans signature et inconnus peut nuire sérieusement aux données de votre ordinateur. Êtes-vous certain de vouloir exécuter le script et les actions ?** Ceci peut être le résultat d'incohérences au sein du script (en-tête endommagé, titre de section endommagé, ligne vide manquante entre les sections, etc.). Vous pouvez soit rouvrir le fichier de script et corriger les erreurs qu'il contient, soit créer un autre script de service.

## 5.5.5 FAQ

### L'exécution de ESET SysInspector requiert-elle des privilèges d'administrateur ?

Bien que ESET SysInspector puisse être exécuté sans privilèges d'administrateur, certaines des informations qu'il recueille peuvent être consultées uniquement via un compte administrateur. Une exécution en tant qu'utilisateur standard ou utilisateur disposant d'un accès restreint entraînera la collecte d'un volume inférieur d'informations sur l'environnement d'exploitation.

### ESET SysInspector crée-t-il un fichier journal ?

ESET SysInspector peut créer un fichier journal sur la configuration de votre ordinateur. Pour en enregistrer un, dans la fenêtre principale du programme, cliquez sur **Fichier > Enregistrer le journal**. Les journaux sont enregistrés au format XML. Par défaut, les fichiers sont enregistrés dans le répertoire %USERPROFILE%\My Documents\ selon la nomenclature « SysInspector-%COMPUTERNAME%-AAMMJJ-HHMM.XML ». Vous pouvez changer l'emplacement et le nom du fichier avant la sauvegarde si vous le souhaitez.

### Comment puis-je consulter le fichier journal de ESET SysInspector ?

Pour consulter un fichier journal créé par ESET SysInspector, exécutez le programme et choisissez **Fichier > Ouvrir le journal** dans la fenêtre principale du programme. Vous pouvez également faire glisser les fichiers journaux et les déposer sur l'application ESET SysInspector. Si vous devez consulter fréquemment les fichiers journaux ESET SysInspector, il est conseillé de créer un raccourci vers le fichier SYSINSPECTOR.exe sur le Bureau ; vous pourrez ensuite faire glisser les fichiers et les déposer sur ce raccourci. Pour des raisons de sécurité, Windows Vista/7 peut ne pas autoriser la fonction glisser-déposer entre des fenêtres dont les autorisations diffèrent.

### Existe-t-il une spécification pour le format du fichier journal ? Ou un SDK ?

Pour l'instant, il n'existe ni spécifications pour le fichier journal, ni SDK, car le programme en est toujours au stade du développement. Après la diffusion du programme, nous fournirons ces éléments sur la base des commentaires et des demandes des clients.

### Comment ESET SysInspector évalue-t-il le risque que pose un objet en particulier ?

Dans la majorité des cas, ESET SysInspector attribue des niveaux de risque aux objets (fichiers, processus, clés de Registre, etc.) sur la base d'une série de règles heuristiques qui examinent les caractéristiques de chaque objet, puis qui évaluent le potentiel d'activité malveillante. Cette analyse heuristique attribue aux objets un niveau de risque allant de **1 - OK (vert)** à **9 - Risqué (rouge)**. Dans le volet de navigation gauche, la couleur des sections est définie par le niveau de risque le plus élevé d'un des objets qu'elles contiennent.

### Un niveau de risque « 6 - Inconnu (rouge) » signifie-t-il que l'objet est dangereux ?

Les évaluations de ESET SysInspector ne garantissent pas qu'un objet est malveillant. Cette réponse doit être apportée par l'expert en sécurité. ESET SysInspector a été développé pour fournir aux experts en sécurité une évaluation rapide afin qu'ils puissent identifier les objets d'un système qui devront faire l'objet d'un examen plus approfondi en cas de comportement étrange.

### Pourquoi ESET SysInspector se connecte-t-il à Internet ?

À l'instar de nombreuses applications, ESET SysInspector possède un « certificat » avec une signature numérique qui permet de garantir que le logiciel a bien été diffusé par ESET et qu'il n'a pas été modifié. Afin de vérifier le certificat, le système d'exploitation contacte une autorité de certification pour confirmer l'identité de l'éditeur de logiciels. Il s'agit d'un comportement normal pour tous les programmes avec signature numérique sous Microsoft Windows.

### Qu'est ce que la technologie Anti-Stealth ?

La technologie Anti-Stealth offre une détection efficace des rootkits.

Quand un système est attaqué par un code malveillant qui se comporte comme un rootkit, l'utilisateur est exposé à la perte ou au vol de données. Sans outil spécial de lutte contre les rootkits, il est pratiquement impossible de les détecter.

### Pourquoi y-a-t-il parfois des fichiers marqués comme « Signé par MS » avec une valeur différente dans le champ « Nom de la société » ?

Lorsque ESET SysInspector tente d'identifier la signature numérique d'un fichier exécutable, il vérifie d'abord si le fichier intègre une signature numérique. Si une signature numérique est détectée, le fichier est validé à l'aide de ces informations. Si aucune signature numérique n'est détectée, ESET SysInspector lance la recherche du fichier CAT correspondant (Catalogue de sécurité - %systemroot%\system32\catroot) qui contient les informations sur le fichier exécutable traité. Si le fichier CAT pertinent est trouvé, la signature numérique du fichier CAT est appliquée dans la procédure de validation du fichier exécutable.

