ESET NOD32 Antivirus 4

Business Edition pour Mac ordinateur

Manuel d'installation et Guide de l'utilisateur

ESET NOD32 Antivirus 4

Assistance à la clientèle Monde : www.eset.eu/support
Assistance à la clientèle Amérique du Nord : www.eset.com/support

RÉV. 8.12.2010

Contenu

1. ESET NOD32 Antivirus

En raison de la popularité grandissante des systèmes d'exploitation basés sur Unix, les utilisateurs de logiciels malveillants sont en train de développer de nouvelles menaces ciblant les utilisateurs de ce système d'exploitation. ESET NOD32 Antivirus offre une protection puissante et efficace contre ces menaces. ESET NOD32 Antivirus a la capacité de détecter les menaces pour Windows, protégeant ainsi les utilisateurs de ce système d'exploitation lorsqu'ils interagissent avec les utilisateurs Windows et vice-versa. Bien que les logiciels malveillants basés sur Windows ne constituent pas une menace directe pour Mac, désactiver les logiciels malveillants qui ont infecté une machine Mac les empêchera de se répandre sur les ordinateurs basés sur Windows par l'entremise d'un réseau local ou d'Internet.

1.1 Configuration minimale requise

Pour assurer le bon fonctionnement de ESET NOD32 Antivirus, la configuration matérielle et logicielle minimale requise est la suivante :

ESET NOD32 Antivirus:

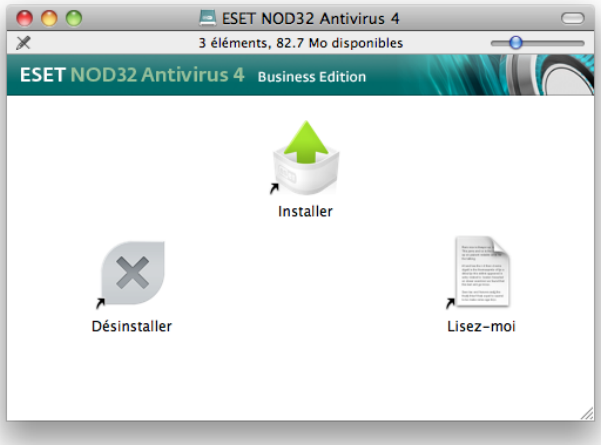
	Configuration minimale requise
Architecture de processeur	Intel® 32 bits ou 64 bits
Système d'exploitation	Mac OS X 10.5 et suivantes
Mémoire	512 Mo
Espace disque libre	100 Mo

2. Installation

Avant de commencer le processus d'installation, veuillez fermer tous les programmes ouverts sur votre ordinateur. ESET NOD32 Antivirus contient des composants qui peuvent entrer en conflit avec d'autres logiciels antivirus pouvant être déjà installés sur votre ordinateur. ESET recommande vivement de supprimer tout autre logiciel pour éviter tout problème potentiel. Vous pouvez installer ESET NOD32 Antivirus à partir d'un CD d'installation ou à partir d'un fichier disponible sur le site Web d'ESET.

Pour lancer l'Assistant d'installation, effectuez l'une des opérations suivantes :

- Si vous installez le logiciel à partir du CD d'installation, insérez le CD dans le lecteur de cédérom. L'écran du menu s'affichera. Double-cliquez sur l'icône d'installation ESET NOD32 Antivirus pour lancer l'installation.
- Si vous installez le logiciel à partir d'un fichier téléchargé, double-cliquez sur ce fichier pour lancer le programme d'installation.
- Les autres fonctionnalités, y compris les manuels, la formation et la désinstallation, sont accessibles par un double-clic sur l'icône appropriée de l'écran du menu.



Lancez le programme d'installation; l'Assistant Installation vous guidera dans les opérations de configuration de base. Après avoir accepté le contrat de licence de l'utilisateur final, vous pourrez sélectionner le mode d'installation approprié parmi les différents types :

- Installation standard 5
- Installation personnalisée 6
- Installation à distance 6

2.1 Installation standard

L'installation standard comprend les options de configuration appropriées pour la majorité des utilisateurs. Les paramètres offrent un maximum de sécurité, combiné à une excellente performance système. L'installation standard est l'option par défaut, donc l'option recommandée si vous n'avez aucune exigence particulière quant aux paramètres.

Après avoir sélectionné le mode d'installation **Standard (recommandé)**, vous serez invité à entrer votre nom d'utilisateur et votre mot de passe pour activer les mises à jour automatiques du programme. Ces mises à jour jouent un rôle important dans le maintien d'une protection continue du système. Entrez votre **nom d'utilisateur** et votre **mot de passe** (les données d'authentification reçues après l'achat ou l'enregistrement de votre produit) dans les champs correspondants. Si vous n'avez pas votre nom d'utilisateur et votre mot de passe à portée de main, vous pouvez sélectionner l'option **Définir les paramètres de mise à jour ultérieurement** pour poursuivre l'installation. Vous pourrez entrer votre nom d'utilisateur et votre mot de passe directement dans le programme plus tard.

