

ESET **NOD32 ANTIVIRUS 5**

Guide de l'utilisateur

(versions 5.0 et ultérieures)

Microsoft® Windows® 7 / Vista / XP / 2000 / Home Server / NT4 (SP6)

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

ESET **NOD32 Antivirus**

Copyright ©2011 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.

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/contact

RÉV. 9/8/2011

Table des

1. ESET NOD32 Antivirus 5.....	5
1.1 Nouveautés.....	5
1.2 Configuration système.....	6
1.3 Prévention.....	6
2. Installation.....	8
2.1 Installation standard.....	9
2.2 Installation personnalisée.....	11
2.3 Mise à niveau vers une version plus récente.....	14
2.4 Saisie du nom d'utilisateur et du mot de passe.....	15
2.5 Analyse d'ordinateur.....	16
3. Guide du débutant.....	17
3.1 Présentation de l'interface utilisateur.....	17
3.2 Que faire lorsque le programme ne fonctionne pas correctement ?.....	18
3.3 Configuration des mises à jour.....	19
3.4 Configuration du serveur proxy.....	20
3.5 Protection des paramètres.....	21
4. Utiliser ESET NOD32 Antivirus.....	22
4.1 Ordinateur.....	23
4.1.1 Protection antivirus et antispyware.....	24
4.1.1.1 Protection en temps réel du système de fichiers.....	24
4.1.1.1.1 Supports à analyser.....	25
4.1.1.1.2 Analyser quand (analyse déclenchée par un événement).....	25
4.1.1.1.3 Options d'analyse avancées.....	25
4.1.1.1.4 Niveaux de nettoyage.....	25
4.1.1.1.5 Quand faut-il modifier la configuration de la protection en temps réel.....	26
4.1.1.1.6 Vérification de la protection en temps réel.....	26
4.1.1.1.7 Que faire si la protection en temps réel ne fonctionne pas ?.....	26
4.1.1.2 Protection des documents.....	27
4.1.1.3 Analyse d'ordinateur.....	28
4.1.1.3.1 Type d'analyse.....	28
4.1.1.3.1.1 Analyse intelligente.....	28
4.1.1.3.1.2 Analyse personnalisée.....	29
4.1.1.3.2 Cibles à analyser.....	29
4.1.1.3.3 Profils d'analyse.....	29
4.1.1.3.4 Progression de l'analyse.....	30
4.1.1.4 Analyse au démarrage.....	31
4.1.1.5 Exclusions.....	32
4.1.1.6 Configuration des paramètres du moteur ThreatSense.....	33
4.1.1.6.1 Objets.....	33
4.1.1.6.2 Options.....	34
4.1.1.6.3 Nettoyage.....	34
4.1.1.6.4 Extension.....	35
4.1.1.6.5 Limites.....	35
4.1.1.6.6 Autre.....	36
4.1.1.7 Une infiltration est détectée.....	36
4.1.2 Analyse et blocage de supports amovibles.....	37
4.1.3 Système HIPS (Host Intrusion Prevention System).....	38
4.2 Internet et messagerie.....	40
4.2.1 Protection de l'accès au Web.....	40
4.2.1.1 HTTP, HTTPS.....	41
4.2.1.1.1 Mode actif pour les navigateurs Web.....	41
4.2.1.2 Gestion d'adresse URL.....	42
4.2.2 Protection du client de messagerie.....	44
4.2.2.1 Filtre POP3, POP3S.....	45
4.2.2.2 Contrôle de protocole IMAP, IMAPS.....	46
4.2.2.3 Intégration aux clients de messagerie.....	46
4.2.2.3.1 Configuration de la protection du client de messagerie.....	47
4.2.2.4 Suppression d'infiltrations.....	48
4.2.3 Filtrage des protocoles.....	48
4.2.3.1 Applications exclues.....	49
4.2.3.2 Adresses exclues.....	50
4.2.3.3 Contrôle de protocole SSL.....	50
4.2.3.3.1 Certificats.....	51
4.2.3.3.1.1 Certificats approuvés.....	52
4.2.3.3.1.2 Certificats exclus.....	52
4.3 Mise à jour du programme.....	52
4.3.1 Configuration des mises à jour.....	56
4.3.1.1 Profils de mise à jour.....	57
4.3.1.2 Configuration avancée des mises à jour.....	57
4.3.1.2.1 Mode de mise à jour.....	57
4.3.1.2.2 Serveur proxy.....	58
4.3.1.2.3 Connexion au réseau local.....	60
4.3.2 Comment créer des tâches de mise à jour.....	61
4.4 Outils.....	61
4.4.1 Fichiers journaux.....	62
4.4.1.1 Maintenance des journaux.....	63
4.4.2 Planificateur.....	64
4.4.2.1 Création de nouvelles tâches.....	67
4.4.3 Statistiques de protection.....	68
4.4.4 Quarantaine.....	69
4.4.4.1 Mise en quarantaine de fichiers.....	69
4.4.4.2 Restauration depuis la quarantaine.....	69
4.4.4.3 Soumission de fichiers de quarantaine.....	70
4.4.5 Surveiller l'activité.....	71
4.4.6 ESET SysInspector.....	71
4.4.7 Processus en cours.....	72
4.4.7.1 ESET Live Grid.....	73
4.4.7.1.1 Fichiers suspects.....	74
4.4.8 Soumission de fichiers pour analyse.....	75
4.4.9 Mises à jour système.....	75
4.4.10 Diagnostics.....	75
4.5 Interface utilisateur.....	76
4.5.1 Graphiques.....	76
4.5.2 Alertes et notifications.....	77
4.5.2.1 Configuration avancée.....	78
4.5.3 Fenêtres de notification masquées.....	78
4.5.4 Configuration de l'accès.....	79
4.5.5 Menu contextuel.....	79
4.5.6 Mode joueur.....	80
5. Utilisateur chevronné.....	81
5.1 Configuration du serveur proxy.....	81
5.2 Importer et exporter les paramètres.....	82
5.3 Raccourcis clavier.....	83
5.4 Ligne de commande.....	83
5.5 ESET SysInspector.....	84
5.5.1 Introduction à ESET SysInspector.....	84
5.5.1.1 Démarrage d'ESET SysInspector.....	85
5.5.2 Interface utilisateur et utilisation de l'application.....	85
5.5.2.1 Contrôles du programme.....	85
5.5.2.2 Navigation dans ESET SysInspector.....	87
5.5.2.3 Comparer.....	88
5.5.3 Paramètres de la ligne de commande.....	89
5.5.4 Script de service.....	89
5.5.4.1 Création d'un script de service.....	89
5.5.4.2 Structure du script de service.....	90
5.5.4.3 Exécution des scripts de services.....	92
5.5.5 Raccourcis.....	92
5.5.6 Configuration système.....	94

5.5.7	FAQ	94
5.5.8	ESET SysInspector en tant que composant de ESET NOD32 Antivirus.....	95
5.6	ESET SysRescue.....	96
5.6.1	Configuration minimale requise	96
5.6.2	Procédure de création d'un CD de dépannage	96
5.6.3	Sélection de la cible	96
5.6.4	Paramètres.....	97
5.6.4.1	Dossiers.....	97
5.6.4.2	ESET Antivirus.....	97
5.6.4.3	Paramètres avancés.....	98
5.6.4.4	Protocole Internet.....	98
5.6.4.5	Périphérique USB d'amorçage.....	98
5.6.4.6	Graver	98
5.6.5	Travailler avec ESET SysRescue	99
5.6.5.1	Travailler avec ESET SysRescue.....	99
6.	Glossaire.....	100
6.1	Types d'infiltrations.....	100
6.1.1	Virus	100
6.1.2	Vers	100
6.1.3	Chevaux de Troie.....	101
6.1.4	Rootkits.....	101
6.1.5	Logiciels publicitaires.....	101
6.1.6	Logiciels espions.....	102
6.1.7	Applications potentiellement dangereuses.....	102
6.1.8	Applications potentiellement indésirables.....	102
6.2	Courrier électronique.....	103
6.2.1	Publicités.....	103
6.2.2	Canulars.....	103
6.2.3	Hameçonnage.....	104
6.2.4	Reconnaissance du courrier indésirable.....	104

1. ESET NOD32 Antivirus 5

ESET NOD32 Antivirus 5 représente une nouvelle approche de sécurité informatique véritablement intégrée. La dernière version du moteur d'analyse ThreatSense® fait appel à la vitesse et à la précision pour maintenir votre ordinateur en sécurité. Le résultat est un système intelligent et constamment en alerte, qui protège votre ordinateur des attaques et des programmes malveillants.

ESET NOD32 Antivirus 5 est une solution complète de sécurité ; c'est le résultat d'un effort de longue haleine qui associe protection maximale et encombrement minimal. Des technologies avancées basées sur l'intelligence artificielle sont capables de faire barrage de manière proactive à l'infiltration de virus, de logiciels espions, de chevaux de Troie, de vers, de logiciels publicitaires, de rootkits et d'autres attaques provenant d'Internet, sans réduire les performances ni perturber votre ordinateur.

1.1 Nouveautés

HIPS

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, afin de bloquer activement et d'empêcher toute tentative de ce type.

ESET Live Grid

ESET Live Grid est un système d'avertissement anticipé avancé qui vous protège des nouvelles menaces en fonction de la réputation. Le laboratoire ESET utilise le flux en temps réel d'informations concernant les menaces issues du service de cloud computing pour maintenir les défenses à jour. Vous bénéficiez d'un niveau de protection constant. L'utilisateur peut prendre connaissance de la réputation des processus et des fichiers en cours depuis l'interface du programme ou à partir d'un menu contextuel comprenant des informations supplémentaires mises à disposition par ESET Live Grid. Le programme indique le niveau de risque de chaque élément, ainsi que le nombre d'utilisateurs et l'heure de la première détection.

Contrôle des supports amovibles

ESET NOD32 Antivirus permet de contrôler les supports amovibles (CD/DVD/USB/...). Ce module permet d'analyser, de bloquer ou d'ajuster les filtres étendus/autorisations, et de contrôler la façon dont l'utilisateur peut accéder à un périphérique pour l'utiliser. Ce procédé peut être utile si l'administrateur souhaite empêcher les utilisateurs d'insérer des supports amovibles stockant du contenu non sollicité.

Mode joueur

Le mode joueur est une fonctionnalité destinée aux joueurs qui ne veulent pas être interrompus lors de l'utilisation de leur jeu. Ils ne souhaitent pas être dérangés par des fenêtres contextuelles et veulent réduire l'utilisation du processeur. Le mode joueur peut également être utilisé en tant que mode de présentation, ce qui permet d'éviter toute interruption 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.

Rechercher les mises à jour du produit

Outre les mises à jour de la base des signatures de virus et des modules de programme, ESET NOD32 Antivirus peut également être configuré pour vérifier régulièrement la dernière version du produit. Au cours de l'installation, si vous utilisez un package ancien, vous pouvez choisir de télécharger et d'installer automatiquement la dernière version de ESET NOD32 Antivirus.

Nouvelle conception

La fenêtre principale ESET NOD32 Antivirus entièrement repensée et la configuration avancée plus intuitive simplifient la navigation.

1.2 Configuration système

Pour garantir le fonctionnement correct d'ESET NOD32 Antivirus, le système doit répondre à la configuration suivante :

Windows 2000, XP

400 MHz 32 bits (x86)/64 bits (x64)
128 Mo de RAM de mémoire système
320 Mo d'espace disponible
Super VGA (800 x 600)

Windows 7, Vista

1 GHz 32 bits (x86)/64 bits (x64)
512 Mo de RAM de mémoire système
320 Mo d'espace disponible
Super VGA (800 x 600)

1.3 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 lié aux [infiltrations et attaques](#). Pour bénéficier d'une protection maximale, il est essentiel d'utiliser le système antivirus correctement et de respecter quelques règles essentielles.

Mettre à jour régulièrement

Selon les statistiques de ESET Live Grid, des milliers de nouvelles infiltrations sont créées chaque jour pour contourner les dispositifs de sécurité existants et servir leurs auteurs, aux dépens des autres utilisateurs. Les spécialistes du laboratoire d'ESET analysent ces menaces chaque jour et conçoivent des mises à jour visant à améliorer en continu le niveau de protection des utilisateurs du programme antivirus. Une mise à jour mal configurée altère l'efficacité du programme. Pour plus d'informations sur la configuration des mises à jour, [cliquez ici](#).

Télécharger les patches de sécurité

Les auteurs de programmes malveillants préfèrent exploiter diverses failles du système pour assurer une meilleure propagation du code malveillant. C'est pourquoi les sociétés qui commercialisent des logiciels recherchent activement l'apparition de nouvelles failles dans leurs applications pour concevoir les mises à jour de sécurité permettant d'éliminer régulièrement les menaces potentielles. Il est important de télécharger ces mises à jour de sécurité au moment de leur sortie. Ces mises à jour concernent par exemple le système d'exploitation de Windows ou le navigateur Internet Explorer.

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 des dommages importants au niveau des données. Il est important de sauvegarder régulièrement vos données importantes et sensibles sur une source externe, telle que DVD ou 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

Une analyse automatique régulière de votre ordinateur avec les paramètres adéquats peut permettre de supprimer les infiltrations qui ont pu être ignorées si votre ordinateur comporte d'anciennes mises à jour de signatures de virus.

Suivre les règles de sécurité de base

Cette règle est la plus utile et la plus efficace de toutes : soyez toujours prudent. Actuellement, de nombreuses infiltrations nécessitent l'intervention de l'utilisateur pour être exécutées et propagées. Si vous êtes prudent lorsque vous ouvrez de nouveaux fichiers, vous éviterez de perdre un temps et une énergie considérable à nettoyer votre ordinateur. Respectez les règles suivantes :

- 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

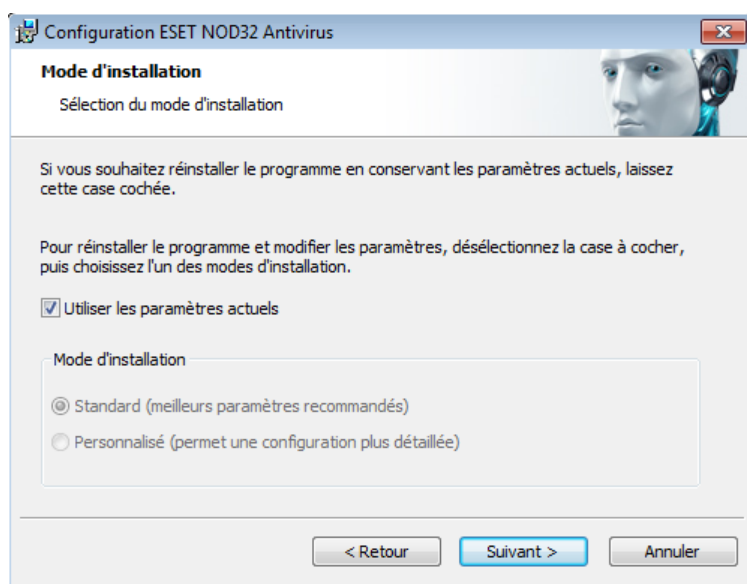
Lancez le programme d'installation ; l'assistant d'installation vous guide dans les opérations de configuration de base.

Important : Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si plusieurs solutions antivirus sont installées sur un même ordinateur, elles risquent de provoquer des conflits. Nous recommandons de désinstaller tout autre antivirus de votre système. Reportez-vous également à notre [article de base de connaissances](#) (disponible en anglais et dans plusieurs autres langues).

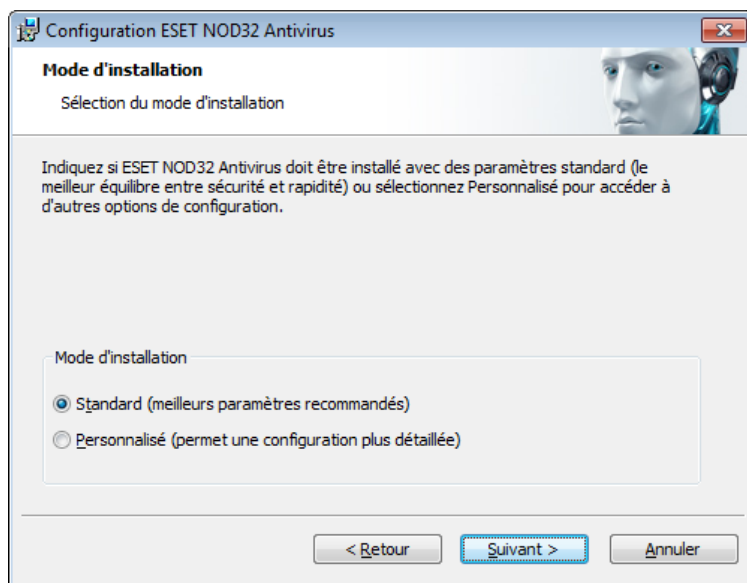
Tout d'abord, le programme vérifie si une version plus récente de ESET NOD32 Antivirus est disponible.

Si vous sélectionnez l'option de **téléchargement et d'installation de la nouvelle version**, la nouvelle version est téléchargée et l'installation se poursuit. Le contrat de licence de l'utilisateur final (CLUF) apparaît à l'étape suivante. Veuillez en prendre connaissance, puis cliquez sur **Accepter** pour confirmer que vous acceptez les clauses du contrat de licence de l'utilisateur final. L'installation se poursuit ensuite selon l'un des deux scénarios suivants :

1. Installation de ESET NOD32 Antivirus sur une version antérieure de ce logiciel. La fenêtre suivante vous permet de choisir si vous souhaitez utiliser les paramètres du programme en cours pour votre nouvelle installation ou, si vous désélectionnez la case **Utiliser les paramètres actuels** de choisir le mode d'installation [standard](#) ou [personnalisée](#).



2. Si vous installez ESET NOD32 Antivirus sur un ordinateur sans version précédente du programme, la fenêtre ci-dessous apparaît lorsque vous acceptez le **contrat de licence de l'utilisateur final**. Vous avez le choix entre une installation [standard](#) ou [personnalisée](#) et accédez aux options correspondantes.



2.1 Installation standard

Le mode d'installation standard comprend des options de configuration qui correspondent à la plupart des utilisateurs. Ces paramètres offrent un excellent système de sécurité très facile à utiliser et des performances système très élevées. Le mode d'installation standard est l'option par défaut qui est recommandée si vous n'avez pas d'exigence particulière pour certains paramètres.

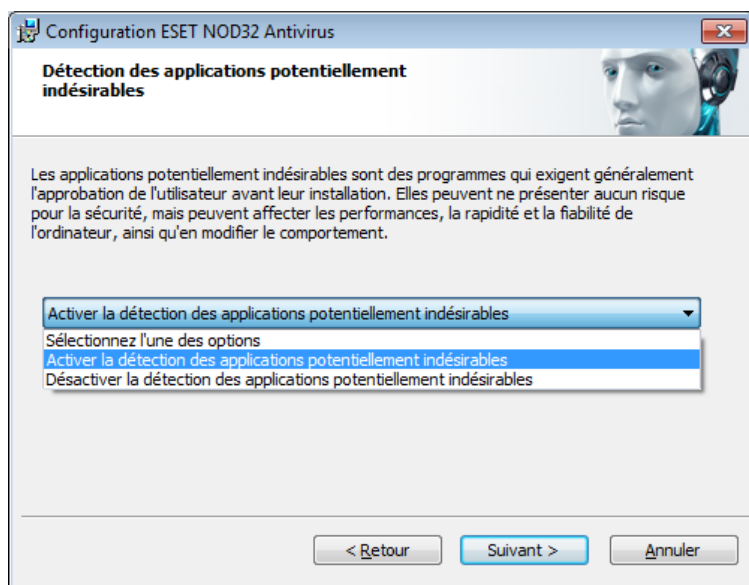
L'étape suivante consiste à configurer ESET Live Grid. Le système ESET Live Grid contribue à garantir qu'ESET est informé immédiatement et en continu des nouvelles infiltrations, afin de protéger ses clients dans les meilleurs délais. Le système permet de soumettre les nouvelles menaces au laboratoire d'ESET, où elles sont analysées, traitées, puis ajoutées à la base des signatures de virus.



Par défaut, l'option **J'accepte de participer à ESET Live Grid** est sélectionnée et active cette fonctionnalité.

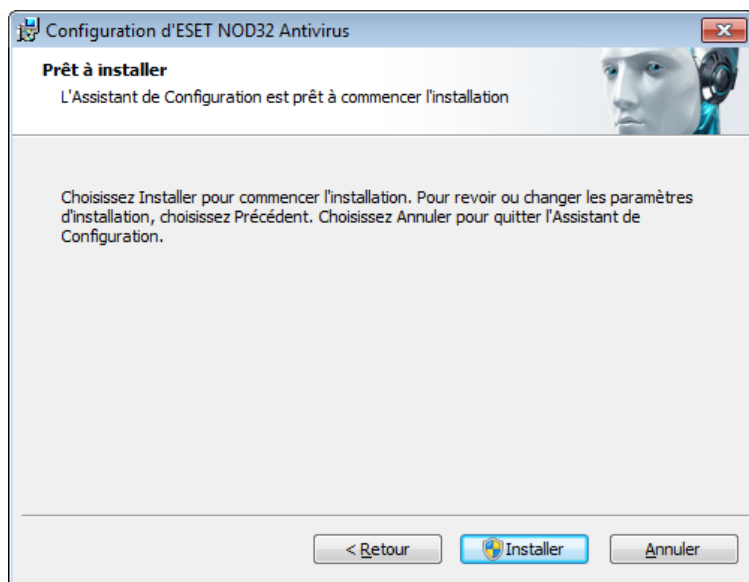
L'étape suivante de l'installation consiste à configurer la détection des applications potentiellement indésirables. Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais peuvent avoir une incidence négative sur le comportement du système d'exploitation.

Ces applications sont souvent associées à d'autres programmes et peuvent être difficiles à remarquer lors de l'installation. Ces applications affichent habituellement une notification pendant l'installation, mais elles peuvent facilement s'installer sans votre consentement.



Sélectionnez l'option **Activer la détection des applications potentiellement indésirables** pour autoriser ESET NOD32 Antivirus à détecter ce type de menace (recommandé).

La dernière étape de l'installation standard consiste à confirmer l'installation en cliquant sur le bouton **Installer**.



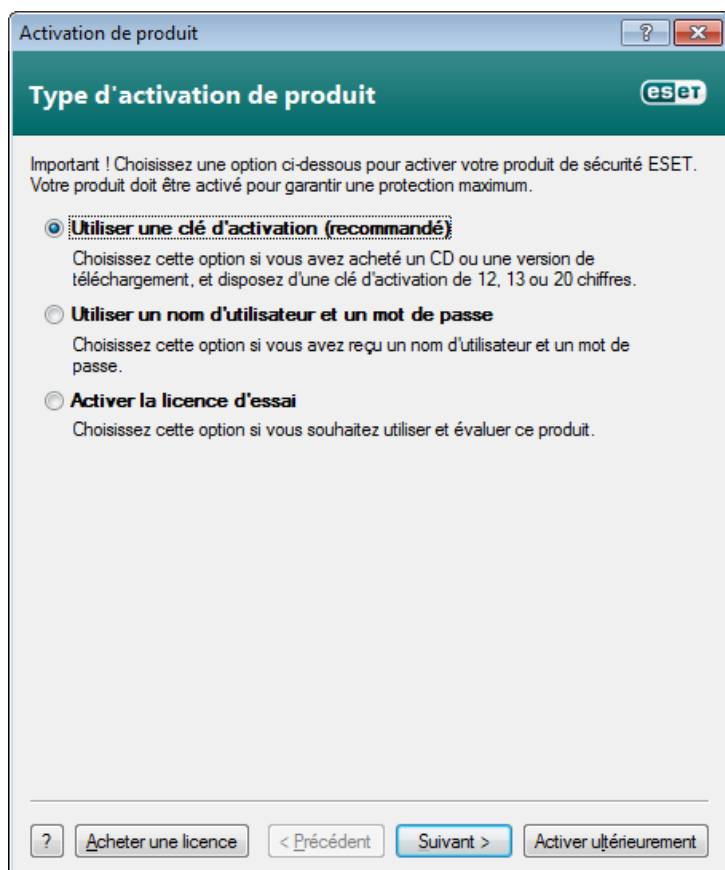
Une fois l'installation terminée, vous êtes invité à activer le produit.

Si vous avez acheté une version du produit dans une boîte au détail, vous trouverez la clé d'activation avec les instructions détaillées d'activation. Cette clé d'activation se trouve généralement à l'intérieur ou au dos de l'emballage du produit. Vous devez entrer la clé d'activation exactement comme elle est indiquée.

Si vous avez reçu un nom d'utilisateur et un mot de passe, sélectionnez l'option **Activer à l'aide d'un nom d'utilisateur et d'un mot de passe**, puis entrez les données de licence dans les champs appropriés.

Si vous souhaitez évaluer ESET NOD32 Antivirus avant d'en faire l'acquisition, sélectionnez l'option **Activer la licence d'essai**. 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 de test ne peuvent être activées qu'une seule fois par client.

Si vous n'avez pas de licence et souhaitez en acheter une, cliquez sur l'option **Acheter une licence**. Cette opération vous redirigera vers le site Web de votre distributeur ESET local.



Sélectionnez l'option **Activer ultérieurement** si vous souhaitez évaluer rapidement notre produit sans l'activer immédiatement.

Vous pouvez activer votre copie de ESET NOD32 Antivirus directement à partir du programme. Cliquez sur l'icône ESET NOD32 Antivirus située dans l'angle supérieur droit, ou cliquez avec le bouton droit sur l'icône ESET NOD32 Antivirus dans la partie système de la barre des tâches, puis cliquez sur **Activation de produit...** dans le menu.



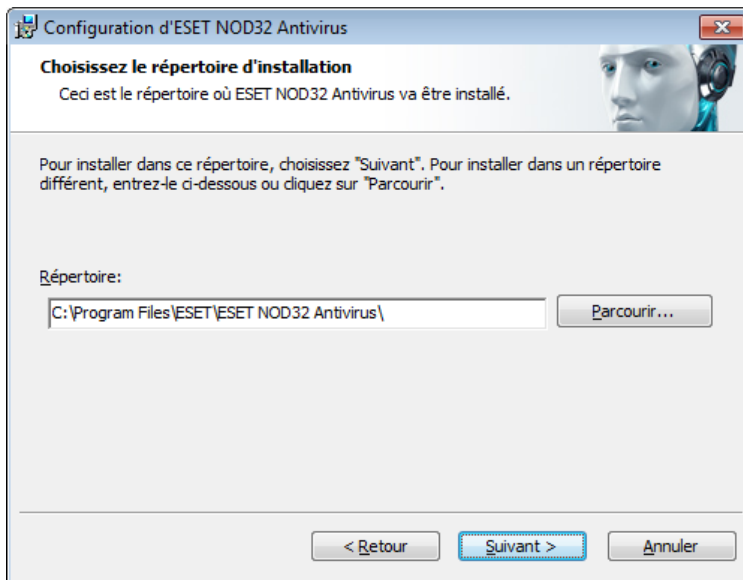
2.2 Installation personnalisée

Le mode d'installation personnalisée est destiné à des utilisateurs qui ont une certaine expérience de l'optimisation de programmes, et qui veulent modifier les paramètres avancés pendant l'installation.

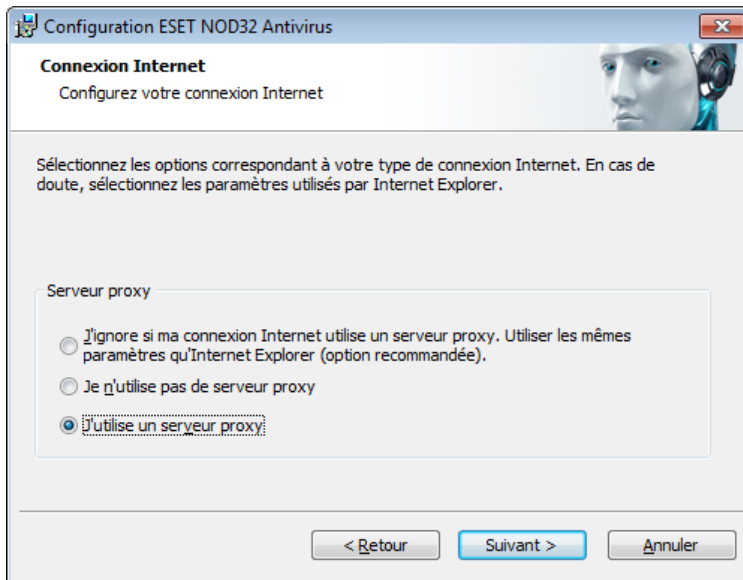
Après avoir sélectionné le mode d'installation et cliqué sur **Suivant**, vous êtes invité à sélectionner un emplacement de destination pour l'installation. Par défaut, le programme s'installe dans le dossier

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

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



Cliquez sur **Suivant** pour configurer la connexion Internet.

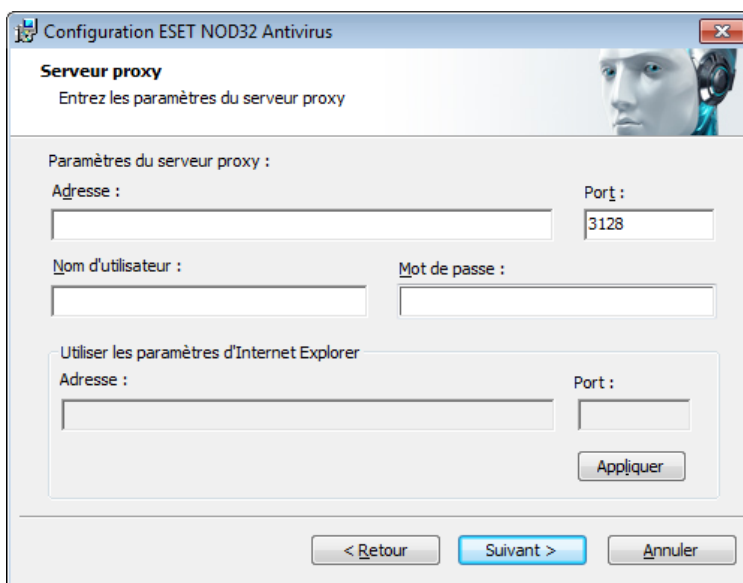


The screenshot shows the 'Configuration ESET NOD32 Antivirus' window with the 'Connexion Internet' tab selected. The title bar reads 'Configuration ESET NOD32 Antivirus'. Below the title bar, the tab is labeled 'Connexion Internet' with the subtitle 'Configurez votre connexion Internet'. The main text says: 'Sélectionnez les options correspondant à votre type de connexion Internet. En cas de doute, sélectionnez les paramètres utilisés par Internet Explorer.' There are three radio button options under the heading 'Serveur proxy':

- ☐ J'ignore si ma connexion Internet utilise un serveur proxy. Utiliser les mêmes paramètres qu'Internet Explorer (option recommandée).
- ☐ Je n'utilise pas de serveur proxy
- ☒ J'utilise un serveur proxy.

At the bottom, there are three buttons: '< Retour', 'Suivant >', and 'Annuler'.

Si vous utilisez un serveur proxy, ce dernier doit être configuré correctement pour que les mises à jour des signatures de virus fonctionnent. Si vous n'êtes pas sûr d'utiliser un serveur proxy pour la connexion à Internet, sélectionnez **Je ne sais pas si ma connexion Internet utilise un serveur proxy. Utiliser les mêmes paramètres qu'Internet Explorer (option recommandée)**, et cliquez sur **Suivant**. Si vous n'utilisez pas de serveur proxy, sélectionnez l'option **Je n'utilise pas de serveur proxy**.



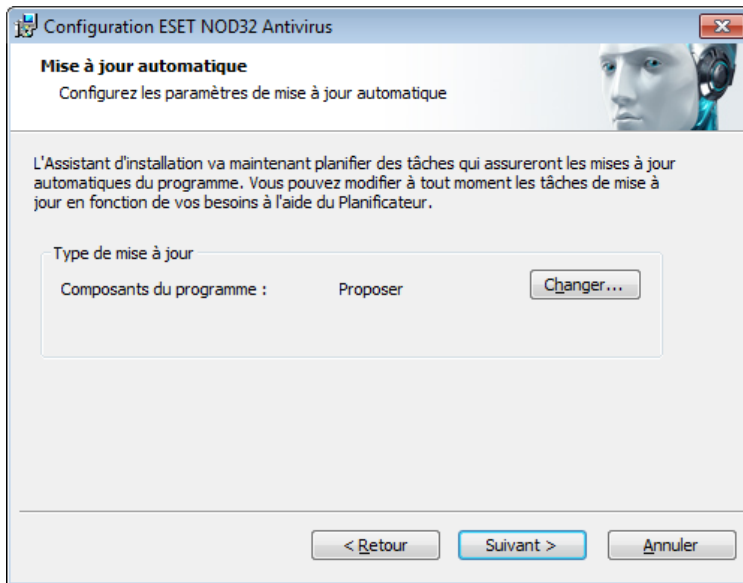
The screenshot shows the 'Configuration ESET NOD32 Antivirus' window with the 'Serveur proxy' tab selected. The title bar reads 'Configuration ESET NOD32 Antivirus'. Below the title bar, the tab is labeled 'Serveur proxy' with the subtitle 'Entrez les paramètres du serveur proxy'. The main text says: 'Paramètres du serveur proxy :'. There are two sections of input fields:

- Paramètres du serveur proxy :**
 - Adresse :** [Empty text box]
 - Port :** [Text box containing '3128']
 - Nom d'utilisateur :** [Empty text box]
 - Mot de passe :** [Empty text box]
- Utiliser les paramètres d'Internet Explorer**
 - Adresse :** [Empty text box]
 - Port :** [Empty text box]

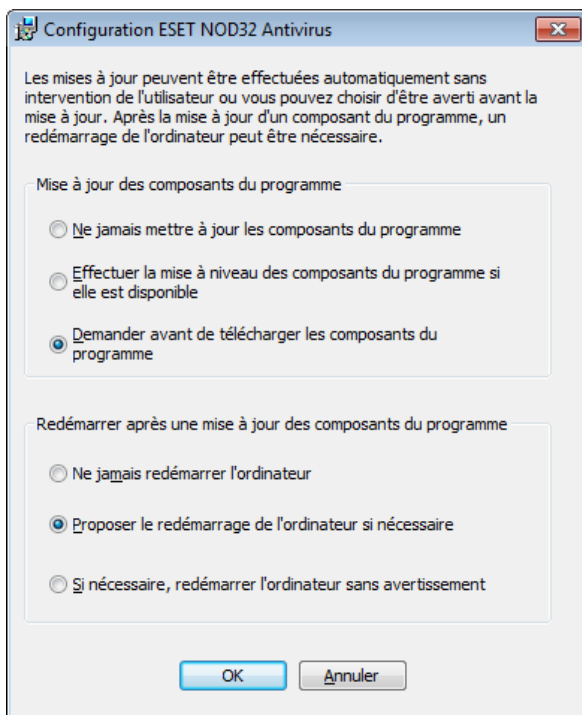
At the bottom right of the input section is an 'Appliquer' button. At the bottom of the window are three buttons: '< Retour', 'Suivant >', and 'Annuler'.

Pour configurer les paramètres du serveur proxy, sélectionnez l'option **J'utilise un serveur proxy** et cliquez sur **Suivant**. Entrez l'adresse IP ou l'adresse URL de votre serveur proxy dans le champ **Adresse**. Dans le champ **Port**, spécifiez le port sur lequel le serveur proxy accepte les connexions (3128 par défaut). Si le serveur proxy exige une authentification, saisissez un **nom d'utilisateur** et un **mot de passe** pour accorder l'accès au serveur proxy. Les paramètres du serveur proxy peuvent être copiés depuis Internet Explorer. Pour ce faire, cliquez sur le bouton **Appliquer** et confirmez la sélection.

Cette étape d'installation permet d'indiquer la façon dont le système gère les mises à jour automatiques du programme. Cliquez sur **Changer...** pour accéder aux paramètres avancés.

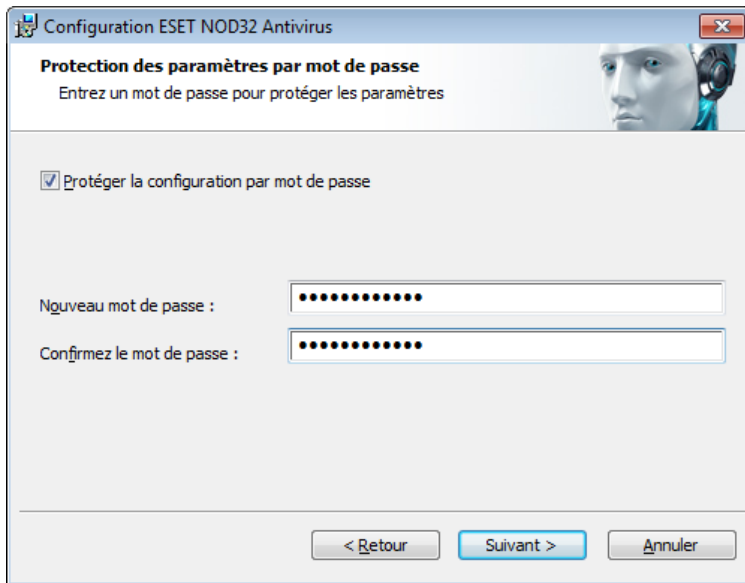


Si vous ne voulez pas que les composants du programme soient mis à jour, sélectionnez l'option **Ne jamais mettre à jour les composants du programme**. Sélectionnez l'option **Demander avant de télécharger les composants du programme** pour afficher une fenêtre de confirmation chaque fois que le système essaie de télécharger les composants du programme. Pour télécharger les mises à niveau des composants du programme, sélectionnez l'option **Toujours mettre à jour les composants du programme**.



REMARQUE : le redémarrage du système est généralement nécessaire après la mise à jour des composants du programme. il est recommandé de sélectionner l'option **Si nécessaire, redémarrer l'ordinateur sans avertissement**.

La fenêtre suivante de l'installation permet d'indiquer un mot de passe afin de protéger les paramètres du programme. Sélectionnez l'option **Protéger la configuration par mot de passe** et choisissez le mot de passe à indiquer dans les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe** : vous en aurez besoin pour changer les paramètres ESET NOD32 Antivirus ou y accéder. Si les deux mots de passe correspondent, cliquez sur **Suivant** pour continuer.



Les deux étapes d'installation suivantes, **Service en ligne de communauté ESET ESET Live Grid** et **Détection des applications potentiellement indésirables** sont identiques aux étapes de l'installation standard (reportez-vous à [Installation standard](#)).

Cliquez sur **Installer** dans la fenêtre **Prêt à installer** pour terminer l'installation. Une fois l'installation terminée, vous êtes invité à activer le produit. Reportez-vous à l'[installation standard](#) pour plus d'informations sur l'activation du produit.

2.3 Mise à niveau vers une version plus récente

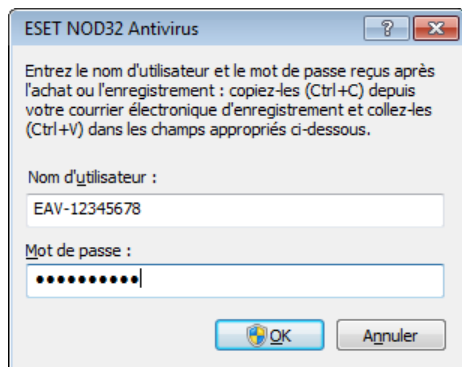
Les nouvelles versions d'ESET NOD32 Antivirus offrent des améliorations ou apportent des solutions aux problèmes que les mises à jour automatiques des modules ne peuvent pas résoudre. La mise à niveau vers une nouvelle version peut s'effectuer de différentes manières :

1. Automatiquement, par l'intermédiaire de la 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 correct soit garanti sur toutes les configurations système. Si vous devez effectuer la mise à niveau vers une nouvelle version dès qu'elle est disponible, utilisez l'une des méthodes suivantes.
2. Manuellement, dans la fenêtre principale du programme, en cliquant sur l'option **d'installation/de vérification** dans **Mettre à jour > Version disponible de ESET NOD32 Antivirus** :
3. Manuellement, en téléchargeant la nouvelle version et en l'installant sur l'installation précédente.
Au début de l'installation, vous pouvez choisir de conserver les paramètres du programme en cochant la case **Utiliser les paramètres actuels**.

2.4 Saisie du nom d'utilisateur et du mot de passe

Le programme doit être mis à jour automatiquement pour assurer un fonctionnement optimal. Ce téléchargement n'est possible que si le nom d'utilisateur et le mot de passe sont saisis dans l'option **Configuration de la mise à jour**.

Si vous n'avez pas entré votre nom d'utilisateur et votre mot de passe lors de l'installation, vous pouvez le faire maintenant. Dans la fenêtre principale, cliquez sur **Mettre à jour et Activation du produit...**, puis entrez dans la fenêtre d'activation du produit les informations de la licence que vous avez reçues avec votre produit de sécurité ESET.