C'est la raison pour laquelle les fichiers sont parfois marqués « Signé par MS » mais ont un « Nom de la société » différent.

Exemple :

Windows 2000 reprend l'application HyperTerminal qui se trouve dans *C:\Program Files\Windows NT*. Le fichier exécutable principal de l'application n'a pas de signature numérique, mais ESET SysInspector l'indique comme étant un fichier signé par Microsoft. Ceci s'explique par une référence dans *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* qui pointe vers *C:\Program Files\Windows NT\hypertrm.exe* (le fichier exécutable principal de l'application HyperTerminal) et *sp4.cat* possède une signature numérique de Microsoft.

### 5.5.6 ESET SysInspector en tant que partie de ESET NOD32 Antivirus

Pour ouvrir la section ESET SysInspector dans ESET NOD32 Antivirus, cliquez sur **Outils > ESET SysInspector**. Le système de gestion de la fenêtre ESET SysInspector est semblable à celui des journaux d'analyse des ordinateurs ou des tâches planifiées. Toutes les opérations effectuées avec des instantanés système (création, affichage, comparaison, suppression et exportation) sont accessibles en un ou deux clics.

La fenêtre ESET SysInspector contient les informations élémentaires concernant les instantanés créés : heure de création, bref commentaire, nom de l'utilisateur auteur de l'instantané et statut de l'instantané.

Pour comparer, créer ou supprimer des instantanés, utilisez les boutons correspondants situés en dessous de la liste des instantanés dans la fenêtre ESET SysInspector. Ces options sont également disponibles dans le menu contextuel. Pour afficher l'instantané du système sélectionné, sélectionnez l'option **Afficher** dans le menu contextuel. Pour exporter l'instantané sélectionné dans un fichier, cliquez dessus avec le bouton droit de la souris et sélectionnez **Exporter**.

Voici la description détaillée des options disponibles :

- **Comparer** : permet de comparer deux journaux. Elle est particulièrement adaptée si vous souhaitez effectuer le suivi des modifications entre le journal actuel et un ancien journal. Pour que cette option entre en vigueur, vous devez sélectionner deux instantanés à comparer.
- **Créer...** : crée un enregistrement. Vous devez d'abord saisir un bref commentaire concernant l'enregistrement. Pour consulter la progression de la création de l'instantané en cours, consultez la colonne **État**. Tous les instantanés terminés ont le statut **Créé**.
- **Supprimer/Supprimer tout** : supprime les entrées de la liste.
- **Exporter...** : cette option enregistre l'entrée sélectionnée dans un fichier XML (également dans une version compressée).

## 5.6 Ligne de commande

Le module antivirus d'ESET NOD32 Antivirus peut être lancé depuis la ligne de commande, manuellement (avec la commande « `ecls` ») ou au moyen d'un fichier de commandes (« `bat` »). Module d'interface à ligne de commande ESET :

```
ecls [OPTIONS...] FILES..
```

Les paramètres suivants peuvent être utilisés lors de l'exécution de l'analyseur à la demande, à partir de la ligne de commande :

### Options

<code>/base-dir=FOLDER</code>	charger les modules depuis le DOSSIER
<code>/quar-dir=FOLDER</code>	DOSSIER de quarantaine
<code>/exclude=MASK</code>	exclure les fichiers correspondant à MASQUE de l'analyse
<code>/subdir</code>	analyser les sous-dossiers (valeur par défaut)
<code>/no-subdir</code>	ne pas analyser les sous-dossiers
<code>/max-subdir-level=LEVEL</code>	sous-niveau maximal de sous-dossiers dans les dossiers à analyser
<code>/symlink</code>	suivre les liens symboliques (valeur par défaut)
<code>/no-symlink</code>	ignorer les liens symboliques
<code>/ads</code>	analyser ADS (valeur par défaut)
<code>/no-ads</code>	ne pas analyser ADS
<code>/log-file=FILE</code>	journaliser les résultats dans un FICHIER
<code>/log-rewrite</code>	écraser le fichier de résultats (valeur par défaut – append)
<code>/log-console</code>	journaliser les résultats sur la console (valeur par défaut)
<code>/no-log-console</code>	ne pas journaliser les résultats sur la console
<code>/log-all</code>	journaliser également les fichiers nettoyés
<code>/no-log-all</code>	ne pas journaliser les fichiers nettoyés (valeur par défaut)
<code>/auid</code>	afficher l'indicateur d'activité
<code>/auto</code>	analyser et nettoyer automatiquement tous les disques locaux