ThreatSense.Net Early Warning System contribue à garantir qu'ESET est immédiatement et continuellement informé des nouvelles infiltrations dans le but de protéger rapidement ses clients. Le système permet de soumettre de nouvelles menaces au laboratoire d'ESET où elles seront alors analysées, traitées puis ajoutées à la base de signatures de virus. Par défaut, la case **Activer le système d'avertissement anticipé ThreatSense.Net** est cochée. Cliquez sur **Configuration...** pour modifier les paramètres détaillés de soumission de fichiers suspects. Pour obtenir plus de détails, consultez la rubrique ThreatSense.Net 22.

L'étape suivante de l'installation est la configuration de la détection des applications potentiellement indésirables. Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais peuvent souvent affecter 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. Bien que ces applications affichent habituellement une notification pendant l'installation, elles peuvent facilement s'installer sans votre consentement. Activez l'option **Activer la détection d'applications potentiellement indésirables** pour permettre à ESET NOD32 Antivirus de détecter ce type de menace (recommandé). Si vous ne voulez pas activer cette fonction, sélectionnez l'option **Désactiver la détection des applications potentiellement indésirables**.

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

Installer.

2.2 Installation personnalisée

L'installation personnalisée est destinée aux utilisateurs d'expérience qui veulent modifier les paramètres avancés pendant la procédure d'installation.

Après avoir sélectionné l'installation **personnalisée**, votre devrez entrer votre **nom d'utilisateur** et votre **mot de passe** (les données d'authentification reçues après l'achat ou l'enregistrement du produit) dans les champs correspondants. Si vous n'avez pas votre nom d'utilisateur et votre mot de passe à portée de main, vous pouvez sélectionner l'option **Définir les paramètres de mise à jour ultérieurement** pour poursuivre l'installation. Vous pourrez entrer votre nom d'utilisateur et mot de passe par la suite.

Si vous utilisez un serveur mandataire, vous pouvez maintenant en définir les paramètres en sélectionnant l'option **J'utilise un serveur mandataire**. Entrez l'adresse IP ou l'adresse URL de votre serveur mandataire dans le champ **Adresse**. Dans le champ Port, précisez le port sur lequel le serveur mandataire accepte les connexions (3128 par défaut). Si le serveur mandataire exige une authentification, entrez un **nom d'utilisateur** et un **mot de passe** valides donnant accès à ce serveur. Si vous êtes certain qu'aucun serveur mandataire ne sera utilisé, vous pouvez choisir l'option **Je n'utilise pas de serveur mandataire**.Si vous n'en êtes pas certain, vous pouvez utiliser les paramètres actuels de votre système en sélectionnant **Utiliser les paramètres système (recommandé)**.

Si ESET NOD32 Antivirus sera administré par ESET Remote Administrator (ERA), vous pouvez régler les paramètres de ERA Server (nom du serveur, port et mot de passe) pour que ESET NOD32 Antivirus se connecte automatiquement au serveur ERA Server après l'installation.

Dans la prochaine étape, vous pourrez **définir les utilisateurs privilégiés** qui pourront modifier la configuration du programme. De la liste des utilisateurs affichée à gauche, sélectionnez les utilisateurs et **ajoutez**-les à la liste des **utilisateurs privilégiés**. Pour afficher tous les utilisateurs du système, sélectionnez l'option **Afficher tous les utilisateurs**.

ThreatSense.Net Early Warning System contribue à garantir qu'ESET est immédiatement et continuellement informé des nouvelles infiltrations dans le but de protéger rapidement ses clients. Le système permet de soumettre de nouvelles menaces au laboratoire d'ESET où elles seront alors analysées, traitées puis ajoutées à la base de signatures de virus. Par défaut, la case **Activer le système d'avertissement anticipé ThreatSense.Net** est cochée. Cliquez sur **Configuration...** pour modifier les paramètres détaillés de soumission de fichiers suspects. Pour plus de détails, consultez la rubrique ThreatSense.Net 22.

L'étape suivante de l'installation est la configuration de la détection des applications potentiellement indésirables. Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais peuvent souvent affecter 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. Bien que ces applications affichent habituellement une notification pendant l'installation, elles peuvent facilement s'installer sans votre consentement. Activez l'option **Activer la détection d'applications potentiellement indésirables** pour permettre à ESET NOD32 Antivirus de détecter ce type de menace (recommandé).

Cliquez sur **Installer** pour installer ESET NOD32 Antivirus sur un disque **Macintosh HD** standard. Si vous souhaitez sélectionner un autre disque, cliquez sur **Changer d'emplacement d'installation...**

2.3 Installation à distance

L'installation à distance vous permet de créer un ensemble d'installation qui pourra être installé sur les ordinateurs cibles à l'aide d'un logiciel de bureau à distance. ESET NOD32 Antivirus peut ensuite être géré à distance par l'entremise de ESET Remote Administrator.