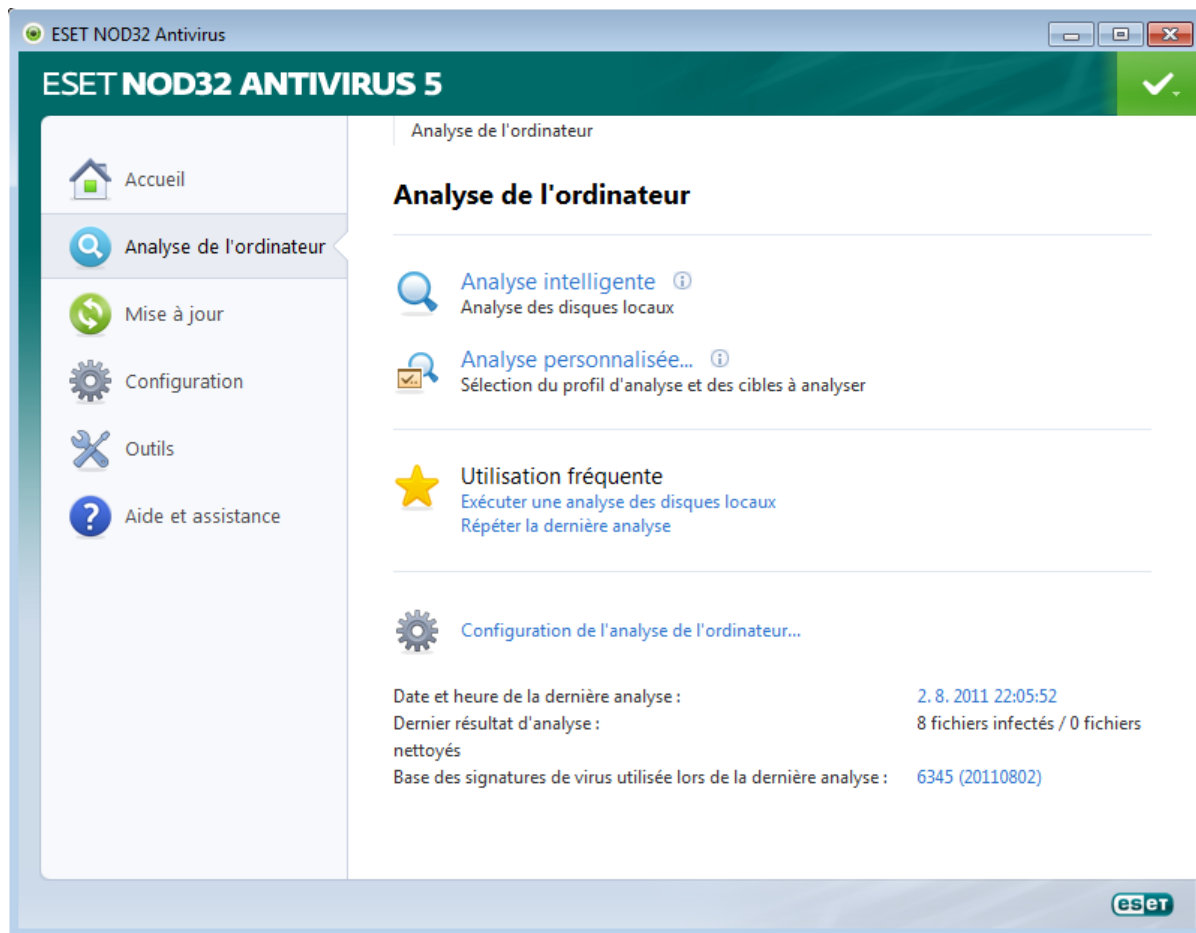
Lors de la saisie de votre **nom d'utilisateur** et de votre **mot de passe**, il est important de saisir ces informations exactement telles qu'elles sont écrites :

- Le nom d'utilisateur et le mot de passe font la distinction entre les majuscules et les minuscules, et le tiret dans le nom d'utilisateur est obligatoire.
- Le mot de passe se compose de dix caractères, tous en minuscules.
- Nous n'utilisons pas la lettre « L » dans les mots de passe (utilisez le numéro un (1) à la place).
- Le « O » est le chiffre zéro et le « o » est la lettre minuscule o.

Il est recommandé de copier et de coller les données du message d'enregistrement.

2.5 Analyse d'ordinateur

Après l'installation d'ESET NOD32 Antivirus, vous devez effectuer une analyse de l'ordinateur afin de rechercher tout code malveillant éventuel. Dans la fenêtre principale du programme, cliquez sur **Analyse de l'ordinateur**, puis sur **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 Présentation de l'interface utilisateur

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.

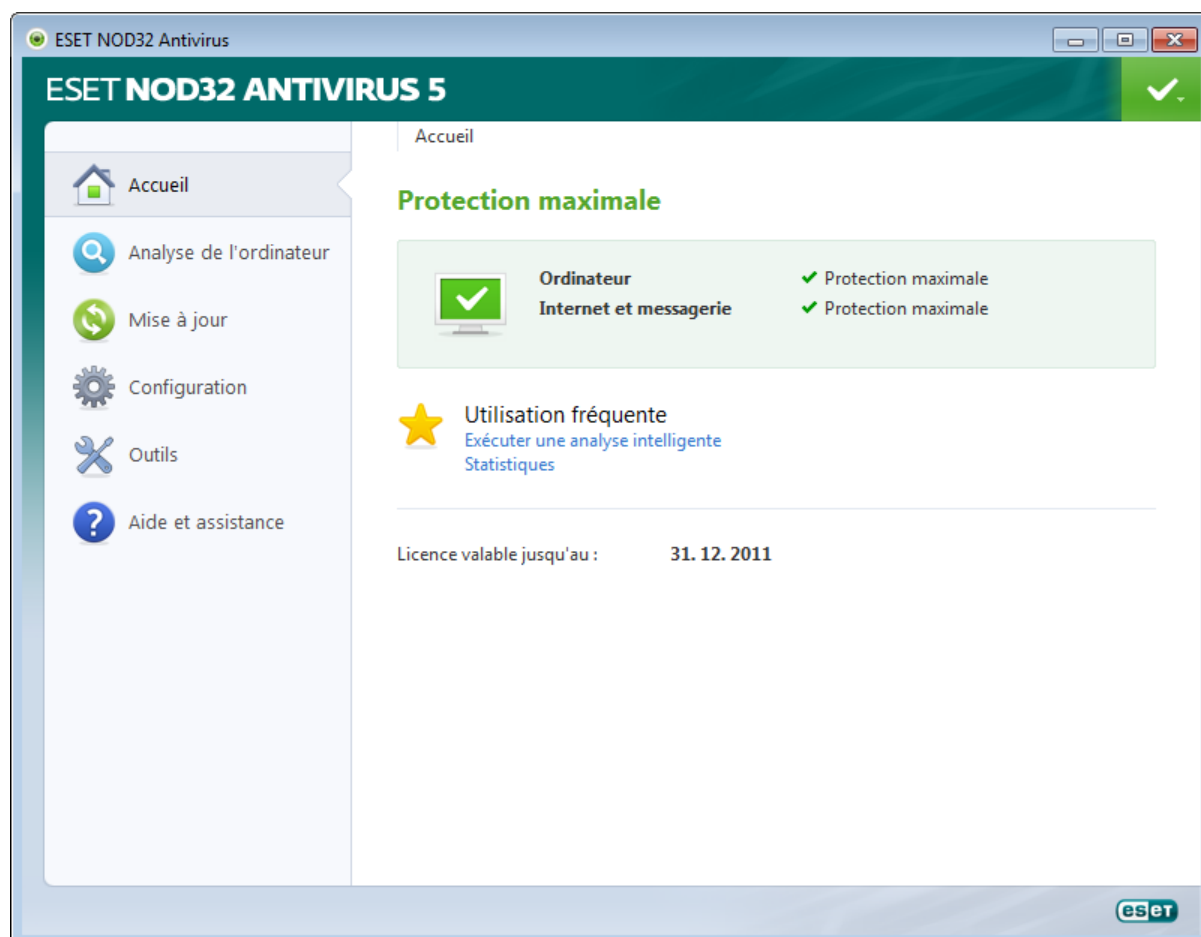
Analyse de l'ordinateur - Cette option permet de configurer et de lancer l'analyse intelligente ou l'analyse personnalisée.

Mettre à jour - Affiche des informations sur les mises à jour de la base des signatures de virus.

Configuration - Sélectionnez cette option pour ajuster le niveau de sécurité de votre ordinateur, d'Internet et de la messagerie.

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

Aide et assistance - Permet d'accéder aux fichiers d'aide, à la base de connaissances ESET, au site Internet d'ESET et aux liens nécessaires à l'ouverture d'une requête auprès du service client.

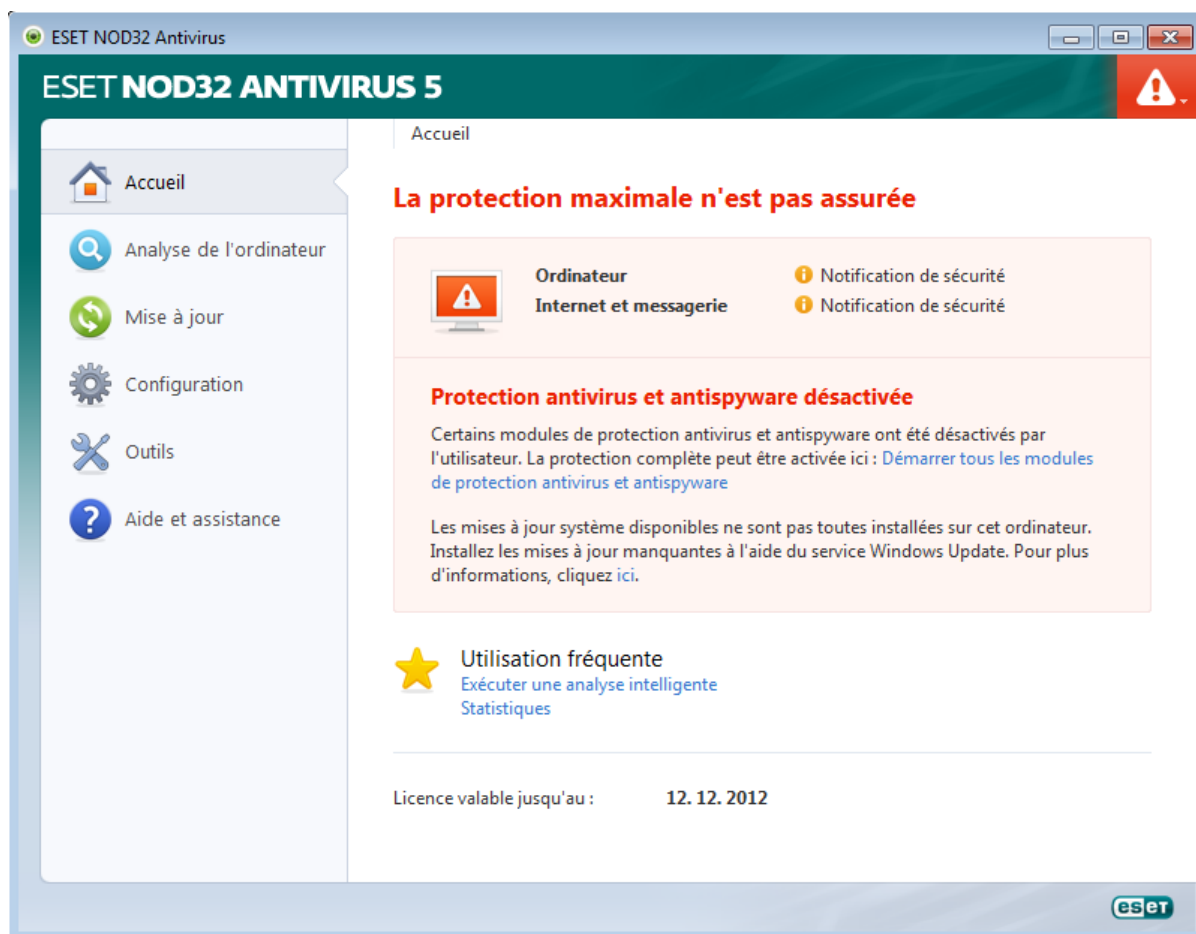


L'écran **Accueil** vous informe sur le niveau actuel de sécurité et de protection de l'ordinateur. L'icône verte d'état **Protection maximale** indique qu'une protection maximale est assurée.

La fenêtre d'état affiche également les fonctionnalités utilisées fréquemment dans ESET NOD32 Antivirus. La date d'expiration du programme figure également ici.

3.2 Que faire lorsque le programme ne fonctionne pas correctement ?

Une coche verte s'affiche en regard de chaque module activé et fonctionnant correctement. Dans le cas contraire, un point d'exclamation rouge ou orange et des informations supplémentaires sur le module s'affichent dans la partie supérieure de la fenêtre. Une suggestion de solution pour corriger le module est également affichée. Pour changer l'état des différents modules, cliquez sur **Configuration** dans le menu principal puis sur le module souhaité.



L'icône rouge signale des problèmes critiques ; la protection maximale de votre ordinateur n'est pas assurée. Les raisons possibles sont les suivantes :

- la protection en temps réel du système de fichiers est désactivée ;
- la base des signatures de virus est obsolète ,
- le produit n'est pas activé ;
- la licence du produit est expirée.

L'icône orange indique que l'accès Web ou la protection du client de messagerie est désactivé, qu'il y a un problème de mise à jour de programme (la base des signatures de virus est obsolète et ne peut pas être mise à jour) ou que la licence approche de sa date d'expiration.

Produit non activé - Ce problème est signalé par un avertissement en rouge et une notification de sécurité à côté de l'élément **Ordinateur**. Vous pouvez activer ESET NOD32 Antivirus depuis le menu du programme à l'aide de l'option **Activation de produit...** Le menu du programme est situé dans la partie supérieure droite de la fenêtre.

Protection antivirus et antispyware désactivée - Ce problème est signalé par un affichage en rouge et une notification de sécurité à côté de l'élément **Ordinateur**. Vous pouvez réactiver la protection antivirus en cliquant sur **Démarrer tous les modules de protection antivirus et antispyware**.

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

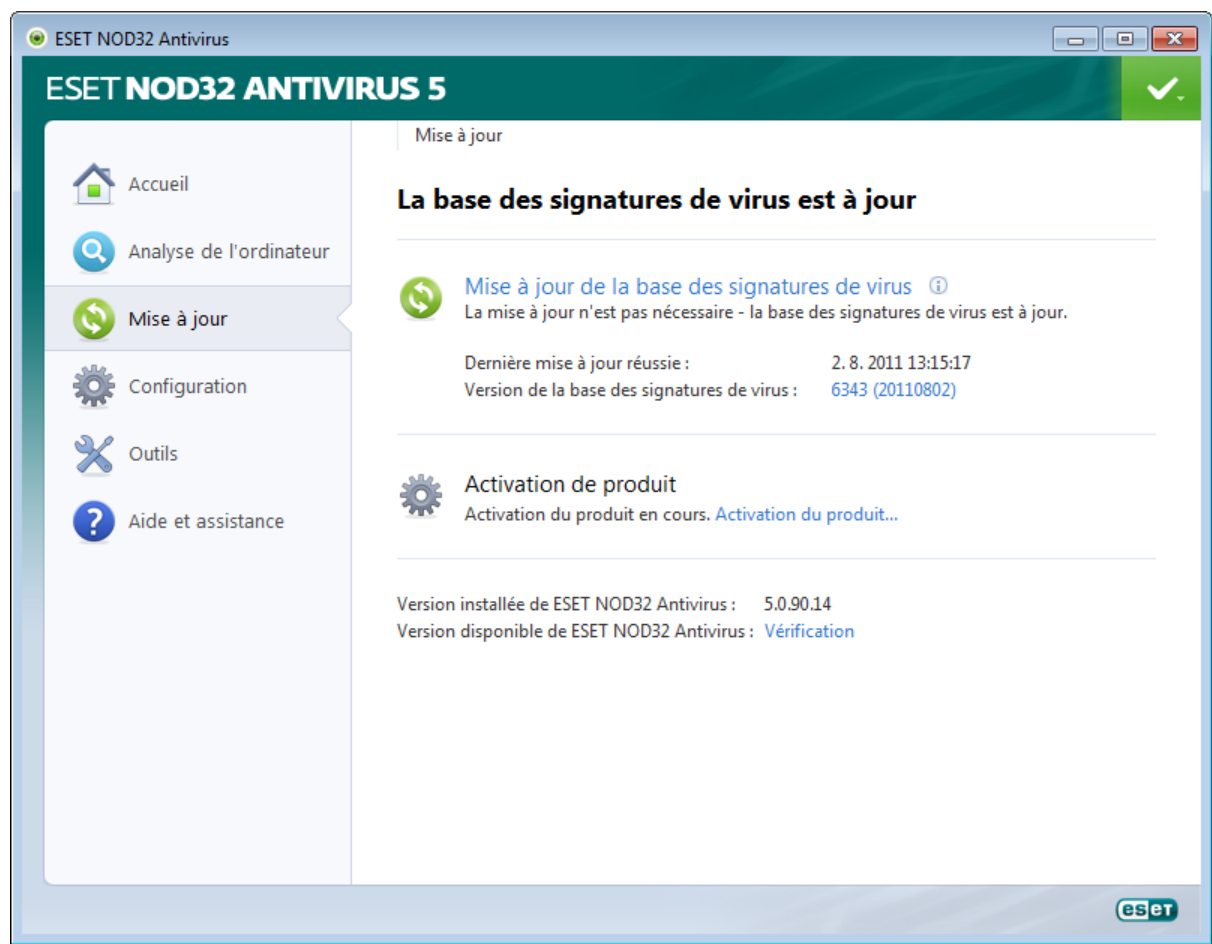
Licence arrivée à expiration - Cette information est indiquée par l'icône d'état de protection qui devient rouge. Le programme ne peut plus effectuer de mise à jour à partir de ce moment. Nous vous recommandons de suivre les instructions de la fenêtre d'alerte pour renouveler la licence.

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. Si vous avez encore besoin d'aide, vous pouvez soumettre une demande au service client d'ESET. Ce dernier répondra très rapidement à vos questions et vous permettra de déterminer une solution.

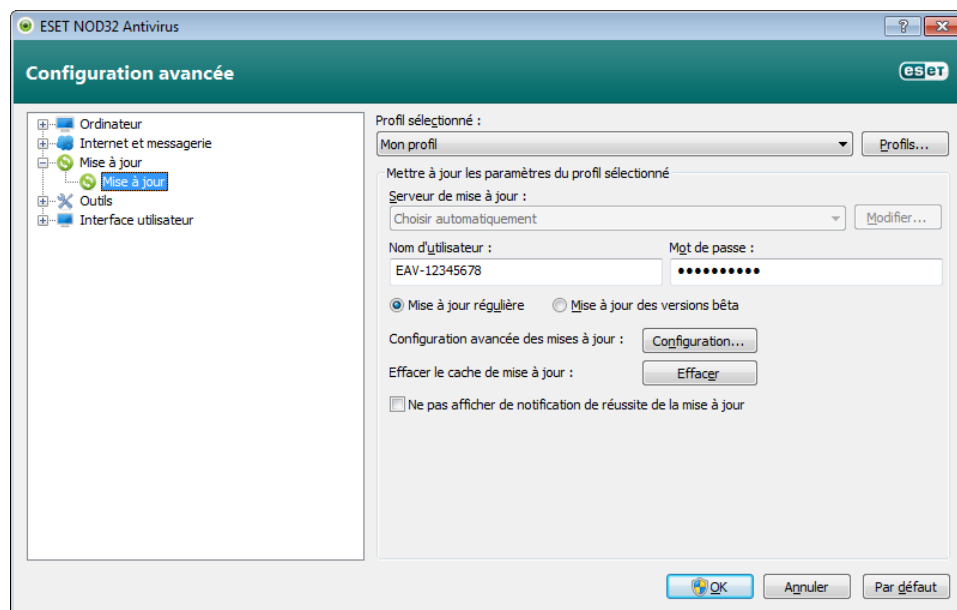
3.3 Configuration des mises à jour

La mise à jour de la base des signatures de virus et celle des composants du programme sont des opérations importantes qui assurent la protection totale 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, sélectionnez **Mise à jour** et cliquez sur **Mettre à jour la base des signatures de virus** dans la fenêtre principale pour rechercher toute nouvelle mise à jour de la base de données.

Si le nom d'utilisateur et le mot de passe n'ont pas été entrés lors de l'installation ou de l'activation de ESET NOD32 Antivirus, vous êtes invité à les indiquer à cette étape.

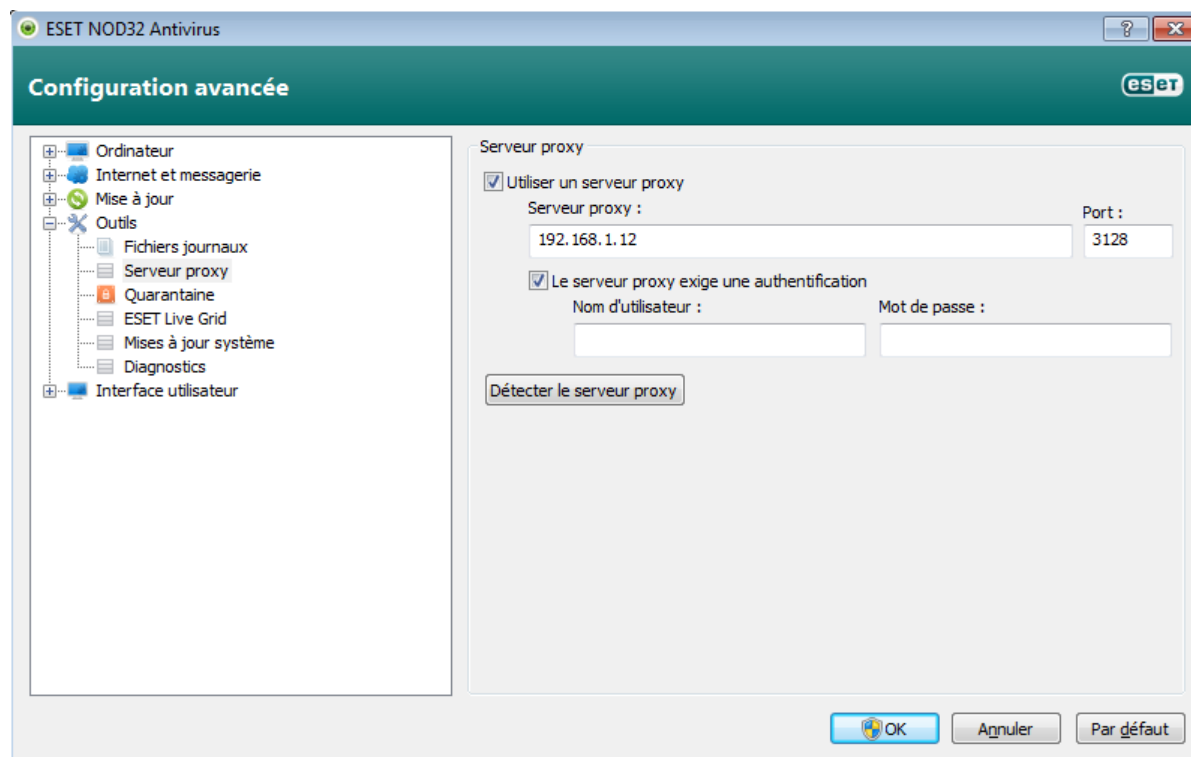


La fenêtre Configuration avancée (cliquez sur **Configuration** dans le menu principal et sur **Accéder à la configuration avancée...**, ou appuyez sur la touche F5 de votre clavier) comporte d'autres options de mise à jour. Cliquez sur **Mettre à jour** dans l'arborescence Configuration avancée à gauche. Le menu déroulant **Serveur de mise à jour** doit être défini sur **Choisir automatiquement**. 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 le bouton **Configuration...**



3.4 Configuration du serveur proxy

Si vous utilisez un serveur proxy pour contrôler les connexions Internet sur un système à l'aide de ESET NOD32 Antivirus, ce serveur doit être spécifié dans la configuration avancée. Pour accéder à la fenêtre de configuration du serveur proxy, appuyez sur la touche F5 pour ouvrir la fenêtre Configuration avancée et cliquez sur **Outils > Serveur proxy** depuis l'arborescence Configuration avancée. Sélectionnez l'option **Utiliser un serveur proxy**, puis remplissez les champs **Serveur proxy** (adresse IP) et **Port**. Si nécessaire, sélectionnez l'option **Le serveur proxy nécessite une authentification**, puis saisissez le **nom d'utilisateur** et le **mot de passe**.



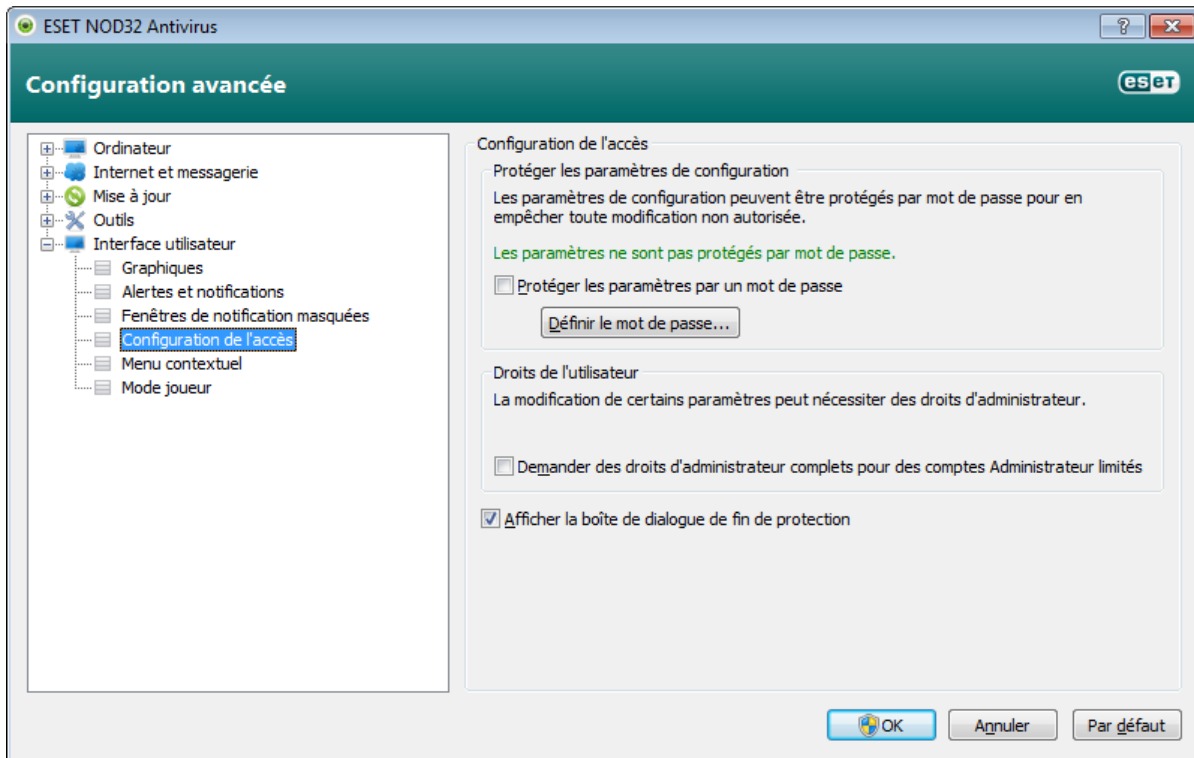
Si ces informations ne sont pas disponibles, vous pouvez essayer de détecter automatiquement les paramètres du serveur proxy en cliquant sur l'option **Détecter le serveur proxy**.

REMARQUE : les options du serveur proxy peuvent varier selon les profils de mise à jour. Si c'est le cas, configurez les

différents profils de mise à jour dans Configuration avancée en cliquant sur Mettre à jour dans l'arborescence.

3.5 Protection des paramètres

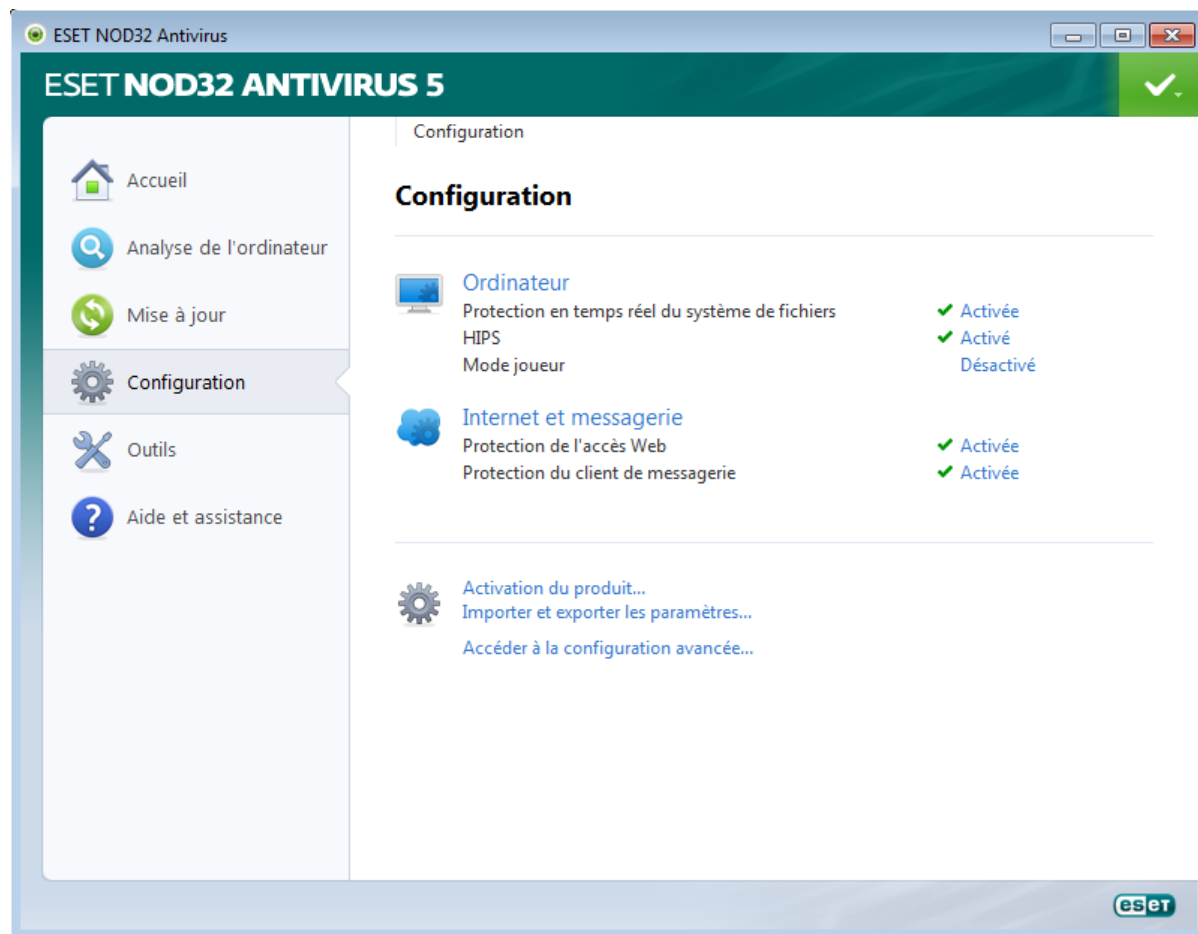
Les paramètres ESET NOD32 Antivirus peuvent être très importants pour votre stratégie de sécurité. Des modifications non autorisées peuvent mettre en danger la stabilité et la protection de votre système. Pour protéger par mot de passe les paramètres de configuration, cliquez dans le menu principal sur **Configuration > Accéder à la configuration avancée... > Interface utilisateur > Configuration de l'accès**, sélectionnez l'option **Protection des paramètres par mot de passe** et cliquez sur le bouton **Définir le mot de passe...**



Saisissez un mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**, puis cliquez sur **OK**. Ce mot de passe sera nécessaire à toute modification apportée à ESET NOD32 Antivirus.

4. Utiliser ESET NOD32 Antivirus

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



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

- **Ordinateur**
- **Internet et messagerie**

Cliquez sur n'importe quel 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 :

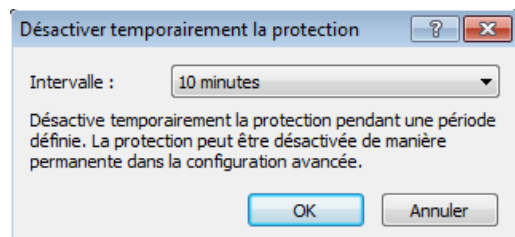
- **Protection en temps réel du système de fichiers** - Lorsque ces fichiers sont ouverts, créés ou exécutés sur l'ordinateur, elle les analyse pour y rechercher la présence éventuelle de code malveillant.
- **Protection des documents** - La fonctionnalité de protection des documents analyse les documents Microsoft Office avant leur ouverture, ainsi que les fichiers téléchargés automatiquement par Internet Explorer, tels que des éléments Microsoft ActiveX.
- **HIPS** - L'outil [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 jaune lorsque le mode joueur est activé.

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

- **Protection de l'accès au Web** - Si cette option est activée, tout le trafic HTTP ou HTTPS est analysé à la recherche de codes malveillants.
- **Protection du client de messagerie** - La protection de la messagerie offre le contrôle de la communication par courrier électronique effectuée via les protocoles POP3 et IMAP.

REMARQUE : la protection de documents n'apparaît que si l'option **Accéder à la configuration avancée... (F5) > Ordinateur > Antivirus et antispyware > Protection des documents > Intégrer dans le système** est activée.

Une fois que vous avez cliqué sur **Activé**, la boîte de dialogue **Désactiver temporairement la protection** apparaît. Cliquez sur **OK** pour désactiver le composant de sécurité sélectionné. Le menu déroulant **Intervalle** représente la période pendant laquelle le composant sélectionné est désactivé.



Pour réactiver la protection du composant de sécurité désactivé, cliquez sur **Désactivée**.

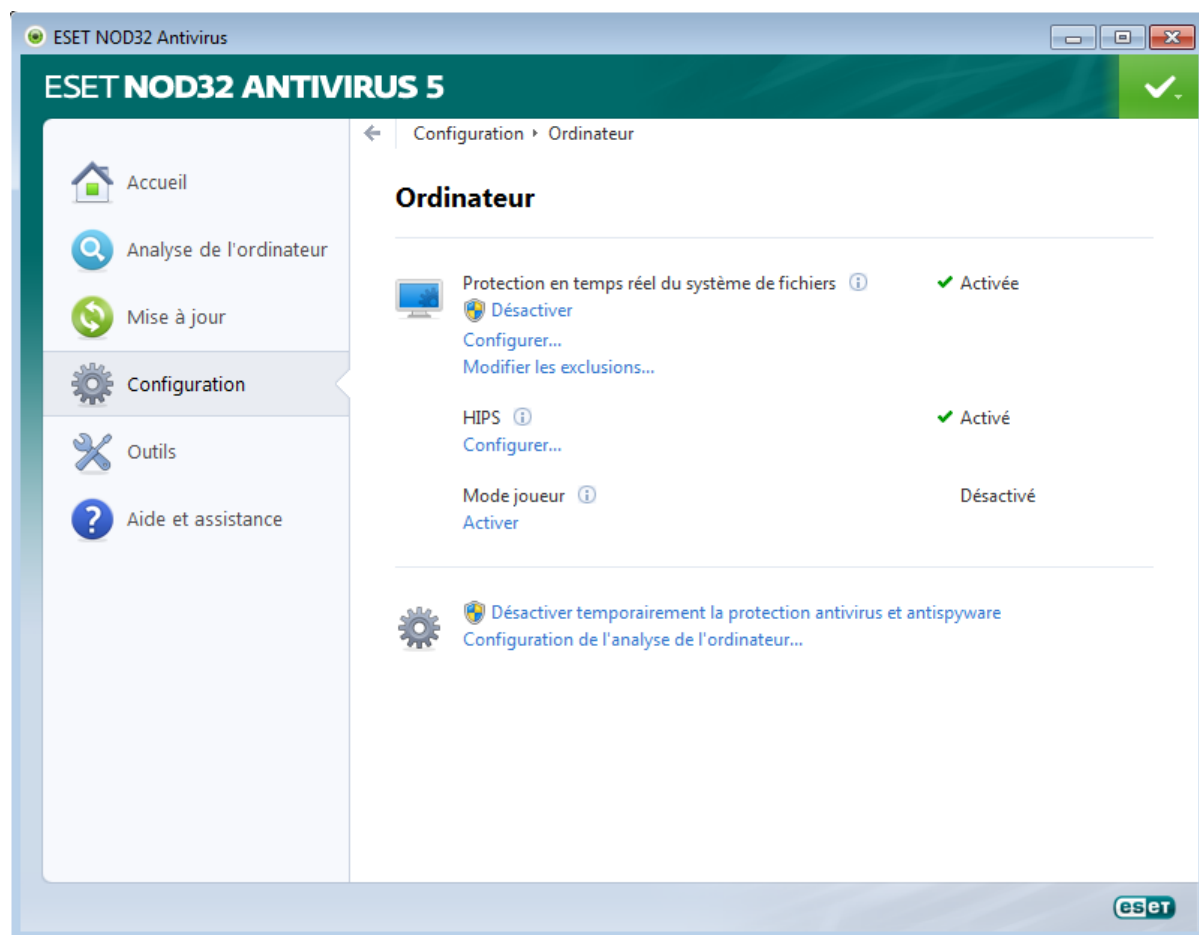
REMARQUE : lorsque vous désactivez la protection à l'aide de cette méthode, tous les composants désactivés de la protection sont activés au redémarrage de l'ordinateur.

D'autres options sont disponibles au bas de la fenêtre de configuration. Utilisez le lien **Activation de produit...** pour ouvrir un formulaire d'enregistrement qui nous permet d'activer le produit de sécurité ESET et de vous envoyer un courrier électronique avec vos données d'authentification (nom d'utilisateur et mot de passe). Pour charger les paramètres de configuration à l'aide d'un fichier de configuration **.xml** ou pour enregistrer les paramètres de configuration dans un fichier de configuration, utilisez l'option **Importer et exporter les paramètres...**

4.1 Ordinateur

La configuration de l'ordinateur est disponible dans le volet **Configuration** lorsque vous cliquez sur l'intitulé **Ordinateur**. Elle affiche un aperçu de tous les modules de protection. Pour désactiver temporairement des modules individuels, cliquez sur **Désactiver** sous le module souhaité. Notez que cela peut abaisser le niveau de protection de l'ordinateur. Pour accéder aux paramètres détaillés de chaque module, cliquez sur **Configurer...**

Cliquez sur **Modifier les exclusions...** pour ouvrir la fenêtre de configuration des [exclusions](#) qui permet d'exclure des fichiers et des dossiers de l'analyse antivirus.



Désactiver temporairement la protection antivirus et antispyware - Désactive tous les modules de protection antivirus et antispyware. La boîte de dialogue **Désactiver temporairement la protection** avec le menu déroulant

Intervalle de temps apparaît. Le menu déroulant **Intervalle** représente la période pendant laquelle la protection est désactivée. Cliquez sur **OK** pour confirmer.

Configuration de l'analyse de l'ordinateur... - Cliquez ici pour régler les paramètres d'analyse à la demande (analyse lancée manuellement).

4.1.1 Protection antivirus et antispyware

La protection antivirus et antispyware vous protège 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.

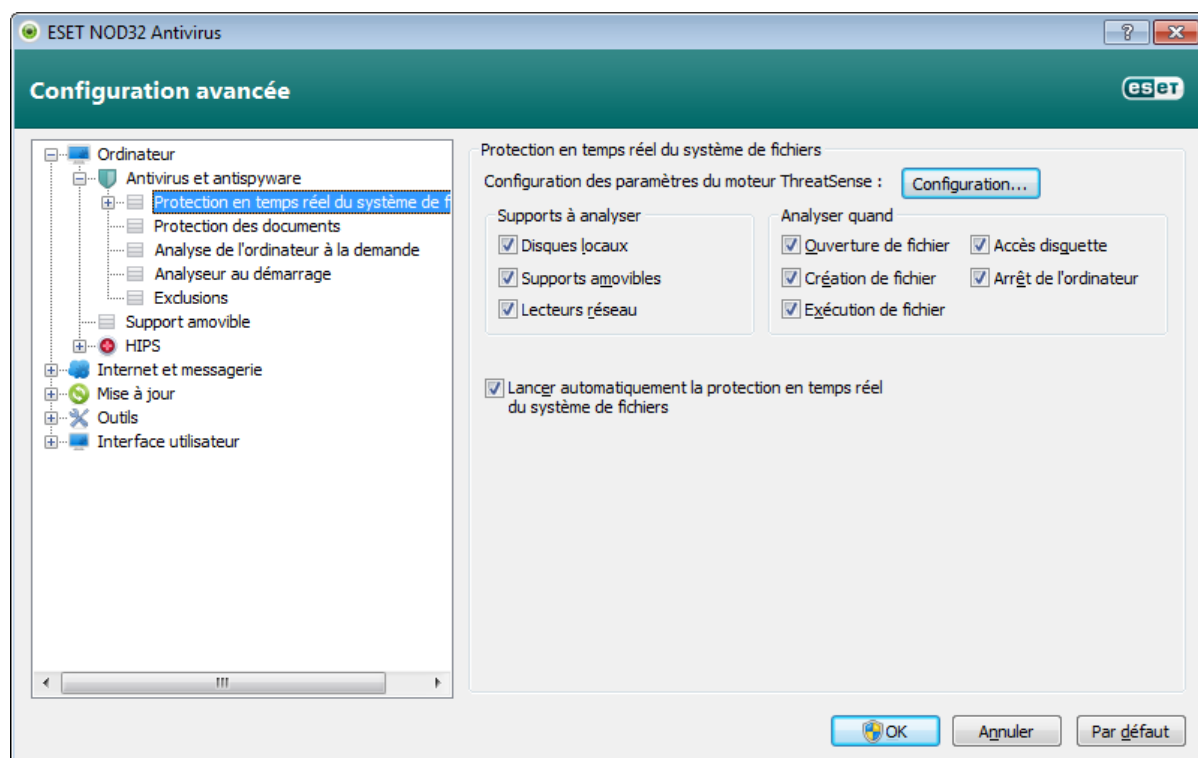
4.1.1.1 Protection en temps réel du système de fichiers

La protection en temps réel du système de fichiers contrôle tous les événements liés à l'antivirus dans le système. Elle analyse tous les fichiers à la recherche de code malveillant lors de l'ouverture, de la création ou de l'exécution de ces fichiers sur l'ordinateur. La protection en temps réel du système de fichiers est lancée au démarrage du système.