### Options de l'analyseur

<code>/files</code>	analyser les fichiers (valeur par défaut)
<code>/no-files</code>	ne pas analyser les fichiers
<code>/memory</code>	analyser la mémoire
<code>/boots</code>	analyser les secteurs d'amorçage
<code>/no-boots</code>	ne pas analyser les secteurs d'amorçage (valeur par défaut)
<code>/arch</code>	analyser les archives (valeur par défaut)
<code>/no-arch</code>	ne pas analyser les archives
<code>/max-obj-size=SIZE</code>	analyser uniquement les fichiers plus petits que TAILLE Mo (valeur par défaut 0 = illimité)
<code>/max-arch-level=LEVEL</code>	sous-niveau maximal d'archives à analyser dans les archives (archives imbriquées)
<code>/scan-timeout=LIMIT</code>	analyser les archives pendant un maximum de LIMITE secondes
<code>/max-arch-size=SIZE</code>	n'analyser les fichiers contenus dans une archive que s'ils sont plus petits que TAILLE (valeur par défaut 0 = illimité)
<code>/max-sfx-size=SIZE</code>	n'analyser les fichiers d'une archive auto-extractible que s'ils sont plus petits que TAILLE Mo (valeur par défaut 0 = illimité)
<code>/mail</code>	analyser les fichiers des courriers électroniques (valeur par défaut)
<code>/no-mail</code>	ne pas analyser les fichiers des courriers électroniques
<code>/mailbox</code>	analyser les boîtes aux lettres (valeur par défaut)
<code>/no-mailbox</code>	ne pas analyser les boîtes aux lettres
<code>/sfx</code>	analyser les archives auto-extractibles (valeur par défaut)
<code>/no-sfx</code>	ne pas analyser les archives auto-extractibles
<code>/rtp</code>	analyser les fichiers exécutables compressés par un compresseur d'exécutables (valeur par défaut)
<code>/no-rtp</code>	ne pas analyser les fichiers exécutables compressés

/unsafe	rechercher les applications potentiellement dangereuses
/no-unsafe	ne pas rechercher les applications potentiellement dangereuses (valeur par défaut)
/unwanted	rechercher les applications potentiellement indésirables
/no-unwanted	ne pas rechercher les applications potentiellement indésirables (valeur par défaut)
/suspicious	rechercher les applications suspectes (valeur par défaut)
/no-suspicious	ne pas rechercher les applications suspectes
/pattern	utiliser les signatures (valeur par défaut)
/no-pattern	ne pas utiliser les signatures
/heur	activer l'heuristique (valeur par défaut)
/no-heur	désactiver l'heuristique
/adv-heur	activer l'heuristique avancée (valeur par défaut)
/no-adv-heur	désactiver l'heuristique avancée
/ext=EXTENSIONS	analyser uniquement les EXTENSIONS délimitées par deux-points
/ext-exclude=EXTENSIONS	exclure de l'analyse les EXTENSIONS délimitées par deux-points
/clean-mode=MODE	utiliser le MODE de nettoyage pour les objets infectés
Les options disponibles sont les suivantes :	
<ul style="list-style-type: none"> <li>• <b>aucun nettoyage</b> – Aucun nettoyage automatique ne se produit.</li> <li>• <b>nettoyage standard</b> (valeur par défaut) – ecls.exe tente automatiquement de nettoyer ou de supprimer les fichiers infectés.</li> <li>• <b>nettoyage strict</b> – 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).</li> <li>• <b>nettoyage rigoureux</b> – ecls.exe supprime les fichiers sans tenter de les nettoyer, quel que soit leur type.</li> <li>• <b>suppression</b> – 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.</li> </ul>	
/quarantine	copier les fichiers infectés (si nettoyés) vers Quarantaine
/no-quarantine	(complète l'action effectuée lors du nettoyage) 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	certain fichiers n'ont pas pu être analysés (peuvent être des menaces)
50	menace détectée
100	erreur

### REMARQUE

un code sortie supérieur à 100 signale un fichier non analysé qui est potentiellement infecté.



## 6. Glossaire

### 6.1 Types d'infiltrations

Une infiltration est un élément de logiciel malveillant qui tente de s'introduire dans l'ordinateur d'un utilisateur et/ou de l'endommager.

#### 6.1.1 Virus

Un virus d'ordinateur est un fragment de code malveillant qui est ajouté à des fichiers qui sont sur votre ordinateur. Les virus informatiques sont comparables aux virus biologiques parce qu'ils utilisent des techniques similaires pour se propager d'un ordinateur à l'autre. Le terme « virus » est quant à lui souvent utilisé de manière abusive pour décrire tout type de menace. On tend à le remplacer progressivement par le terme « logiciel malveillant » ou « malware » en anglais.

Les virus informatiques attaquent principalement les fichiers et documents exécutables. En bref, un virus informatique fonctionne de la manière suivante : après l'exécution d'un fichier infecté, le code malveillant est appelé et exécuté avant l'exécution de l'application originale. Un virus peut infecter tous les fichiers pour lesquels l'utilisateur a des droits d'écriture.

Les virus peuvent varier en fonction de leur gravité et de leur cible. Certains sont extrêmement dangereux parce qu'ils ont la capacité de supprimer délibérément des fichiers du disque dur. D'autres, en revanche, ne causent pas de réels dommages : ils ne servent qu'à gêner l'utilisateur et à démontrer les compétences techniques de leurs auteurs.

Si votre ordinateur est infecté par un virus et qu'il est impossible de le nettoyer, soumettez-le au laboratoire de recherche ESET pour examen. Dans certains cas, les fichiers infectés peuvent avoir subi des modifications telles, qu'il est impossible de les nettoyer. Il faut alors les remplacer par une copie propre.

#### 6.1.2 Vers

Un ver est un programme contenant un code malveillant qui attaque les ordinateurs hôtes et se propage via un réseau. La différence fondamentale entre les virus et les vers réside dans le fait que les vers ont la capacité de se propager par eux-mêmes. Ils ne dépendent pas des fichiers hôtes (ou des secteurs d'amorçage). Les vers se propagent par l'intermédiaire des adresses de messagerie de votre liste de contacts ou exploitent les vulnérabilités de sécurité des applications réseau.