L'installation à distance s'effectue en deux phases :

1. Création de l'ensemble d'installation à distance par l'entremise de l'installateur d'ESET 6
2. Installation à distance à l'aide du logiciel de bureau à distance 7

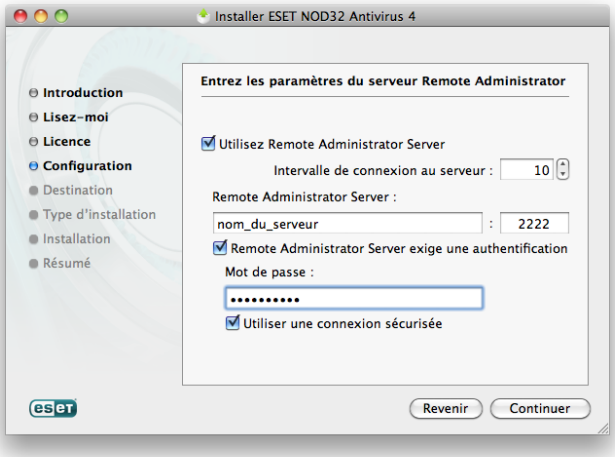
2.3.1 Création d'un ensemble d'installation à distance

Après avoir sélectionné le mode d'installation **A distance**, vous serez invité à entrer votre nom d'utilisateur et votre mot de passe pour activer les mises à jour automatiques de ESET NOD32 Antivirus. Entrez votre **nom d'utilisateur** et votre **mot de passe** (les données d'authentification reçues après l'achat ou l'enregistrement de votre produit) dans les champs correspondants. Si vous n'avez pas votre nom d'utilisateur et votre mot de passe à portée de main, vous pouvez sélectionner l'option **Définir les paramètres de mise à jour ultérieurement** pour poursuivre l'installation. Vous pourrez entrer votre nom d'utilisateur et votre mot de passe directement dans le programme,plus tard.

La prochaine étape consiste à configurer votre connexion Internet. Si vous utilisez un serveur mandataire, vous pouvez maintenant en définir les paramètres en sélectionnant l'option **J'utilise un**

serveur mandataire. Si vous êtes certain qu'aucun serveur mandataire ne sera utilisé, vous pouvez choisir l'option **Je n'utilise pas de serveur mandataire**. Si vous n'en êtes pas certain, vous pouvez utiliser les paramètres actuels de votre système en sélectionnant **Utiliser la configuration système**.

Configurez les paramètres de ERA Server (nom du serveur, port et mot de passe) pour qu'il connecte automatiquement ESET NOD32 Antivirus au serveur ERA Server après l'installation.



Dans la prochaine étape, vous pourrez **définir les utilisateurs privilégiés** qui pourront modifier la configuration du programme. De la liste des utilisateurs affichée à gauche, sélectionnez les utilisateurs et **ajoutez**-les à la liste des **utilisateurs privilégiés**. Pour afficher tous les utilisateurs du système, sélectionnez l'option **Afficher tous les utilisateurs**.

ThreatSense.Net Early Warning System contribue à garantir qu'ESET est immédiatement et continuellement informé des nouvelles infiltrations dans le but de protéger rapidement ses clients. Le système permet de soumettre de nouvelles menaces au laboratoire d'ESET où elles seront alors analysées, traitées puis ajoutées à la base de signatures de virus. Par défaut, la case **Activer le système d'avertissement anticipé ThreatSense.Net** est cochée. Cliquez sur **Configuration...** pour modifier les paramètres détaillés de soumission de fichiers suspects. Pour plus de détails, consultez la rubrique ThreatSense.Net 22.

L'étape suivante de l'installation est la configuration de la détection des applications potentiellement indésirables. Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais peuvent souvent affecter 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. Bien que ces applications affichent habituellement une notification pendant l'installation, elles peuvent facilement s'installer sans votre consentement. Activez l'option **Activer la détection d'applications potentiellement indésirables** pour permettre à ESET NOD32 Antivirus de détecter ce type de menace (recommandé).

La dernière étape de l'assistant d'installation permet de choisir un dossier de destination et de cliquer sur **Enregistrer**. L'installateur d'ESET créera l'ensemble d'installation *(EAV4_Remote_Install.pkg)* et le script d'environnement d'exécution de la désinstallation *(EAV4_Remote_UnInstall.sh)*.

2.3.2 Installation à distance sur les ordinateurs cibles

ESET NOD32 Antivirus peut être installé sur les ordinateurs cibles à l'aide de Apple Remote Desktop ou de tout autre outil qui prend en charge l'installation des packages Mac standard (*.pkg*), en copiant les fichiers et en exécutant le script d'environnement d'exécution sur les ordinateurs cibles.

Pour installer ESET NOD32 Antivirus à l'aide de Apple Remote Desktop, il vous suffit d'exécuter la commande **Install packages...**, de trouver le fichier *EAV4_Remote_Install.pkg* et de cliquer sur **Install**.

Pour des instructions détaillées sur la façon d'administrer les ordinateurs clients avec ESET Remote Administrator, veuillez consulter le guide d'utilisateur de ESET Remote Administrator.