La protection en temps réel du système de fichiers vérifie tous les types de supports. Elle est déclenchée par différents événements système, l'accès à un fichier par exemple. L'utilisation des méthodes de détection de la technologie ThreatSense (décrites dans la section intitulée [Configuration des paramètres du moteur ThreatSense](#)), la protection du système de fichiers en temps réel est différente pour les nouveaux fichiers et pour les fichiers existants. Pour les nouveaux fichiers, il est possible d'appliquer un niveau de contrôle plus approfondi.

Pour réduire l'impact 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 de la base des signatures de virus. Ce comportement est configuré à l'aide de l'**optimisation intelligente**. Si cette fonction est désactivée, tous les fichiers sont analysés à chaque accès. Pour modifier cette option, appuyez sur la touche F5 pour ouvrir la fenêtre Configuration avancée et cliquez sur **Ordinateur > Antivirus et antispyware > Protection des documents** dans l'arborescence de configuration avancée. Cliquez ensuite sur le bouton **Configuration...** à côté de l'option **Configuration des paramètres du moteur ThreatSense**, cliquez sur **Autre** et sélectionnez ou désélectionnez l'option **Activer l'optimisation intelligente**.

Par défaut, la protection en temps réel est lancée au démarrage du système d'exploitation, assurant ainsi une analyse ininterrompue. Dans certains cas (conflit avec un autre analyseur en temps réel par exemple), il est possible de mettre fin à la protection en temps réel en désactivant l'option **Lancer automatiquement la protection en temps réel du système de fichiers**.



4.1.1.1.1 Supports à analyser

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

Disques locaux - Contrôle tous les disques durs système.

Supports amovibles - Disquettes, périphériques USB, etc.

Disques réseau - Analyse tous les lecteurs mappés.

Nous recommandons de conserver 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.

4.1.1.1.2 Analyser quand (analyse déclenchée par un événement)

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

Ouverture de fichier - Active/désactive l'analyse des fichiers ouverts.

Création de fichier - Active/désactive l'analyse des fichiers créés ou modifiés.

Exécution de fichier - Active/désactive l'analyse des fichiers exécutés.

Accès disquette - Active/désactive l'analyse déclenchée par l'accès au lecteur de disquette.

Arrêt de l'ordinateur - Active ou désactive le contrôle des secteurs d'amorçage du disque dur lors de l'arrêt de l'ordinateur. Bien que les virus d'amorçage soient rares de nos jours, il est recommandé de laisser ces options activées, car le risque existe toujours d'une infection par un virus d'amorçage provenant d'autres sources.

4.1.1.1.3 Options d'analyse avancées

Vous trouverez des options de configuration détaillées dans **Ordinateur > Antivirus et antispyware > Protection en temps réel du système de fichiers > Configuration avancée**.

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

Autres paramètres ThreatSense pour les fichiers exécutés : par défaut, l'heuristique avancée n'est pas utilisée lors de l'exécution des fichiers. Toutefois, vous souhaitez dans certains cas activer cette option (en cochant l'option **Heuristique avancée à l'exécution du fichier**). Notez que l'heuristique avancée peut ralentir l'exécution de certains programmes en raison de l'augmentation de la charge système. Si l'option **Heuristique avancée à l'exécution de fichiers à partir de supports amovibles** est activée et que vous souhaitez exclure certains ports USB du support amovible de l'analyse par heuristique avancée lors de l'exécution des fichiers, cliquez sur **Exceptions...** pour ouvrir la fenêtre d'exclusions du support amovible. Vous pouvez alors personnaliser les paramètres en sélectionnant ou en désélectionnant les cases à cocher qui représentent chaque port.

4.1.1.1.4 Niveaux de nettoyage

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

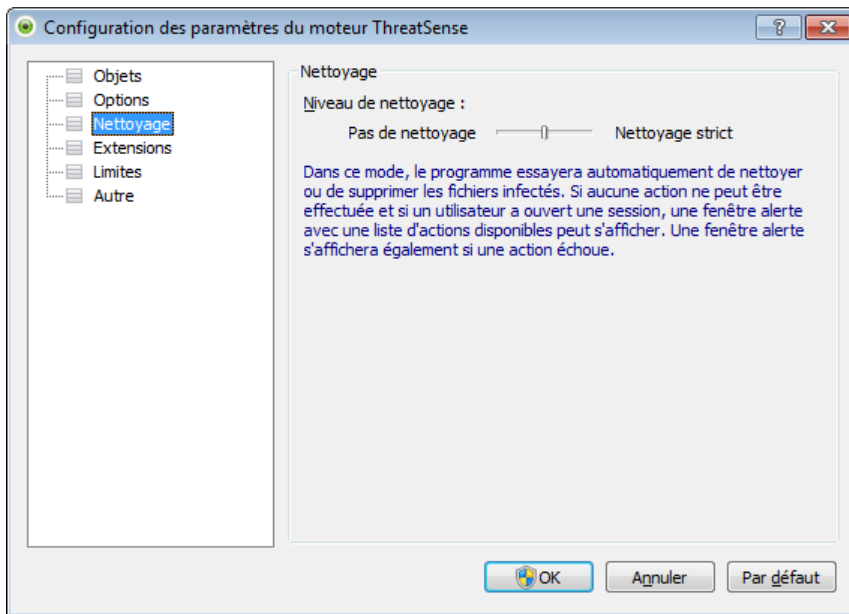
Pas de nettoyage - Les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche alors une fenêtre d'avertissement et laisse l'utilisateur choisir une action. Ce niveau est conçu pour les utilisateurs expérimentés qui connaissent les actions à entreprendre en cas d'infiltration.

Niveau par défaut - Le programme tente de nettoyer ou de supprimer automatiquement tout fichier infecté en fonction d'une action prédéfinie (sur la base du type d'infiltration). La détection et la suppression d'un fichier infecté sont signalées par un message d'information affiché 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 n'a pas pu 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 (**Niveau par défaut**), 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.



4.1.1.1.5 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. Ce peut être le cas notamment lorsqu'il y a conflit avec une autre application ou avec l'analyseur en temps réel d'un autre logiciel antivirus.

Après l'installation d'ESET NOD32 Antivirus, tous les paramètres sont optimisés pour garantir le niveau maximum de système de sécurité aux utilisateurs. Afin de restaurer les paramètres par défaut, cliquez sur le bouton **Par défaut** situé dans la partie inférieure droite de la fenêtre **Protection en temps réel (Configuration avancée > Ordinateur > Antivirus et antispyware > Protection en temps réel du système de fichiers)**.

4.1.1.1.6 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 spécial 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 eicar.com est téléchargeable depuis <http://www.eicar.org/download/eicar.com>

4.1.1.1.7 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** et cliquez sur **Protection en temps réel du système de fichiers** dans la fenêtre principale du programme.

Si la protection en temps réel ne se lance pas au démarrage du système, c'est probablement dû au fait que l'option **Lancer automatiquement la protection en temps réel du système de fichiers** est désactivée. Pour activer cette option, sélectionnez Configuration avancée (F5) et cliquez sur **Ordinateur > Antivirus et antispyware > Protection en temps réel du système de fichiers** dans l'arborescence Configuration avancée. Dans la section **Configuration avancée** dans la partie inférieure de la fenêtre, vérifiez que la case **Lancer automatiquement la protection en temps réel du**

système de fichiers est cochée.

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

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

La protection en temps réel ne démarre pas

Si la protection en temps réel n'est pas lancée au démarrage du système (et si l'option **Lancer automatiquement la protection en temps réel du système de fichiers** est activée), le problème peut provenir de conflits avec d'autres programmes. Dans ce cas, consultez les spécialistes du service client ESET.

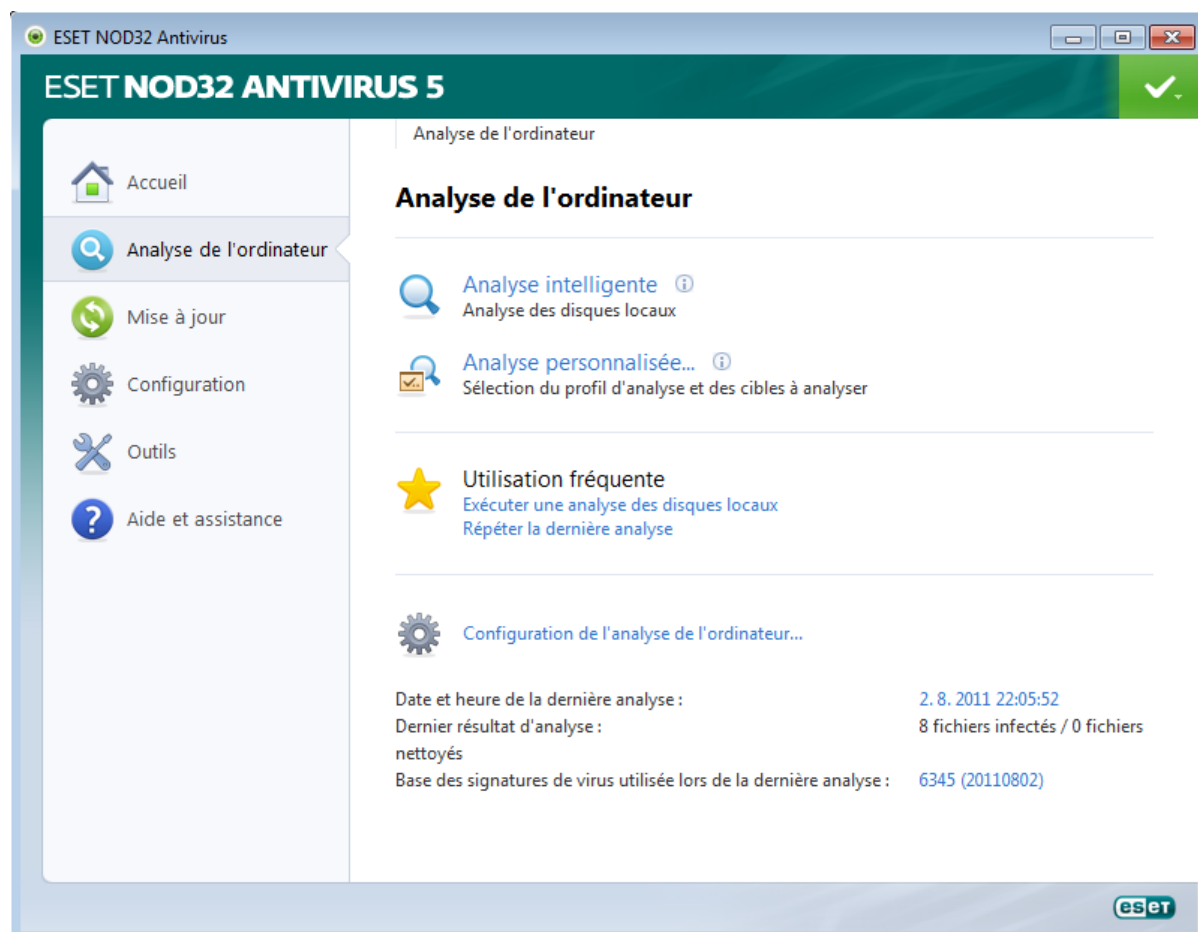
4.1.1.2 Protection des documents

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. L'option **Intégration du système** active le système de protection. Pour modifier cette option, appuyez sur la touche F5 pour ouvrir la fenêtre Configuration avancée et cliquez sur **Ordinateur > Antivirus et antispyware > Protection des documents** dans l'arborescence de configuration avancée. Lorsque cette option est activée, la protection des documents peut être affichée dans la fenêtre principale de ESET NOD32 Antivirus dans l'option **Configuration > Ordinateur**.

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

4.1.1.3 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 non seulement en cas de suspicion d'une infection, mais aussi régulièrement dans le cadre de mesures de sécurité routinières. Nous vous recommandons d'effectuer des analyses en profondeur de votre système de façon régulière afin d'y détecter tout virus éventuel qui n'aurait pas été capturé 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 est désactivée au moment de l'infection, si la base des signatures de virus n'est plus à jour ou si le fichier n'a pas été détecté comme virus lors de son enregistrement sur le disque.



Deux types d'**analyses de l'ordinateur** sont disponibles. L'[analyse intelligente](#) analyse le système sans exiger de reconfiguration des paramètres d'analyse. L'[analyse personnalisée](#) permet de sélectionner l'un des profils d'analyse prédéfinis, ainsi que de choisir des cibles spécifiques à analyser.

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

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**.

4.1.1.3.1 Type d'analyse

4.1.1.3.1.1 Analyse intelligente

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

4.1.1.3.1.2 Analyse personnalisée

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

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

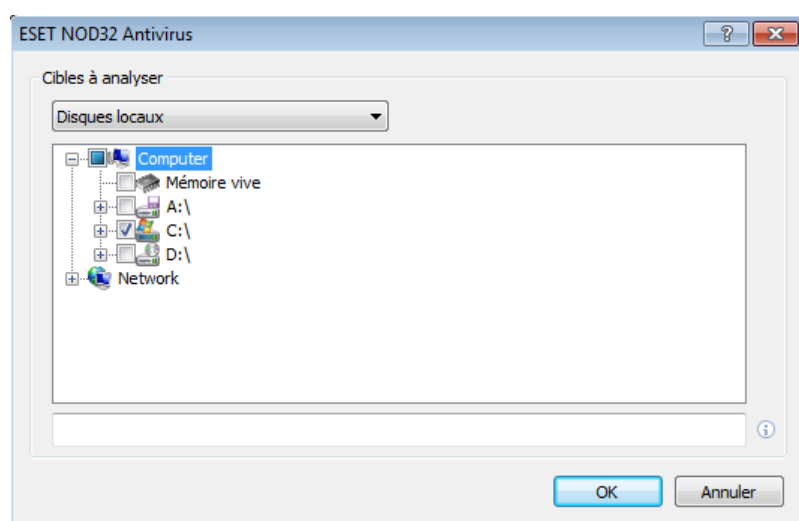
L'exécution d'analyses personnalisées de l'ordinateur convient aux utilisateurs chevronnés qui maîtrisent l'utilisation de programmes antivirus.

4.1.1.3.2 Cibles à analyser

La fenêtre Sélectionner les cibles à analyser permet de définir les objets (mémoire, lecteurs, secteurs, fichiers et dossiers) dans lesquels rechercher des infiltrations. Le menu déroulant **Cibles à analyser** permet de sélectionner des cibles à analyser prédéfinies :

- **Par les paramètres de profil** - Permet de sélectionner les cibles indiquées dans le profil d'analyse sélectionné.
- **Supports amovibles** - Permet de sélectionner les disquettes, les périphériques USB, les CD/DVD, etc.
- **Disques locaux** - Permet de sélectionner tous les disques durs système.
- **Lecteurs réseau** - Permet de sélectionner tous les disques réseau mappés.
- **Aucune sélection** - Annule toutes les sélections.

Vous pouvez également définir une cible d'analyse en entrant le chemin du dossier ou des fichiers à inclure dans l'analyse. Sélectionnez les cibles dans l'arborescence des périphériques disponibles sur l'ordinateur.



Pour accéder rapidement à une cible d'analyse ou ajouter directement une cible souhaitée, entrez-la dans le champ vide sous la liste de dossiers. Cela n'est possible que si aucun objet n'est sélectionné dans la liste de dossiers. Aucune cible ne doit être sélectionnée dans l'arborescence et le menu **Cibles à analyser** doit être défini sur **Aucune sélection**.

4.1.1.3.3 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.

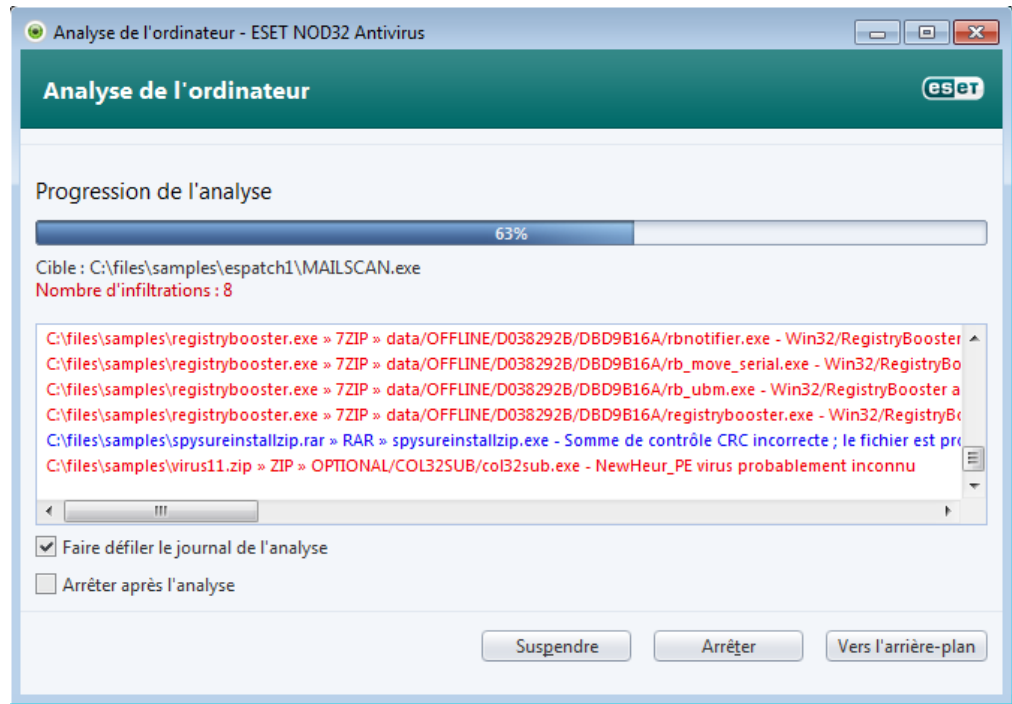
Pour créer un nouveau profil, ouvrez la fenêtre Configuration avancée (F5) et cliquez sur **Analyse de l'ordinateur > Profils...** La fenêtre **Profils de configuration** dispose d'un menu déroulant répertoriant les profils d'analyse existants, ainsi qu'une option permettant de créer un profil. Pour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

Exemple : Supposons la situation suivante : vous souhaitez créer votre propre profil d'analyse et la configuration

d'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**. Dans la fenêtre **Profils de configuration**, cliquez sur le bouton **Ajouter...** Saisissez le nom de votre nouveau profil dans le champ **Nom du profil** et sélectionnez **Analyse intelligente** dans le menu déroulant **Copier les paramètres depuis le profil**. Adaptez ensuite les autres paramètres à vos besoins.

4.1.1.3.4 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 des 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 le pourcentage des objets déjà numérisés par rapport aux objets qui ne sont pas encore analysés. La valeur est issue d'un nombre entier d'objets intégrés dans l'analyse.

Cible - Taille de l'élément analysé et emplacement.

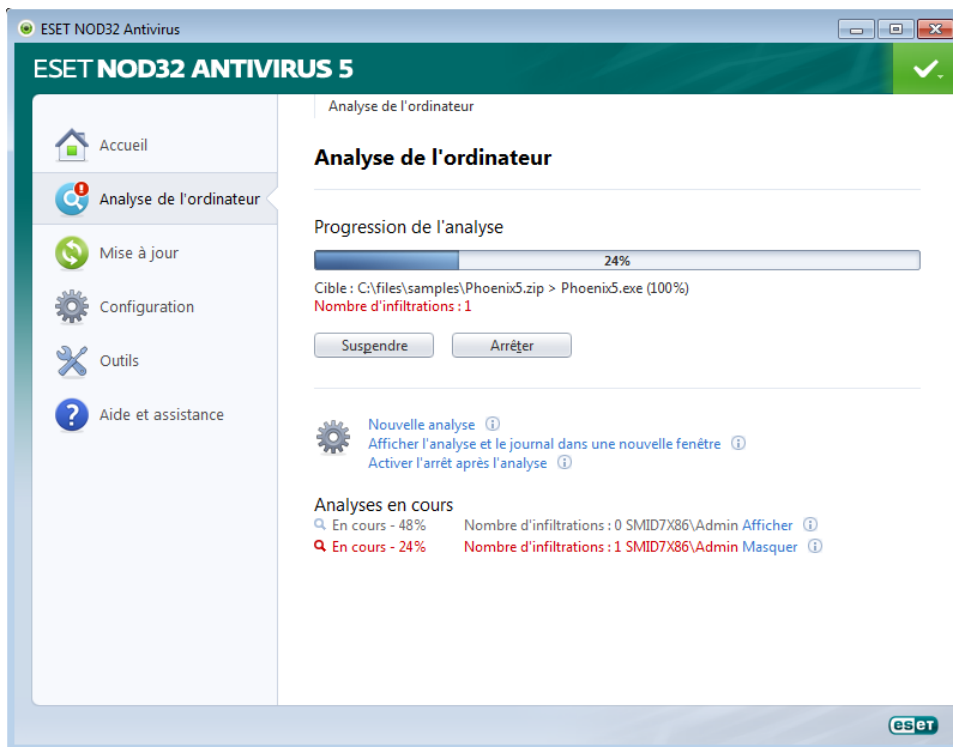
Nombre de menaces - Indique le nombre total de menaces détectées pendant l'analyse.

Interrompre - Interrompt l'analyse.

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

Arrêter - Met fin à l'analyse.

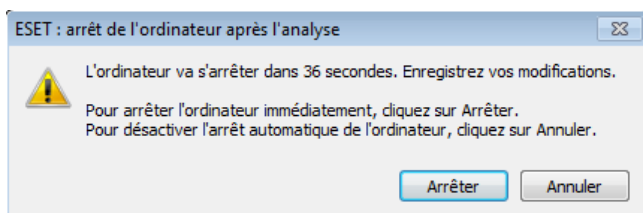
Vers l'arrière-plan - Vous pouvez exécuter une autre analyse en parallèle. L'analyse en cours s'exécute en arrière-plan.



Cliquez sur **Placer au premier plan** pour revenir 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.

Activer l'arrêt après l'analyse - Active un arrêt planifié à la fin de l'analyse à la demande de l'ordinateur. Une boîte de dialogue de confirmation d'arrêt s'ouvre pendant 60 secondes. Cliquez sur **Annuler** si vous souhaitez désactiver l'arrêt demandé.

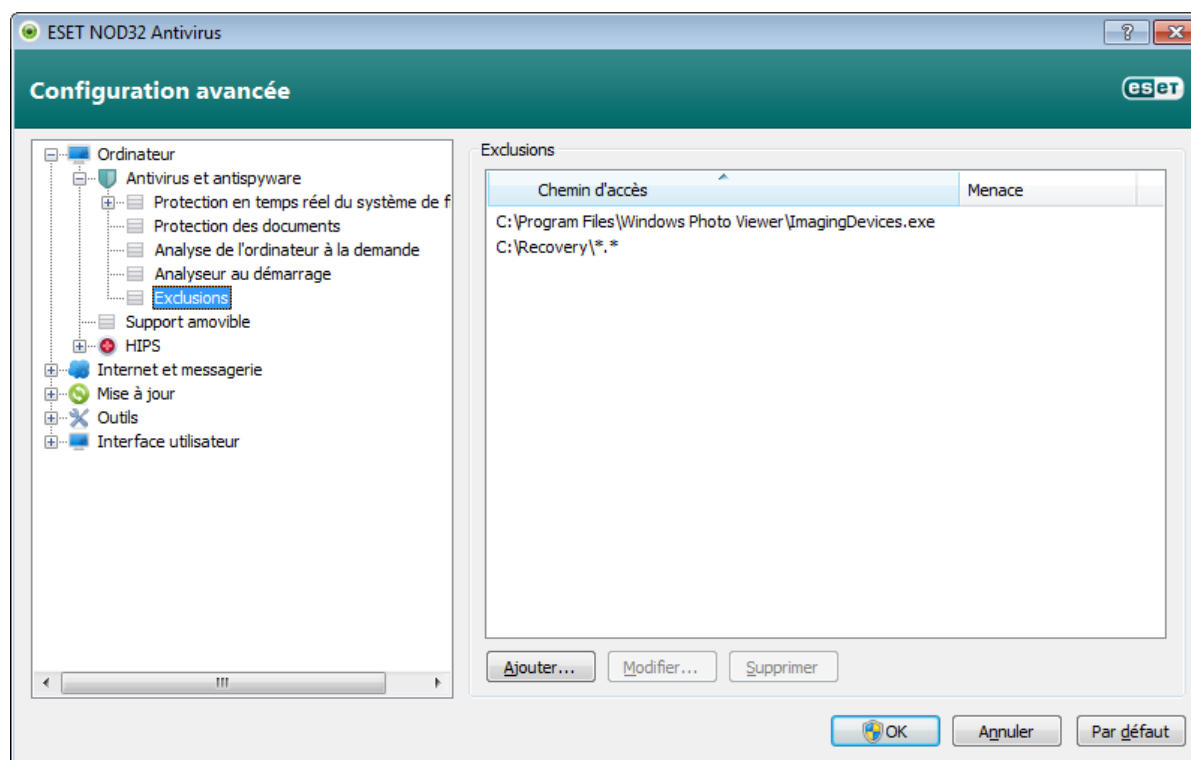


4.1.1.4 Analyse au démarrage

Lorsque la protection en temps réel du système de fichiers est activée, la vérification automatique des fichiers au démarrage est effectuée au démarrage du système ou lors de la mise à jour de la base des signatures de virus. Cette analyse dépend de la configuration et des tâches du **Planificateur**.

4.1.1.5 Exclusions

Les exclusions permettent d'exclure des fichiers et dossiers de l'analyse. Pour que tous les objets fassent l'objet d'une recherche de menaces, il est recommandé de ne pas modifier ces options. Toutefois, dans certains cas, il peut être utile d'exclure un objet. Par exemple, lorsque les entrées de bases de données volumineuses risquent de ralentir l'ordinateur pendant l'analyse ou lorsque le logiciel présente des conflits avec l'analyse.



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. Par conséquent, 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 **Configuration > Quarantaine** à l'aide de l'option du menu contextuel **Restaurer et exclure de la détection** du fichier en quarantaine.

Ajouter... - Exclut les objets de la détection.

Modifier... - Permet de modifier des entrées sélectionnées.

Supprimer - Supprime les entrées sélectionnées.

Pour exclure un objet de l'analyse :

1. Sélectionnez **Ajouter...**,
2. Entrez le chemin d'un objet ou sélectionnez-le dans l'arborescence ci-dessous.

Lorsque vous configurez des exclusions, vous pouvez utiliser des symboles spéciaux, des caractères génériques, tels que « * » et « ? ».

Exemples

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

4.1.1.6 Configuration des paramètres du moteur ThreatSense

ThreatSense est une technologie qui comprend de nombreuses méthodes de détection de menaces complexes. C'est une technologie proactive : elle fournit une protection dès les premières heures de propagation d'une nouvelle menace. Elle utilise une combinaison de plusieurs méthodes (analyse de code, émulation de code, signatures génériques, 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, ce qui maximise l'efficacité et le taux de détection. La technologie ThreatSense élimine avec succès les rootkits.

Les options de configuration de la technologie ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

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

Pour ouvrir la fenêtre de configuration, cliquez sur le bouton **Configuration...** situé dans la fenêtre de configuration de tous les modules qui utilisent 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 ;
- protection des documents ;
- protection du client de messagerie ;
- protection de l'accès au 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.

4.1.1.6.1 Objets

La section **Objets** 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) n'ont pas besoin de programmes spécialisés pour être décompressées.

Fichiers exécutables compressés par un compresseur d'exécutables - Contrairement aux archiveurs standard, ces fichiers se décompressent en mémoire. Outre les compacteurs statiques standard (UPX, yoda, ASPack, FSG, etc.), l'analyseur prend en charge de nombreux autres types de compacteurs (grâce à l'émulation de code).

4.1.1.6.2 Options

Utilisez la section **Options** pour sélectionner les méthodes à utiliser lors de la recherche d'infiltrations dans le système. Les options disponibles sont les suivantes :

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

Heuristique avancée/ADN/Signatures intelligentes - La méthode heuristique avancée utilise un algorithme heuristique 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. Grâce à l'heuristique avancée, les capacités de détection du programme sont très élevées. 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).

Les **applications potentiellement indésirables** ne sont pas nécessairement malveillantes, mais elles sont susceptibles d'affecter les performances de votre ordinateur. Ces applications sont habituellement installées après consentement. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Voici les changements les plus significatifs :

- affichage de nouvelles fenêtres (fenêtres contextuelles, publicités) ;
- activation et exécution de processus cachés ;
- augmentation de l'utilisation des ressources système ;
- modification des résultats de recherche ;
- communication de l'application avec des serveurs distants.

Applications potentiellement dangereuses - Les [applications potentiellement dangereuses](#) constituent la classification des logiciels commerciaux légitimes. 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.

ESET Live Grid - Grâce à la technologie de réputation d'ESET, les informations sur les fichiers analysés sont comparées aux données issues du système d'avertissement anticipé [ESET Live Grid](#) du service de cloud computing. Cette comparaison permet d'améliorer la détection tout en accélérant l'analyse.

4.1.1.6.3 Nettoyage

Les paramètres de nettoyage déterminent le comportement de l'analyseur lors du nettoyage des fichiers infectés. Trois niveaux de nettoyage sont possibles :

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.

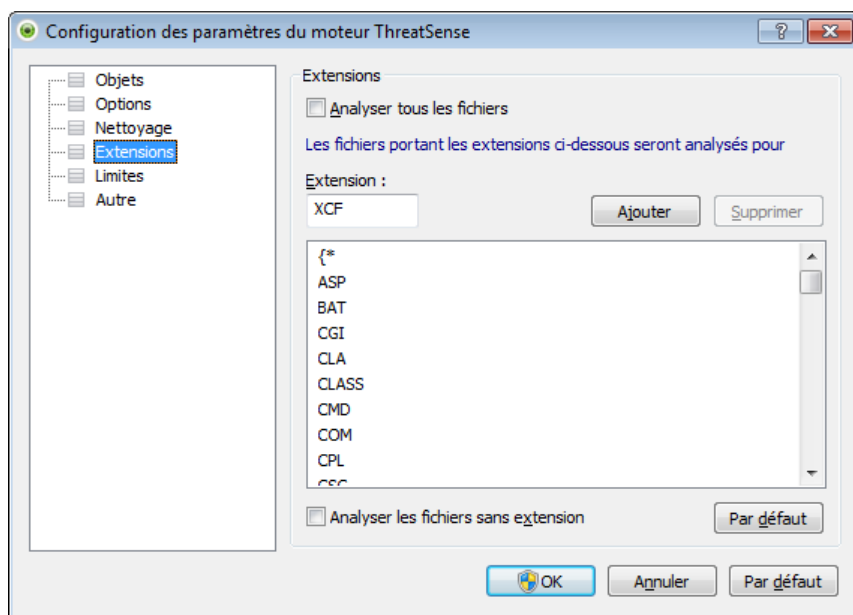
Niveau par défaut - Le programme tente de nettoyer ou de supprimer automatiquement tout fichier infecté en fonction d'une action prédéfinie (sur la base du type d'infiltration). La détection et la suppression d'un fichier infecté sont signalées par un message d'information affiché dans l'angle inférieur 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 n'a pas pu 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 (**Niveau par défaut**), 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.

4.1.1.6.4 Extension

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. Si l'option **Analyser tous les fichiers** est désélectionnée, la liste change et affiche toutes les extensions des fichiers analysés.

Pour activer l'analyse des fichiers sans extension, sélectionnez l'option **Analyser les fichiers sans extension**. L'option **Ne pas analyser les fichiers sans extension** devient disponible lorsque l'option **Analyser tous les fichiers** est activée.

L'exclusion de fichiers peut être utile si l'analyse de certains types de fichiers provoque un dysfonctionnement du programme utilisant ces 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. Le fait de taper une **extension** active le bouton **Ajouter** et permet d'ajouter cette nouvelle extension à la liste. Cliquez sur une extension de la liste, puis sur **Supprimer** pour supprimer l'extension de la liste.

Vous pouvez utiliser les symboles spéciaux « * » (astérisque) et « ? » (point d'interrogation). L'astérisque remplace n'importe quelle chaîne de caractères, tandis que le point d'interrogation remplace n'importe quel caractère. Un soin particulier doit être apporté à la spécification des adresses exclues, car la liste ne doit contenir que des adresses sûres et de confiance. De la même manière, veillez à employer correctement les symboles « * » et « ? » dans cette liste.

Cliquez sur le bouton **Défaut** et confirmez pour n'analyser que l'ensemble des extensions par défaut.

4.1.1.6.5 Limites

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

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

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

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*.

Si l'analyse d'une archive prend fin prématurément pour ces raisons, la case de l'archive reste non vérifiée.

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.

4.1.1.6.6 Autre

Vous pouvez configurer les options suivantes dans la section **Autre** :

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.

Lors de la configuration d'une analyse d'ordinateur, vous disposez des trois options suivantes pour les paramètres du moteur ThreatSense :

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.

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 mettre à jour (par exemple pour les utiliser avec des systèmes de sauvegarde de données).

Faire défiler le journal de l'analyse - Cette option permet d'autoriser/interdire le défilement du journal. Si cette option est sélectionnée, les informations défilent vers le haut dans la fenêtre d'affichage.

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.).

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 intelligente](#)),
- Lorsque l'analyse est terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés.

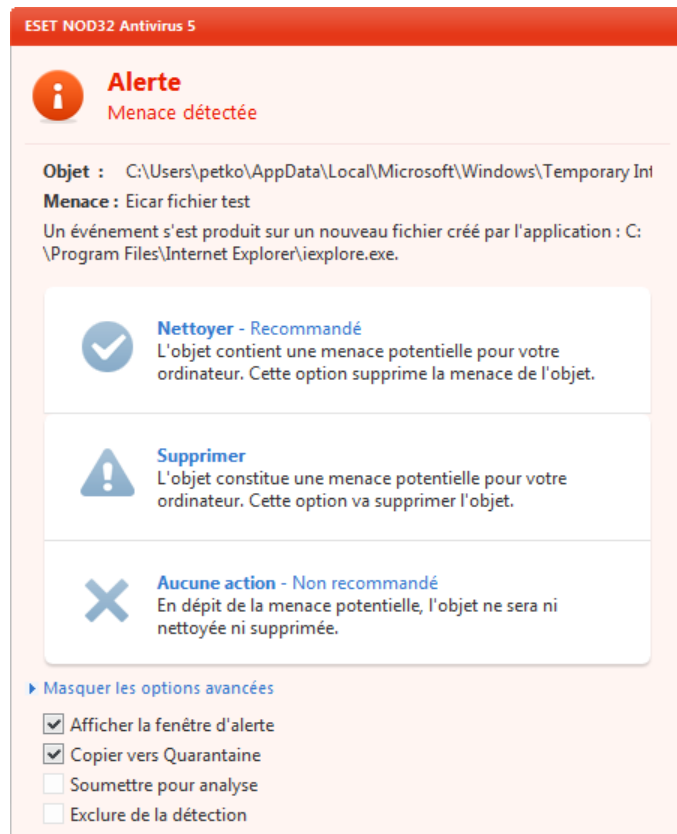
Si vous ne souhaitez analyser qu'une certaine partie de votre disque, cliquez sur **Analyse personnalisée** et sélectionnez des cibles à analyser.

Pour donner un exemple général de la façon dont les infiltrations sont traitées dans ESET NOD32 Antivirus, supposons qu'une infiltration soit détectée par la protection en temps réel du système de fichiers, qui utilise le niveau de nettoyage par défaut. Le programme tente de nettoyer ou de supprimer le fichier. Si aucune action n'est prédéfinie pour le module de protection en temps réel, 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 les fichiers infectés seraient conservés tels quels. La seule exception concerne les situations où vous êtes sûr que le fichier est inoffensif et qu'il a été détecté par erreur.

Nettoyage et suppression

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).

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. Cependant, soyez prudent si vous choisissez un nettoyage strict : dans ce mode, l'archive est supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

4.1.2 Analyse et blocage de supports amovibles

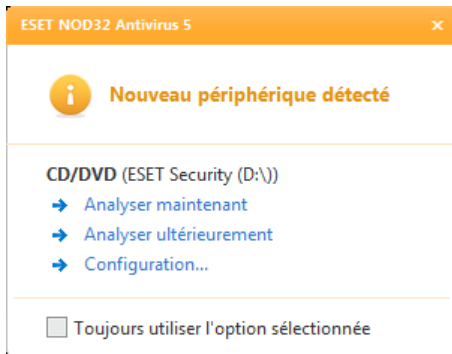
ESET NOD32 Antivirus permet de contrôler automatiquement les supports amovibles (CD/DVD/USB...). Ce module permet d'analyser, de bloquer ou d'ajuster les filtres étendus/autorisations, et de sélectionner la façon dont l'utilisateur peut accéder à un périphérique pour l'utiliser. Ce procédé peut être utile si l'administrateur souhaite empêcher les utilisateurs d'insérer des supports amovibles stockant du contenu non sollicité.

Supports amovibles pris en charge

- CD/DVD/Blu-ray
- Clé USB
- Lecteur USB
- FireWire

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 :

- **Analyser maintenant** - Le support amovible inséré fait l'objet d'une analyse à la demande.
- **Analyser ultérieurement** - Aucune action n'est exécutée et la fenêtre **Nouveau périphérique détecté** se ferme.
- **Configuration...** - Ouvre la section de configuration des supports amovibles.



Règles de blocage de support amovible - Sélectionnez cette option pour bloquer tous les supports amovibles connectés à l'ordinateur. Si vous voulez que certains supports soient disponibles, excluez-les du blocage.

Cliquez sur **Règles...** pour autoriser ou bloquer l'accès au support amovible sélectionné. Vous pouvez gérer dans cette fenêtre des règles étendues pour le support amovible. Les règles peuvent être filtrées par exemple par taille de support, numéro de série et type de périphérique. Chaque règle dispose de ses propres autorisations : vous pouvez donc autoriser, limiter ou bloquer l'accès au support amovible sélectionné.

4.1.3 Système HIPS (Host Intrusion Prevention System)

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, afin de bloquer activement et d'empêcher toute tentative de ce type.

Le système HIPS est disponible dans **Configuration avancée** (F5) en cliquant sur **Ordinateur > HIPS**. L'état HIPS (activé/désactivé) apparaît dans la fenêtre principale ESET NOD32 Antivirus, dans le volet **Configuration**, dans la partie droite de la section **Ordinateur**.

Avertissement : les modifications apportées aux paramètres HIPS ne sont effectuées que par un utilisateur expérimenté.

ESET NOD32 Antivirus intègre la technologie *Auto-défense* qui empêche les logiciels malveillants d'endommager ou de désactiver la protection antivirus et antispyware ; vous avez la garantie que votre système est protégé en permanence. Les modifications apportées aux paramètres **Activer HIPS** et **Activer l'auto-défense** entrent en vigueur après le redémarrage du système d'exploitation Windows. La désactivation de l'intégralité du système **HIPS** nécessite également un redémarrage de l'ordinateur. Le filtrage peut être effectué dans l'un des quatre modes :

Mode automatique avec règles - Les opérations sont activées, à l'exception des règles prédéfinies qui protègent votre système.

Mode interactif - L'utilisateur est invité à confirmer les opérations.