Les vers sont ainsi susceptibles de vivre beaucoup plus longtemps que les virus. Par le biais d'Internet, ils peuvent se propager à travers le monde en quelques heures seulement et parfois en quelques minutes. Leur capacité à se répliquer indépendamment et rapidement les rend plus dangereux que les autres types de programmes malveillants.

Un ver activé dans un système peut être à l'origine de plusieurs dérèglements : il peut supprimer des fichiers, dégrader les performances du système ou même désactiver certains programmes. Par nature, il peut servir de « moyen de transport » à d'autres types d'infiltrations.

Si votre ordinateur est infecté par un ver, il est recommandé de supprimer les fichiers infectés, car ils contiennent probablement du code malveillant.

### 6.1.3 Chevaux de Troie

Les chevaux de Troie ont été définis comme une catégorie de menaces dont la particularité est de se présenter comme des programmes utiles pour duper ensuite les utilisateurs qui acceptent de les exécuter.

La catégorie étant très vaste, elle est souvent divisée en plusieurs sous-catégories :

- **Téléchargeur** – Programmes malveillants qui sont en mesure de télécharger d'autres menaces sur Internet.
- **Dropper** – Programmes malveillants qui sont en mesure de déposer d'autres types de logiciels malveillants sur des ordinateurs infectés.
- **Backdoor** – Programmes malveillants qui communiquent avec des pirates distants, leur permettant d'accéder à l'ordinateur et d'en prendre le contrôle.
- **Keylogger** – Programme qui enregistre chaque touche sur laquelle tape l'utilisateur et envoie les informations aux pirates.
- **Composeur** – Programmes malveillants destinés à se connecter à des numéros surtaxés au lieu du fournisseur de services Internet de l'utilisateur. Il est presque impossible qu'un utilisateur remarque la création d'une nouvelle connexion. Les composeurs ne peuvent porter préjudice qu'aux utilisateurs ayant des modems par ligne commutée, qui sont de moins en moins utilisés.

Si un fichier est identifié comme cheval de Troie sur votre ordinateur, il est recommandé de le supprimer, car il est fort probable qu'il ne contienne rien d'autre que du code malveillant.

### 6.1.4 Rootkits

Les rootkits sont des programmes malveillants qui procurent aux pirates un accès illimité à un système tout en dissimulant leur présence. Après avoir accédé au système (généralement en exploitant une faille), les rootkits utilisent des fonctions du système d'exploitation pour se protéger des logiciels antivirus : ils dissimulent des processus, des fichiers et des données de la base de registre Windows. Pour cette raison, il est presque impossible de les détecter à l'aide des techniques de test ordinaires.

Il existe deux niveaux de détection permettant d'éviter les rootkits :

1. Lorsqu'ils essaient d'accéder au système : Ils ne sont pas encore installés et donc inactifs. La plupart des antivirus sont en mesure d'éliminer les rootkits à ce niveau (en supposant qu'ils détectent effectivement les fichiers comme infectés).
2. Lorsqu'ils sont inaccessibles aux tests habituels : Les utilisateurs ESET NOD32 Antivirus bénéficient de la technologie Anti-Stealth qui permet de détecter et d'éliminer les rootkits en activité.

### 6.1.5 Logiciels publicitaires

Le terme anglais « adware » désigne les logiciels soutenus par la publicité. Les programmes qui affichent des publicités entrent donc dans cette catégorie. Les logiciels publicitaires ouvrent généralement une nouvelle fenêtre contextuelle automatiquement dans un navigateur Internet. Cette fenêtre contient de la publicité ou modifie la page de démarrage du navigateur. Ils sont généralement associés à des programmes gratuits et permettent aux développeurs de couvrir les frais de développement de leurs applications (souvent utiles).

Les logiciels publicitaires en tant que tels ne sont pas dangereux ; ils dérangent simplement les utilisateurs en affichant des publicités. Le danger réside dans le fait qu'ils peuvent également avoir des fonctions d'espionnage (comme les logiciels espions).

Si vous décidez d'utiliser un logiciel gratuit, soyez particulièrement attentif au programme d'installation. La plupart des programmes d'installation vous avertissent en effet qu'ils installent également un programme publicitaire. Dans la plupart des cas, vous pourrez désactiver cette installation supplémentaire et installer le programme sans logiciel publicitaire.

Certains programmes refusent de s'installer sans leur logiciel publicitaire ou voient leurs fonctionnalités limitées. Cela signifie que les logiciels publicitaires accèdent souvent au système de manière « légale », dans la mesure où les utilisateurs l'ont accepté. Dans ce cas, il est préférable de procéder avec prudence. Si un logiciel publicitaire est détecté sur votre ordinateur, il est conseillé de le supprimer, car il est fort probable qu'il contienne du code malveillant.

### 6.1.6 Logiciels espions

Cette catégorie englobe toutes les applications qui envoient des informations confidentielles sans le consentement des utilisateurs et à leur insu. Les logiciels espions utilisent des fonctions de traçage pour envoyer diverses données statistiques telles que la liste des sites Web visités, les adresses e-mail de la liste de contacts de l'utilisateur ou la liste des touches du clavier utilisées.