2.3.3 Désinstallation à distance

Pour désinstaller ESET NOD32 Antivirus des ordinateurs clients :

1. utilisez la commande **Copy Items...** dans Apple Remote Desktop pour trouver le script d'environnement d'exécution de la désinstallation *(EAV4_Remote_UnInstall.sh* - créé avec l'ensemble d'installation) et le copier sur les ordinateurs cibles.
2. exécutez la commande **Send Unix Command...** dans Apple Remote Desktop. Si la désinstallation réussit, vous verrez un journal de console s'afficher.

2.3.4 Mise à niveau à distance

La mise à niveau à distance de ESET NOD32 Antivirus est effectuée par la commande **Install packages...** dans Apple Remote Desktop.

REMARQUE : les paramètres enregistrés dans l'ensemble d'installation à distance d'ESET ne sont pas appliqués aux ordinateurs cibles lors de la mise à niveau. ESET Remote Administrator devrait être utilisé pour effectuer la configuration à distance de ESET NOD32 Antivirus après la mise à niveau.

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

Pour assurer un fonctionnement optimal, il important de régler le programme pour qu'il télécharge automatiquement les mises à jour de la base des signatures de virus. Ce n'est possible que si le **nom d'utilisateur** et le **mot de passe** corrects sont entrés lors de la configuration des mises à jour 18.

2.5 Analyse de l'ordinateur à la demande

Après l'installation de ESET NOD32 Antivirus, une analyse de l'ordinateur visant à détecter tout code malveillant devrait être effectuée. De la fenêtre principale du programme, cliquez sur **Analyse de l'ordinateur** puis sur **Analyse intelligente**. Pour plus de détails sur les analyses à la demande, consultez la rubrique Analyse de l'ordinateur à la demande 13.

3. Guide pour les débutants

Cette rubrique présente un aperçu initial de ESET NOD32 Antivirus et de ses paramètres de base.

3.1 Présentation de l'interface utilisateur : les modes

La fenêtre principale de ESET NOD32 Antivirus est divisée en deux sections principales. La fenêtre principale, du côté droit, affiche l'information qui correspond à l'option sélectionnée à partir du menu principal de gauche.

Voici une description des options disponibles dans le menu principal :

- **État de la protection** - Fournit de l'information sur l'état de la protection de ESET NOD32 Antivirus. Si le **mode avancé** est activé, le sous-menu **Statistiques** sera affiché.
- **Analyse de l'ordinateur** - Permet de configurer et de démarrer l'**analyse de l'ordinateur à la demande**.
- **Mettre à jour** - Affiche l'information sur les mises à jour à la base des signatures de virus.
- **Configuration** - Permet de régler le niveau de sécurité de votre ordinateur. Si le **mode avancé** est activé, le sous-menu **Antivirus et antispyware** s'affichera.
- **Outils** - Permet d'accéder aux fonctions **Fichiers journaux**, **Quarantaine** et **Planificateur**. Cette option ne s'affiche que dans le **mode Avancé**.
- **Aide** - Fournit de l'information sur le programme, l'accès aux fichiers d'aide, la base de connaissances sur Internet et le site Web d'ESET.

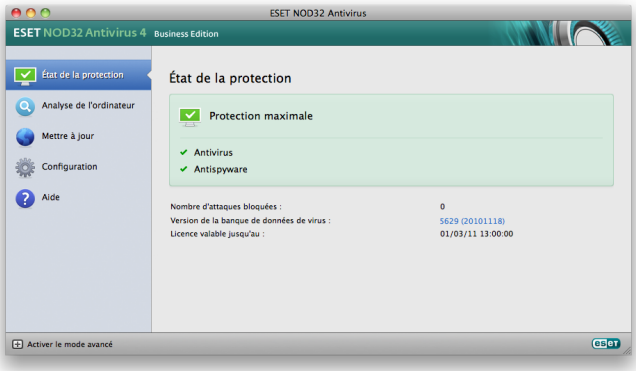
L'interface utilisateur de ESET NOD32 Antivirus permet aux utilisateurs de basculer entre les modes Standard et Avancé. Le mode standard donne accès aux fonctionnalités nécessaires aux opérations ordinaires. Il n'affiche aucune option avancée. Pour basculer entre les modes, cliquez sur l'icône plus à côté d'**Activer le mode avancé**/**Activer le mode standard** dans le coin inférieur droit de la fenêtre principale du programme.

Le mode Standard donne accès aux fonctionnalités nécessaires aux opérations ordinaires. Il n'affiche aucune option avancée.

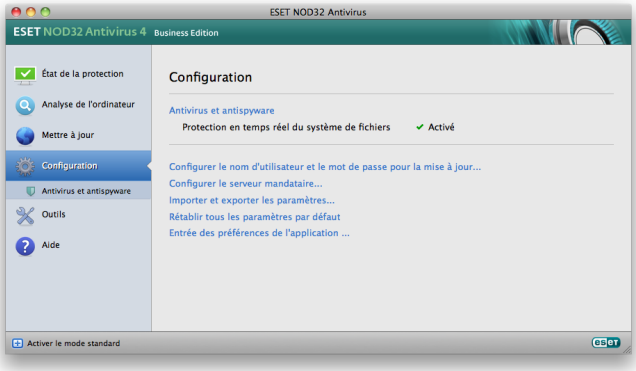
Le passage au mode avancé ajoute l'option **Outils** dans le menu principal. L'option **Outils** permet d'accéder aux sous-menus **Fichiers journaux**, **Quarantaine** et **Planificateur**.