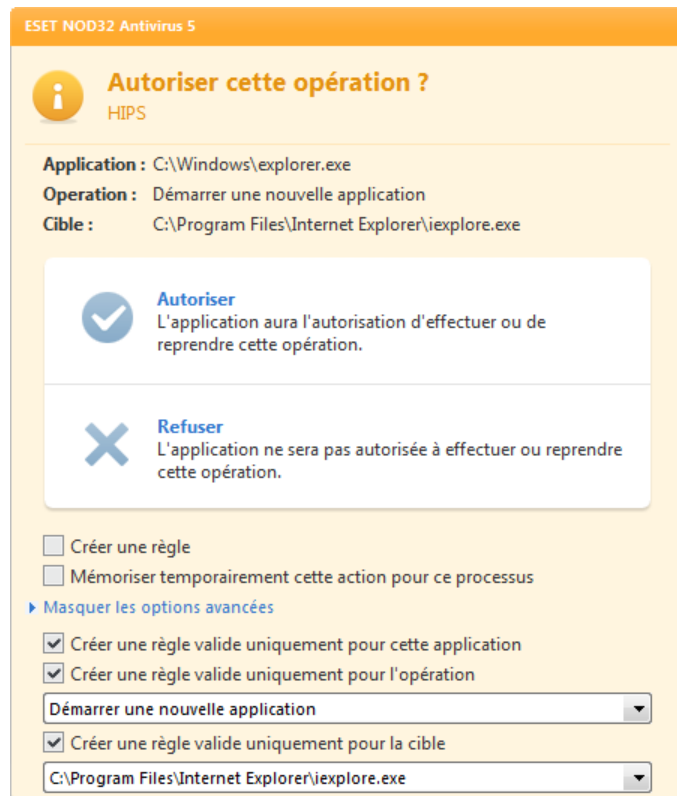
Mode basé sur des règles personnalisées - Les opérations sont bloquées.

Mode d'apprentissage - Les opérations sont activées et une règle est créée après chaque opération. Les règles créées dans ce mode peuvent être affichées dans l'**éditeur de règles**, mais leur priorité est inférieure à celle des règles créées à la main ou en mode automatique. Après la sélection du **mode d'apprentissage**, l'option **Notifier l'expiration de mode d'apprentissage dans X jours** devient disponible. À la fin de cette période, le mode d'apprentissage est de nouveau désactivé. La durée maximum est de 14 jours. À l'issue de cette période, une fenêtre contextuelle apparaît dans laquelle vous pouvez modifier les règles et sélectionner un autre mode de filtrage.

Le système HIPS surveille les événements dans le système d'exploitation et réagit en fonction des règles qui sont semblables à celles du pare-feu personnel.

Cliquez sur **Configurer les règles...** pour ouvrir la fenêtre de gestion des règles HIPS. Les règles y sont stockées et vous pouvez les sélectionner ou les supprimer.

Une boîte de dialogue apparaît chaque fois que l'option par défaut est **Demander**. L'utilisateur peut choisir de **refuser** ou d'**autoriser** l'opération. Si l'utilisateur ne choisit aucune action dans la période donnée, une nouvelle action est sélectionnée en fonction des règles.

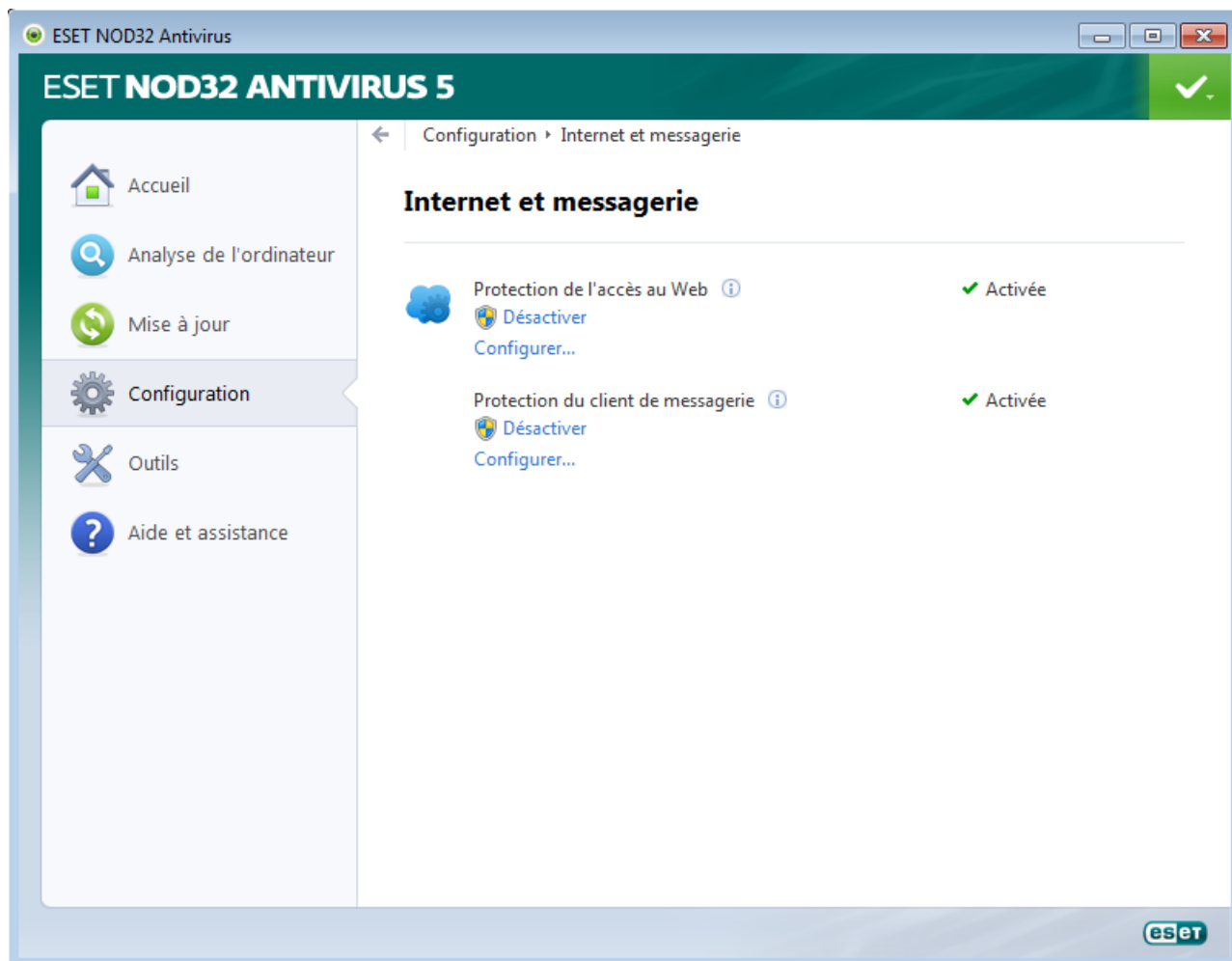


La boîte de dialogue permet de créer des règles en fonction du déclencheur et de ses conditions. Les paramètres exacts peuvent être définis une fois que vous cliquez sur **Afficher les options**. Les règles créées de cette manière sont égales aux règles créées manuellement ; la règle créée depuis une 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.

L'option **Mémoriser temporairement cette action pour ce processus** provoque la mémorisation de l'action (**Autoriser** / **Refuser**) de ce processus et l'utilise chaque fois que cette opération déclenche l'affichage d'une boîte de dialogue. Ces paramètres sont uniquement temporaires. Si les règles ou le mode de filtrage sont modifiés, pas la mise à jour d'un module HIPS ou le redémarrage du système, et ils sont supprimés.

4.2 Internet et messagerie

La configuration d'Internet et messagerie est disponible dans le volet **Configuration** lorsque vous cliquez sur l'intitulé **Internet et messagerie**. Elle permet également d'accéder à des paramètres plus détaillés du programme.



La connectivité Internet est une fonctionnalité standard des ordinateurs personnels. Elle est malheureusement devenue le principal mode de transfert des codes malveillants. Il est donc essentiel de surveiller de près la **protection de l'accès Internet**.

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 concernant le client de messagerie (POP3, MAPI, IMAP, HTTP).

Désactiver - Désactive la protection Internet/de messagerie des clients de messagerie.

Configurer... - Ouvre les paramètres avancés de protection Internet/de messagerie .

4.2.1 Protection de l'accès au Web

La connectivité Internet est une fonctionnalité standard des ordinateurs personnels. Elle est malheureusement devenue le principal mode de transfert des codes malveillants. Il est donc essentiel de surveiller de près la protection de l'accès à Internet.

Nous vous recommandons vivement d'activer l'option de protection de l'accès Internet. Cette option est disponible dans **Configuration > Internet et messagerie > Protection de l'accès au Web**.

4.2.1.1 HTTP, HTTPS

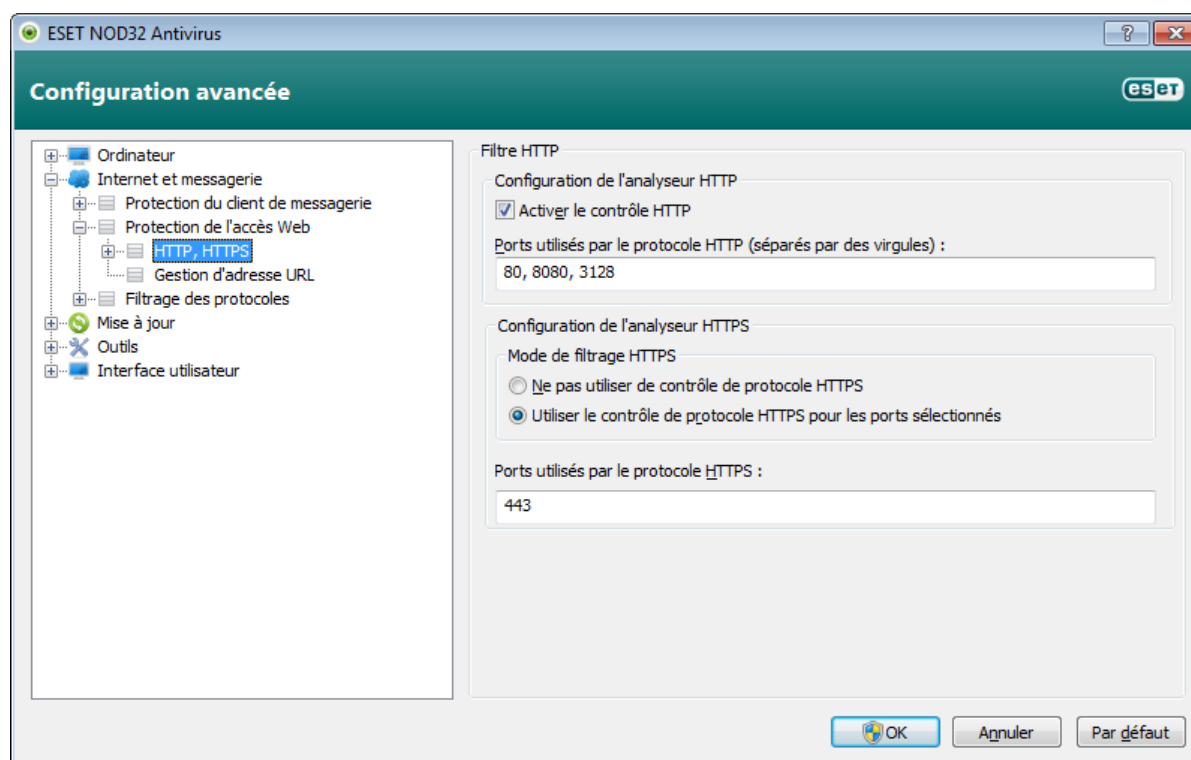
La protection de l'accès au Web opère par surveillance des communications entre les navigateurs Internet et les serveurs distants, conformément aux règles des protocoles HTTP et HTTPS (communications chiffrées). ESET NOD32 Antivirus prend en charge la vérification du protocole HTTPS. Ce type de communication 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). Par défaut, ESET NOD32 Antivirus est configuré pour utiliser les normes de la plupart des navigateurs Internet. Toutefois, vous pouvez modifier les options de configuration de l'analyseur HTTP dans la section **Configuration avancée** (F5) > **Antivirus et antispyware** > **Protection de l'accès au Web** > **HTTP, HTTPS**. Dans la fenêtre principale du filtre HTTP, vous pouvez activer ou désactiver l'option **Activer le contrôle HTTP**. Vous pouvez également définir les numéros de port utilisés pour la communication HTTP. Par défaut, les numéros de ports 80, 8080 et 3128 sont prédéfinis. Le contrôle HTTPS peut être effectué dans les modes suivants :

Ne pas utiliser de contrôle de protocole HTTPS - Les communications chiffrées ne sont pas vérifiées.

Utiliser le contrôle de protocole HTTPS pour les ports sélectionnés - Le contrôle HTTPS n'a lieu que pour les ports définis dans **Ports utilisés par le protocole HTTPS**.

Utiliser le contrôle de protocole HTTPS pour les ports sélectionnés - Le programme ne contrôle que les applications spécifiées dans la section Navigateurs et qui utilisent les ports définis dans **Ports utilisés par le protocole HTTPS**. Le port 443 est défini par défaut.

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 [Contrôle de protocole SSL](#) dans la section Configuration avancée (Internet et messagerie > Filtrage des protocoles > SSL) et activez l'option **Toujours analyser le protocole SSL**.

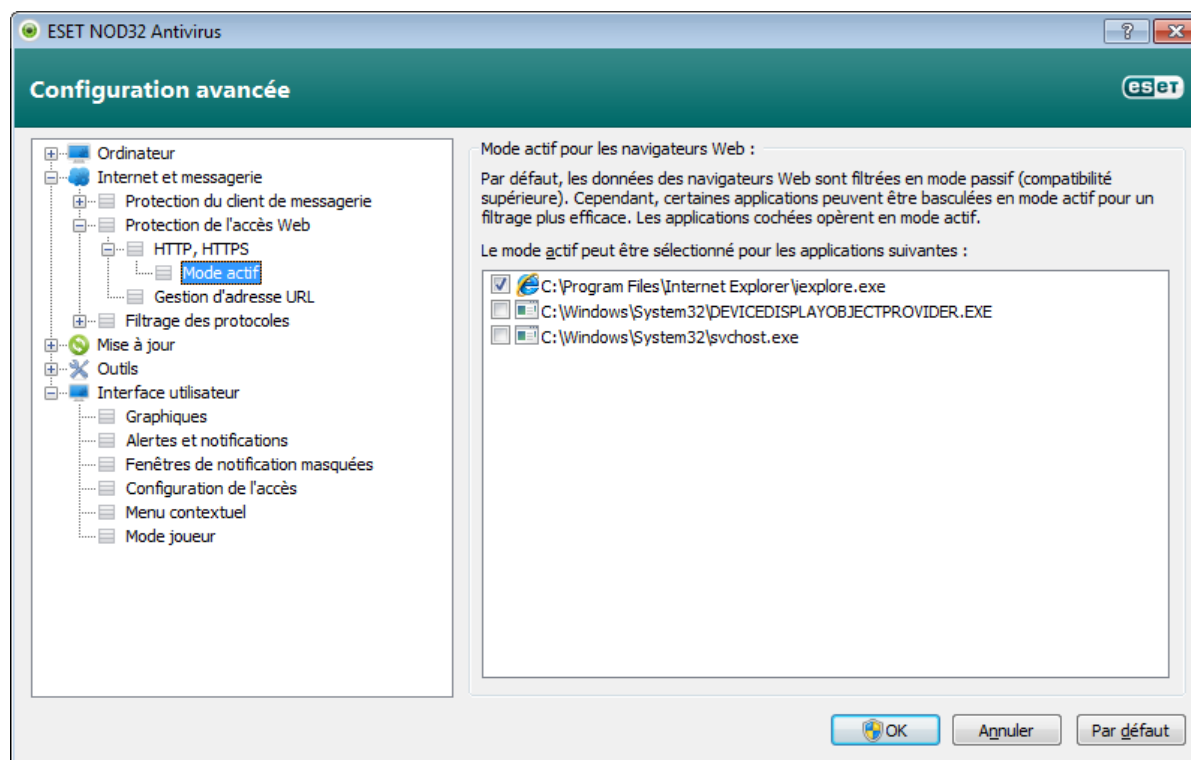


4.2.1.1.1 Mode actif pour les navigateurs Web

ESET NOD32 Antivirus contient également le sous-menu **Mode actif** qui définit le mode de contrôle des navigateurs Internet.

Le **mode actif** est utile, car il examine les données transférées des applications qui accèdent à Internet, qu'elles soient marquées comme navigateurs Web ou pas (pour plus d'informations, voir [Navigateurs Internet](#)). Si l'option n'est pas activée, la communication des applications est contrôlée progressivement, par lots. La vérification des données est alors moins efficace, mais la compatibilité avec les applications répertoriées est meilleure. Si le Mode actif ne pose pas de problèmes, nous recommandons de l'activer en cochant la case située à côté de l'application souhaitée. Voici comment fonctionne le mode actif : lorsqu'une application contrôlée télécharge des données, ces dernières sont sauvegardées dans un fichier temporaire créé par ESET NOD32 Antivirus. Les données ne sont pas encore accessibles par l'application. Une fois le téléchargement terminé, les données sont vérifiées afin de rechercher toute présence de code malveillant. Si aucune infiltration n'est trouvée, les données sont envoyées à l'application. Avec ce processus, les communications

réalisées par des applications contrôlées sont intégralement contrôlées. Si le mode passif est activé, les données sont envoyées à l'application par petites quantités pour éviter tout retard.

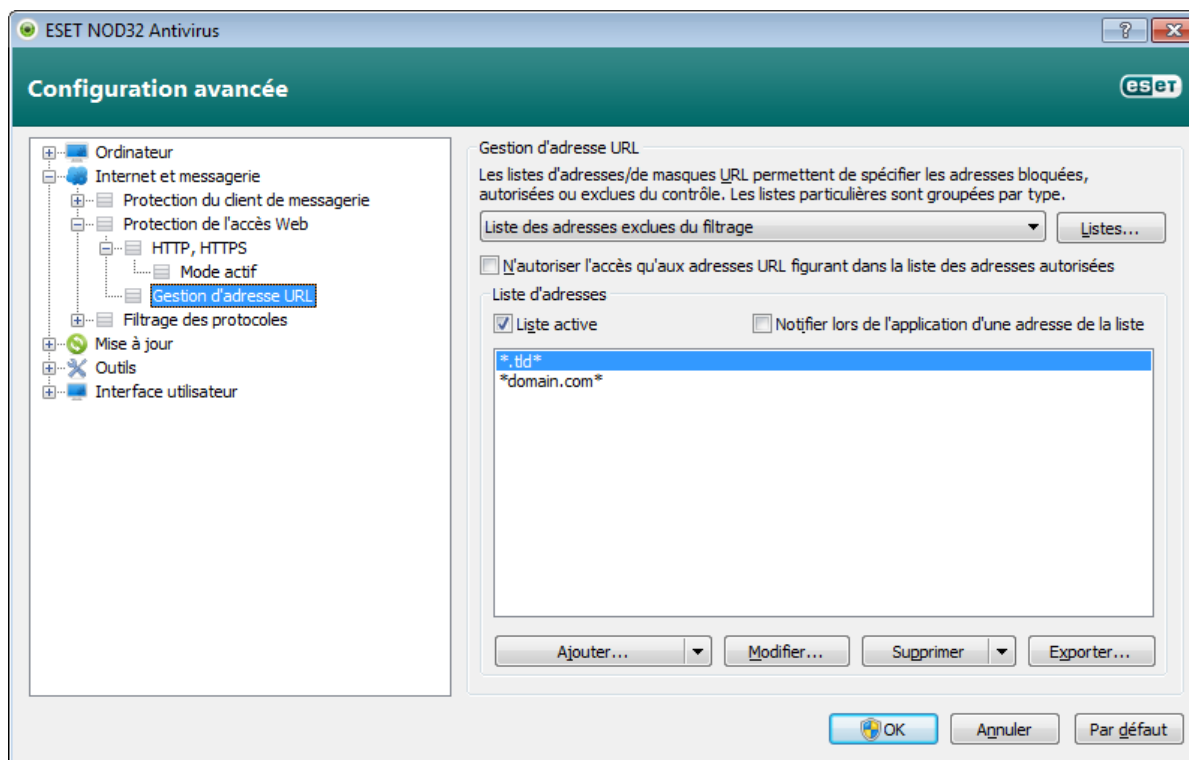


4.2.1.2 Gestion d'adresse URL

La section Gestion d'adresse URL permet de spécifier des listes d'adresses HTTP qui seront bloquées, autorisées ou exclues de la vérification. Les boutons **Ajouter**, **Modifier**, **Supprimer** et **Exporter** permettent de gérer les listes d'adresses. Les sites Web figurant dans la liste des adresses bloquées ne seront pas accessibles. Les sites Web figurant dans la liste des adresses exclues sont accessibles sans aucune analyse de code malveillant. Si vous sélectionnez l'option **N'autoriser l'accès qu'aux adresses HTTP figurant dans la liste des adresses autorisées** ; seules les adresses figurant dans la liste des adresses autorisées sont accessibles ; toutes les autres adresses HTTP sont bloquées.

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**. Lorsque vous cliquez sur le bouton **Listes...**, la fenêtre **Listes d'adresses HTTP/masques** apparaît. Vous pouvez **ajouter** ou **supprimer** des listes d'adresses. Pour ajouter une adresse URL HTTPS à la liste, l'option **Toujours analyser le protocole SSL** doit être actif.

Dans toutes les listes, vous pouvez utiliser les symboles spéciaux « * » (astérisque) et « ? » (point d'interrogation). L'astérisque remplace n'importe quelle chaîne de caractères, tandis que le point d'interrogation remplace n'importe quel caractère. Un soin particulier doit être apporté à la spécification des adresses exclues, car la liste ne doit contenir que des adresses sûres et de confiance. De la même manière, veillez à employer correctement les symboles « * » et « ? » dans cette liste. Pour activer une liste, sélectionnez l'option **Liste active**. Pour être informé lors de l'entrée d'une adresse à partir de la liste actuelle, sélectionnez l'option **Notifier lors de l'application d'une adresse de la liste**.



Ajouter.../À partir du fichier - Permet d'ajouter une adresse à la liste, soit manuellement (**Ajouter**), soit à partir d'un simple fichier texte (**À partir du fichier**). L'option **À partir du fichier** permet d'ajouter plusieurs adresses de messagerie qui sont enregistrées dans un fichier texte.

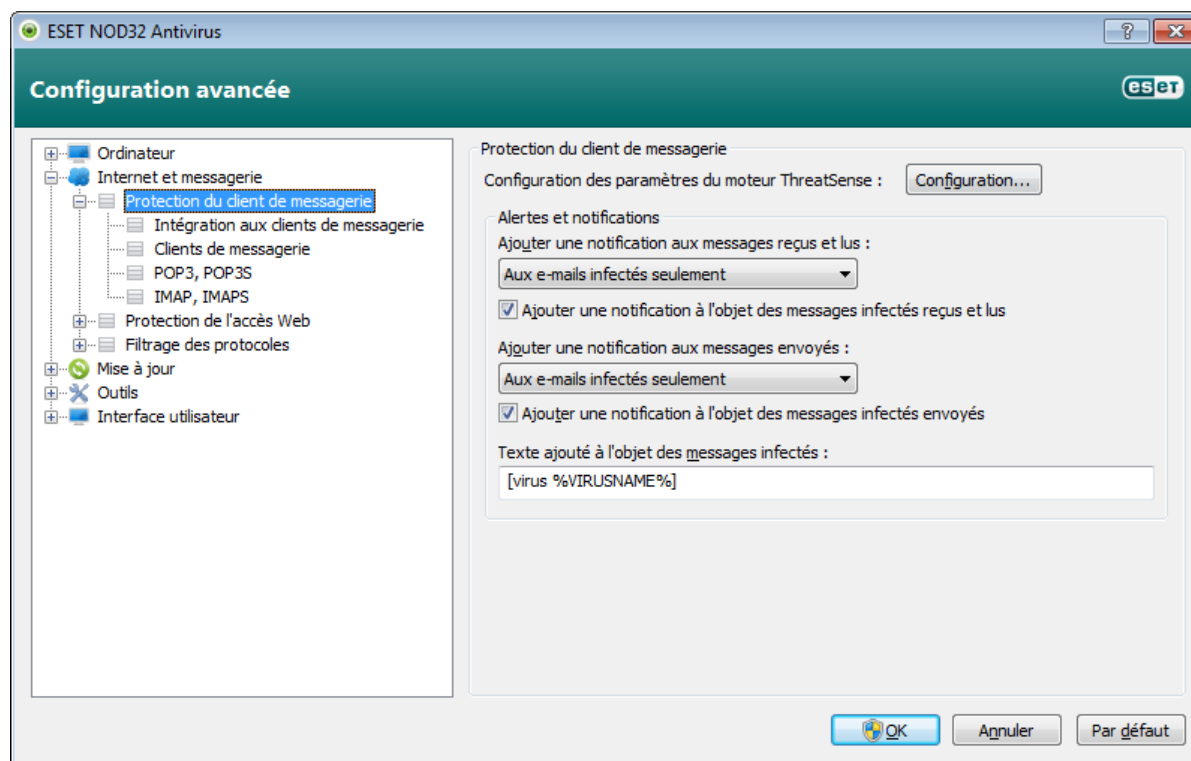
Modifier... - Permet de modifier manuellement des adresses, par exemple en ajoutant un masque (« * » et « ? »).

Supprimer/Supprimer tout - Cliquez sur **Supprimer** pour supprimer l'adresse sélectionnée dans la liste. Pour supprimer toutes les adresses, cliquez sur **Tout supprimer**.

Exporter... - Cette option permet d'enregistrer des adresses de la liste actuelle dans un simple fichier texte.

4.2.2 Protection du client de messagerie

La protection de la messagerie offre le contrôle de la communication par courrier électronique effectuée 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 offertes par le moteur d'analyse ThreatSense. Autrement dit, la détection des programmes malveillants s'effectue avant la comparaison avec la base des signatures de virus. 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 > Internet et messagerie > Protection du client de messagerie**.

Configuration des paramètres du moteur ThreatSense - La configuration avancée de l'analyseur de virus permet de configurer les cibles à analyser, les méthodes de détection, etc. Cliquez sur **Configuration...** pour afficher la fenêtre de configuration détaillée de l'analyseur de virus.

Après la vérification d'un courrier, une notification avec le résultat de l'analyse peut être ajoutée au message. Vous pouvez sélectionner les options **Ajouter une notification aux messages reçus et lus** et **Ajouter une notification aux messages envoyés**. Les notifications ne peuvent pas être transmises sans question, car elles risquent d'être ignorées par les messages HTML problématiques ou même faussées par certains virus. Les notifications peuvent être ajoutées au courrier reçu/lu ou envoyé (ou les deux). Les options disponibles sont les suivantes :

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

Ajouter une note à l'objet des messages infectés reçus et lus/envoyés - Cochez cette case si vous souhaitez que la protection de la messagerie ajoute un avertissement de virus dans l'objet d'un e-mail 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 augmente également la crédibilité du destinataire et, en cas de détection d'une infiltration, fournit des informations précieuses sur le niveau de menace d'un message ou d'un expéditeur.

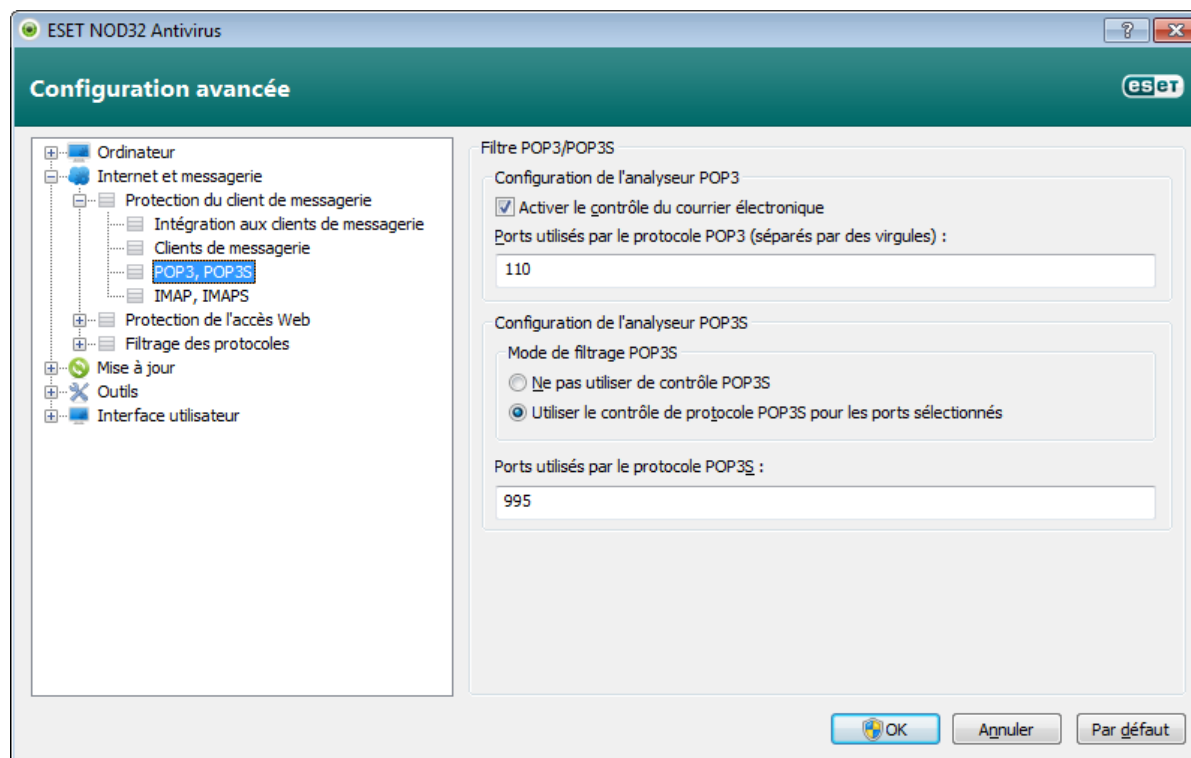
Texte ajouté à l'objet des messages infectés - Modifiez ce texte si vous souhaitez modifier le format du préfixe de l'objet d'un courrier infecté. Cette fonction remplace l'objet du message "Bonjour" par le préfixe "[virus]" au format suivant : "[virus] Bonjour". La variable %VIRUSNAME% représente la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

4.2.2.1 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 numéros de ports doivent être séparés par des virgules.

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 [Contrôle de protocole SSL](#) dans la section Configuration avancée (**Internet et messagerie** > **Filtrage des protocoles** > **SSL**) et activez l'option **Toujours analyser le protocole SSL**.



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**.

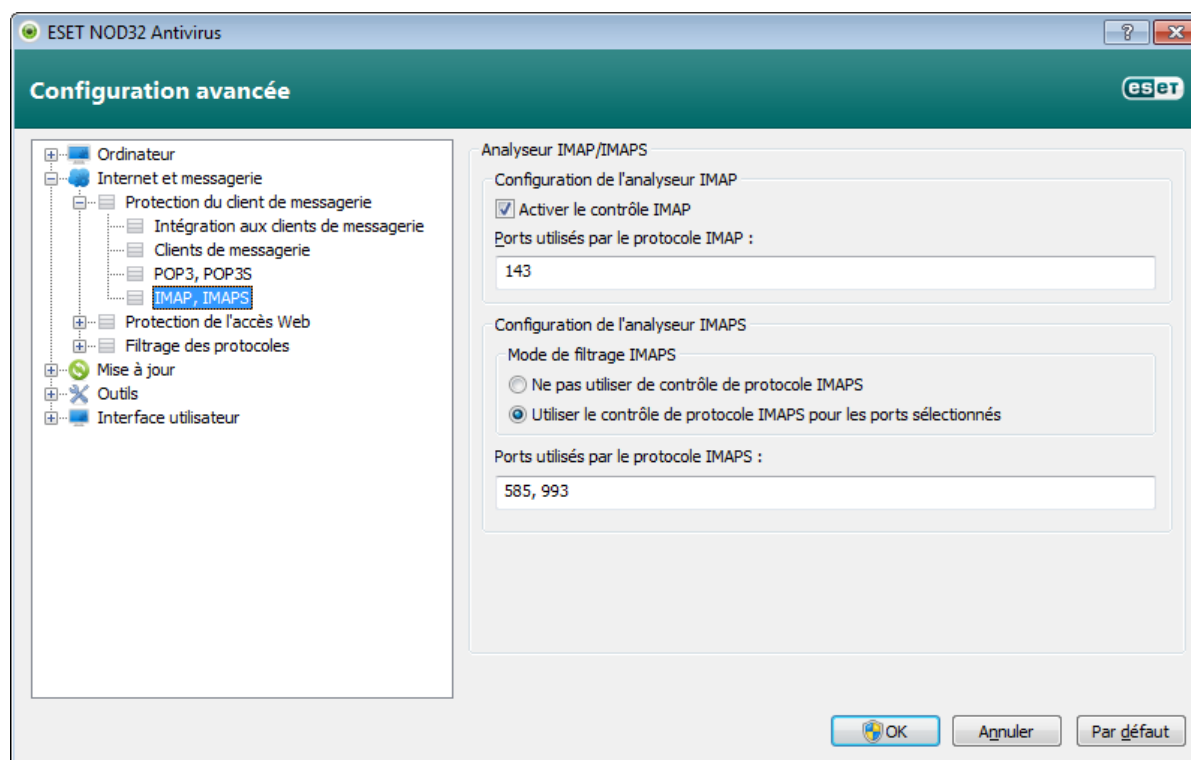
Ports utilisés par le protocole POP3S - Liste des ports POP3S à contrôler (995 par défaut).

4.2.2.2 Contrôle de protocole IMAP, IMAPS

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 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 IMAP s'effectue automatiquement sans qu'il faille reconfigurer le client de messagerie. Par défaut, toute communication sur le port 143 est soumise à une analyse, mais d'autres ports de communication peuvent être ajoutés au besoin. Les numéros de ports doivent être séparés par des virgules.

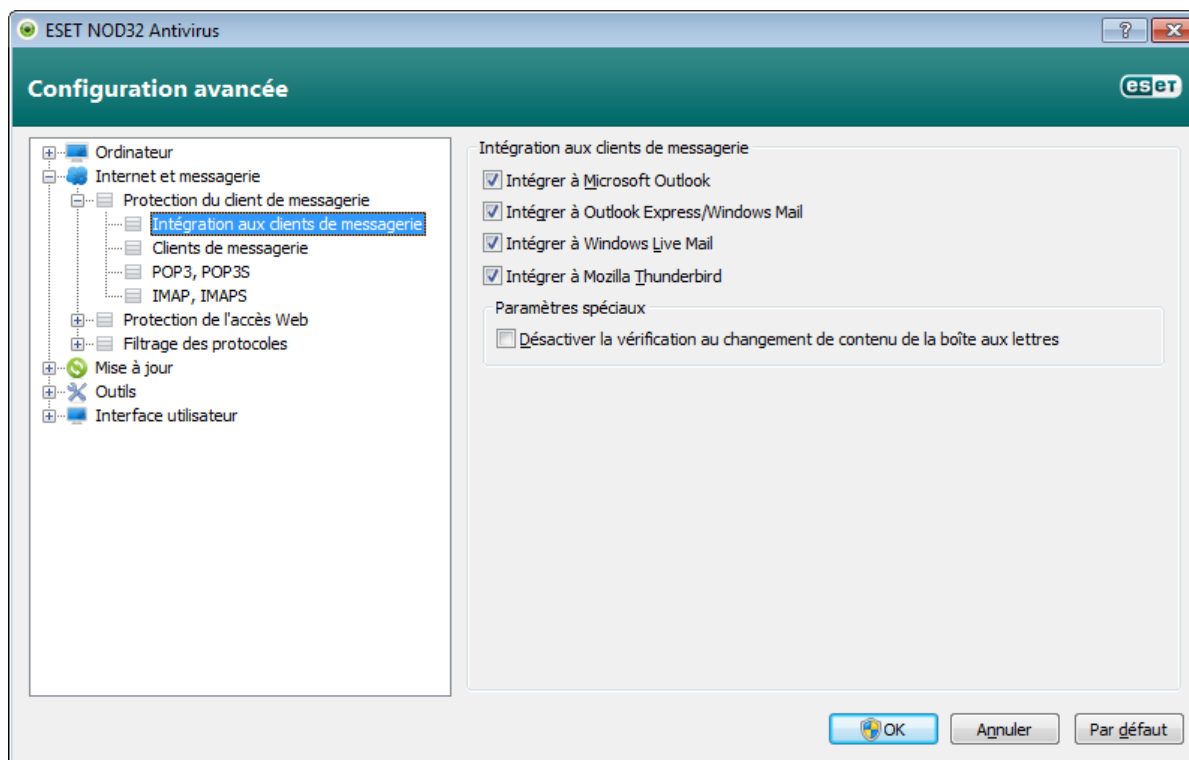
La communication chiffrée n'est pas vérifiée. Pour activer l'analyse de la communication chiffrée et afficher la configuration de l'analyseur, accédez à l'option [Contrôle de protocole SSL](#) dans la section Configuration avancée (**Internet et messagerie > Filtrage des protocoles > SSL**) et activez l'option **Toujours analyser le protocole SSL**.



4.2.2.3 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, cette intégration peut être activée dans ESET NOD32 Antivirus. Si 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 se trouvent dans la section **Configuration > Accéder à la configuration avancée... > Internet et messagerie > Protection du client de messagerie > Intégration aux clients de messagerie**. Les clients de messagerie pris en charge sont Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail et Mozilla Thunderbird.

Sélectionnez 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 du client de messagerie. Une telle situation peut se présenter lors du téléchargement de messages à partir du magasin Kerio Outlook Connector.



4.2.2.3.1 Configuration de la protection du client de messagerie

Le module de protection des messages prend en charge les clients de messagerie suivants : Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail et Mozilla Thunderbird. Ce module fonctionne comme un module plugin pour ces programmes. L'avantage principal du contrôle par 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.

Courriers électroniques à analyser

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 effectuer sur les courriers électroniques infectés

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 informe l'utilisateur des infiltrations et supprime le courrier.

Déplacer les courriers vers le dossier Éléments supprimés - Les courriers infectés sont déplacés automatiquement dans le dossier **Éléments supprimés**.

Déplacer les courriers vers le dossier - Spécifiez le dossier personnalisé dans lequel les courriers infectés doivent être déplacés lors de leur détection.

Autre

Répéter l'analyse après mise à jour - Active/désactive la réanalyse après la mise à jour de la base de données des signatures de virus.

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.

4.2.2.4 Suppression d'infiltrations

En cas de réception d'un message infecté, une fenêtre d'alerte s'affiche. Cette fenêtre indique le nom de l'expéditeur, son message et le nom de l'infiltration. La partie inférieure de la fenêtre présente les options disponibles concernant l'objet détecté : **Nettoyer**, **Supprimer** ou **Aucune action**. Dans la plupart des cas, nous recommandons de sélectionner **Nettoyer** ou **Supprimer**. Dans les situations particulières où vous souhaitez vraiment recevoir le fichier infecté, sélectionnez **Aucune action**. Si le niveau **Nettoyage strict** est activé, une fenêtre d'information sans options s'affiche.

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 contrôle fonctionne automatiquement, indépendamment du navigateur Internet ou du client de messagerie utilisés. Pour les communications chiffrées (SSL), voir **Filtrage des protocoles > SSL**.

Intégrer dans le système - Active le pilote de la fonctionnalité de filtre de protocole ESET NOD32 Antivirus.

Activer le filtrage du contenu des protocoles d'application - Si cette option est activée, tout le trafic HTTP(S), POP3(S) et IMAP(S) est contrôlé par l'analyseur antivirus.