Les auteurs de ces logiciels espions affirment que ces techniques ont pour but d'en savoir plus sur les besoins et intérêts des utilisateurs afin de mieux cibler les offres publicitaires. Le problème est qu'il n'y a pas de distinction claire entre les applications utiles et les applications malveillantes, et que personne ne peut garantir que les informations récupérées ne sont pas utilisées à des fins frauduleuses. Les données récupérées par les logiciels espions peuvent être des codes de sécurité, des codes secrets, des numéros de compte bancaire, etc. Les logiciels espions sont souvent intégrés aux versions gratuites d'un programme dans le but de générer des gains ou d'inciter à l'achat du logiciel. Les utilisateurs sont souvent informés de la présence d'un logiciel espion au cours de l'installation d'un programme qui vise à les inciter à acquérir la version payante qui en est dépourvue.

Parmi les produits logiciels gratuits bien connus qui contiennent des logiciels espions, on trouve les applications clients de réseaux P2P (poste à poste). Spyfalcon ou Spy Sheriff (et beaucoup d'autres) appartiennent à une sous-catégorie spécifique de logiciels espions : ils semblent être des programmes antispyware alors qu'ils sont en réalité eux-mêmes des logiciels espions.

Si un fichier est détecté comme logiciel espion sur votre ordinateur, il est préférable de le supprimer, car il est fort probable qu'il contienne du code malveillant.

### 6.1.7 Compresseurs

Le compresseur est un fichier exécutable auto-extractible qui regroupe plusieurs genres de programmes malveillants dans un seul package.

Les compresseurs les plus courants sont UPX, PE\_Compact, PKLite et ASPack. Le même programme malveillant peut être détecté différemment lorsqu'il est compressé à l'aide d'un compresseur différent. Les compresseurs sont capables de faire muter leur « signature » au fil du temps, les programmes malveillants deviennent ainsi plus difficiles à détecter et à supprimer.

### 6.1.8 Applications potentiellement dangereuses

Il existe de nombreux programmes authentiques qui permettent de simplifier l'administration des ordinateurs en réseau. Toutefois, s'ils tombent entre de mauvaises mains, ces programmes sont susceptibles d'être utilisés à des fins malveillantes. ESET NOD32 Antivirus permet de détecter ces menaces.

**Applications potentiellement dangereuses** est la classification utilisée pour les logiciels commerciaux légitimes. Cette classification comprend les programmes d'accès à distance, les applications de résolution de mot de passe ou les keyloggers (programmes qui enregistrent chaque frappe au clavier de l'utilisateur).

Si vous découvrez qu'une application potentiellement dangereuse est présente et fonctionne sur votre ordinateur (sans que vous ne l'ayez installée), consultez l'administrateur réseau ou supprimez l'application.

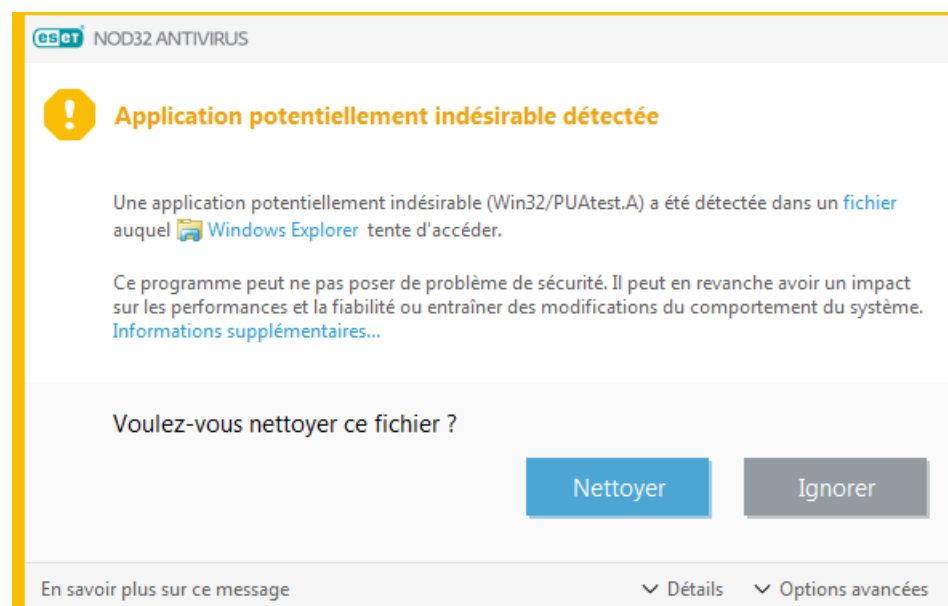
### 6.1.9 Applications potentiellement indésirables

Une application potentiellement indésirable est un programme qui contient un logiciel publicitaire, qui installe des barres d'outils ou dont les objectifs ne sont pas clairs. Dans certains cas, un utilisateur peut estimer que les avantages offerts par une application potentiellement indésirable dépassent de loin les risques. Pour cette raison, ESET classe les applications de ce type dans une catégorie à faible risque par rapport aux autres types de logiciels malveillants (chevaux de Troie ou vers, par exemple).