REMARQUE : Toutes les instructions qui suivent dans ce guide seront effectuées en **mode avancé**.

Mode standard :

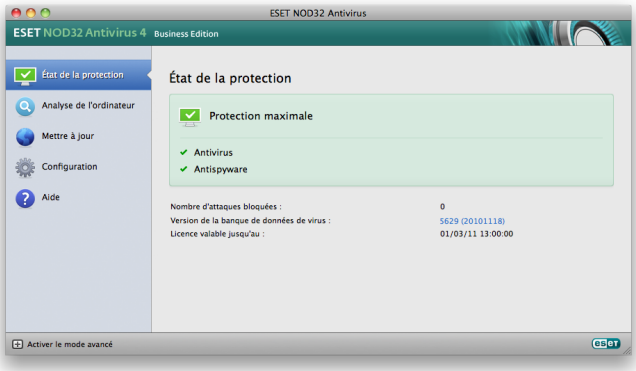


Mode avancé :



3.1.1 Contrôle du fonctionnement du système

Pour afficher l'**État de la protection**, cliquez sur l'option du haut, dans le menu principal. Un résumé de l'état de fonctionnement de ESET NOD32 Antivirus s'affiche dans la fenêtre principale, avec un sous-menu comprenant l'option **Statistiques**. Sélectionnez-la pour obtenir des renseignements et statistiques détaillés sur les analyses ayant été effectuées sur votre système. La fenêtre Statistiques n'est disponible qu'en mode avancé.



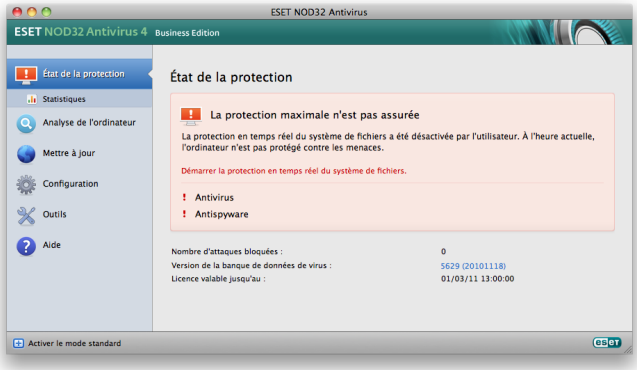
3.1.2 Que faire lorsque le programme ne fonctionne pas correctement

Une marque verte s'affiche à côté de chaque module activé et fonctionnant correctement. Dans le cas contraire, un point d'exclamation rouge ou orange et des données 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.

Si vous ne pouvez régler un problème à l'aide des solutions suggérées, cliquez sur **Aide** pour accéder aux fichiers d'aide ou effectuer une recherche dans la base de connaissances.

Si vous avez besoin d'aide, vous pouvez également communiquer avec l'assistance à la clientèle d'ESET sur le site Web d'ESET. Les spécialistes d'ESET répondront rapidement à vos questions et essaieront de trouver une solution à votre problème.



4. Fonctionne avec ESET NOD32 Antivirus

4.1 Protection antivirus et antispyware

La protection antivirus vous protège des attaques contre le système en modifiant les fichiers qui représentent des menaces potentielles. Si une menace comportant du code malveillant est détectée, le module Antivirus peut alors l'éliminer en la bloquant, puis en nettoyant, en supprimant ou en mettant en quarantaine l'objet infecté.

4.1.1 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 au moment 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.

4.1.1.1 Configuration de la protection en temps réel

La protection en temps réel du système de fichiers vérifie tous les types de supports et l'analyse peut être déclenchée par différents événements. À l'aide des méthodes de détection de la technologie ThreatSense (décrites dans la rubrique Configuration du moteur ThreatSense 14), la protection en temps réel du système de fichiers peut différer pour les fichiers nouvellement créés et les fichiers existants. Ainsi, pour les fichiers nouvellement créés, il est possible d'appliquer un niveau de contrôle plus approfondi.

Par défaut, la protection en temps réel est lancée au démarrage du système d'exploitation et assure une analyse ininterrompue. Dans des cas particuliers (en cas de conflit avec un autre analyseur en temps réel, par ex.), il est possible d'arrêter la protection en temps réel en cliquant sur l'icône ESET NOD32 Antivirus située dans votre barre de menus (haut de l'écran), puis en sélectionnant l'option **Désactiver la protection en temps réel du système de fichiers**. Il est également possible d'arrêter la protection en temps réel à partir de la fenêtre principale du programme (**Configuration** > **Antivirus et anti-logiciel espion** > **Désactiver**).

Pour modifier les paramètres avancés de la protection en temps réel, allez à **Configuration** > **Entrée des préférences de l'application...** > **Protection** > **Protection en temps réel** et cliquez sur le bouton **Configurer...** adjacent à **Options avancées** (décrites dans la rubrique Options d'analyse avancée 11).