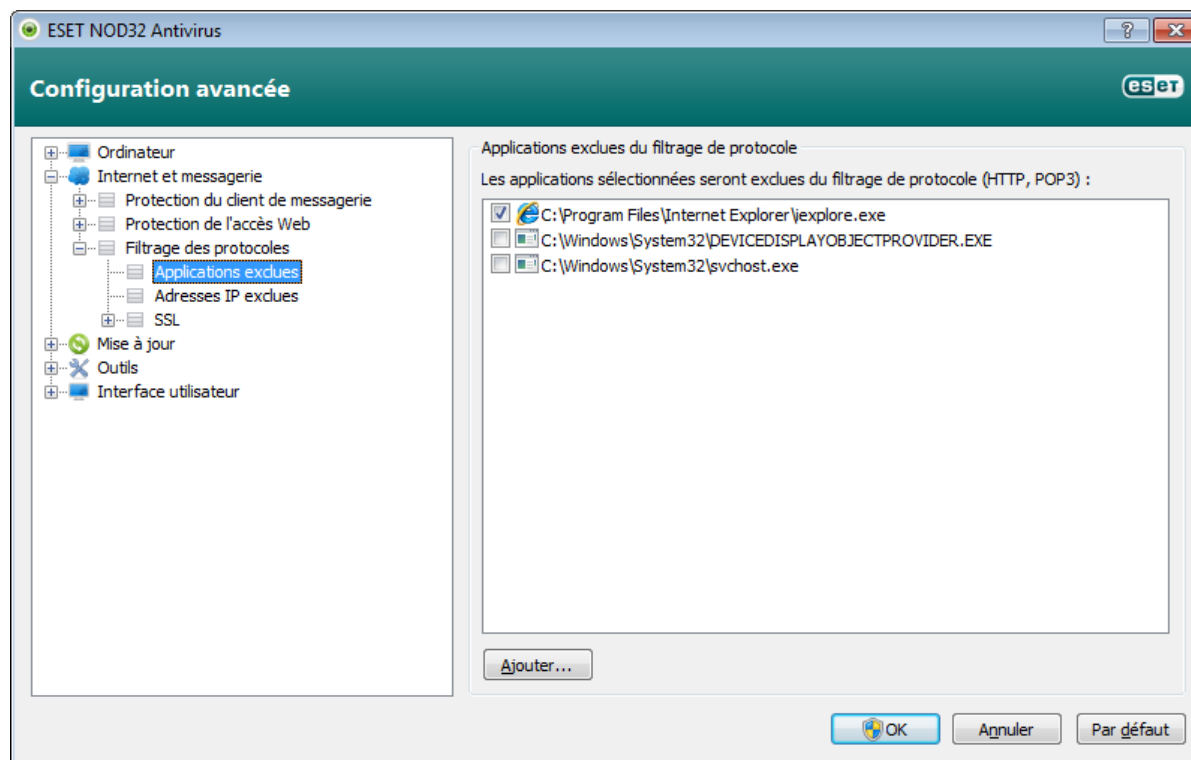
REMARQUE : à partir de Windows Vista Service Pack 1 et de Windows Server 2008, la nouvelle architecture de plateforme de filtrage Windows (WFP, Windows Filtering Platform) est utilisée pour contrôler les communications réseau. Étant donné que la technologie WFP utilise des techniques de surveillance spéciales, les options suivantes sont indisponibles :

- **Ports HTTP et POP3** - Limite le routage du trafic vers le serveur proxy interne uniquement pour les ports HTTP et POP3.
- **Applications marquées comme navigateurs Internet et clients de messagerie** - Limite le routage du trafic vers le serveur proxy interne uniquement pour les applications marquées comme navigateurs Internet et clients de messagerie. (**Internet et messagerie > Filtrage des protocoles > Web et clients de messagerie**).
- **Ports et applications marqués comme navigateurs Web ou clients de messagerie** - Active tout le trafic des ports HTTP et POP3, ainsi que toutes les communications des applications marquées comme navigateurs Internet et clients de messagerie vers le serveur proxy interne

4.2.3.1 Applications exclues

Pour exclure du filtrage de contenu la communication de certaines applications sensibles au réseau, sélectionnez ces applications dans la liste. Aucune recherche de menace n'est effectuée sur la communication HTTP/POP3 des applications sélectionnées. 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 le bouton **Ajouter...** pour sélectionner manuellement une application qui ne figure pas dans la liste des filtrages de protocole.

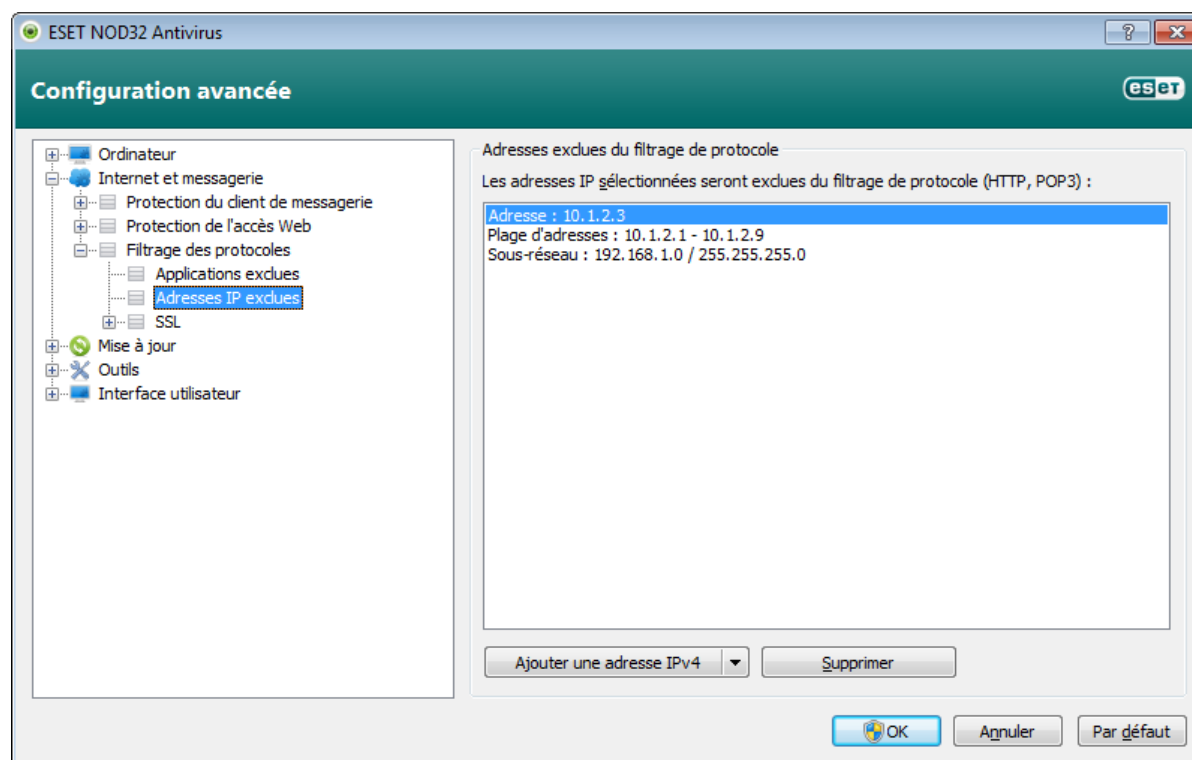


4.2.3.2 Adresses exclues

Les entrées de la liste sont exclues du filtrage de contenu. Aucune recherche de menace n'est effectuée sur les communications HTTP/POP3 des adresses sélectionnées. Il est recommandé d'utiliser cette option uniquement pour les adresses fiables.

Ajouter une adresse IPv4 - Cette option permet d'ajouter une adresse/une plage d'adresses/un sous-réseau IP d'un point distant auquel la règle doit être appliquée.

Supprimer - Supprime les entrées sélectionnées de la liste.



4.2.3.3 Contrôle de protocole SSL

ESET NOD32 Antivirus vous permet de vérifier les protocoles encapsulés dans le protocole SSL. Vous pouvez utiliser plusieurs modes d'analyse pour les communications SSL protégées à l'aide de certificats approuvés, de certificats inconnus ou de certificats exclus de la vérification des communications SSL protégées.

Toujours analyser le protocole SSL - 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 et que vous marquez comme étant approuvé (il est ajouté à la liste des certificats approuvés), la communication vers le serveur est autorisée et le contenu du canal de communication est filtré.

Demander pour les sites non visités (des exclusions peuvent être définies) - Si vous accédez à un nouveau site protégé par SSL (dont le certificat est inconnu), vous êtes invité à confirmer que vous souhaitez le visiter avant d'être autorisé à le faire. Ce mode vous permet de créer la liste des certificats SSL qui seront exclus de l'analyse.

Ne pas analyser le protocole SSL - Si cette option est activée, le programme n'analyse pas les communications SSL.

Appliquer les exceptions créées sur la base de certificats - Active l'utilisation d'exclusions spécifiées dans les certificats exclus et fiables pour l'analyse de la communication SSL. Cette option est disponible si vous sélectionnez **Toujours analyser le protocole SSL**.

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

4.2.3.3.1 Certificats

Pour que la communication SSL fonctionne correctement dans les navigateurs/clients de messagerie, il est essentiel d'ajouter le certificat racine pour ESET, spol s r.o. à la liste des certificats racines connus (éditeurs). Par conséquent, l'option **Ajouter le certificat racine aux navigateurs connus** doit être activée. Activez cette option pour ajouter manuellement le certificat racine d'ESET aux navigateurs connus (Opera, 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 serveur 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 l'option **Interroger sur la validité du certificat** est activée (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.

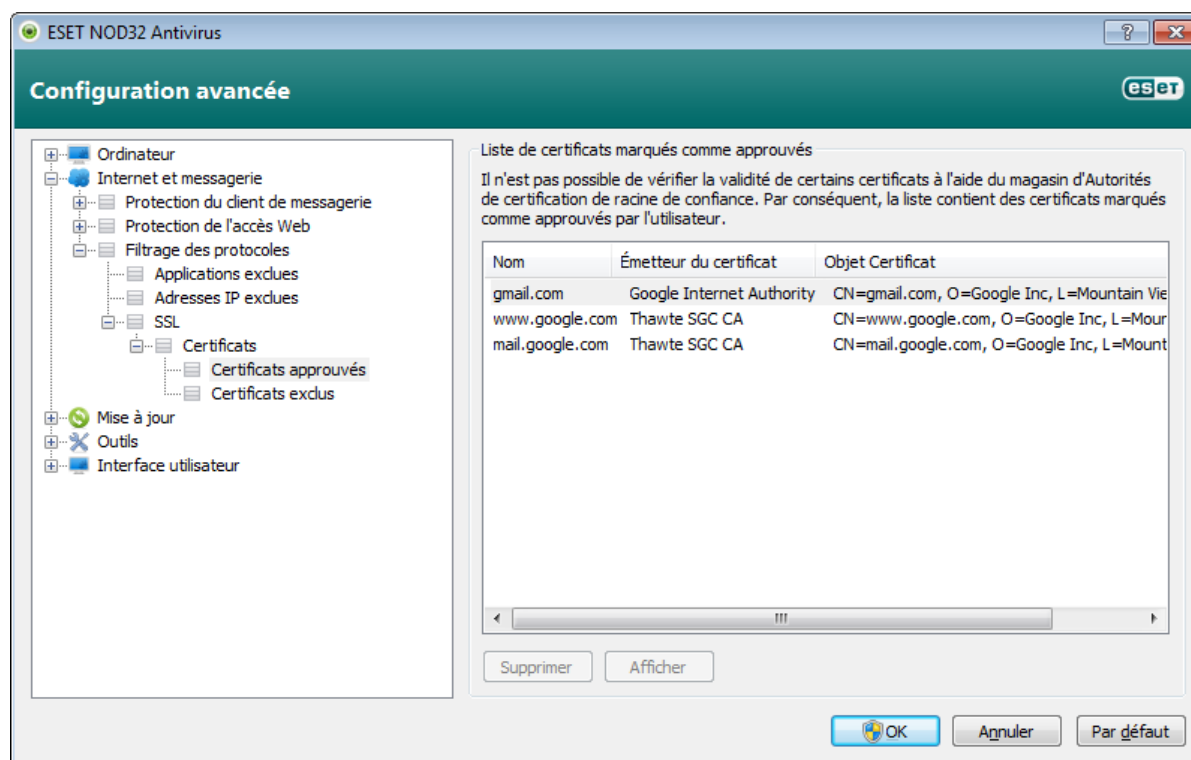


Vous pouvez définir l'option **Bloquer toute communication utilisant le certificat** pour toujours mettre fin à la connexion chiffrée au site utilisant le certificat non vérifié.

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.

4.2.3.3.1.1 Certificats approuvés

Outre le magasin TRCA intégré dans lequel ESET NOD32 Antivirus stocke les certificats approuvés, vous pouvez créer une liste personnalisée de certificats approuvés qui est disponible dans **Configuration avancée (F5) > Internet et messagerie > Filtrage des protocoles > SSL > Certificats > Certificats approuvés**. ESET NOD32 Antivirus vérifie le contenu des communications chiffrées qui utilisent les certificats figurant dans cette liste.



Pour supprimer des éléments sélectionnés dans la liste, cliquez sur le bouton **Supprimer**. Cliquez sur l'option **Afficher** (ou double-cliquez sur le certificat) pour afficher les informations concernant le certificat sélectionné.

4.2.3.3.1.2 Certificats exclus

La section Certificats exclus contient des certificats considérés comme étant sûrs. Le contenu des communications chiffrées qui utilisent les certificats répertoriés dans la liste des certificats exclus ne fait pas l'objet de recherche de menaces. Il est recommandé de n'exclure que les certificats Web qui sont garantis comme étant sécurisés et dont la communication utilisant les certificats n'a pas besoin d'être vérifiée. Pour supprimer des éléments sélectionnés dans la liste, cliquez sur le bouton **Supprimer**. Cliquez sur l'option **Afficher** (ou double-cliquez sur le certificat) pour afficher les informations concernant le certificat sélectionné.

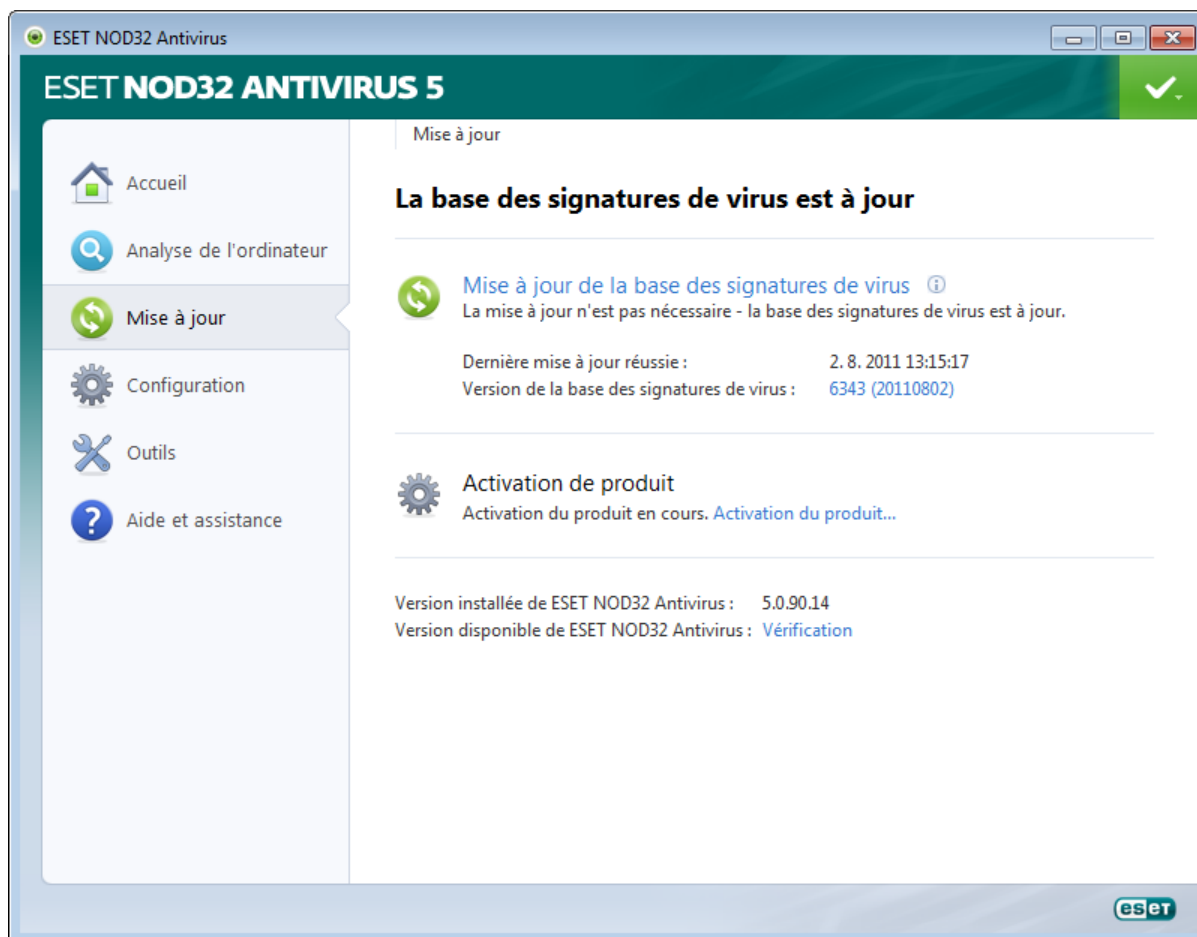
4.3 Mise à jour du programme

La mise à jour régulière d'ESET NOD32 Antivirus est la meilleure méthode pour bénéficier le niveau maximum de sécurité de votre ordinateur. Le module de mise à jour veille à ce que le programme soit toujours à jour de deux façons : en mettant à jour la base des signatures de virus et en mettant à jour les composants système.

En cliquant sur **Mettre à jour** dans le menu principal, 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. La fenêtre Mise à jour contient également la version de la base des signatures de virus. Cette indication numérique est un lien actif vers le site Web d'ESET, qui répertorie toutes les signatures ajoutées dans cette mise à jour.

Par ailleurs, il est possible de démarrer manuellement la mise à jour à l'aide de l'option **Mettre à jour la base des signatures de virus**. La mise à jour de la base des signatures de virus et celle des composants du programme sont des opérations importantes qui assurent la protection totale contre les attaques des codes malveillants. Il convient donc d'apporter une grande attention à leur configuration et à leur fonctionnement. Si vous n'avez pas saisi les détails de la licence pendant l'installation, vous pouvez indiquer vos nom d'utilisateur et le mot de passe lors de la mise à jour pour accéder aux serveurs de mise à jour ESET.

REMARQUE : le nom d'utilisateur et le mot de passe sont fournis par ESET après l'achat d'ESET NOD32 Antivirus.



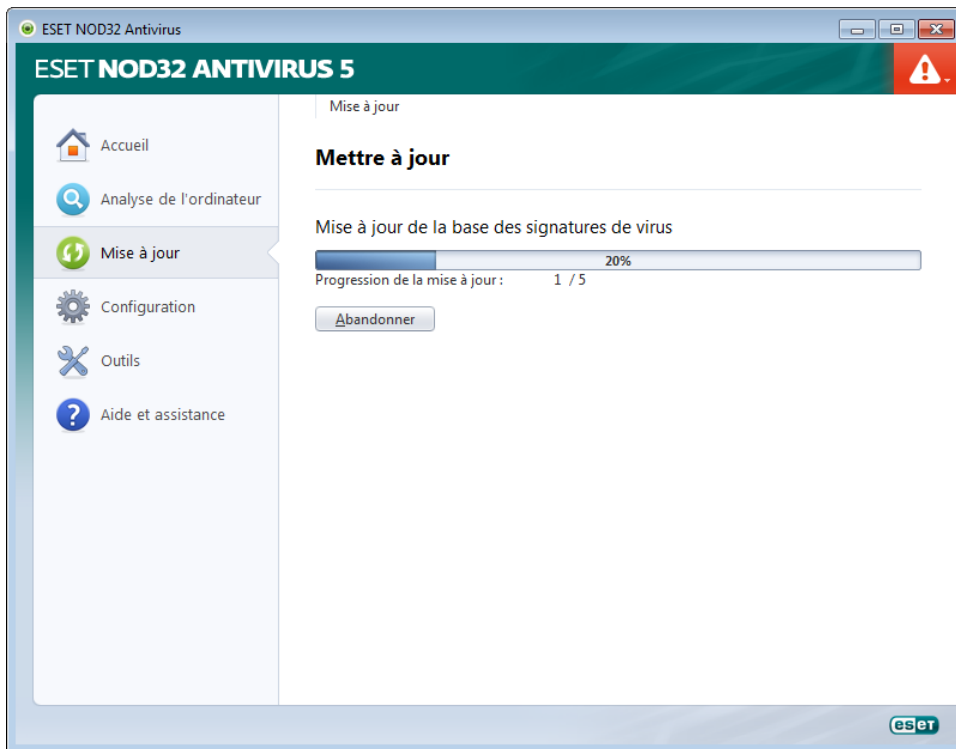
Dernière mise à jour réussie - Date de la dernière mise à jour. Vérifiez qu'il s'agit d'une date récente indiquant que la base des signatures de virus est à jour.

Version de la base des signatures de virus - Numéro de base des signatures de virus ; il s'agit également d'un lien actif vers le site Web d'ESET. Cliquez ici pour afficher la liste de toutes les signatures ajoutées dans la mise à jour.

Cliquez sur l'option de **vérification** afin de déterminer si vous disposez de la dernière **Version disponible de ESET NOD32 Antivirus** de votre produit de sécurité ESET.

Processus de mise à jour

Une fois que vous avez cliqué sur le bouton **Mettre à jour la base des signatures de virus**, le processus de téléchargement commence. La barre de progression qui s'affiche indique le temps de téléchargement restant. Pour interrompre la mise à jour, cliquez sur **Abandonner**.

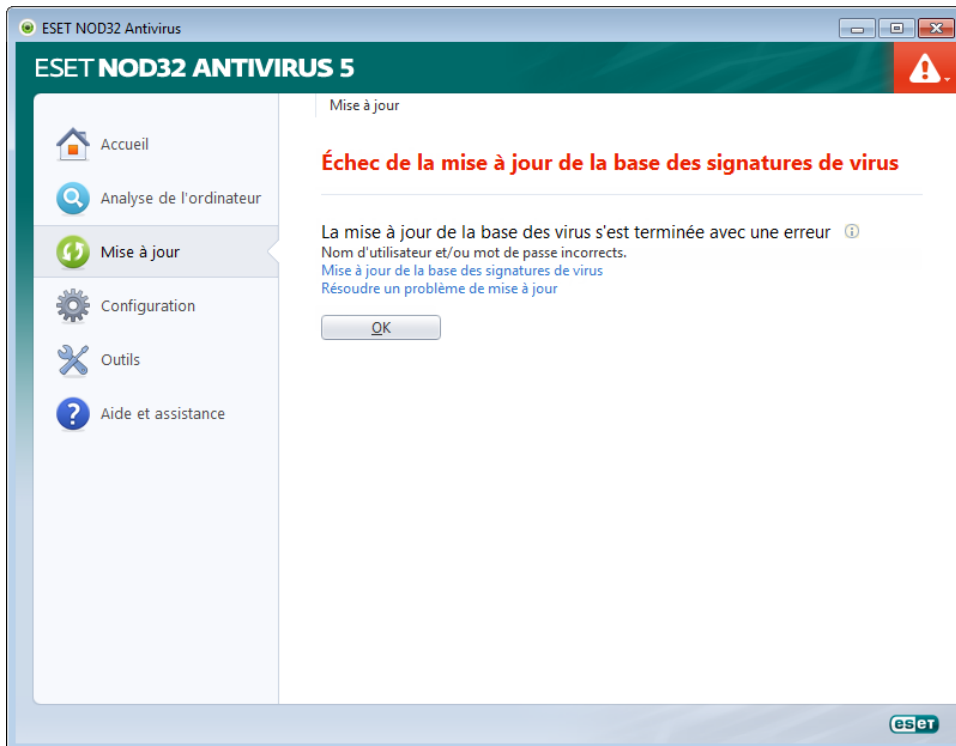


Important : dans des circonstances normales, lorsque les mises à jour sont téléchargées correctement, le message **Mise à jour non nécessaire - la base des signatures de virus installée est à jour** s'affiche dans la fenêtre **Mise à jour**. Si ce n'est pas le cas, le programme n'est pas à jour et le risque d'infection est accru. Veuillez à mettre à jour la base des signatures de virus dès que possible. Dans d'autres circonstances, l'un des messages d'erreur suivants s'affiche :

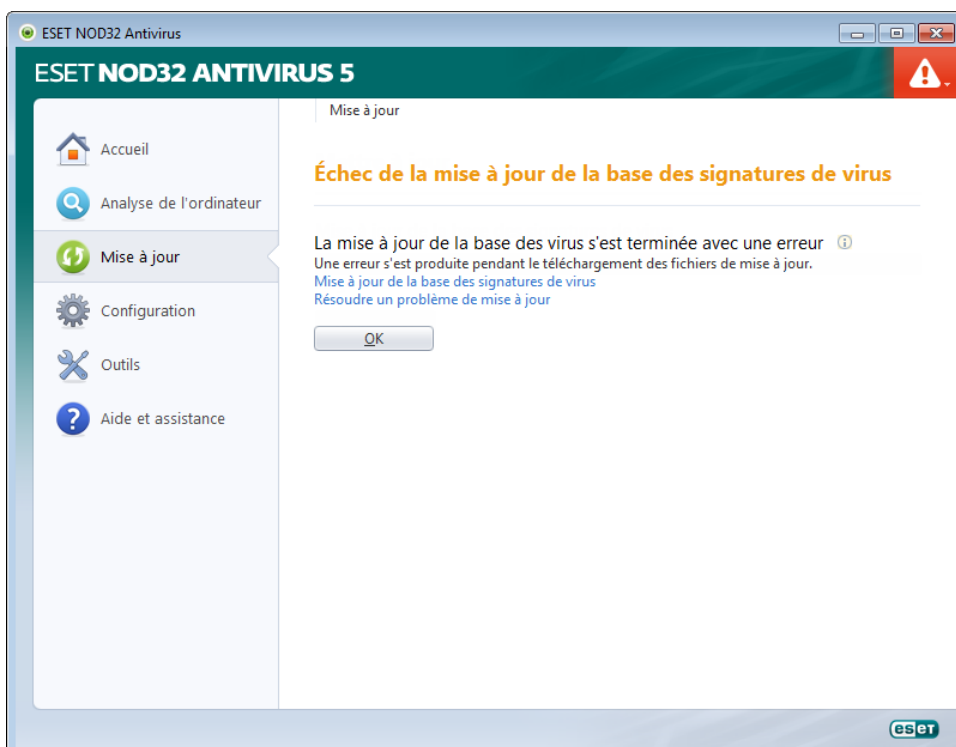
La base des signatures de virus n'est plus à jour - Cette erreur apparaît après plusieurs tentatives infructueuses de mise à jour de la base des signatures de virus. Nous vous conseillons de vérifier les paramètres de mise à jour. Cette erreur provient généralement de l'entrée incorrecte de [données d'authentification](#) ou de la configuration incorrecte des [paramètres de connexion](#).

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

Le nom d'utilisateur et le mot de passe entrés dans la configuration de mise à jour sont incorrects. Nous vous recommandons de vérifier vos [données d'authentification](#). La fenêtre Configuration avancée (cliquez sur **Configuration** dans le menu principal et sur **Accéder à la configuration avancée...** ou appuyez sur la touche F5 de votre clavier) comporte d'autres options de mise à jour. Cliquez sur **Mettre à jour** > **Mettre à jour** dans l'arborescence Configuration avancée à gauche.



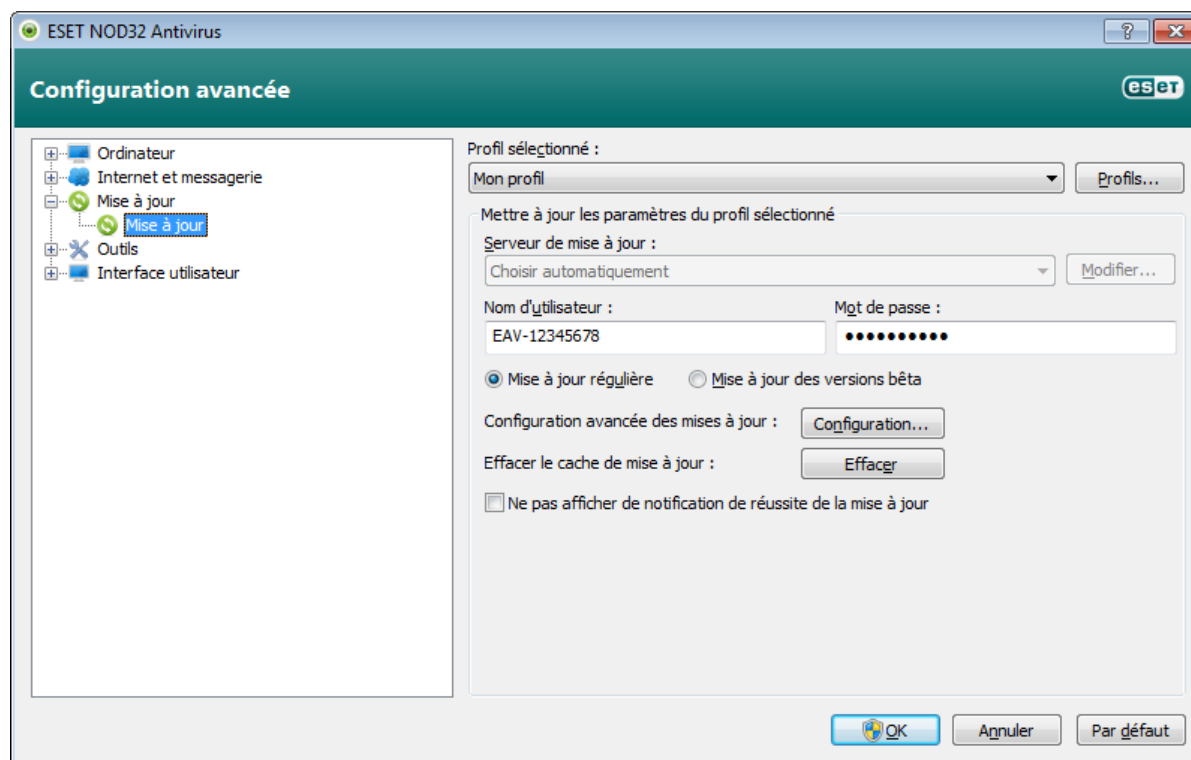
Échec de la mise à jour de la base des signatures de virus - L'erreur peut être due à des [paramètres de connexion Internet](#) incorrects. Nous vous recommandons de vérifier votre connectivité à Internet (en ouvrant un site Web dans votre navigateur). Si le site Web ne s'ouvre pas, cela est probablement dû au fait qu'aucune connexion à Internet n'est établie ou que votre ordinateur a des problèmes de connectivité. Consultez votre fournisseur de services Internet si vous n'avez pas de connexion Internet active.



4.3.1 Configuration des mises à jour

La section de la configuration des mises à jour permet de spécifier les informations concernant les sources des mises à jour, telles que les serveurs de mise à jour et les données d'authentification donnant accès à ces serveurs. Par défaut, le menu déroulant **Serveur de mise à jour** est défini sur l'option **Choisir automatiquement**, ce qui garantit que les fichiers de mise à jour sont téléchargés automatiquement depuis le serveur ESET en utilisant le moins de ressources réseau possible. Les options de configuration des mises à jour sont disponibles dans l'arborescence **Configuration avancée** (touche F5), dans **Mise à jour > Mise à jour**.

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



Le profil de mise à jour utilisé affiche le menu déroulant **Profil sélectionné**. Cliquez sur **Profils...** pour créer un nouveau profil.

La liste des serveurs de mise à jour disponibles est accessible par l'intermédiaire du menu déroulant **Serveur de mise à jour**. Le serveur de mise à jour est l'emplacement où sont stockées les mises à jour. Si vous utilisez un serveur ESET, laissez l'option par défaut **Choisir automatiquement** sélectionnée. Pour ajouter un nouveau serveur de mise à jour, cliquez sur **Modifier...** dans la section **Mettre à jour les paramètres du profil sélectionné**, puis cliquez sur le bouton **Ajouter**. Si un serveur local HTTP, appelé également miroir, est utilisé, le serveur de mise à jour doit être configuré comme suit :

`http://nom_ordinateur_ou_son_adresse_IP:2221.`

L'authentification des serveurs de mise à jour est basée sur le **nom d'utilisateur** et le **mot de passe** générés et qui vous ont été envoyés après l'achat. En cas d'utilisation d'un serveur miroir local, la vérification dépend de sa configuration. Par défaut, aucune vérification n'est exigée : les champs **Nom d'utilisateur** et **Mot de passe** restent vides.

Si l'option **Mode test** est activée, les modules bêta sont téléchargés pendant la mise à jour, ce qui permet à l'utilisateur de tester les nouvelles fonctionnalités du produit. La liste des modules en cours est disponible dans **Aide et assistance > À propos d'ESET NOD32 Antivirus**. Il est recommandé pour les utilisateurs non avertis de conserver la sélection par défaut de l'option **Mise à jour régulière**.

Cliquez sur le bouton **Configuration...** à côté de l'option **Configuration avancée des mises à jour** pour afficher une fenêtre des options de mise à jour avancée.

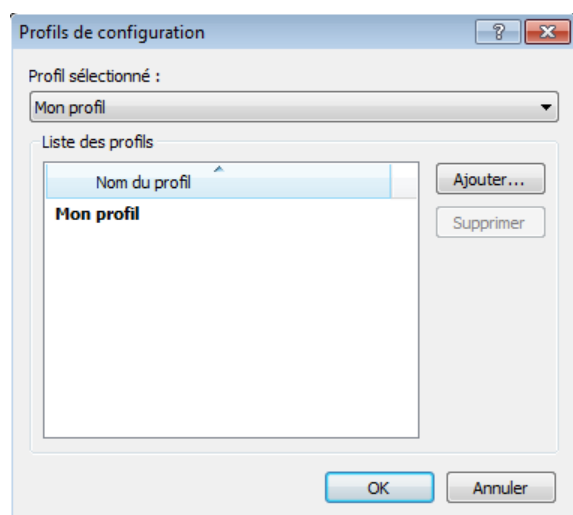
En cas de problème de mise à jour, cliquez sur le bouton **Effacer...** pour vider le dossier contenant les fichiers temporaires de mise à jour.

Ne pas afficher de 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 peuvent créer un autre profil correspondant aux propriétés de connexion Internet qui changent régulièrement.

Le menu déroulant **Profil sélectionné** affiche le profil sélectionné ; il est défini par défaut sur **Mon profil**. Pour créer un nouveau profil, cliquez sur les boutons **Profils...** et **Ajouter...**, puis indiquez votre propre **nom du profil**. Lors de la création d'un nouveau profil, vous pouvez copier les paramètres d'un profil existant en le sélectionnant dans le menu déroulant **Copier les paramètres depuis le profil**.



Dans la fenêtre de configuration du profil, vous pouvez indiquer le serveur de mise à jour dans la liste des serveurs disponibles ou encore ajouter un nouveau serveur. La liste des serveurs de mise à jour existants est accessible par l'intermédiaire du menu déroulant **Serveur de mise à jour**. Pour ajouter un nouveau serveur de mise à jour, cliquez sur **Modifier...** dans la section **Mettre à jour les paramètres du profil sélectionné**, puis cliquez sur le bouton **Ajouter**.

4.3.1.2 Configuration avancée des mises à jour

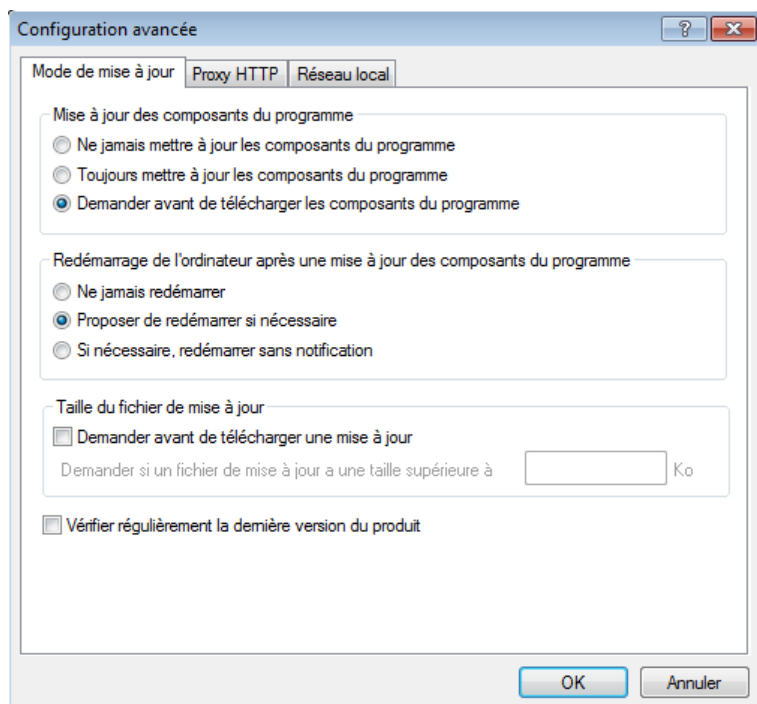
Pour afficher la configuration avancée des mises à jour, cliquez sur le bouton **Configuration....** Les options de configuration avancée de mise à jour englobent les options **Mode de mise à jour**, **Proxy HTTP** et **Réseau local**.

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 des composants du programme. Le programme vous permet de prédéfinir son comportement si une nouvelle mise à niveau de composant programme est disponible.

La mise à niveau des composants du programme offre de nouvelles fonctionnalités ou modifie les versions précédentes. Cette mise à jour peut s'effectuer sans intervention de l'utilisateur ou après sa notification. Le redémarrage de l'ordinateur peut être nécessaire après la mise à niveau des composants du programme. Dans la section **Mise à jour des composants du programme**, trois options sont disponibles :

- **Ne jamais mettre à jour les composants du programme** - Aucune mise à jour des composants du programme n'a lieu. Cette option convient aux serveurs, car ces derniers ne peuvent généralement être redémarrés qu'en cas de maintenance.
- **Effectuer la mise à niveau des composants du programme si elle est disponible** - Une mise à niveau de composants du programme est téléchargée et installée automatiquement. Notez que le redémarrage du système peut être nécessaire.
- **Demander avant de télécharger les composants du programme** - Option par défaut. Vous êtes invité à confirmer ou à refuser les mises à jour de composants de programme lorsqu'elles sont disponibles.



Après l'installation d'une mise à jour de composants du programme, il est peut-être nécessaire de redémarrer l'ordinateur afin de bénéficier de toutes les fonctionnalités des modules. La section **Redémarrer après une mise à jour des composants du programme** vous permet de sélectionner l'une des options suivantes :

- **Ne jamais redémarrer** - Vous n'êtes pas invité à redémarrer le système, même si c'est obligatoire. Notez qu'il n'est pas recommandé de sélectionner cette option, car l'ordinateur pourrait ne pas bien fonctionner jusqu'au prochain redémarrage.
- **Proposer le redémarrage de l'ordinateur si nécessaire** - Option par défaut. Après la mise à niveau de composants du programme, la boîte de dialogue qui apparaît invite à redémarrer l'ordinateur.
- **Si nécessaire, redémarrer sans notification** - Après la mise à niveau des composants du programme, l'ordinateur redémarre (si nécessaire).

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

Si l'option **Demander avant de télécharger une mise à jour** est cochée, une notification s'affiche lorsqu'une nouvelle mise à jour est disponible.

Si la taille du fichier de mise à jour est supérieure à la valeur **Demander si un fichier de mise à jour a une taille supérieure à** spécifiée, le programme affiche une notification.

L'option **Vérifier régulièrement la dernière version du produit** active la tâche planifiée correspondante (consultez la section [Planificateur](#)).

4.3.1.2.2 Serveur proxy

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 le bouton **Configuration...** à droite de l'option **Configuration avancée des mises à jour**. Cliquez sur l'onglet **Proxy HTTP** et sélectionnez l'une des trois options suivantes :

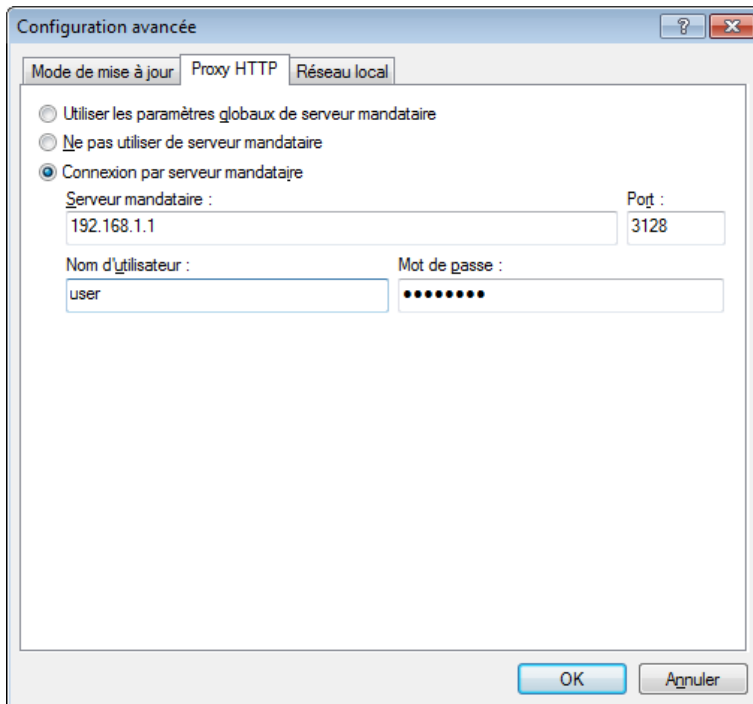
- **Utiliser les paramètres globaux de serveur proxy**
- **Ne pas utiliser de serveur proxy**
- **Connexion via un serveur proxy**

L'option **Utiliser les paramètres globaux de serveur proxy** utilise les options de configuration de serveur proxy déjà indiquées dans la branche **Outils > Serveur proxy** de l'arborescence Configuration avancée.

Sélectionnez l'option **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 serveur proxy doit être utilisé pour mettre à jour ESET NOD32 Antivirus et si ce serveur est différent de celui indiqué dans les paramètres globaux (**Outils > Serveur proxy**). Si c'est le cas, des paramètres supplémentaires doivent être spécifiés : **Serveur proxy** adresse, communication **Port**, plus **Nom utilisateur** et **MdP** pour le serveur proxy, si nécessaire.
- Les paramètres de serveur proxy n'ont pas été 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 la suite (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.