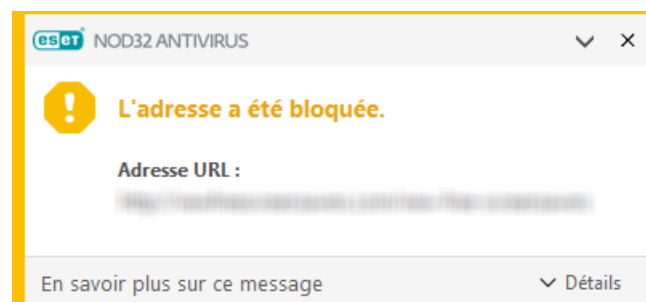
#### Avertissement - Menace potentielle détectée

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

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



Si une application potentiellement indésirable est détectée et si elle ne peut pas être nettoyée, la notification **L'adresse a été bloquée** s'affiche. Pour plus d'informations sur cet événement, accédez à **Outils > Fichiers journaux > Sites Web filtrés** dans le menu principal.



## Applications potentiellement indésirables - Paramètres

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



The screenshot shows the ESET NOD32 ANTIVIRUS installation window. At the top, the ESET logo and 'NOD32 ANTIVIRUS' are displayed. Below the title bar, there is a section titled 'L'union fait la force. Bénéficiez du niveau maximal de protection.' followed by a paragraph explaining the ESET LiveGrid system. A checkbox is checked, labeled 'Activer le système de commentaires ESET LiveGrid® (recommandé)'. Below this, a section titled 'Détection des applications potentiellement indésirables' contains a paragraph explaining that ESET can detect potentially unwanted applications and request confirmation before installation. Two radio buttons are present: 'Activer la détection d'applications potentiellement indésirables' (which is selected) and 'Désactiver la détection d'applications potentiellement indésirables'. At the bottom, there are two buttons: 'Installer' and 'Modifier le dossier d'installation'.

### AVERTISSEMENT

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

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

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

# Configuration avancée

x
?

ANTIVIRUS 2

Protection en temps réel du système de fichiers

Analyse de l'ordinateur à la demande

Analyse en cas d'inactivité

Analyse au démarrage

Périphériques amovibles

Protection des documents

HIPS 3

MISE À JOUR 2

INTERNET ET MESSAGERIE 3

CONTRÔLE DE PÉRIPHÉRIQUE 1

OUTILS

INTERFACE UTILISATEUR

GÉNÉRAL

OPTION DU MOTEUR D'ANALYSE

Activer la détection d'applications potentiellement indésirables

☐
x
i

Activer la détection d'applications potentiellement dangereuses

☐
x
i

Activer la détection des applications suspectes

☒
i

Activer l'analyse initiale

☐
x
i

ANTI-STEALTH

Activer la technologie Anti-Stealth

☒
i

EXCLUSIONS

Chemins d'accès à exclure de l'analyse

Modifier

i

Par défaut

OK

Annuler

## Applications potentiellement indésirables - Wrappers logiciels

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

Consultez cet [article de la base de connaissances ESET](#) pour obtenir une version mise à jour de cette page d'aide.

## 6.2 Technologie ESET

### 6.2.1 Bloqueur d'exploit

Le bloqueur d'exploit est conçu pour renforcer les types d'applications connues pour être très vulnérables aux exploits (navigateurs, lecteurs de fichiers PDF, clients de messagerie et composants MS Office). Il surveille le comportement des processus et recherche toute activité suspecte pouvant indiquer un exploit.

Lorsqu'il identifie un processus suspect, le bloqueur d'exploit peut arrêter ce processus immédiatement. Il enregistre les données concernant la menace et les envoie au système ThreatSense dans le cloud. Ces données sont traitées par le laboratoire de recherche ESET et permettent de mieux protéger tous les utilisateurs contre les menaces inconnues et les attaques immédiates (logiciels malveillants très récents n'ayant encore aucun remède préconfiguré).

### 6.2.2 Scanner de mémoire avancé

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 et/ou au chiffrement. Dans les cas où l'émulation ou l'heuristique classique ne détecte pas la menace, le scanner de mémoire avancé est en mesure d'identifier le comportement suspect et il analyse les menaces lorsqu'elles apparaissent dans la mémoire système. Cette solution est efficace même sur les logiciels malveillants fortement obscurcis.

Contrairement au bloqueur d'exploit, le scanneur de mémoire avancé est une méthode ultérieure à l'exécution. Cela signifie que des activités malveillantes ont pu avoir le temps de s'exécuter avant que cette menace soit détectée. Toutefois, si les autres techniques de détection ont échoué, il apporte une couche supplémentaire de sécurité.

### 6.2.3 ESET LiveGrid®

Conçu sur le système d'avertissement anticipé de ThreatSense.Net®, ESET LiveGrid® collecte les données soumises par les utilisateurs ESET du monde entier avant de les envoyer au laboratoire de recherche ESET. En fournissant des métadonnées et des exemples suspects, ESET LiveGrid® vous permet de réagir immédiatement aux besoins de nos clients et à ESET de répondre aux dernières menaces. Les chercheurs ESET spécialisés dans les logiciels malveillants utilisent ces informations pour concevoir un instantané précis de la nature et de l'ampleur des menaces. Nous pouvons alors nous concentrer sur les cibles pertinentes. Les données ESET LiveGrid® jouent un rôle important dans la configuration des priorités de notre traitement automatisé.