4.1.1.1.1 Date de l'analyse (analyse déclenchée par un événement)

Par défaut, tous les fichiers sont analysés lorsqu'ils sont **ouverts**, **créés** ou **exécutés**. Nous recommandons de conserver les paramètres par défaut, car ils offrent le niveau maximum de protection en temps réel pour votre ordinateur.

4.1.1.1.2 Options d'analyse avancée

Dans cette fenêtre, vous pouvez définir les types d'objets qui seront analysés par le moteur ThreatSense , activer et désactiver l'**heuristique avancée** et modifier les paramètres des archives et du cache de fichiers.

Nous ne recommandons pas de modifier les valeurs par défaut dans la rubrique **Paramètres par défaut des archives** à moins que cela ne soit requis pour résoudre un problème particulier puisque les valeurs d'imbrication élevée des archives peuvent avoir des répercussions sur la performance du système.

Vous pouvez basculer l'heuristique avancée de ThreatSense pour les fichiers exécutés ainsi que pour les fichiers respectivement créés et modifiés, en cliquant sur la case à cocher **Heuristique avancée** dans chacune des sections portant sur les paramètres ThreatSense.

Pour éviter le plus possible les répercussions sur le système lorsque la protection en temps réel est activée, vous pouvez également définir la taille du cache d'optimisation. Ce comportement sera actif lorsque vous utiliserez l'option **Activer le nettoyage du cache de fichiers**. Si cette fonction est désactivée, tous les fichiers seront analysés chaque fois que l'ordinateur y accédera. Les fichiers ne seront pas analysés de façon répétitive après avoir été mis en cache (à moins qu'ils n'aient été modifiés), jusqu'à la taille du cache définie. Les fichiers seront cependant immédiatement réanalysés après chaque mise à jour de la base des signatures de virus.

Cliquez sur **Activer le nettoyage du cache de fichiers** pour activer ou désactiver cette fonction. Pour définir la quantité de fichiers à cacher, entrez simplement la valeur voulue dans le champ d'entrée adjacent à **Taille de la mémoire cache**.

Les paramètres d'analyse supplémentaire peuvent être définis dans la fenêtre **Configuration du moteur ThreatSense**. Vous pouvez définir quel type d'**objets** devraient être analysés, avec quelles **options** et quel niveau de **nettoyage**, ainsi que définir les **extensions** et les **limites** de taille du fichier de la protection en temps réel. Vous pouvez ouvrir la fenêtre de configuration du moteur ThreatSense en cliquant sur le bouton **Configurer...** adjacent à **Moteur ThreatSense** dans la fenêtre Configuration avancée. Pour plus de détails sur les paramètres du moteur ThreatSense, consultez la rubrique Configuration du moteur ThreatSense 14.

4.1.1.1.3 Exclusions de l'analyse

Cette rubrique permet d'exclure certains fichiers et dossiers de l'analyse.

- **Chemin** - chemin d'accès des fichiers et des dossiers exclus

- **Menace** - si un nom de menace est indiqué à côté d'un fichier exclu, cela signifie que le fichier ne peut être exclu que de l'analyse pour cette menace et non de l'analyse globale. De ce fait, si ce fichier devient ensuite infecté par d'autres logiciels malveillants, ceux-ci seront détectés par le module antivirus.

- **Ajouter...** - exclut les objets de la détection. Entrez le chemin vers un objet (vous pouvez également utiliser les caractères génériques * et ?) ou sélectionner le dossier ou le fichier à partir de la structure de l'arborescence.
- **Modifier...** - permet de modifier des entrées sélectionnées
- **Supprimer** - retire des entrées sélectionnées
- **Défaut** - annule toute exclusion.

4.1.1.2 À quel moment faut-il modifier la configuration de la protection en temps réel

La protection en temps réel est le composant le plus essentiel de la sécurisation du système. Soyez très prudent lorsque vous en modifiez les paramètres. Il est recommandé de ne changer les paramètres de ce module que dans des cas précis. Par exemple, lorsqu'il y a conflit avec une autre application ou avec l'analyseur en temps réel d'un autre logiciel antivirus.

Après l'installation de ESET NOD32 Antivirus, tous les paramètres sont optimisés pour garantir le niveau maximal de sécurité système pour les utilisateurs. Pour restaurer les paramètres par défaut, cliquez sur le bouton **Défaut** dans la partie inférieure gauche de la fenêtre **Protection en temps réel** (**Configuration** > **Entrée des préférences de l'application...** > **Protection** > **Protection en temps réel**).