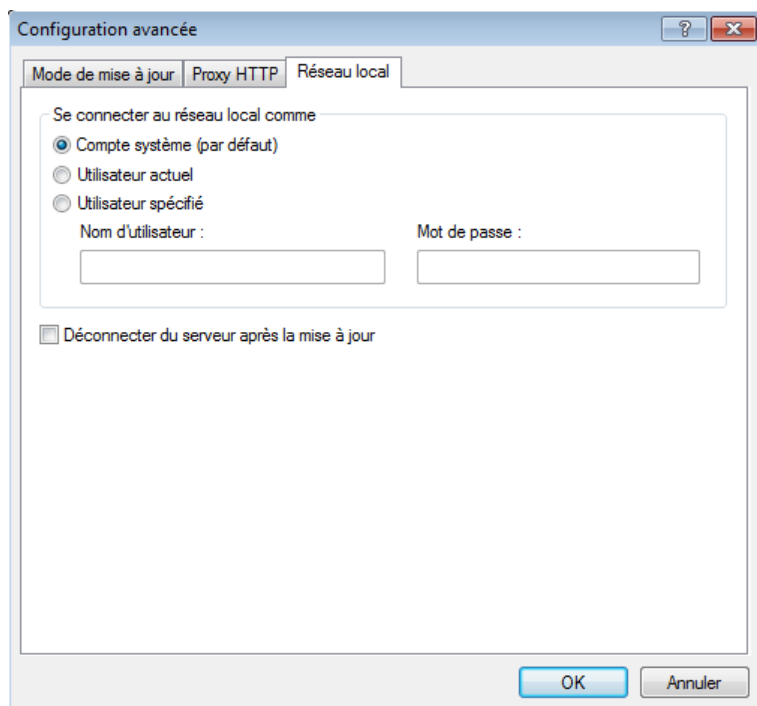
L'option par défaut pour le serveur proxy est **Utiliser les paramètres globaux de serveur proxy**.

REMARQUE : les données d'authentification telles que **Nom d'utilisateur** et **Mot de passe** permettent d'accéder au serveur proxy. Ne remplissez ces champs que si un nom d'utilisateur et un mot de passe sont requis. Notez que ces champs ne sont pas ceux du mot de passe/nom d'utilisateur d'ESET NOD32 Antivirus et ne doivent être remplis que si vous savez que vous avez besoin d'un mot de passe pour accéder à Internet via un serveur proxy.

4.3.1.2.3 Connexion au réseau local

Lors de mise à jour depuis un serveur local sur un système d'exploitation NT, une authentification est par défaut exigée pour chaque connexion réseau. Dans la plupart des cas, un compte système local n'a pas suffisamment de droits pour accéder au dossier miroir (ce dossier contient des copies des fichiers de mise à jour). Dans ce cas, entrez un nom d'utilisateur et un mot de passe dans la section de configuration des mises à jour ou spécifiez un compte avec lequel le programme peut accéder au serveur de mise à jour (miroir).

Pour configurer un compte de ce type, cliquez sur l'onglet **Réseau local**. La section **Se connecter au réseau local comme** propose les options **Compte système (par défaut)**, **Utilisateur actuel** et **Utilisateur spécifié**.



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

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

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

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

Sélectionnez l'option **Déconnecter du serveur après la mise à jour** si la connexion au serveur reste active, même après le téléchargement des mises à jour.

4.3.2 Comment créer des tâches de mise à jour

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

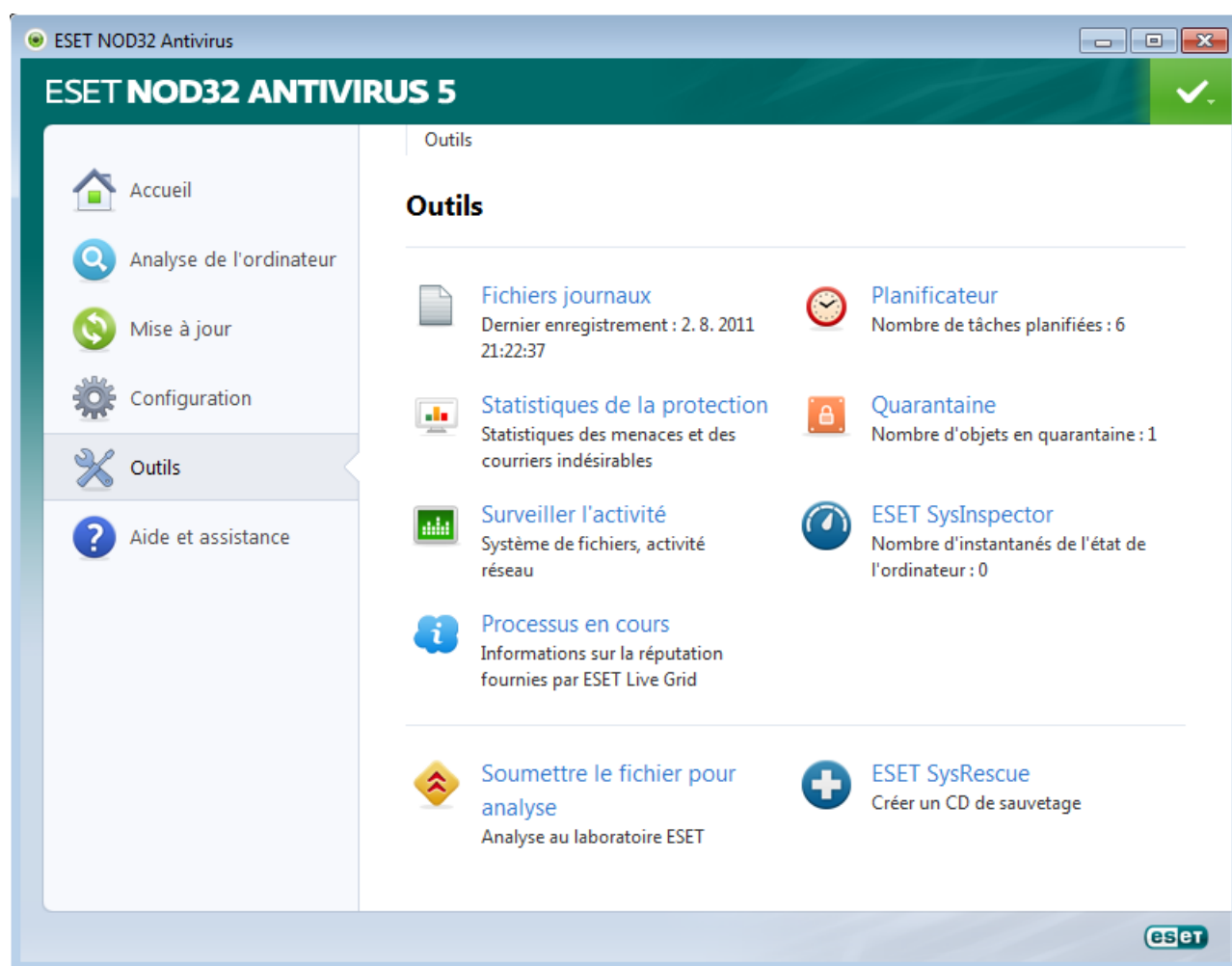
Les mises à jour peuvent également être exécutées sous forme de tâches planifiées. Pour configurer une tâche planifiée, cliquez sur **Outils > Planificateur**. Par défaut, les tâches suivantes sont activées dans ESET NOD32 Antivirus :

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

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

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.



Ce menu comprend les éléments suivants :

- [Fichiers journaux](#)
- [Statistiques de protection](#)
- [Surveiller l'activité](#)
- [Processus en cours](#)
- [Planificateur](#)
- [Quarantaine](#)
- [ESET SysInspector](#)

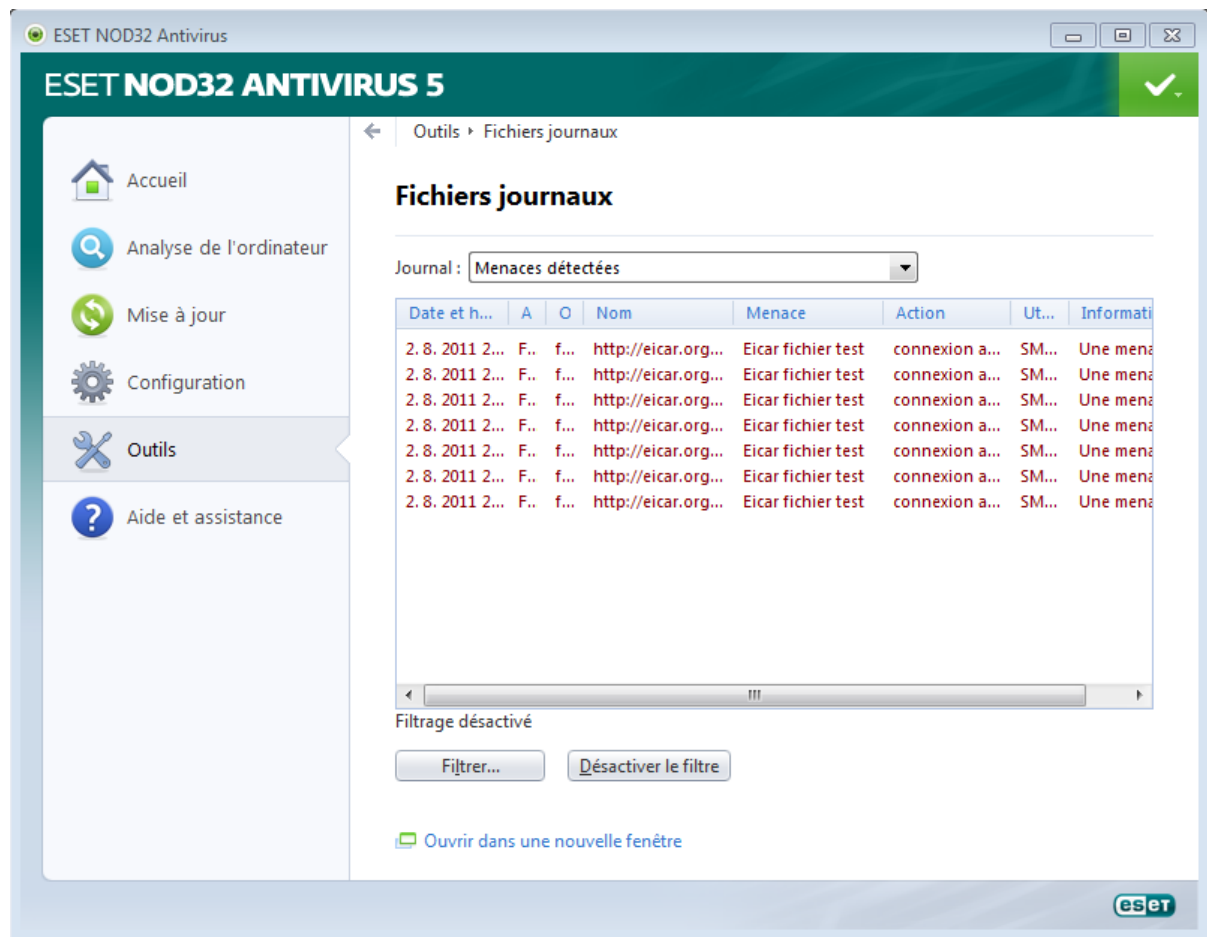
Soumettre le fichier pour analyse - Permet de soumettre un fichier suspect pour analyse aux laboratoires d'ESET. La

boîte de dialogue qui s'affiche lorsque vous cliquez sur cette option est décrite dans la section [Soumission de fichiers pour analyse](#).

ESET SysRescue - Lance l'assistant de création ESET SysRescue.

4.4.1 Fichiers journaux

Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées. La consignment représente un puissant outil pour l'analyse système, la détection de menaces et le dépannage. La consignment 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 le menu principal en cliquant sur **Outils > Fichiers journaux**. Sélectionnez le type de journal souhaité dans le menu déroulant **Journal**, en haut de la fenêtre. Les journaux suivants sont disponibles :

- **Menaces détectées** - Le journal des menaces contient des informations sur les infiltrations détectées par les modules 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 les journaux des événements. Le journal d'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. Ces informations peuvent souvent contribuer 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 spécifiques qui ont été marquées pour enregistrement. Le protocole affiche l'application qui a appelé l'opération, le résultat (si la règle a été autorisée ou bloquée), ainsi que le nom de la règle créée.

Dans chaque section, vous pouvez copier les informations affichées dans chaque section directement dans le Presse-papiers (à l'aide du raccourci clavier Ctrl+C) en sélectionnant l'entrée souhaitée, puis en cliquant sur le bouton **Copier**. Pour sélectionner plusieurs entrées, vous pouvez utiliser les touches CTRL et MAJ.

Vous pouvez afficher le menu contextuel d'une entrée en cliquant sur cette entrée avec le bouton droit de la souris. Vous disposez dans le menu contextuel des options suivantes :

- **Filtrer les entrées du même type** - Si vous activez ce filtre, le système n'affiche que les entrées d'un même type (diagnostics, avertissements...).
- **Filtrer.../Rechercher...** - Lorsque vous cliquez sur cette option, vous pouvez définir les critères de filtre dans la fenêtre **Filtrage des journaux**.
- **Désactiver le filtre** - Supprime tous les paramètres du filtre (décrit ci-dessus).
- **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.
- **Dérouler 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 Maintenance des 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 :

Supprimer automatiquement les entrées - Les entrées des journaux plus anciennes que le nombre de jours spécifiés dans **Supprimer les entrées vieilles de plus de X jours** seront automatiquement supprimées.

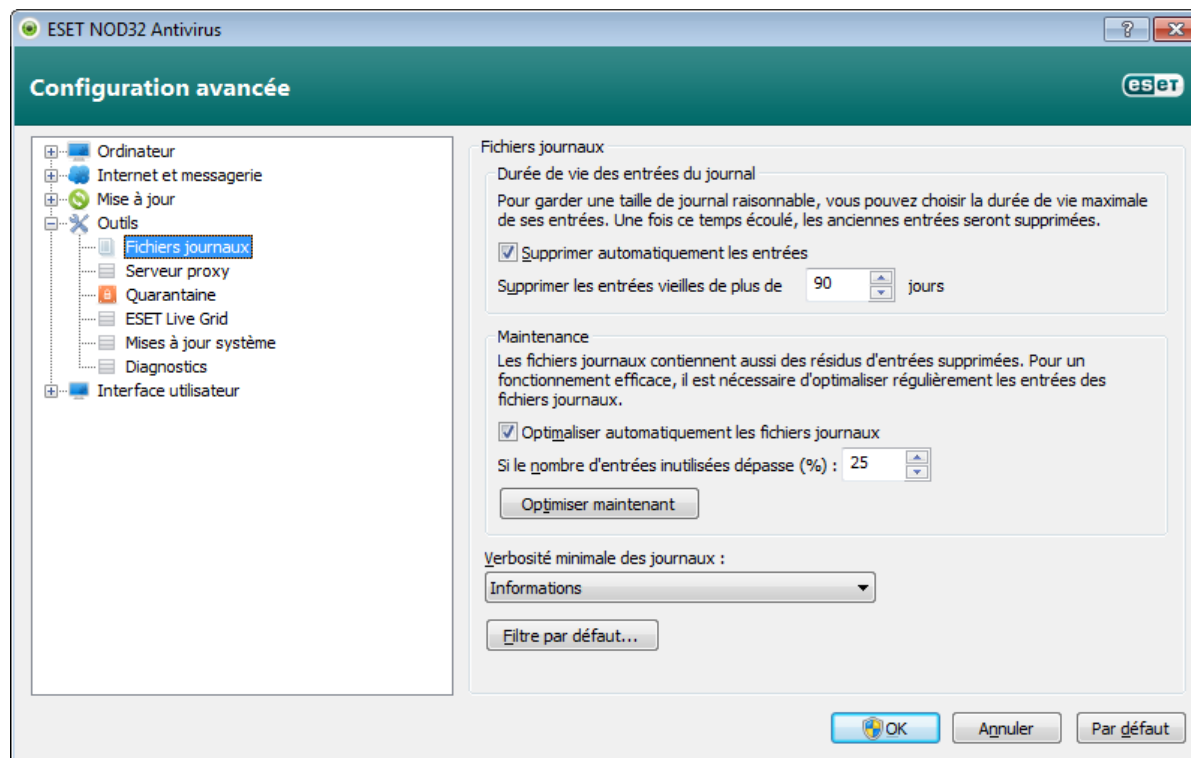
Optimiser automatiquement les fichiers journaux - Si cette fonction est activée, les fichiers journaux sont automatiquement défragmentés si le pourcentage est plus grand que la valeur spécifiée dans la zone **Si le nombre d'entrées inutilisées dépasse (%)**.

Cliquez sur **Optimiser maintenant** 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.

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

- **Diagnostic** - Consigne toutes les informations nécessaires pour un réglage détaillé 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, les erreurs et les messages d'avertissement.
- **Erreurs** - Les erreurs de type *Erreur de téléchargement de fichier* et les erreurs critiques sont enregistrées.
- **Critique** - Répertoire toutes les erreurs critiques (erreur de démarrage de la protection antivirus, etc...).

Cliquez sur le bouton **Filtre par défaut...** pour ouvrir la fenêtre Filtrage des journaux. Cochez les types d'entrées à afficher dans les journaux et cliquez sur **OK**.

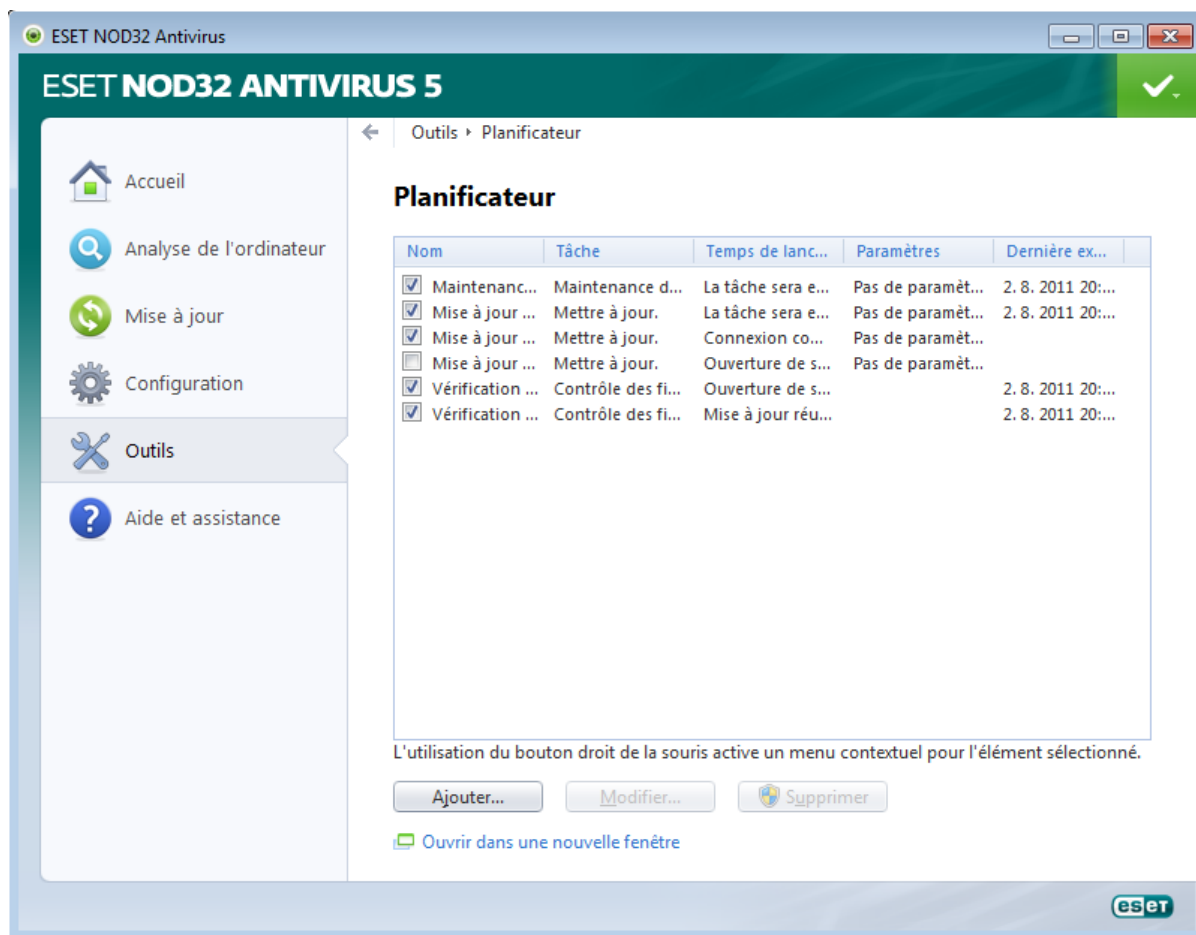


4.4.2 Planificateur

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

Le planificateur est accessible depuis le menu principal de ESET NOD32 Antivirus, dans **Outils**. 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 de la base des signatures de virus, 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.



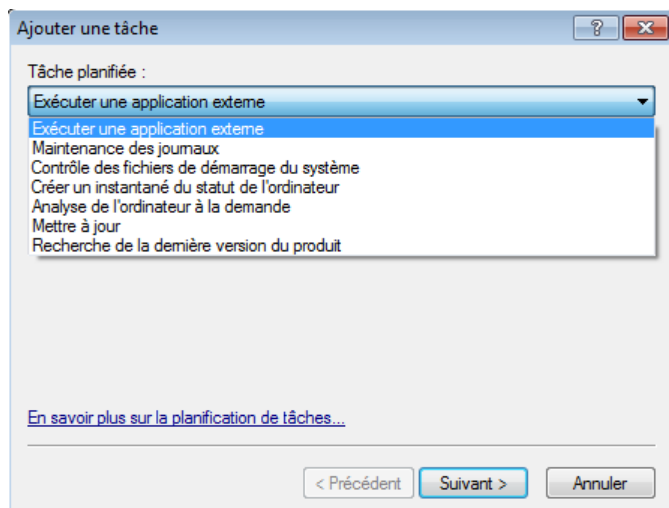
Par défaut, les tâches planifiées suivantes sont affichées dans le **planificateur** :

- **Maintenance des journaux**
- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion commutée**
- **Mise à jour automatique après ouverture de session utilisateur**
- **Recherche régulière de la dernière version du produit**
- **Vérification des fichiers de démarrage** (après l'ouverture de session de l'utilisateur)
- **Vérification des fichiers de démarrage** (après la mise à jour réussie de la base des signatures de virus)

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

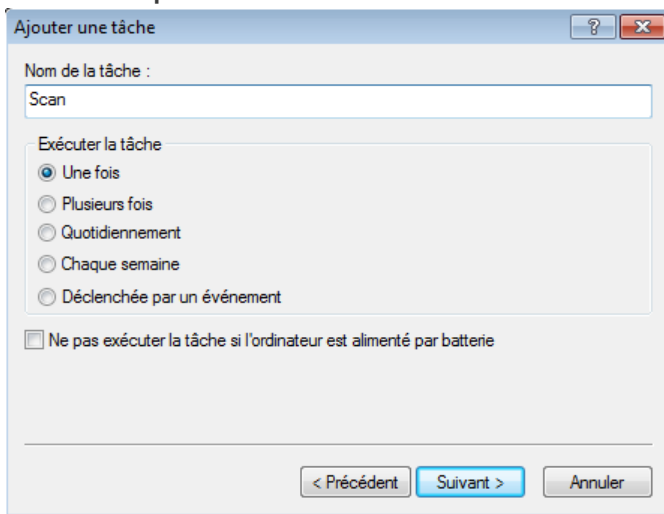
Ajout d'une nouvelle tâche

1. Cliquez sur **Ajouter...** dans la partie inférieure de la fenêtre.
2. Sélectionnez la tâche souhaitée dans le menu déroulant.



3. Entrez le nom de la tâche, puis sélectionnez l'une des options de périodicité suivantes :

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



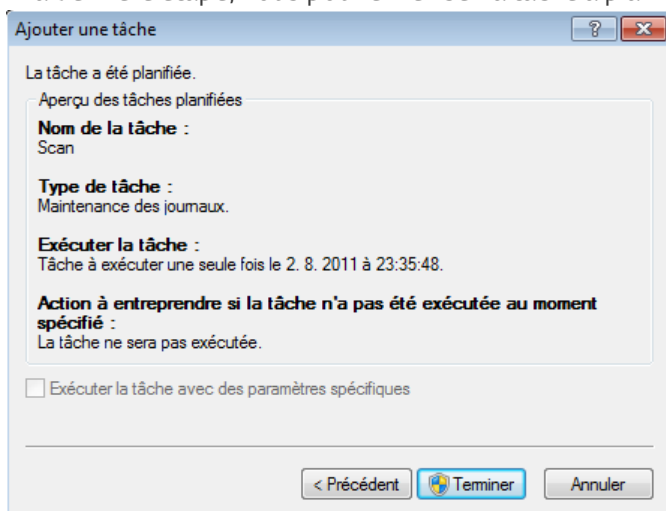
4. En fonction de l'option de périodicité que vous choisissez à l'étape précédente, l'une des boîtes de dialogue suivantes apparaît :

- **Une fois** - La tâche sera exécutée à la date et à l'heure prédéfinies.
- **Plusieurs fois** - La tâche est exécutée aux intervalles indiqués.
- **Tous les jours** - La tâche va s'exécuter tous les jours à l'heure définie.
- **Chaque semaine** - La tâche est exécutée à l'heure et au jour prédéfinis.

5. Si la tâche n'a pas pu être exécutée au moment défini, vous pouvez désigner le moment auquel elle doit être réexécutée :

- Patienter jusqu'à la prochaine heure planifiée
- Exécuter la tâche dès que possible
- Exécuter la tâche immédiatement si le temps écoulé depuis la dernière exécution est supérieur à -- heures.

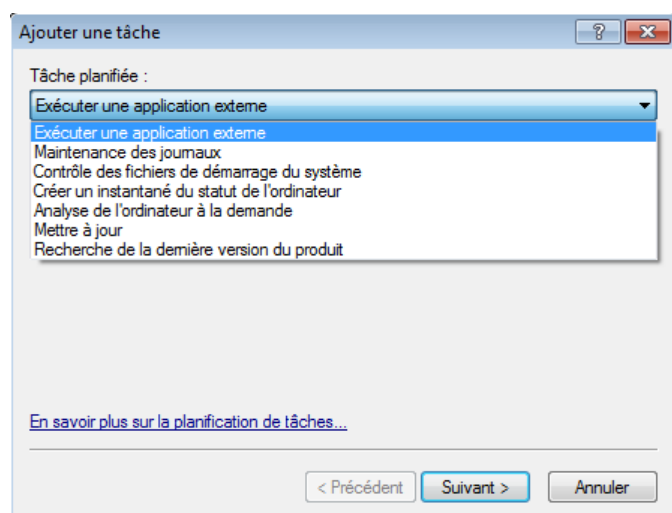
6. À la dernière étape, vous pouvez réviser la tâche à planifier. Cliquez sur **Terminer** pour appliquer la tâche.



4.4.2.1 Création de nouvelles tâches

Pour créer une nouvelle tâche dans le planificateur, cliquez sur le bouton **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 des entrées supprimées. 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 instantané du statut de l'ordinateur** - Crée l'instantané d'ordinateur [ESET SysInspector](#) - 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** - Analyse les fichiers et dossiers de votre ordinateur.
- **Mettre à jour** - Planifie une tâche de mise à jour en mettant à jour la base des signatures de virus et les modules du programme.
- **Recherche régulière de la dernière version du produit**



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 **Mettre à jour**. Cliquez sur **Suivant** et saisissez le nom de la tâche dans le champ **Nom de la tâche**. Sélectionnez la fréquence de la tâche. Les options disponibles sont les suivantes : **Une fois**, **Plusieurs fois**, **Quotidiennement**, **Hebdo** et **Déclenchée par un événement**. Utilisez l'option **Ne pas exécuter la tâche si l'ordinateur est alimenté par batterie** pour diminuer les ressources système lorsque l'ordinateur portable fonctionne sur batterie. Selon la fréquence sélectionnée, vous êtes invité à choisir différents paramètres de mise à jour. Vous pouvez définir ensuite l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée. Les trois options suivantes sont disponibles :

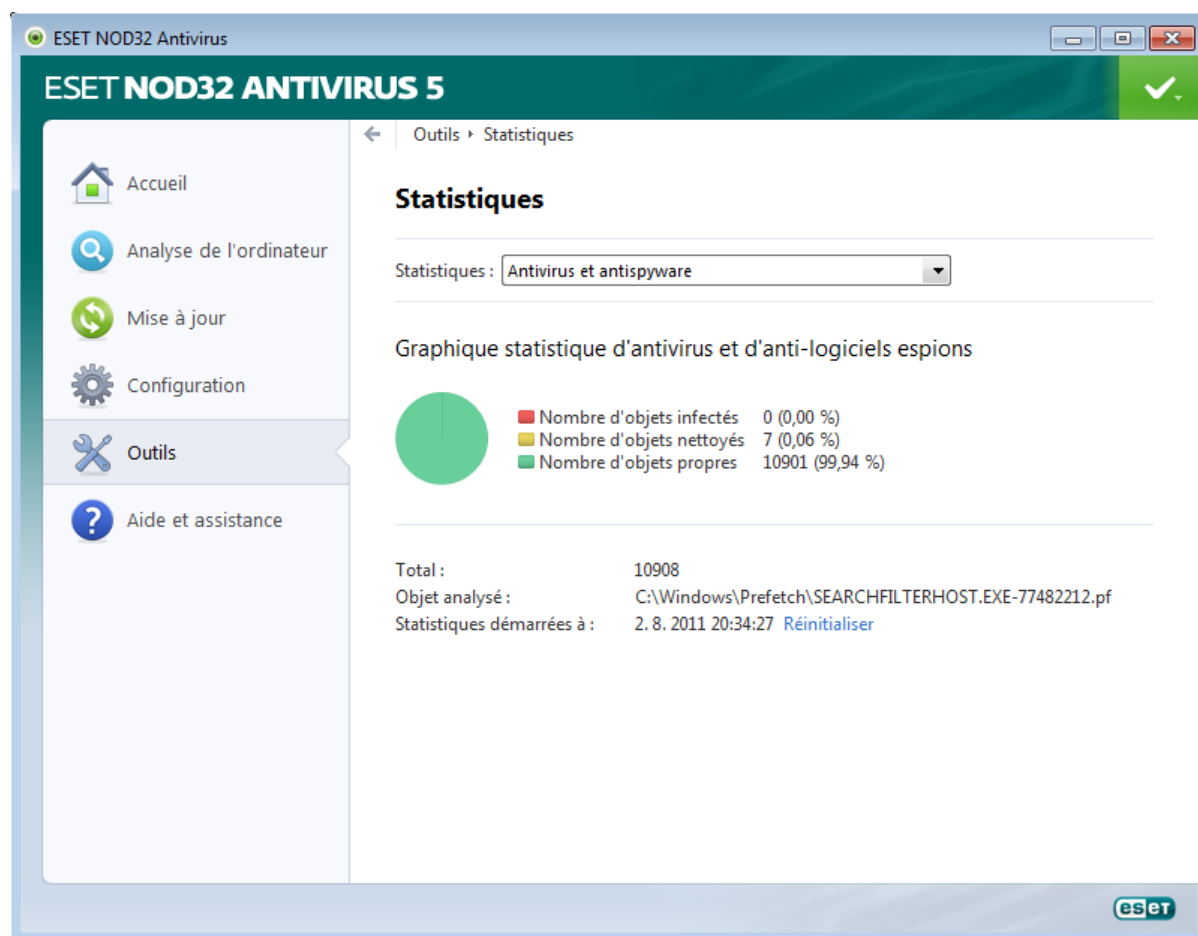
- **Patienter jusqu'à la prochaine heure planifiée**
- **Exécuter la tâche dès que possible**
- **Exécuter la tâche immédiatement si le temps écoulé depuis la dernière exécution dépasse l'intervalle spécifié** (l'intervalle peut être défini à l'aide de la zone de liste déroulante Intervalle minimal entre deux tâches)

La prochaine étape affiche dans une fenêtre un résumé complet de la tâche planifiée courante ; l'option **Exécuter la tâche avec des paramètres spécifiques** doit être automatiquement activée. Cliquez sur le bouton **Terminer**.

La boîte de dialogue qui apparaît permet de sélectionner les profils à utiliser pour la tâche planifiée. L'utilisateur peut spécifier un profil principal et un profil secondaire qui sera utilisé si la tâche ne peut s'exécuter à l'aide du profil principal. Confirmez en cliquant sur **OK** de la fenêtre **Profils de mise à jour**. La nouvelle tâche planifiée est ajoutée à la liste des tâches planifiées.

4.4.3 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 :

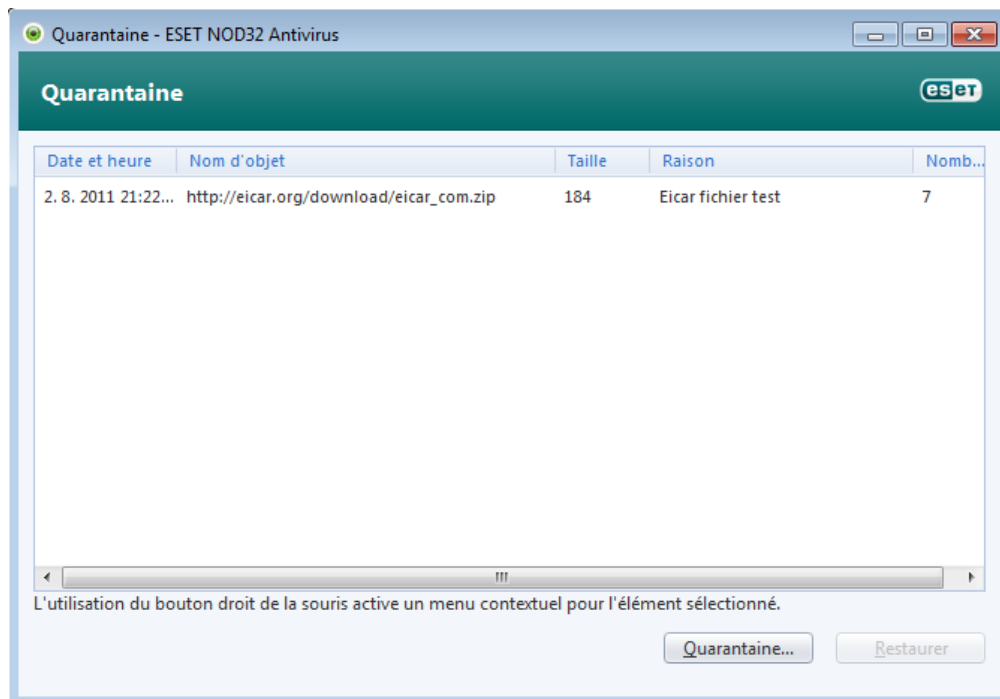
- **Protection antivirus et antispyware** - Affiche le nombre d'objets infectés et nettoyés.
- **Protection en temps réel du système de fichiers** - Affiche uniquement les objets lus ou écrits dans le système de fichiers.
- **Protection du client de messagerie** - Affiche uniquement les objets envoyés ou reçus par les clients de messagerie.
- **Protection de l'accès au Web** - 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.

4.4.4 Quarantaine

La principale fonction de la quarantaine consiste à 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 errone ment par ESET NOD32 Antivirus.

Vous pouvez choisir de mettre n'importe quel fichier en quarantaine. Cette action est conseill e si un fichier se comporte de fa on suspecte, mais n'a pas  t  d tect  par l'analyseur antivirus. Les fichiers de la quarantaine peuvent  tre soumis pour analyse au laboratoire de recherche d'ESET.



Les fichiers du dossier de quarantaine peuvent  tre visualis s dans un tableau qui affiche la date et l'heure de mise en quarantaine, le chemin de l'emplacement d'origine du fichier infect , sa taille en octets, la raison (par exemple, objet ajout  par l'utilisateur) et le nombre de menaces (s'il s'agit d'une archive contenant plusieurs infiltrations par exemple).

4.4.4.1 Mise en quarantaine de fichiers

ESET NOD32 Antivirus d place automatiquement les fichiers supprim s en quarantaine (si vous n'avez pas annul  cette option dans la fen tre 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 supprim  de son emplacement initial. Il est  galement possible d'utiliser le menu contextuel   cette fin : cliquez avec le bouton droit dans la fen tre **Quarantaine** et s lectionnez l'option **Quarantaine...**

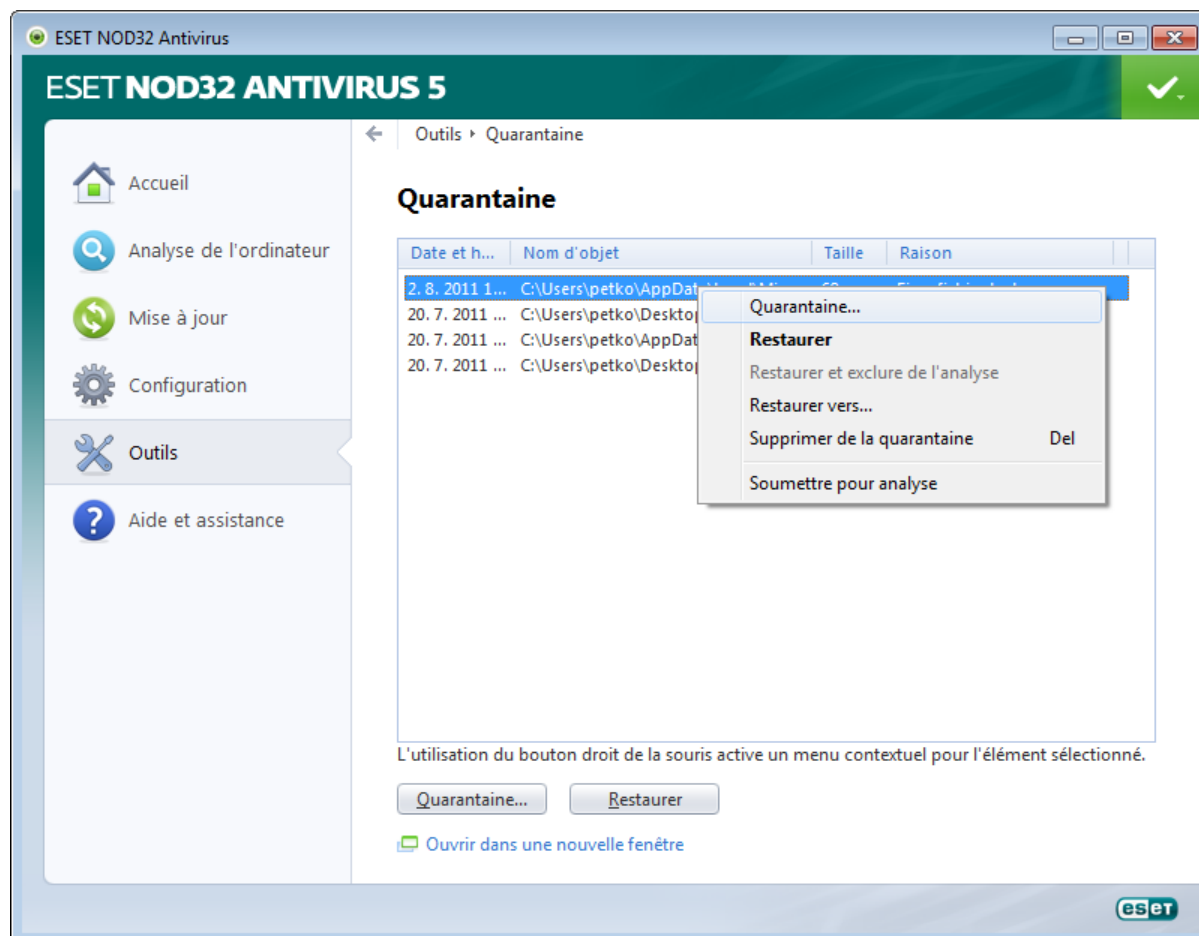
4.4.4.2 Restauration depuis la quarantaine

Les fichiers mis en quarantaine peuvent aussi  tre restaur s   leur emplacement d'origine. Pour ce faire, utilisez la fonctionnalit  **Restaurer** du menu contextuel apr s avoir cliqu  avec le bouton droit sur un fichier dans la fen tre de quarantaine. Le menu contextuel offre  galement l'option **Restaurer vers...** qui permet de restaurer des fichiers vers un emplacement autre que celui d'origine dont ils ont  t  supprim s.