Par ailleurs, elles permettent de mettre en œuvre un système de réputation qui améliore l'efficacité globale de nos solutions anti-logiciels malveillants. Lorsqu'une archive ou un fichier exécutable est inspecté sur le système d'un ordinateur, son hash tag est d'abord comparé à une base de données d'éléments répertoriés sur une liste noire et une liste blanche. S'il figure dans la liste blanche, le fichier inspecté est considéré comme étant nettoyé et il est identifié de manière à être exclu des prochaines analyses. S'il figure dans la liste noire, les mesures appropriées sont prises en fonction de la nature de la menace. Si aucune correspondance n'est trouvée, le fichier est analysé intégralement. En fonction des résultats de cette analyse, les fichiers sont classés comme menaces ou non-menaces. Cette approche améliore considérablement les performances des analyses.

Ce système de réputation améliore l'efficacité de la détection des exemples de logiciels malveillants, avant même que leur signature atteigne l'ordinateur de l'utilisateur par l'intermédiaire de la base de signatures de virus mise à jour (cette opération s'effectue plusieurs fois par jour).

### 6.2.4 Bloqueur d'exploit Java

Le Bloqueur d'exploit Java est une extension de la protection du Bloqueur d'exploit existant. Il surveille Java et recherche les comportements de type exploit. Les échantillons bloqués peuvent être signalés aux analystes de logiciels malveillants pour leur permettre de créer des signatures afin de les bloquer sur différentes couches (blocage d'URL, téléchargement de fichiers, etc.).

### 6.2.5 Protection contre les attaques basées sur des scripts

La protection contre les attaques basées sur des scripts comprend une protection contre les scripts JavaScript dans les navigateurs Web et une protection AMSI (Antimalware Scan Interface) contre les scripts dans PowerShell.



#### AVERTISSEMENT

Pour que cette fonctionnalité puisse être utilisée, le système HIPS doit être activé.

La protection contre les attaques basées sur des scripts prend en charge les navigateurs Web suivants :

- Mozilla Firefox
- Google Chrome
- Internet Explorer
- Microsoft Edge

#### REMARQUE

Les versions postérieures prises en charge des navigateurs Web peuvent varier en raison de la modification fréquente de la signature de fichier des navigateurs. La version la plus récente du navigateur Web est toujours prise en charge.

### 6.2.6 Protection antirangiciels

Un rançongiciel est un type de logiciel malveillant qui empêche les utilisateurs d'accéder à leur système en verrouillant l'écran de celui-ci ou en chiffrant les fichiers. La protection antirangiciels permet de surveiller le comportement des applications et des processus qui tentent de modifier vos informations personnelles. Si le comportement d'une application est considéré comme malveillant ou si une analyse basée sur la réputation indique qu'une application est malveillante, celle-ci est bloquée ou l'utilisateur se voit [demander](#) de la bloquer ou de l'activer.

#### IMPORTANT

Pour que la protection antirangiciels fonctionne correctement, ESET Live Grid doit être activé.

## 6.3 Courrier électronique

Le courrier électronique est une forme de communication moderne qui offre beaucoup d'avantages. Adaptable, rapide et direct, il a joué un rôle crucial dans l'expansion d'Internet au début des années 90.

Malheureusement, le grand anonymat des courriers électroniques et Internet a laissé libre champ aux activités illégales telles que le « spamming » (le fait d'envoyer des messages indésirables à un grand nombre de personnes). Les courriers indésirables comprennent les publicités indésirables, les canulars et les logiciels malveillants. Les désagréments et le danger augmentent, car l'envoi de tels messages ne coûte rien et les auteurs de courrier indésirable disposent de nombreux outils qui leur permettent de se procurer facilement de nouvelles adresses de messagerie. Par ailleurs, le volume et la variété du courrier indésirable ne facilitent pas la réglementation. Plus vous utilisez votre adresse de messagerie, plus vous augmentez la possibilité d'aboutir dans un moteur de base de données de courrier indésirable. Voici quelques conseils de prévention :

- Évitez de publier votre adresse de messagerie sur Internet.
- Ne donnez votre adresse de messagerie qu'à des personnes fiables.
- Évitez d'utiliser des pseudonymes communs : un pseudonyme compliqué est moins susceptible d'être traqué.
- Ne répondez pas au courrier indésirable qui est arrivé dans votre boîte de réception.
- Faites attention lorsque vous remplissez des formulaires sur Internet : soyez particulièrement attentif aux options du type « Oui, je voudrais recevoir des informations concernant ... ».
- Utilisez des adresses de messagerie « spécialisées », par exemple une adresse pour votre travail, une autre pour communiquer avec vos amis, etc.
- Changez vos adresses de messagerie de temps en temps.
- Utilisez une solution antispam.

### 6.3.1 Publicités

La publicité via Internet est une des formes de publicité les plus en vogue. D'un point de vue marketing, la publicité présente plusieurs avantages : ses coûts sont minimes, elle est très directe et les messages sont transmis presque immédiatement. De nombreuses entreprises utilisent des outils de marketing par courrier électronique pour communiquer de manière efficace avec leurs clients et prospects.

Ce mode de publicité est légitime, car vous pourriez être intéressé par la réception d'informations commerciales sur certains produits. Toutefois, de nombreuses entreprises envoient des masses de messages commerciaux non sollicités. La publicité par e-mail dépasse alors les limites et devient du courrier indésirable, ou spam.

La quantité de messages publicitaires non sollicités est devenue un réel problème, car elle ne montre aucun signe de ralentissement. Les auteurs de messages non sollicités tentent souvent de déguiser le courrier indésirable sous des dehors de messages légitimes.