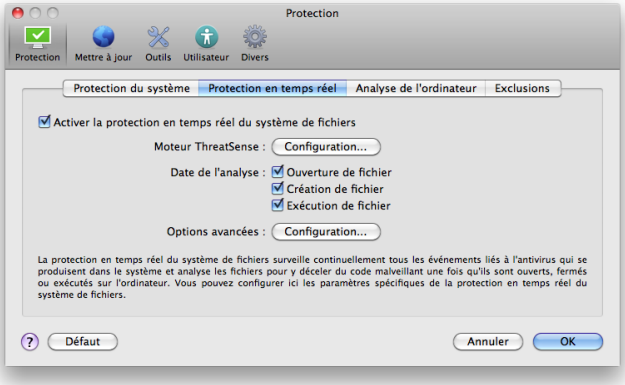
4.1.1.3 Vérification de la protection en temps réel

Pour vérifier si la protection en temps réel fonctionne et détecte les virus, utilisez le fichier de test eicar.com. Ce fichier test est un fichier inoffensif spécial pouvant être détecté par tous les programmes antivirus. Il a été créé par la société EICAR (European Institute for Computer Antivirus Research) pour tester la fonctionnalité des programmes antivirus. Le fichier *eicar.com* est téléchargeable depuis http://www.eicar.org/anti_virus_test_file.htm.

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

Dans cette rubrique, nous décrivons des problèmes qui peuvent survenir avec 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, accédez à **Configuration** > **Antivirus et antispyware**, puis cliquez sur le lien **Activer la protection en temps réel du système de fichiers** (à droite) dans la fenêtre principale du programme. Vous pouvez également activer la protection en temps réel du système de fichiers dans la fenêtre de Configuration avancée, sous **Protection** > **Protection en temps réel** en sélectionnant l'option **Activer la protection en temps réel du système de fichiers**.



La protection en temps réel ne détecte ni ne nettoie 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 conflit entre les deux. Nous recommandons de désinstaller tout autre antivirus pouvant se trouver sur votre système.

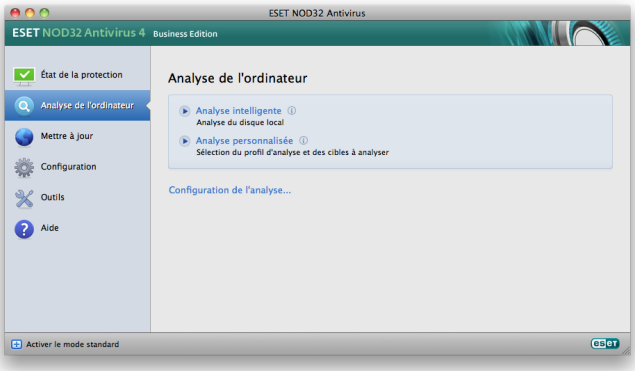
La protection en temps réel ne démarre pas
Si la protection en temps réel ne démarre pas au moment du démarrage du système, cela peut être dû à des conflits avec d'autres programmes. Dans ce cas, consultez les spécialistes de l'assistance à la clientèle

d'ESET.

4.1.2 Analyse de l'ordinateur à la demande

Si vous pensez que votre ordinateur peut être infecté (en raison d'un comportement anormal), exécutez **Analyse de l'ordinateur** > **Analyse intelligente** pour rechercher d'éventuelles infiltrations. Pour assurer une protection maximale, les analyses de l'ordinateur devraient être effectuées régulièrement, dans le cadre des mesures de sécurité de routine et non seulement lorsqu'une infection est soupçonnée. Une analyse régulière pourra détecter des infiltrations n'ayant pas été détectées par l'analyseur en temps réel lors de leur enregistrement sur le disque. Cela peut se produire si l'analyseur en temps réel est désactivé au moment de l'infection ou si la base de signatures de virus est obsolète.

Nous recommandons d'exécuter une analyse à la demande au moins une fois par mois. Cette analyse peut être configurée comme tâche planifiée dans **Outils** > **Planificateur**.



4.1.2.1 Type d'analyse

Deux types d'analyse de l'ordinateur à la demande sont disponibles. L'**analyse intelligente** analyse rapidement le système sans exiger de reconfiguration des paramètres d'analyse. L'**analyse personnalisée** permet, quant à elle, de sélectionner l'un des profils d'analyse prédéfinis ainsi que de choisir les cibles particulières de l'analyse.

4.1.2.1.1 Analyse intelligente

L'analyse intelligente vous permet de lancer rapidement une analyse de l'ordinateur et de nettoyer les fichiers infectés sans intervention de l'utilisateur. Ses principaux avantages incluent sa facilité d'utilisation et l'absence d'une configuration détaillée de l'analyse. L'analyse intelligente vérifie tous les fichiers dans tous les dossiers et nettoie ou supprime automatiquement les infiltrations détectées. Le niveau de nettoyage est automatiquement réglé à sa valeur par défaut. Pour plus de détails sur les types de nettoyage, consultez la rubrique Nettoyage 15.

4.1.2.1.2 Analyse personnalisée

L'**analyse personnalisée** est la solution optimale si vous voulez préciser des paramètres d'analyse tels que les cibles et les méthodes d'analyse. L'avantage d'utiliser l'analyse personnalisée est la possibilité de configurer les paramètres de manière détaillée. Différentes configurations peuvent ainsi être enregistrées comme profils d'analyse définis par l'utilisateur, ce qui peut être utile pour effectuer régulièrement une analyse avec les mêmes paramètres.