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

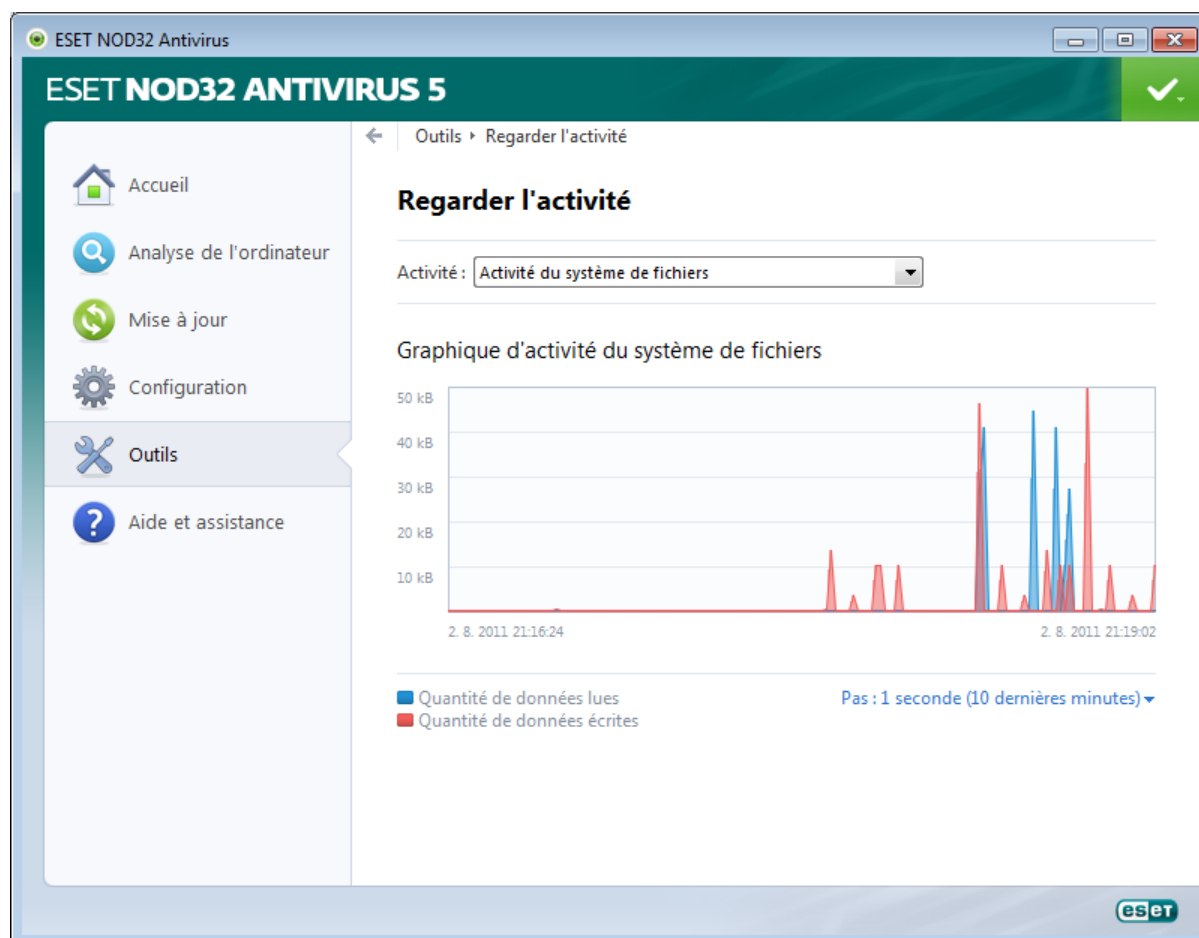
4.4.4.3 Soumission de fichiers de quarantaine

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 de la quarantaine, cliquez avec le bouton droit sur le fichier et sélectionnez l'option **Soumettre le fichier pour analyse** dans le menu contextuel.



4.4.5 Surveiller l'activité

Pour voir l'**activité actuelle du système de fichiers** sous forme graphique, cliquez sur **Outils > Surveiller l'activité**. Au bas du graphique figure une chronologie qui enregistre en temps réel l'activité du système de fichiers sur la base de l'intervalle sélectionné. Pour changer l'échelle, cliquez sur l'option **Pas 1...** située dans la partie inférieure droite de la fenêtre.



Les options disponibles sont les suivantes :

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

L'axe vertical **Graphique d'activité du système de fichiers** représente les données lues (en rouge) et les données écrites (en bleu). Les deux valeurs sont exprimées en Ko. 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.

4.4.6 ESET SysInspector

[ESET SysInspector](#) est une application qui inspecte complètement votre ordinateur, réunit des informations détaillées sur les composants système, tels que les pilotes et applications installés, les connexions réseau ou des 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 logiciel malveillant.

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

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

Les actions disponibles sont les suivantes :

- **Comparer** - Compare deux journaux existants.
- **Créer...** - Crée un journal. Veuillez patienter jusqu'à ce que le journal ESET SysInspector soit prêt (l'option **État** indique Créé).
- **Supprimer** - Supprime les journaux sélectionnés de la liste.

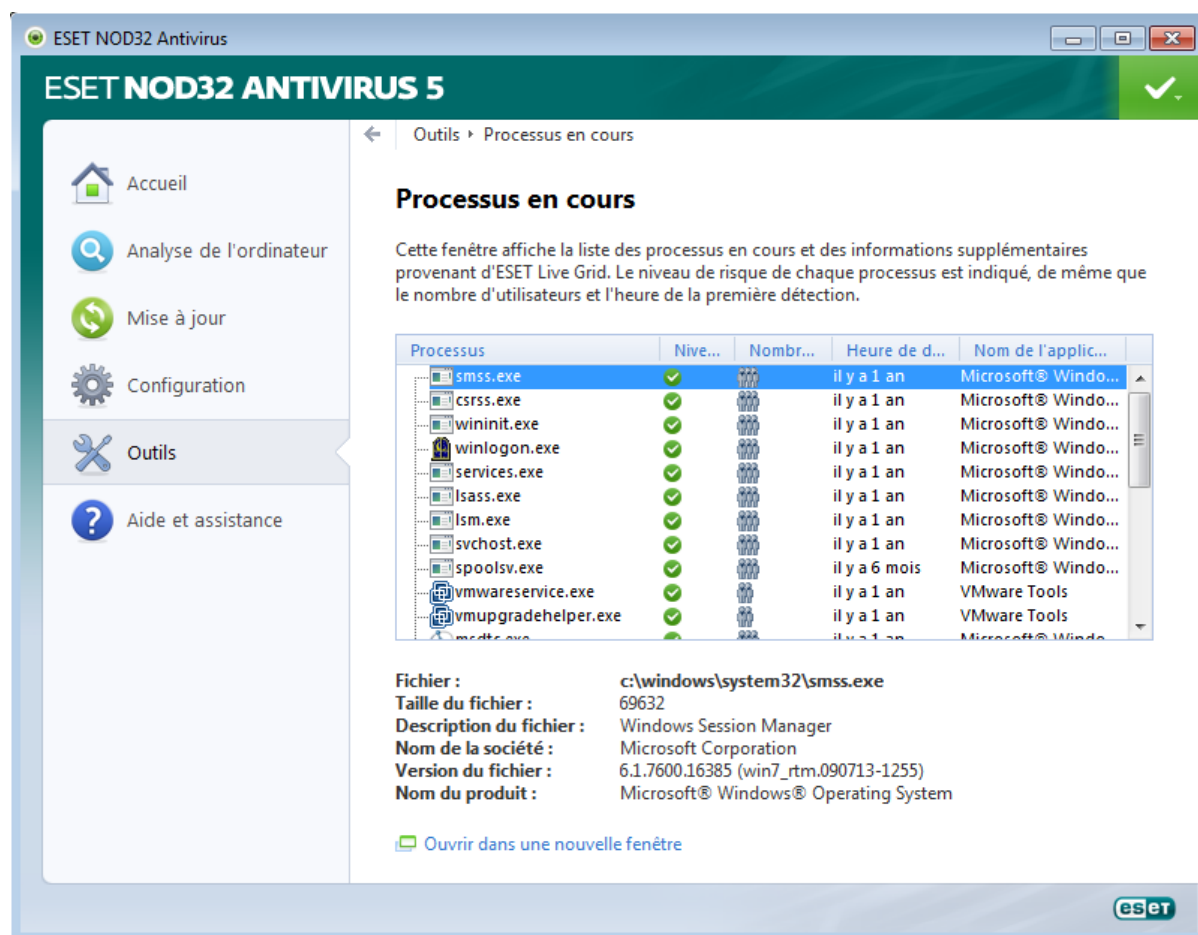
Une fois que vous avez cliqué avec le bouton droit de la souris sur un ou plusieurs journaux sélectionnés, les options supplémentaires suivantes sont disponibles dans le menu contextuel :

- **Afficher** - Ouvre le journal sélectionné dans ESET SysInspector (équivalent à double-cliquer sur un journal).
- **Supprimer tout** - Supprime tous les journaux.
- **Exporter...** - Exporte le journal dans un fichier xml ou un fichier xml compressé.

4.4.7 Processus en cours

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

Remarque : la réputation peut également être exécutée sur des fichiers qui n'agissent pas en tant que programmes/processus en cours. Marquez les fichiers que vous souhaitez vérifier, cliquez dessus avec le bouton droit et, dans le menu contextuel, sélectionnez **Options avancées > Évaluer la réputation des fichiers à l'aide d'ESET Live Grid**.



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

Risque - Dans la majorité des cas, ESET NOD32 Antivirus attribue, à l'aide de la technologie ESET Live Grid, 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 **1 - OK (vert)** sont saines (répertoriées dans la liste blanche) et sont

exclues de l'analyse, ce qui améliore la vitesse de l'analyse d'ordinateur à la demande ou de la protection du système en temps réel sur votre ordinateur.

Utilisateurs - Nombre d'utilisateurs utilisant une application. Ces informations sont collectées par la technologie ESET Live Grid.

Détection - Période depuis la détection de l'application par la technologie ESET Live Grid.

REMARQUE : lorsque l'application est marquée comme ayant le niveau de sécurité **9 : Risqué (rouge)**, il ne s'agit pas nécessairement d'un logiciel malveillant. Il s'agit généralement d'une nouvelle application. Si un fichier vous semble suspect, vous pouvez le [soumettre pour analyse](#) au laboratoire ESET. Si le fichier s'avère être une application malveillante, sa détection sera ajoutée dans l'une des mises à jour suivantes.

Nom - Nom d'un programme ou d'un processus.

Ouvrir dans une nouvelle fenêtre - Les informations concernant les processus en cours d'exécution apparaissent dans une nouvelle fenêtre.

Lorsque vous cliquez sur une application située au bas de la fenêtre, les informations suivantes apparaissent dans la partie inférieure de la fenêtre :

- **Fichier** - Emplacement d'une application sur l'ordinateur.
- **Taille du fichier** - Taille du fichier en Ko (kilo-octets).
- **Description du fichier** - Caractéristiques du fichier basées sur sa description du système d'exploitation.
- **Nom de la société** - Nom du fournisseur ou du processus de l'application.
- **Versión du fichier** - Informations fournies par l'éditeur de l'application.
- **Nom du produit** - Nom de l'application et/ou nom de l'entreprise.

4.4.7.1 ESET Live Grid

ESET Live Grid (la nouvelle génération d'ESET ThreatSense.Net) est un système d'avertissement anticipé avancé qui vous protège des nouvelles menaces en fonction de la réputation. Le laboratoire ESET utilise le flux en temps réel d'informations concernant les menaces issues du service de cloud computing pour maintenir les défenses à jour. Vous bénéficiez d'un niveau de protection constant. L'utilisateur peut prendre connaissance de la réputation des processus et des fichiers en cours depuis l'interface du programme ou à partir d'un menu contextuel comprenant des informations supplémentaires mises à disposition par ESET Live Grid. Deux options sont possibles :

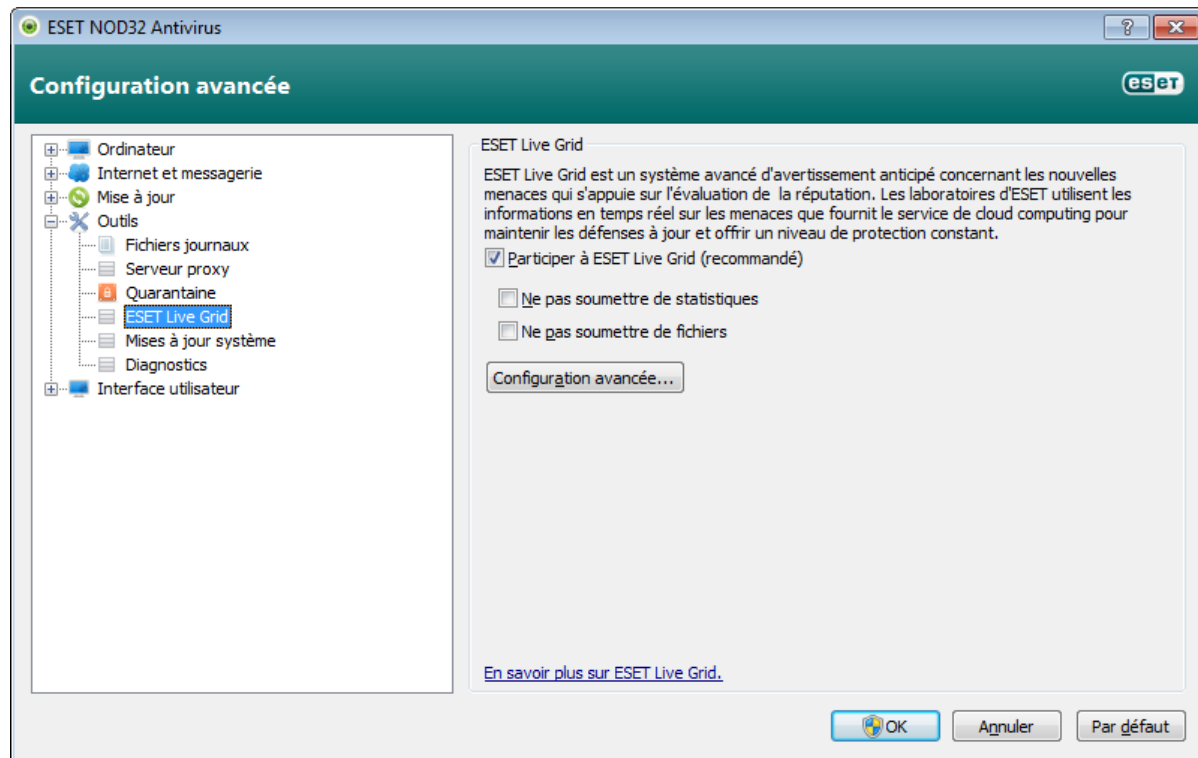
1. Vous pouvez décider de ne pas activer ESET Live Grid. Vous ne perdez rien de la fonctionnalité du logiciel et vous bénéficiez toujours la meilleure protection que nous offrons.
2. Vous pouvez configurer ESET Live Grid afin d'envoyer des informations anonymes qui concernent les nouvelles menaces et 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 Live Grid 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.

Certaines informations vous concernant ou concernant votre ordinateur (noms d'utilisateur dans un chemin de répertoire) sont divulguées au laboratoire d'ESET, mais ces informations ne sont utilisées à AUCUNE autre fin que pour répondre immédiatement aux nouvelles menaces.

Par défaut, ESET NOD32 Antivirus est configuré pour demander confirmation avant de soumettre au laboratoire d'ESET les fichiers suspects 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 Live Grid propose différentes options permettant d'activer et de désactiver ESET Live Grid. 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, dans **Outils > ESET Live Grid**.



Participer à ESET Live Grid (recommandé) - Active et désactive ESET Live Grid. Ce système sert à soumettre les fichiers suspects aux laboratoires d'ESET et à fournir des informations statistiques anonymes.

Ne pas soumettre de statistiques - Sélectionnez cette option si vous ne souhaitez pas soumettre d'informations anonymes concernant votre ordinateur depuis ESET Live Grid. Ces informations concernent les nouvelles menaces détectées. Il peut s'agir du nom de l'infiltration, de la date et de l'heure de la détection, de la version d'ESET NOD32 Antivirus et d'informations sur la version du système d'exploitation de votre ordinateur et ses paramètres régionaux. Les statistiques sont normalement fournies au serveur d'ESET une ou deux fois par jour.

Ne pas soumettre de fichiers - Les fichiers suspects, qui ressemblent à des infiltrations par leur contenu ou leur comportement, ne sont pas envoyés pour analyse à ESET par le biais de la technologie ESET Live Grid.

Configuration avancée... - Ouvre une fenêtre avec d'autres paramètres ESET Live Grid.

Si vous avez déjà utilisé le système ESET Live Grid et l'avez désactivé, il est possible qu'il reste des paquets de données à envoyer. Même après la désactivation, ces paquets seront transmis à ESET à la prochaine occasion. Par la suite, plus aucun paquet ne sera créé.

4.4.7.1.1 Fichiers suspects

L'onglet **Fichiers** dans la configuration avancée ESET Live Grid permet de configurer le mode de soumission des menaces au laboratoire de recherche sur les menaces d'ESET pour analyse.

Si vous trouvez un fichier suspect, vous pouvez le soumettre à notre laboratoire de recherche sur les menaces 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 d'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 électronique de contact (facultatif) - 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 l'option **Activer la journalisation** pour créer un journal d'événements permettant d'enregistrer les soumissions des fichiers et des informations statistiques. Cette option active la consignation dans le [journal des](#)

[événements](#) lorsque les fichiers ou les statistiques sont envoyés.

4.4.8 Soumission de fichiers pour analyse

La boîte de dialogue Soumission de fichiers permet d'envoyer un fichier à ESET pour analyse ; elle est accessible depuis **Outils > Soumettre le fichier pour analyse**. Si vous trouvez sur votre ordinateur un fichier dont le comportement est suspect, vous pouvez le soumettre au laboratoire d'ESET pour analyse. Si le fichier s'avère être une application malveillante, sa détection sera ajoutée dans l'une des mises à jour suivantes.

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. 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 l'un des critères suivants : (i) le fichier n'est pas détecté du tout (ii) le fichier est détecté incorrectement en tant que menace. Vous ne recevrez pas de réponse, excepté si des informations complémentaires sont nécessaires à l'analyse.

Motif de soumission du fichier - Sélectionnez la description correspondant le mieux à votre message. Sélectionnez l'une des trois options suivantes : **Fichier suspect**, **Faux positif** et **Autre**.

Fichier - Chemin d'accès au fichier 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. 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.

4.4.9 Mises à jour système

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 en téléchargement.
- **Mises à jour optionnelles** - Les mises à jour marquées comme étant faiblement prioritaires et plus sont proposées pour le téléchargement.
- **Mises à jour recommandées** - Les mises à jour marquées comme étant communes et plus sont proposées pour le téléchargement.
- **Mises à jour importantes** - Les mises à jour marquées comme étant importantes et plus sont proposées pour le 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.

4.4.10 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. Deux types de fichier d'image mémoire sont disponibles :

- **Fichier d'image mémoire 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.
- **Minifichier d'image mémoire** - Enregistre le plus petit ensemble d'informations utiles qui peuvent 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.
- Sélectionnez **Ne pas générer de fichier d'image mémoire** (option par défaut) pour désactiver cette fonctionnalité.

Répertoire cible - Répertoire dans lequel est généré le fichier d'image mémoire lors de la défaillance. Cliquez sur **Ouvrir le dossier...** pour ouvrir ce répertoire dans une nouvelle fenêtre de l'Explorateur Windows.

4.5 Interface utilisateur

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

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.

Si vous choisissez de ne pas afficher certaines notifications, ces dernières apparaissent dans les [fenêtres de notification masquées](#). Vous pouvez vérifier leur état, afficher des détails supplémentaires ou supprimer des notifications de cette fenêtre.

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](#).

Le [menu contextuel](#) est le menu qui s'affiche lorsque vous cliquez sur un objet avec le bouton droit de la souris. Utilisez cet outil pour intégrer les options ESET NOD32 Antivirus dans le menu contextuel.

Le [mode joueur](#) est utile pour les amateurs de jeux et, plus généralement, pour tous les utilisateurs qui souhaitent travailler sans être interrompus par des fenêtres contextuelles, des tâches planifiées et tout autre composant qui pourrait augmenter la charge du processeur et de la mémoire RAM.

4.5.1 Graphiques

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

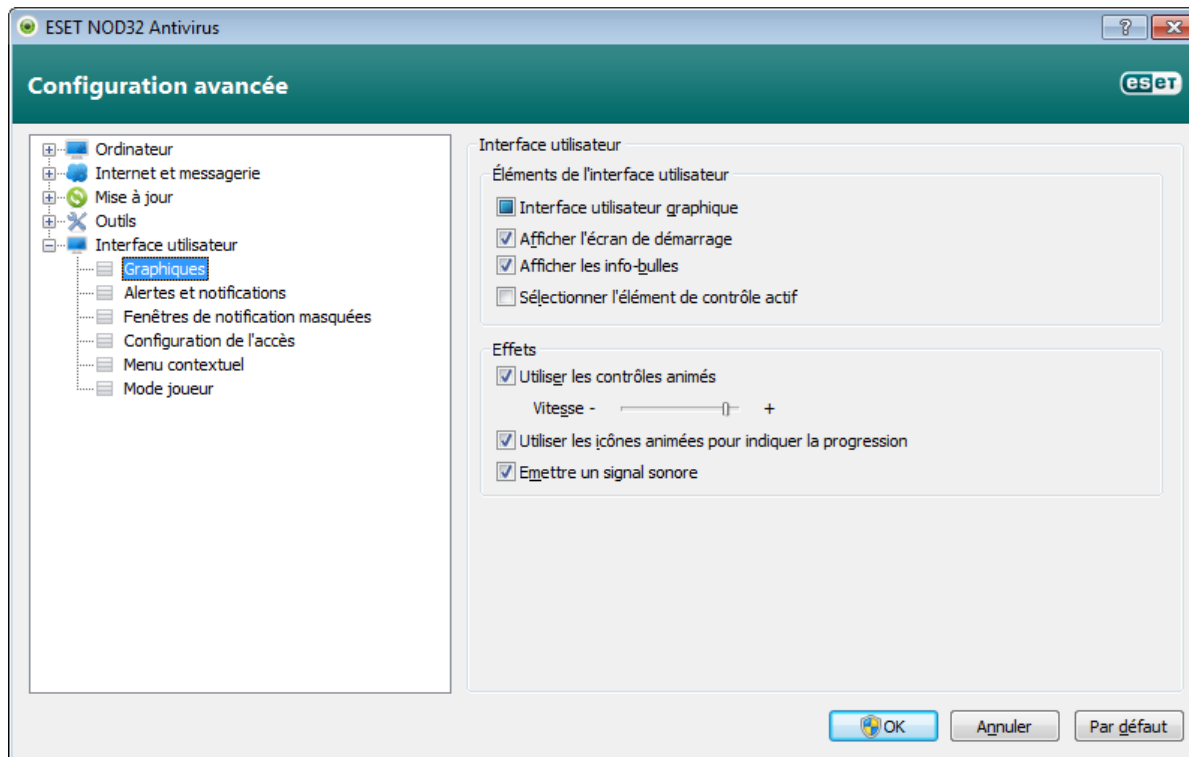
Dans la section **Éléments de l'interface utilisateur**, l'**interface utilisateur graphique** doit être désactivée si les éléments graphiques ralentissent les performances de l'ordinateur ou causent d'autres problèmes. De la même manière, il est peut-être nécessaire de désactiver l'interface utilisateur graphique pour les utilisateurs malvoyants, car elle peut créer un conflit avec des applications spéciales utilisées pour la lecture de textes affichés à l'écran.

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

Si l'option **Afficher les info-bulles** est activée, une brève description de toute option s'affiche si le curseur est placé dessus. Lorsque l'option **Sélectionner l'élément de contrôle actif** est sélectionnée, le système met en évidence tout élément situé dans la zone active du curseur de la souris. L'élément mis en évidence est activé si l'utilisateur clique dessus.

Pour diminuer ou augmenter la vitesse des effets animés, sélectionnez l'option **Utiliser les contrôles animés** et déplacez le curseur **Vitesse** vers la gauche ou vers la droite.

Pour activer l'utilisation des icônes animées afin d'afficher la progression des différentes opérations, sélectionnez l'option **Utiliser les icônes animées pour indiquer la progression**. Si vous souhaitez que le programme émette un son d'avertissement si un événement important se produit, sélectionnez l'option **Émettre un signal sonore**.



4.5.2 Alertes et notifications

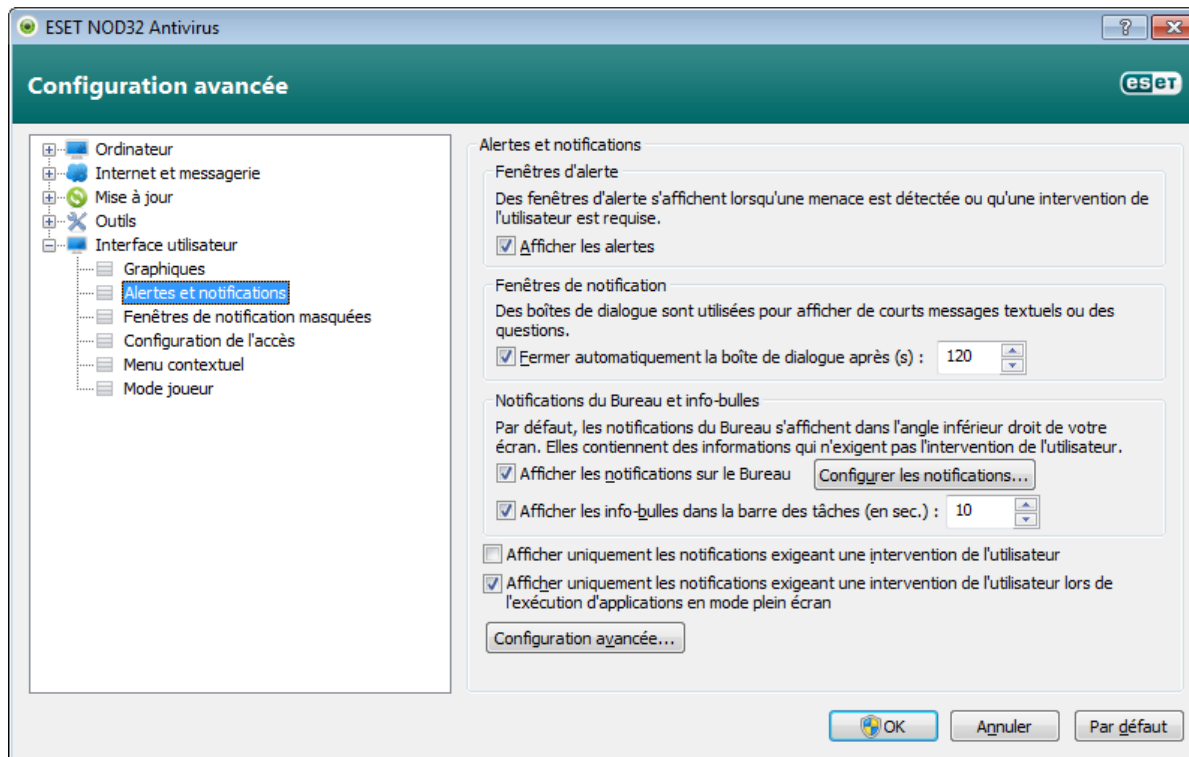
La section **Configurer les alertes et notifications** dans **Interface utilisateur** vous permet de configurer le mode de traitement des alertes en cas de menace et des notifications système dans ESET NOD32 Antivirus. Vous pouvez également configurer l'heure d'affichage et le niveau de transparence des notifications dans la barre d'état système (ne s'applique qu'aux systèmes prenant en charge ces notifications).

La première option est **Afficher les alertes**. Lorsqu'elle 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).

Pour fermer automatiquement les fenêtres d'alerte après un certain délai, sélectionnez l'option **Fermer automatiquement la boîte de dialogue après (s)**. Si les fenêtres d'alerte ne sont pas fermées manuellement, le système les ferme automatiquement une fois le laps de temps écoulé.

Les notifications sur le bureau et les infobulles sont fournies à titre d'information uniquement et ne permettent ni 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**. D'autres options détaillées (la durée d'affichage des notifications et la transparence de la fenêtre) peuvent être modifiées en cliquant sur le bouton **Configurer les notifications...** Pour prévisualiser le comportement des notifications, cliquez sur le bouton **Aperçu**.

Pour configurer la durée d'affichage des infobulles, utilisez l'option **Afficher les infobulles dans la barre des tâches (en sec.)**.



L'option **Afficher uniquement les notifications exigeant une intervention de l'utilisateur** vous permet d'activer/de désactiver l'affichage des alertes et des notifications qui n'exigent aucune interaction de l'utilisateur. Sélectionnez **Afficher uniquement les notifications exigeant une intervention de l'utilisateur lors de l'exécution d'applications en mode plein écran** pour supprimer toutes les notifications non interactives.

Cliquez sur **Configuration avancée...** pour accéder aux options supplémentaires de configuration **Alertes et notification**.

4.5.2.1 Configuration avancée

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

- **Diagnostic** - Consigne toutes les informations nécessaires pour un réglage détaillé 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, les erreurs et les messages d'avertissement.
- **Erreurs** - Les erreurs de type *Erreur de téléchargement de fichier* et les erreurs critiques sont enregistrées.
- **Critique** - Répertoire 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 un utilisateur qui reçoit les notifications système et autres sur les systèmes autorisant 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 Fenêtres de notification masquées

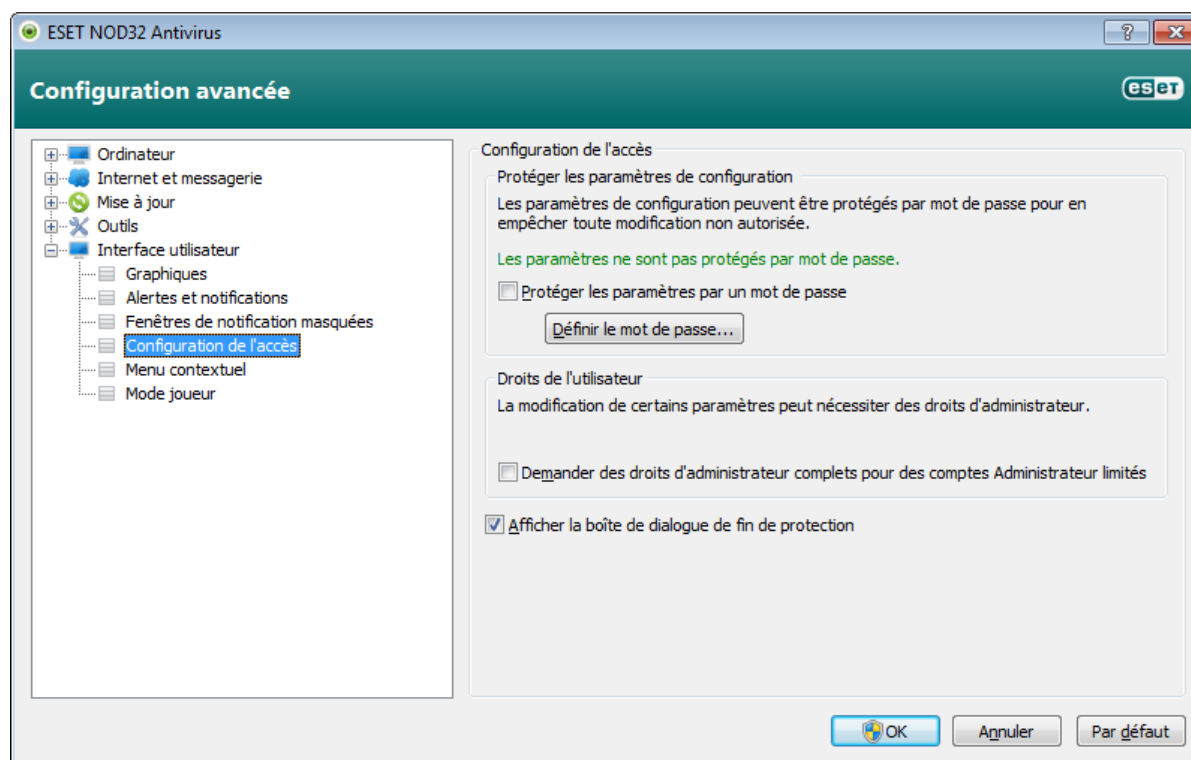
Si l'option **Ne plus afficher ce message** a été sélectionnée pour une fenêtre de notification (alerte) affichée précédemment, cette fenêtre figure dans la liste des fenêtres de notification masquées. Les actions désormais exécutées automatiquement s'affichent dans la colonne intitulée **Confirmer**.

Afficher - Affiche un aperçu des fenêtres de notification non affichées pour lesquelles une action automatique est configurée.

Supprimer - Supprime les éléments de la liste **Boîtes de message masquées**. Toutes les fenêtres de notification supprimées de la liste s'affichent de nouveau.

4.5.4 Configuration de l'accès

Il est essentiel qu'ESET NOD32 Antivirus soit correctement configuré pour garantir une sécurité maximale du système. Tout changement inapproprié peut faire perdre des données importantes. Cette option se trouve dans le sous-menu **Configuration de l'accès**, dans **Interface utilisateur**. Pour éviter des modifications non autorisées, les paramètres de la configuration d'ESET NOD32 Antivirus peuvent être protégés par mot de passe.



Protection des paramètres par mot de passe - Verrouille ou déverrouille les paramètres de configuration du programme. Activez ou désactivez la case à cocher pour ouvrir la fenêtre de configuration du mot de passe.

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

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 d'utilisateur et un mot de passe d'administrateur lors de la modification de certains paramètres du système (semblable au contrôle UAC dans Windows Vista). Elles portent également sur la désactivation des modules de protection.

Afficher la boîte de dialogue de fin de protection - Si cette option est sélectionnée, un message d'invite apparaît, tandis que la désactivation temporaire de la protection s'effectue depuis le menu des programmes ou dans la section **ESET NOD32 Antivirus > Configuration**. Le menu déroulant **Intervalle** de la fenêtre **Désactiver temporairement la protection** représente la période pendant laquelle toutes les protections sont désactivées.

4.5.5 Menu contextuel

Le menu contextuel est le menu qui s'affiche lorsque vous cliquez sur un élément avec le bouton droit de la souris. Le menu répertorie toutes les options disponibles applicables à l'objet.

Il est possible d'intégrer les options ESET NOD32 Antivirus dans le menu contextuel. Les options avancées contiennent des options de configuration plus détaillées pour cette fonctionnalité dans les sections **Interface utilisateur** et **Menu contextuel**.

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

Les options suivantes sont disponibles dans le menu contextuel **Type de menu** :

- **Complet (analyse en premier)** - Active toutes les options de menu contextuel ; le menu principal affiche l'option **Analyser avec ESET NOD32 Antivirus**.
- **Complet (nettoyage en premier)** - Active toutes les options de menu contextuel ; le menu principal affiche l'option **Nettoyer avec ESET NOD32 Antivirus**.
- **Analyse uniquement** - Seule l'option **Analyser avec ESET NOD32 Antivirus** apparaît dans le menu contextuel.
- **Nettoyage uniquement** - Seule l'option **Nettoyer avec ESET NOD32 Antivirus** apparaît dans le menu contextuel.

Confirmations - Affiche un avertissement supplémentaire lorsque l'utilisateur essaie d'appliquer une option de menu contextuel sur un nombre d'objets supérieur à celui indiqué dans **Demander si le nombre de fichiers dépasse**. Par défaut, cette option est configurée sur huit objets.

4.5.6 Mode joueur

Le mode joueur est une fonctionnalité destinée aux joueurs qui ne veulent pas être interrompus lors de l'utilisation de leur jeu. Ils ne souhaitent pas être dérangés par des fenêtres contextuelles et veulent réduire l'utilisation du processeur. Le mode joueur peut également être utilisé en tant que mode de présentation, ce qui permet d'éviter toute interruption 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 ESET NOD32 Antivirus, dans le volet **Configuration** situé à droite, ou après avoir accédé au menu de configuration avancée. Vous pouvez accéder au menu de configuration avancée en cliquant sur l'option **Accéder à la configuration avancée...** située au bas de la fenêtre principale, puis en sélectionnant **Interface utilisateur > Mode joueur**. Cochez la case **Activer le mode joueur** située à droite pour activer cette fonctionnalité. 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 indique un symbole d'avertissement. Vous pouvez également voir cet avertissement dans la fenêtre principale ESET NOD32 Antivirus, dans le menu **Accueil** où apparaît l'option **Mode joueur activé**, en orange.

Lorsque vous cochez la case **Activer le mode joueur lors de l'exécution automatique d'applications en mode plein écran**, le mode joueur démarre lorsque vous lancez une application en plein écran et s'arrête lorsque vous quittez l'application. Ce procédé est particulièrement utile, car il permet de démarrer le mode joueur directement après le démarrage d'un jeu, l'ouverture en plein écran d'une application ou le démarrage d'une présentation.

Vous pouvez également sélectionner l'option **Désactiver le mode joueur automatiquement après X minutes** en cochant la case et en indiquant la durée (la valeur par défaut est de 1 minute). Cette option est utilisée si vous n'avez besoin du mode joueur que pendant une période donnée et que vous souhaitez le désactiver automatiquement ensuite.

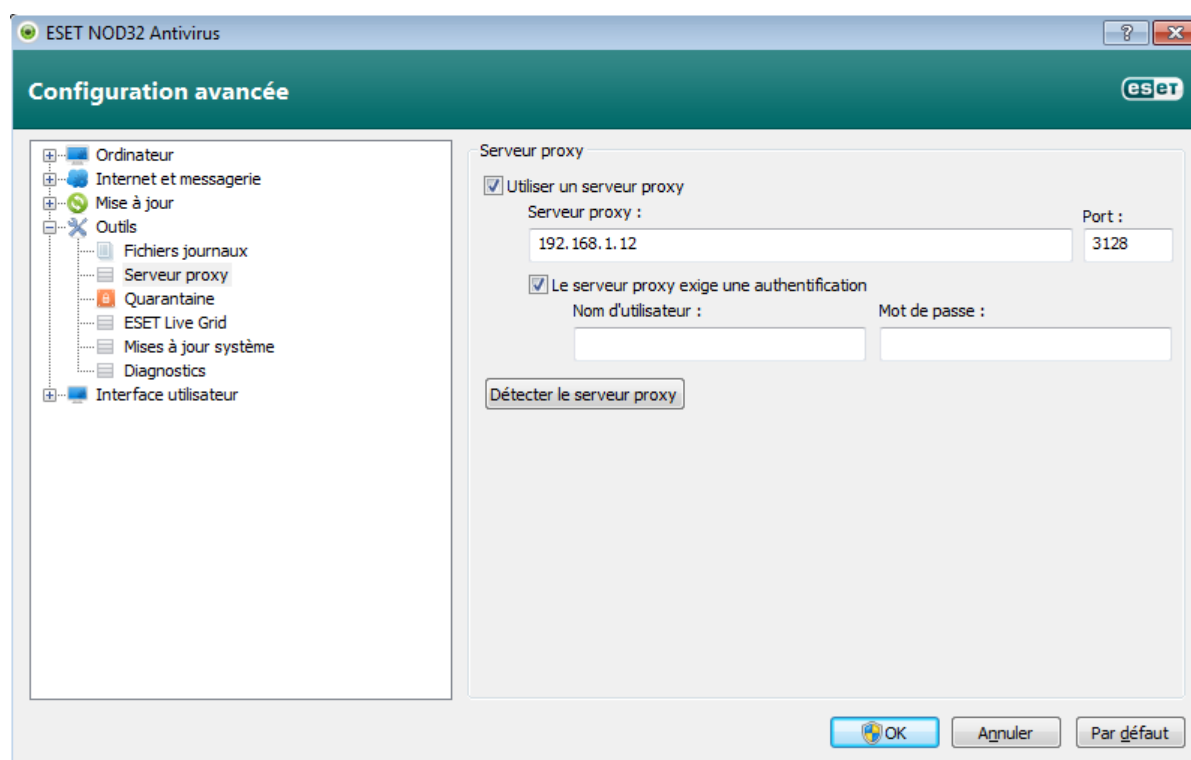
5. Utilisateur chevronné

5.1 Configuration du serveur proxy

Dans les grands réseaux locaux, la connexion de votre ordinateur à Internet peut s'effectuer par l'intermédiaire d'un serveur proxy. Si c'est le cas, les paramètres suivants doivent être définis. Dans le cas contraire, le programme ne pourra pas se mettre à jour automatiquement. Dans ESET NOD32 Antivirus, la configuration du serveur proxy est disponible dans deux sections de l'arborescence de configuration avancée.

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 exigeant une connexion à Internet.

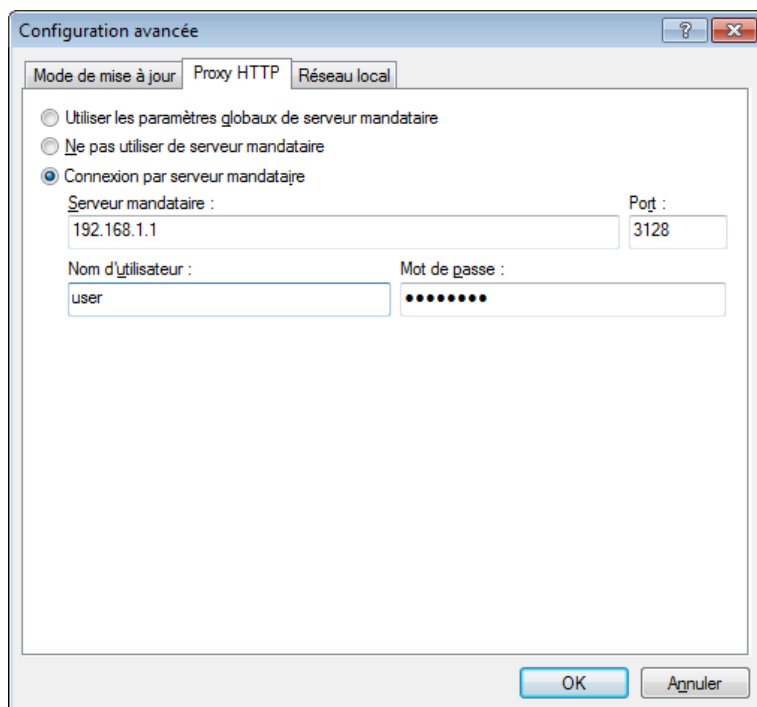
Pour spécifier des paramètres de serveur proxy à ce niveau, cochez la case **Utiliser un serveur proxy**, puis entrez l'adresse du serveur proxy dans le champ **Serveur proxy**, ainsi que le numéro de **port** de ce serveur proxy.