### 6.3.2 Canulars

Un canular (ou hoax) est un message propagé sur Internet. Il est envoyé généralement avec le courrier et parfois par des outils de communication tels que ICQ et Skype. Le message est souvent une blague ou une légende urbaine.

Les canulars essaient de provoquer chez les destinataires de la peur, de l'incertitude et du doute, les amenant à croire qu'un « virus indétectable » supprime tous les fichiers et récupère les mots de passe, ou effectue une activité nuisible sur leur système.

Certains canulars demandent aux destinataires de transmettre des messages à leurs contacts, ce qui a pour conséquence de propager les canulars. Même les téléphones portables reçoivent des canulars et des demandes d'aide (des personnes proposant par exemple de vous envoyer de l'argent depuis l'étranger). Il est souvent impossible de déterminer l'intention du créateur.

Si un message vous demande de le faire suivre à toutes vos connaissances, il peut très bien s'agir d'un canular. Sur Internet, de nombreux sites spécialisés peuvent vérifier la légitimité d'un courrier. Avant de retransmettre un message que vous soupçonnez d'être un canular, faites d'abord une recherche sur Internet à son sujet.

### 6.3.3 Hameçonnage

Le terme d'hameçonnage (phishing en anglais) désigne une activité frauduleuse utilisant des techniques de piratage psychologique qui consistent à manipuler les utilisateurs pour obtenir des informations confidentielles. Son but est d'accéder à des données sensibles, telles que numéros de comptes bancaires, codes secrets, etc.

La technique consiste généralement à envoyer un message électronique en se faisant passer pour une personne ou une entreprise digne de confiance (institution financière, compagnie d'assurance par exemple). Le message peut sembler tout à fait authentique et contenir des graphiques et contenus qui proviennent véritablement de la source dont il se réclame. Vous êtes invité à entrer, sous divers prétextes (vérification de données, opérations financières), certaines de vos données personnelles : numéros de compte en banque ou noms d'utilisateur et mots de passe. Toutes ces données, si elles sont soumises, peuvent facilement être volées et utilisées à des fins illégales.

Les banques, compagnies d'assurance et autres sociétés légales ne demandent jamais de noms d'utilisateur et de mots de passe dans un message non sollicité.

## 7. Questions fréquentes

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

[Comment mise à jour ESET NOD32 Antivirus](#)

[Comment éliminer un virus de mon PC](#)

[Comment créer une tâche dans le Planificateur](#)

[Comment programmer une tâche d'analyse \(toutes les 24 heures\)](#)

Si votre problème n'est pas abordé dans la liste de pages d'aide ci-dessus, consultez les pages d'aide de ESET NOD32 Antivirus.

Si vous ne trouvez pas la solution à votre problème/question dans les pages d'aide, vous pouvez consulter notre [base de connaissances ESET](#) en ligne qui est régulièrement mise à jour. Des liens vers les articles les plus populaires de notre base de connaissances sont mentionnés ci-dessous afin de vous aider à résoudre les problèmes courants :

[J'ai reçu un message d'erreur d'activation pendant l'installation de mon produit ESET. Qu'est-ce que cela signifie ?](#)

[Activer mon produit ESET Windows pour les particuliers à l'aide de mon nom d'utilisateur, de mon mot de passe ou de ma clé de licence](#)

[Désinstaller ou réinstaller mon produit ESET pour les particuliers](#)

[Un message m'indique que l'installation de mon produit ESET s'est terminée prématurément.](#)

[Que dois-je faire après avoir renouvelé ma licence ? \(utilisateurs de la version familiale\)](#)

[Que faire si je change d'adresse de messagerie ?](#)

[Comment démarrer Windows en mode sans échec ou en mode sans échec avec réseau](#)

Au besoin, vous pouvez contacter notre service client pour soumettre vos questions ou problèmes. Le formulaire de contact est disponible dans l'onglet **Aide et support** de ESET NOD32 Antivirus.

### 7.1 Comment mise à jour ESET NOD32 Antivirus

La mise à jour de ESET NOD32 Antivirus peut être effectuée manuellement ou automatiquement. Pour déclencher la mise à jour, cliquez sur **Mise à jour maintenant** dans la section **Mise à jour**.

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

### 7.2 Comment éliminer un virus de mon PC

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

## 7.3 Comment créer une tâche dans le Planificateur

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

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

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

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

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

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

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

## 7.4 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 24 heures. Consultez notre [article de base de connaissances](#) pour obtenir des instructions plus détaillées.

Pour programmer une tâche d'analyse :

1. Cliquez sur **Ajouter** dans l'écran principal du planificateur.
2. Sélectionnez **Analyse de l'ordinateur à la demande** dans le menu déroulant.
3. Saisissez un nom pour la tâche et sélectionnez **Chaque semaine** pour la fréquence de tâche.
4. Choisissez le jour et l'heure d'exécution de la tâche.
5. Sélectionnez **Exécuter la tâche dès que possible** pour exécuter la tâche plus tard si la tâche programmée ne s'exécute pas pour quelque raison que ce soit (par exemple, si l'ordinateur a été mis hors tension).

6. Passez en revue le résumé de la tâche planifiée, puis cliquez sur **Terminer**.
7. Dans le menu déroulant **Cibles**, sélectionnez **Disques locaux**.
8. Cliquez sur **Terminer** pour appliquer la tâche.