Si la communication avec le serveur proxy exige une authentification, cochez la case **Le serveur proxy nécessite une authentification** et entrez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants. Cliquez sur le bouton **Détecter le serveur proxy** pour détecter automatiquement et insérer les paramètres du serveur proxy. Les paramètres indiqués dans Internet Explorer sont copiés.

REMARQUE : cette fonctionnalité ne récupère pas les données d'authentification (nom d'utilisateur et mot de passe) ; vous devez donc les fournir.

Les paramètres de serveur proxy peuvent également être établis dans la configuration avancée de la mise à jour (section **Mise à jour** de l'arborescence **Configuration avancée**). 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 différents emplacements. Pour plus d'informations sur ce paramètre, consultez la section [Configuration avancée des mises à jour](#).



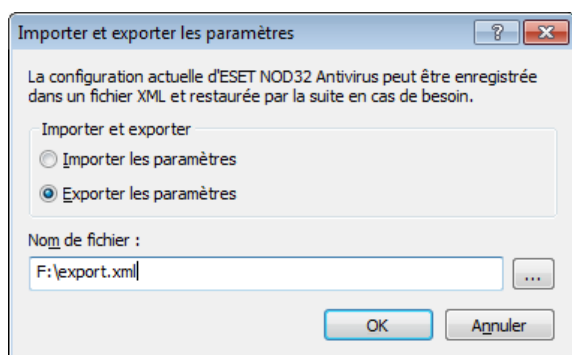
5.2 Importer et exporter les paramètres

L'importation et l'exportation des configurations d'ESET NOD32 Antivirus sont disponibles dans **Configuration**.

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

L'importation d'une configuration est très facile. Dans le menu principal, cliquez sur **Configuration > Importer et exporter les paramètres...**, puis sélectionnez l'option **Importer les paramètres**. Saisissez le chemin 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 le menu principal, cliquez sur **Configuration > Importer et exporter les paramètres...** Sélectionnez l'option **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.



5.3 Raccourcis clavier

Voici les raccourcis clavier disponibles dans ESET NOD32 Antivirus :

Ctrl+G	désactive l'interface utilisateur dans le produit
Ctrl+I	ouvre la page ESET SysInspector
Ctrl+L	ouvre la page des fichiers journaux
Ctrl+S	ouvre la page du planificateur
Ctrl+Q	ouvre la page de quarantaine
Ctrl+U	ouvre une boîte de dialogue permettant d'indiquer le nom d'utilisateur et le mot de passe

Pour simplifier la navigation dans le produit de sécurité 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
*	développe le nœud de l'arborescence Configuration avancée
-	réduit le nœud de l'arborescence Configuration avancée
TAB	déplace le curseur dans une fenêtre
Échap	ferme la boîte de dialogue active

5.4 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 traitement par lots (« bat »). Module d'interface à ligne de commande ESET :

```
ecls [OPTIONS...] FILES..
```

Les paramètres suivants peuvent être utilisés lors de l'exécution de l'analyseur à la demande, à partir de la ligne de commande :

Options

/base-dir=FOLDER	charger les modules depuis le DOSSIER
/quar-dir=FOLDER	DOSSIER de quarantaine
/exclude=MASK	exclure les fichiers correspondant à MASQUE de l'analyse
/subdir	analyser les sous-dossiers (valeur par défaut)
/no-subdir	ne pas analyser les sous-dossiers
/max-subdir-level=LEVEL	sous-niveau maximal de sous-dossiers dans les dossiers à analyser
/symlink	suivre les liens symboliques (valeur par défaut)
/no-symlink	ignorer les liens symboliques
/ads	analyser ADS (valeur par défaut)
/no-ads	ne pas analyser ADS
/log-file=FILE	journaliser les résultats dans un FICHIER
/log-rewrite	écraser le fichier de résultats (valeur par défaut - ajouter)
/log-console	journaliser les résultats sur la console (valeur par défaut)
/no-log-console	ne pas journaliser les résultats sur la console
/log-all	journaliser également les fichiers nettoyés
/no-log-all	ne pas journaliser les fichiers nettoyés (valeur par défaut)
/aind	afficher l'indicateur d'activité
/auto	analyser et nettoyer automatiquement tous les disques locaux

Options de l'analyseur

/files	analyser les fichiers (valeur par défaut)
/no-files	ne pas analyser les fichiers
/memory	analyser la mémoire
/boots	analyser les secteurs d'amorçage
/no-boots	ne pas analyser les secteurs d'amorçage (valeur par défaut)
/arch	analyser les archives (valeur par défaut)
/no-arch	ne pas analyser les archives
/max-obj-size=SIZE	analyser uniquement les fichiers plus petits que TAILLE Mo (valeur par défaut 0 = illimité)

/max-arch-level=LEVEL	sous-niveau maximal d'archives à analyser dans les archives (archives imbriquées)
/scan-timeout=LIMIT	analyser les archives pendant un maximum de LIMITE secondes
/max-arch-size=SIZE	n'analyser les fichiers contenus dans une archive que s'ils sont plus petits que TAILLE (valeur par défaut 0 = illimité)
/max-sfx-size=SIZE	n'analyser les fichiers d'une archive auto-extractible que s'ils sont plus petits que TAILLE Mo (valeur par défaut 0 = illimité)
/mail	analyser les fichiers des courriers électroniques (valeur par défaut)
/no-mail	ne pas analyser les fichiers des courriers électroniques
/mailbox	analyser les boîtes aux lettres (valeur par défaut)
/no-mailbox	ne pas analyser les boîtes aux lettres
/sfx	analyser les archives auto-extractibles (valeur par défaut)
/no-sfx	ne pas analyser les archives auto-extractibles
/rtp	analyser les fichiers exécutables compressés par un compresseur d'exécutables (valeur par défaut)
/no-rtp	ne pas analyser les fichiers exécutables compressés
/adware	rechercher les adware/spyware/riskware (valeur par défaut)
/no-adware	ne pas rechercher les adware/spyware/riskware
/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)
/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 : aucun nettoyage, nettoyage standard (valeur par défaut), nettoyage strict, nettoyage rigoureux, suppression
/quarantine	copier les fichiers infectés vers Quarantaine (complète ACTION)
/no-quarantine	ne pas copier les fichiers infectés vers Quarantaine

Options générales

/help	afficher l'aide et quitter
/version	afficher les informations de version et quitter
/preserve-time	conserver la date et l'heure du dernier accès

Codes de sortie

0	aucune menace détectée
1	menace détectée et nettoyée
10	certaines 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.

5.5 ESET SysInspector

5.5.1 Introduction à ESET SysInspector

ESET SysInspector est une application qui inspecte votre ordinateur en profondeur et qui affiche en détail toutes les données obtenues. 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.

Vous pouvez accéder à ESET SysInspector de deux manières : depuis la version intégrée dans ESET NOD32 Antivirus ou en téléchargeant gratuitement la version autonome (SysInspector.exe) depuis le site Internet d'ESET. Pour ouvrir ESET SysInspector, cliquez sur **Outils > ESET SysInspector**. Les deux versions sont identiques en matière de fonctionnalités et disposent des mêmes contrôles de programme. La seule différence réside dans la façon dont les résultats sont gérés. Les versions téléchargées et intégrées vous 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** (pour plus d'informations, reportez-vous à la section [ESET SysInspector](#)

[comme composant ESET NOD32 Antivirus](#)).

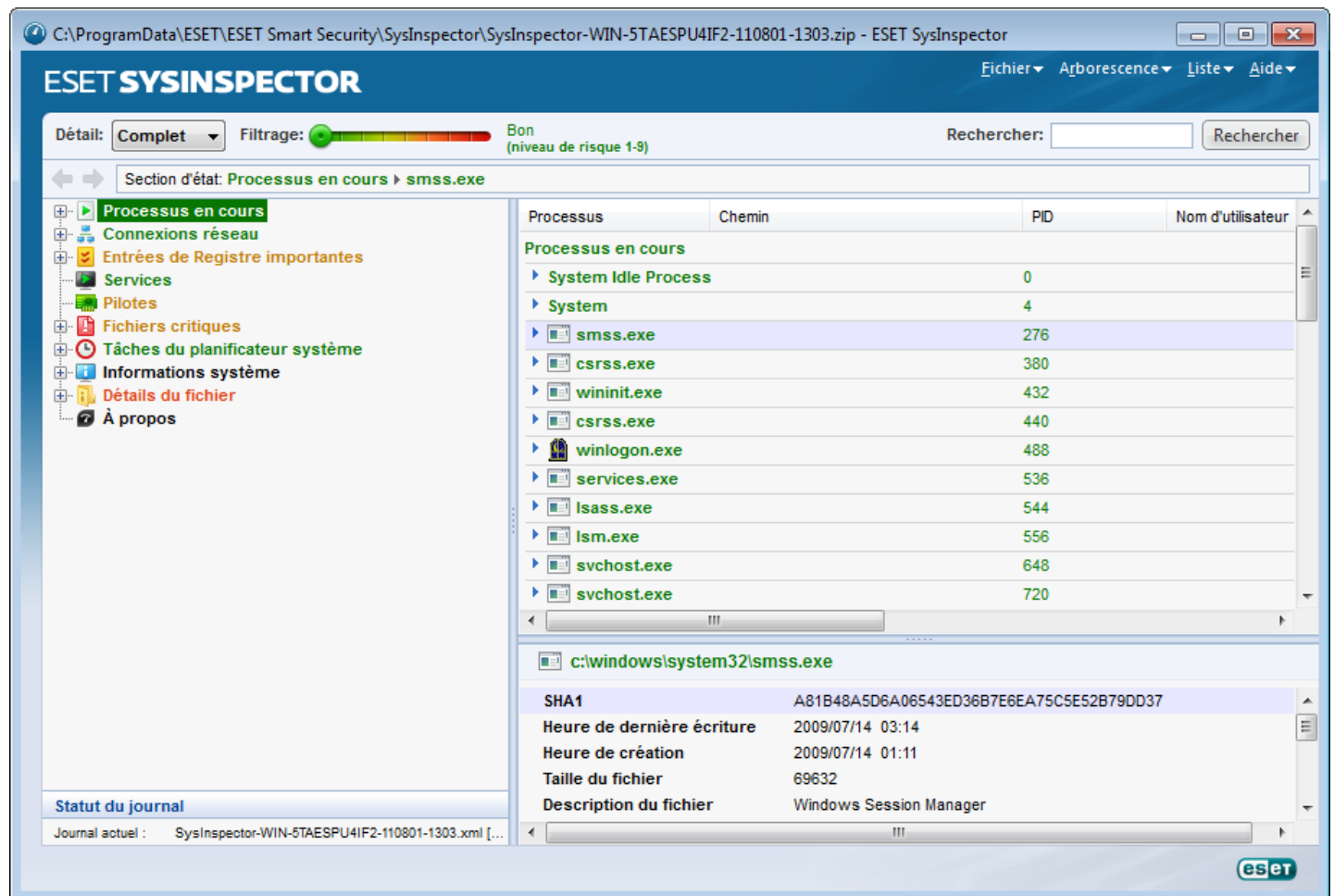
Veuillez patienter pendant qu'ESET SysInspector analyse votre ordinateur. L'analyse peut prendre entre 10 secondes et quelques minutes, en fonction de la configuration de votre matériel, du système d'exploitation et du nombre d'applications installées sur votre ordinateur.

5.5.1.1 Démarrage d'ESET SysInspector

Pour démarrer ESET SysInspector, il suffit de lancer le fichier exécutable *SysInspector.exe* téléchargé depuis le site Web d'ESET. Si vous avez déjà installé un des produits de sécurité d'ESET, vous pouvez exécuter ESET SysInspector directement depuis le menu Démarrer (**Programmes > ESET > ESET NOD32 Antivirus**). Patientez pendant que l'application vérifie le système. Cette opération peut prendre plusieurs minutes, en fonction du matériel et des données à recueillir.

5.5.2 Interface utilisateur et utilisation de l'application

Pour des raisons de clarté, la fenêtre principale 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 à droite au bas. La section État du journal énumère les paramètres de base d'un journal (utilisation des filtres, type de filtre, journal 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 l'option **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 sur 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 des fonctions qui simplifient la navigation dans le programme, ainsi que d'autres fonctionnalités 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, le programme affiche moins de détails. En mode Complet, ESET SysInspector affiche toutes les informations nécessaires pour résoudre des problèmes très précis.

Filtrage des éléments

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 qui sont plus suspects que le niveau 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 d'ESET, nous vous conseillons d'analyser votre système à l'aide d'[ESET Online Scanner](#) si ESET SysInspector a détecté un élément de ce genre. ESET Online Scanner est un service gratuit.

REMARQUE : le niveau de risque d'un élément peut être rapidement déterminé grâce à la couleur que prend le curseur pour indiquer le niveau de risque.

Rechercher

La fonction de recherche permet de trouver rapidement un élément sur la base de son nom ou d'une partie de son nom. 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 les flèches 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 principales appelées 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 l'arborescence 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 comprend les informations sur les applications et les processus en cours d'exécution au moment de la création du journal. La fenêtre Détails comprend 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 et le niveau de risque du fichier.

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 de ces 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 des problèmes système. Il s'agit des entrées qui indiquent les applications de démarrage, les objets d'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.

Informations système

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

Informations sur ESET SysInspector.

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. Accédez au menu **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, utilisez le menu **Fichier > Ouvrir le journal**. Dans la fenêtre principale de l'application, ESET SysInspector affiche toujours un journal à la fois.







Le fait de comparer deux journaux permet d'afficher le journal actif et un journal enregistré dans un fichier. Pour comparer des journaux, choisissez l'option **Fichier > Comparer les journaux**, puis choisissez **Sélectionner un fichier**. Le journal sélectionné est comparé au journal actif dans les fenêtres principales de l'application. Le journal résultant, appelé journal des comparaisons, affiche uniquement les différences entre les deux journaux.

REMARQUE : si vous comparez deux fichiers journaux, choisissez **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 ajoute des symboles qui identifient les différences entre les journaux comparés.

Les éléments marqués par **-** se trouvent uniquement dans le journal actif et sont absents du journal de comparaison ouvert. Les éléments marqués par **+** se trouvent uniquement dans le journal ouvert et ne figurent pas dans le journal actif.

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

- **+** nouvelle valeur, absente du journal précédent.
-  cette section de l'arborescence contient de nouvelles valeurs.
- **-** valeur supprimée, présente uniquement dans le journal précédent.
-  cette section de l'arborescence contient des valeurs supprimées.
-  valeur/fichier modifié.
-  cette section de l'arborescence contient des valeurs/fichiers modifiés.
-  le niveau de risque a diminué/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 ultérieurement :

Exemple

Créez un journal reprenant les informations d'origine du système et enregistrez-le dans un fichier appelé précédent.xml. Après avoir modifié le système, ouvrez ESET SysInspector pour qu'il crée un nouveau journal. Enregistrez ce journal sous le nom *actuel.xml*.

Pour voir les différences entre ces deux journaux, utilisez l'option **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 :

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 :

/gen	crée un journal directement depuis la ligne de commande sans exécuter l'interface utilisateur.
/privacy	crée un journal qui exclut les informations sensibles.
/zip	stocke le journal obtenu directement sur le disque dans un fichier compressé.
/silent	supprime l'affichage de la barre de progression de la création du journal.
/help, /?	affiche des informations sur les paramètres de la ligne de commande.

Exemples

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

Pour créer un journal à l'emplacement actuel, saisissez : `SysInspector.exe /gen`

Pour créer un journal dans un dossier en particulier, saisissez : `SysInspector.exe /gen="c:\dossier\"`

Pour créer un journal dans un fichier/dossier en particulier, saisissez : `SysInspector.exe /gen="c:\dossier\monnouveaujournal.xml"`

Pour créer un journal qui exclut les informations sensibles directement dans un fichier compressé, saisissez : `SysInspector.exe /gen="c:\monnouveaujournal.zip" /privacy /zip`

Pour comparer deux journaux, utilisez : `SysInspector.exe "actuel.xml" "original.xml"`

REMARQUE : si le nom du fichier/dossier contient un espace, saisissez-le entre guillemets.

5.5.4 Script de service

Le script de service supprime très facilement les objets indésirables du système et offre une aide aux clients qui utilisent ESET SysInspector.

Le script de service permet à l'utilisateur d'exporter l'ensemble du journal ESET SysInspector ou certaines parties sélectionnées. Après l'exportation, vous pouvez marquer les objets non souhaités 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 :

- Exécutez ESET SysInspector pour obtenir un nouvel instantané du système.
- Sélectionnez le premier élément de la section à gauche (dans l'arborescence), appuyez sur la touche Ctrl et maintenez-la enfoncée, puis sélectionnez le dernier élément afin de marquer tous les éléments.
- Cliquez avec le bouton droit sur les objets sélectionnés et sélectionnez l'option **Exporter les sections sélectionnées dans un script de service** dans le menu contextuel.
- Les objets sélectionnés sont exportés dans un nouveau journal.
- 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. Assurez-vous que vous n'avez sélectionné aucun objet/fichier important pour le système d'exploitation.
- Ouvrez ESET SysInspector, cliquez sur **Fichier > Exécuter le script de services** et entrez le chemin d'accès au script.
- 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 pas être modifiée.

Le reste du fichier est scindé en sections dont les éléments peuvent être modifiés (elles indiquent les éléments qui sont 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, puis 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'arrête à l'exécution du script.

02) Loaded modules (modules chargés)

Cette section répertorie la 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\khbexb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Dans cet exemple, le module khbexb.dll a été marqué par un « + ». Quand le script est exécuté, il reconnaît les processus qui utilisent ce module 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 localise 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 sont 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 sont supprimées, réduites à des valeurs de 0 octet ou réinitialisées sur leur valeur par défaut lors de l'exécution du script. L'action à appliquer sur chaque entrée dépend de la catégorie de l'entrée et de la valeur de la clé dans ce registre.

07) Services (services)

Cette section répertorie 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 répertorie 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 sont désenregistrés du registre système et supprimés.

09) Critical files (fichiers critiques)

Cette section contient des informations sur les fichiers essentiels au 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 sont soit supprimés, soit restaurés sur leur valeur d'origine.

5.5.4.3 Exécution des scripts de services

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 services** 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 l'exécution correcte du script.

Si le script n'a pu être traité que partiellement, une boîte de dialogue avec le message suivant apparaît : **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 répertorie les opérations qui n'ont pas été exécutées.

Si le script n'a pas été reconnu, une boîte de dialogue apparaît avec le message suivant : **Le script de service sélectionné n'est pas signé. L'exécution de scripts non signés et inconnus peut endommager gravement les données de votre ordinateur. Voulez-vous vraiment exécuter le script et ses actions ?** Ceci peut être le résultat d'incohérences au sein du script (en-tête ou 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 Raccourcis

Voici les raccourcis clavier disponibles dans ESET SysInspector :

Fichier

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

Générer

Ctrl+G	vérification standard de l'état du système
Ctrl+H	vérifie le système et consigne également les informations sensibles

Filtrage des éléments

1, O	affiche les éléments de niveau de risque 1 à 9 (acceptable)
2	affiche les éléments de niveau de risque 2 à 9 (acceptable)
3	affiche les éléments de niveau de risque 3 à 9 (acceptable)
4, U	affiche les éléments de niveau de risque 4 à 9 (inconnu)
5	affiche les éléments de niveau de risque 5 à 9 (inconnu)
6	affiche les éléments de niveau de risque 6 à 9 (inconnu)
7, B	affiche les éléments de niveau de risque 7 à 9 (risqué)
8	affiche les éléments de niveau de risque 8 à 9 (risqué)
9	affiche les éléments de niveau de risque 9 (risqué)
-	diminue le niveau de risque
+	augmente le niveau de risque
Ctrl+9	mode de filtrage, niveau égal ou supérieur
Ctrl+O	mode 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	afficher tous les détails
Ctrl+2	afficher les détails de précision moyenne
Ctrl+1	affichage de base
Retour arrière	revient une étape en arrière
Barre d'espace	avance d'une étape
Ctrl+W	développe l'arborescence
Ctrl+Q	réduit l'arborescence

Autres commandes

Ctrl+T	accède 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	passé 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 indique les éléments présents dans le journal actuel
Ctrl+Alt+3	affiche uniquement les éléments supprimés ; le journal indique 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

5.5.6 Configuration système

Pour garantir le fonctionnement correct d'ESET SysInspector, le système doit répondre à la configuration suivante :

Windows 2000, XP, 2003

400 MHz 32 bits (x86)/64 bits (x64)
128 Mo de RAM de mémoire système
10 Mo d'espace disponible
Super VGA (800 x 600)

Windows 7, Vista, 2008

1 GHz 32 bits (x86)/64 bits (x64)
512 Mo de RAM de mémoire système
10 Mo d'espace disponible
Super VGA (800 x 600)

5.5.7 FAQ

L'exécution d'ESET SysInspector requiert-elle des privilèges d'administrateur ?

Bien qu'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 entraîne 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 le menu principal, sélectionnez **Fichier > Enregistrer le journal**. Les journaux sont enregistrés au format XML. Par défaut, les fichiers sont enregistrés dans le répertoire %USERPROFILE%\Mes documents\, conformément à la convention de dénomination de fichier « SysInspector-%COMPUTERNAME%-AAMMJJ-HHMM.XML ». Vous pouvez changer l'emplacement et le nom du fichier avant de l'enregistrer si vous le souhaitez.

Comment puis-je consulter le fichier journal d'ESET SysInspector ?

Pour consulter un fichier journal créé par ESET SysInspector, exécutez le programme et choisissez **Fichier > Ouvrir le journal** dans le menu principal. 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 peuvent désactiver la fonction glisser-déposer entre des fenêtres dont les autorisations diffèrent.

Existe-t-il une spécification pour le format de fichier journal ? Existe-t-il un kit de développement logiciel (SDK) ?

Pour l'instant, il n'existe ni spécifications pour le fichier journal ni SDK, car le programme est toujours au stade du développement. Après la sortie 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 d'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 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 permet de détecter avec efficacité les rootkits.

Quand un système est attaqué par un code malveillant qui se comporte comme un rootkit, les données risquent d'être endommagées ou volées. 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 » ?

Lorsqu'ESET SysInspector tente d'identifier la signature numérique d'un fichier exécutable, il vérifie d'abord si une signature numérique est intégrée au fichier. Si c'est le cas, l'identification dans le fichier est utilisée pour la validation. Si le fichier ne contient pas de signature numérique, ESI lance la recherche du fichier CAT correspondant (Catalogue de sécurité - %systemroot%\system32\catroot). Si le fichier CAT pertinent est trouvé, sa signature numérique est appliquée dans la procédure de validation du fichier exécutable.

Voilà pourquoi des fichiers sont parfois marqués « Signé par MS » mais ont un « Nom de la société » différent.

Exemple :

Windows 2000 comprend 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 qui possède une signature numérique de Microsoft.

5.5.8 ESET SysInspector en tant que composant de ESET NOD32 Antivirus

Pour ouvrir la section ESET SysInspector dans ESET NOD32 Antivirus, cliquez sur **Outils > ESET SysInspector**. Le système de gestion disponible dans 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, utilisez l'option **Afficher** du 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** - La fonctionnalité 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 le pourcentage de progression de la création de l'instantané en cours, consultez la colonne **État**. Tous les instantanés terminés ont le statut **Créé**.
- **Supprimer** - L'option Supprimer supprime les entrées de la liste.
- **Exporter...** - Cette option enregistre l'entrée sélectionnée dans un fichier XML (également dans une version compressée).

5.6 ESET SysRescue

ESET SysRescue est un utilitaire qui permet de créer un disque d'amorçage contenant ESET NOD32 Antivirus. Le principal avantage d'ESET SysRescue réside dans le fait que ESET NOD32 Antivirus est exécuté indépendamment du système d'exploitation hôte, tout en ayant un accès direct au disque et à l'ensemble du 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.

5.6.1 Configuration minimale requise

ESET SysRescue fonctionne dans l'environnement de préinstallation Microsoft Windows (Windows PE) version 2.x basé sur Windows Vista. Windows PE faisant partie du kit d'installation automatisée de Windows (Windows AIK), ce kit doit être installé avant la création d'ESET SysRescue (<http://go.eset.eu/AIK>). Windows PE prenant en charge la version 32 bits, le package d'installation de ESET NOD32 Antivirus 32 bits doit être installé lors de la création de ESET SysRescue sur des systèmes 64 bits. ESET SysRescue prend en charge Windows AIK 1.1 et les versions ultérieures. ESET SysRescue est disponible dans ESET NOD32 Antivirus 4.0 et les versions ultérieures.

Systèmes d'exploitation pris en charge

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- Windows Server 2003 Service Pack 1 avec KB926044
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 avec KB926044
- Windows XP Service Pack 3

5.6.2 Procédure de création d'un CD de dépannage

Pour lancer l'assistant ESET SysRescue, cliquez sur **Démarrer > Programmes > ESET > ESET NOD32 Antivirus > ESET SysRescue**.

Tout d'abord, l'Assistant vérifie si Windows AIK est installé et si un périphérique adapté pour la création du support d'amorçage est présent. Si *Windows AIK* n'est pas installé sur l'ordinateur (ou si l'installation est endommagée ou incorrecte), l'assistant vous propose de l'installer ou de saisir le chemin d'accès à votre dossier Windows AIK (<http://go.eset.eu/AIK>).

Au cours de l'[étape suivante](#), sélectionnez le support cible où ESET SysRescue sera stocké.

5.6.3 Sélection de la cible

Outre la sauvegarde sur un CD/DVD/périphérique USB, vous pouvez enregistrer ESET SysRescue dans un fichier ISO. Vous pouvez ensuite graver l'image ISO sur un CD/DVD, ou l'utiliser d'une autre manière (dans un environnement virtuel tel que VmWare ou Virtualbox par exemple).

Si vous choisissez le support cible USB, le démarrage peut ne pas fonctionner sur certains ordinateurs. Certaines versions du BIOS peuvent signaler des problèmes de communication entre le BIOS et le gestionnaire de démarrage (par exemple sous Windows Vista) et le démarrage s'arrête sur l'erreur suivante :

```
file : \boot\bcd
status : 0xc000000e
info : an error occurred while attempting to read the boot configuration data (une erreur s'est produite pend
```

Si ce message s'affiche, il est conseillé de sélectionner un CD au lieu du support USB.

5.6.4 Paramètres

Avant de commencer la création d'ESET SysRescue, l'assistant d'installation affiche les paramètres de compilation à la dernière étape de l'assistant ESET SysRescue. Pour les modifier, cliquez sur le bouton **Modifier...** Les options disponibles sont les suivantes :

- [Dossiers](#)
- [ESET Antivirus](#)
- [Paramètres avancés](#)
- [Protocole Internet](#)
- [Périphérique USB d'amorçage](#) (lorsque le périphérique USB de destination est sélectionné)
- [Gravure](#) (lorsque le lecteur de CD/DVD de destination est sélectionné)

Le bouton **Créer** est inactif si aucun package d'installation MSI n'a été défini ou si aucune solution de sécurité d'ESET n'est installée sur l'ordinateur. Pour sélectionner un package d'installation, cliquez sur le bouton **Modifier**, puis accédez à l'onglet **Antivirus ESET**. Si vous ne saisissez pas le nom d'utilisateur et le mot de passe (**Modifier > Antivirus ESET**), le bouton **Créer** est grisé.

5.6.4.1 Dossiers

Le **dossier temporaire** est un dossier de travail dans lequel sont stockés les fichiers nécessaires à la compilation d'ESET SysRescue.

Le **dossier ISO** est un dossier dans lequel est enregistré le fichier ISO après la compilation.

La liste dans cet onglet répertorie tous les disques de réseau locaux et mappés, ainsi que l'espace disponible. Si certains des dossiers sont stockés sur un lecteur ne disposant pas de l'espace suffisant, il est conseillé de sélectionner un autre lecteur avec plus d'espace disponible. Dans le cas contraire, la compilation pourrait s'arrêter prématurément en raison d'un manque d'espace sur le disque.

Applications externes : vous permet d'indiquer des programmes supplémentaires qui seront exécutés ou installés après l'amorçage depuis un support ESET SysRescue.

Inclure les applications externes : permet d'ajouter des programmes externes à la compilation ESET SysRescue.

Dossier sélectionné : dossier dans lequel se trouvent les programmes à ajouter au disque ESET SysRescue.

5.6.4.2 ESET Antivirus

Pour créer le CD ESET SysRescue, vous pouvez sélectionner deux sources de fichiers ESET à utiliser par le compilateur.

Dossier ESS : fichiers déjà contenus dans le dossier dans lequel le produit ESET est installé sur l'ordinateur.

Fichier MSI : les fichiers contenus dans le programme d'installation MSI sont utilisés.

Vous pouvez ensuite choisir de mettre à jour l'emplacement des fichiers d'installation (.nup). L'option par défaut **Dossier ESS/EAV/Fichier MSI** doit normalement être sélectionnée. Dans certains cas, un **dossier de mise à jour** personnalisé peut être choisi, pour utiliser par exemple une version de base des signatures de virus ancienne ou récente.

Vous pouvez utiliser l'une des deux sources suivantes pour le nom d'utilisateur et le mot de passe :

ESS/EAV installé : le nom d'utilisateur et le mot de passe sont copiés depuis la version installée de ESET NOD32 Antivirus.

De l'utilisateur : le nom d'utilisateur et le mot de passe saisis dans les zones de texte correspondantes sont utilisés.

REMARQUE : ESET NOD32 Antivirus sur le CD ESET SysRescue est mis à jour soit via Internet, soit par l'intermédiaire de la solution ESET Security installée sur l'ordinateur d'où le CD ESET SysRescue est exécuté.

5.6.4.3 Paramètres avancés

L'onglet **Avancé** permet d'optimiser le CD ESET SysRescue en fonction de la quantité de mémoire disponible sur l'ordinateur. Sélectionnez **576 Mo et plus** pour écrire le contenu du CD dans la mémoire vive (RAM). Si vous choisissez **moins de 576 Mo**, l'accès au CD de récupération est permanent lorsque WinPE est en exécution.

Pilotes externes : cette section permet d'installer les pilotes de votre matériel (en général, de la carte réseau). Bien que WinPE repose sur Windows Vista PS1 qui prend en charge une large gamme de matériels, il arrive parfois que le matériel ne soit pas reconnu. Dans ce cas, un pilote doit être ajouté manuellement. L'installation du pilote dans la compilation ESET SysRescue peut s'effectuer de deux manières : manuellement (à l'aide du bouton **Ajouter**) et automatiquement (par l'intermédiaire du bouton **Recherche auto**). En cas d'inclusion manuelle, vous devez choisir le chemin d'accès au fichier .inf correspondant (le fichier *.sys applicable doit se trouver également dans le dossier). En cas d'installation automatique, le pilote est détecté automatiquement dans le système d'exploitation de l'ordinateur. Il est conseillé d'utiliser l'inclusion automatique uniquement si ESET SysRescue est utilisé sur un ordinateur qui dispose de la même carte réseau que l'ordinateur sur lequel le CD ESET SysRescue a été créé. Lors de la création d'ESET SysRescue, le pilote est installé dans la compilation, ce qui évite à l'utilisateur d'avoir à le rechercher ultérieurement.

5.6.4.4 Protocole Internet

Cette section permet de configurer les informations réseau de base et les connexions prédéfinies après ESET SysRescue.

Sélectionnez **Adresse IP privée automatique** pour obtenir automatiquement l'adresse IP depuis le serveur DHCP (Dynamic Host Configuration Protocol).

Cette connexion réseau peut également utiliser une adresse IP spécifiée manuellement (appelée également adresse IP statique). Sélectionnez **Personnalisé** pour configurer les paramètres IP appropriés. Si vous sélectionnez cette option, vous devez indiquer une **adresse IP** et, pour les connexions au réseau LAN et les connexions Internet haut débit, un **masque de sous-réseau**. Dans les zones **Serveur DNS préféré** et **Serveur DNS de rechange**, saisissez les adresses des serveurs DNS principal et secondaire.

5.6.4.5 Périphérique USB d'amorçage

Si vous avez choisi le périphérique USB en tant que support cible, vous pouvez choisir l'un des supports USB disponibles dans l'onglet **Périphérique USB d'amorçage** (si plusieurs périphériques USB existent).

Sélectionnez le **périphérique** sur lequel ESET SysRescue doit être installé.

Avertissement : le périphérique USB sélectionné est formaté lors de la création d'ESET SysRescue. Toutes les données du périphérique sont supprimées.

Si vous choisissez l'option de **format rapide**, le formatage supprime tous les fichiers de la partition, mais ne recherche pas les secteurs défectueux du disque. Utilisez cette option si votre périphérique USB a été formaté précédemment et que vous êtes certain qu'il n'est pas endommagé.

5.6.4.6 Graver

Si vous avez choisi le support cible CD/DVD, vous pouvez définir les paramètres de gravure complémentaires dans l'onglet **Graver**.

Supprimer fichier ISO : cochez cette case pour supprimer les fichiers ISO après la création du CD ESET SysRescue.

Suppression activée : permet de choisir entre la suppression rapide et la suppression complète.

Graveur : choisissez le lecteur à utiliser pour la gravure.

Avertissement : il s'agit de l'option par défaut. En cas d'utilisation d'un CD/DVD réinscriptible, toutes les données stockées sur le CD/DVD sont supprimées.

La section Support contient des informations sur le support dans le lecteur de CD/DVD.

Vitesse de gravure : sélectionnez la vitesse souhaitée dans le menu déroulant. Les capacités du périphérique de gravure et le type de CD/DVD utilisé doivent être pris en compte lors de la sélection de la vitesse de gravure.

5.6.5 Travailler avec ESET SysRescue

Pour que le CD/DVD/USB de récupération fonctionne efficacement, l'ordinateur doit être démarré depuis le support d'amorçage ESET SysRescue. La priorité d'amorçage peut être modifiée dans le BIOS. Vous pouvez également utiliser le menu d'amorçage au démarrage de l'ordinateur (généralement à l'aide de l'une des touches F9 à F12, en fonction de la version de la carte mère ou du BIOS).

Une fois l'amorçage depuis le support d'amorçage terminé, ESET NOD32 Antivirus démarre. Comme ESET SysRescue n'est utilisé que dans des situations spécifiques, certains modules de protection et fonctionnalités de programme présents dans la version standard d'ESET NOD32 Antivirus ne sont pas nécessaires ; leur liste est limitée à l'**analyse**, à la **mise à jour** et à certaines sections de la **configuration**. ESET SysRescue peut mettre à jour la base des signatures de virus. C'est la principale fonctionnalité de cette application et nous vous recommandons d'effectuer cette mise à jour avant de lancer l'analyse de l'ordinateur.

5.6.5.1 Travailler avec ESET SysRescue

Supposons que des ordinateurs du réseau aient été infectés par un virus modifiant les fichiers exécutables (.exe). ESET NOD32 Antivirus est capable de nettoyer tous les fichiers infectés, à l'exception d'*explorer.exe* qui ne peut pas être nettoyé, même en mode sans échec.

Cela s'explique par le fait que le fichier *explorer.exe*, c'est-à-dire l'un des principaux processus de Windows, est également lancé en mode sans échec. ESET NOD32 Antivirus n'exécute aucune opération et le fichier reste infecté.

Dans ce type de scénario, vous pouvez utiliser ESET SysRescue pour résoudre le problème. ESET SysRescue ne requiert aucun composant du système d'exploitation hôte et peut traiter (nettoyer, supprimer) n'importe quel fichier du disque.

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 est une infiltration qui endommage les fichiers existants de 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.

Les virus informatiques attaquent principalement les fichiers et documents exécutables. Pour proliférer, un virus attache son « corps » à la fin d'un fichier cible. En bref, un virus informatique fonctionne de la manière suivante : après l'exécution du fichier infecté, le virus s'active lui-même (avant l'application originale) et exécute sa tâche prédéfinie. C'est après seulement que l'application originale peut s'exécuter. Un virus ne peut pas infecter un ordinateur à moins qu'un utilisateur n'exécute ou n'ouvre lui-même (accidentellement ou délibérément) le programme malveillant.

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.

Il est important de noter que, contrairement aux chevaux de Troie et aux logiciels espions, les virus sont de plus en plus rares, car d'un point de vue commercial, ils ne sont pas très attrayants pour les auteurs de programmes malveillants. En outre, le terme « virus » est souvent utilisé mal à propos pour couvrir tout type d'infiltrations. On tend à le remplacer progressivement par le terme « logiciel malveillant » ou « malware » en anglais.

Si votre ordinateur est infecté par un virus, il est nécessaire de restaurer les fichiers infectés à leur état original, c'est-à-dire de les nettoyer à l'aide d'un programme antivirus.

Dans la catégorie des virus, on peut citer : OneHalf, Tenga et Yankee Doodle.

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 répliquer et de voyager par eux-mêmes. Ils ne dépendent pas des fichiers hôtes (ou des secteurs d'amorçage). Les vers se propagent par l'intermédiaire d'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.

Parmi les vers les plus connus, on peut citer : Lovsan/Blaster, Stration/Warezov, Bagle et Netsky.

6.1.3 Chevaux de Troie

Dans le passé, les chevaux de Troie étaient définis comme une catégorie d'infiltrations dont la particularité est de se présenter comme des programmes utiles pour duper ensuite les utilisateurs qui acceptent de les exécuter. Il est cependant important de remarquer que cette définition s'applique aux anciens chevaux de Troie. Aujourd'hui, il ne leur est plus utile de se déguiser. Leur unique objectif est de trouver la manière la plus facile de s'infiltrer pour accomplir leurs desseins malveillants. Le terme « cheval de Troie » est donc devenu un terme très général qui décrit toute infiltration qui n'entre pas dans une catégorie spécifique.

La catégorie étant très vaste, elle est souvent divisée en plusieurs sous-catégories :

- **Téléchargeur** - Programme malveillant qui est en mesure de télécharger d'autres infiltrations sur Internet.
- **Dropper** - Type de cheval de Troie conçu pour déposer d'autres types de logiciels malveillants sur des ordinateurs infectés.
- **Backdoor** - Application qui communique à distance avec les pirates et leur permet d'accéder à un système et d'en prendre le contrôle.
- **Keylogger** - Programme qui enregistre chaque touche sur laquelle tape l'utilisateur et envoie les informations aux pirates.
- **Composeur** - Programme destiné à se connecter à des numéros surtaxés. 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.

Les chevaux de Troie prennent généralement la forme de fichiers exécutables avec l'extension .exe. Si un fichier est identifié comme cheval de Troie sur votre ordinateur, il est recommandé de le supprimer, car il contient sans doute du code malveillant.

Parmi les chevaux de Troie les plus connus, on peut citer :: NetBus, Trojandownloader.Small.ZL, Slapper

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 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.

Les applications potentiellement dangereuses rentrent dans une 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 l'ayez installée), consultez l'administrateur réseau ou supprimez l'application.

6.1.8 Applications potentiellement indésirables

Les **applications potentiellement indésirables** ne sont pas nécessairement malveillantes, mais elles sont susceptibles d'affecter les performances de votre ordinateur. Ces applications sont habituellement installées après consentement. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Voici les changements les plus significatifs :

- affichage de nouvelles fenêtres (fenêtres contextuelles, publicités) ;
- activation et exécution de processus cachés ;
- augmentation de l'utilisation des ressources système ;
- modification des résultats de recherche ;
- communication de l'application avec des serveurs distants.

6.2 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.

6.2.1 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.

6.2.2 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.

6.2.3 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.

6.2.4 Reconnaissance du courrier indésirable

Généralement, peu d'indicateurs contribuent à identifier le courrier indésirable (messages non sollicités) dans une boîte à lettres. Si un message remplit au moins l'un des critères suivants, il s'agit probablement de courrier indésirable.

- L'adresse de l'expéditeur ne figure pas dans la liste de vos contacts.
- Le contenu du message concerne une grosse somme d'argent qui vous est offerte. Pour toucher cette somme, vous devez néanmoins fournir au préalable une petite somme.
- Vous devez 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.
- Le message est écrit dans une langue étrangère.
- Le message vous demande d'acheter un produit qui ne vous intéresse pas. Si vous décidez d'acheter le produit, vérifiez que l'expéditeur du message est un vendeur sérieux (consultez le fabricant original du produit).
- Quelques mots sont mal écrits pour pouvoir passer à travers le filtre de courrier indésirable. Par exemple, « vaigra » au lieu de « viagra », etc.