Pour sélectionner les cibles à analyser, sélectionnez **Analyse de l'ordinateur** > **Analyse personnalisée**, ainsi que les **Cibles à analyser** à partir de la structure de l'arborescence. Une cible d'analyse peut aussi être indiquée plus précisément en entrant le chemin du dossier ou des fichiers à inclure. Si vous ne voulez qu'analyser le système sans effectuer de nettoyage supplémentaire, sélectionnez l'option **Analyser sans nettoyer**. Vous pouvez aussi choisir parmi trois niveaux de nettoyage en cliquant sur **Configuration...** > **Nettoyage**.

L'exécution des analyses personnalisées est recommandée pour les utilisateurs avancés ayant une expérience antérieure avec l'utilisation de programmes antivirus.

4.1.2.2 Cibles à analyser

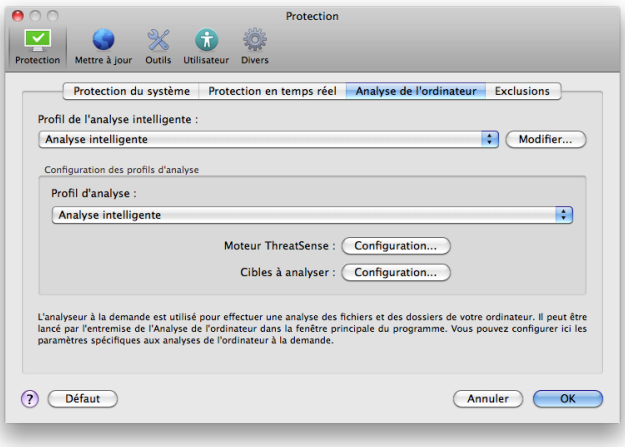
La structure en arborescence des cibles à analyser vous permet de sélectionner les fichiers et dossiers à analyser pour y détecter la présence de virus. Les dossiers peuvent être sélectionnés conformément aux paramètres d'un profil.

Une cible d'analyse peut aussi être précisée de façon spécifique en entrant le chemin du dossier ou des fichiers à inclure dans l'analyse. Sélectionnez les cibles dans l'arborescence qui dresse la liste de tous les dossiers disponibles sur l'ordinateur.

4.1.2.3 Profils d'analyse

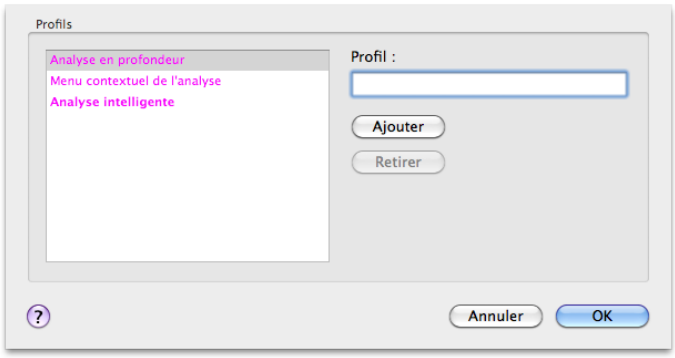
Vos paramètres d'analyse préférés peuvent être enregistrés pour analyse future. Nous vous recommandons de créer un profil différent (avec différentes cibles et méthodes ainsi que d'autres paramètres d'analyse) pour chacune des analyses utilisées régulièrement.

Pour créer un nouveau profil, allez à **Configuration** > **Accéder à l'arborescence de la configuration avancée complète...** > **Protection** > **Analyse de l'ordinateur** et cliquez sur **Modifier...** adjacent à la liste des profils actuels.



Pour vous aider à créer un profil d'analyse répondant à vos besoins, consultez la rubrique Configuration du moteur ThreatSense 14 pour obtenir une description de chacun des paramètres de configuration de l'analyse.

Exemple : Imaginez que vous vouliez créer votre propre profil d'analyse et que la configuration associée au profil Analyse intelligente vous convienne en partie, mais que vous ne voulez ni analyser les fichiers exécutables compressés par un compresseur d'exécutables ni les applications potentiellement dangereuses et que vous voulez également utiliser un nettoyage strict. Dans la fenêtre **Liste des profils de l'analyseur à la demande**, inscrivez le nom du profil, cliquez sur le bouton **Ajouter** et confirmez le tout en appuyant sur **OK**. Réglez ensuite les paramètres selon vos exigences en configurant le **moteur ThreatSense** et les **cibles à analyser**.



4.1.3 Configuration du moteur ThreatSense

La technologie ThreatSense combine des méthodes de détection de menaces complexes. Cette technologie proactive fournit également une protection durant 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 simultanément plusieurs flux de données, maximisant ainsi l'efficacité et le taux de détection. La technologie ThreatSense élimine également les rootkits.

Les options de configuration de la technologie ThreatSense vous permettent également de préciser plusieurs paramètres d'analyse :

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

Pour ouvrir la fenêtre de configuration, cliquez sur **Configuration** > **Antivirus et antispyware** > **Configuration avancée de la protection antivirus et antispyware**, puis cliquez sur le bouton **Configuré...** situé dans les onglets **Protection système**, **Protection en temps réel** et **Analyse de l'ordinateur** qui utilisent tous la technologie ThreatSense (voir ci-dessous). Chaque scénario de sécurité peut exiger une configuration différente. Sachant cela, ThreatSense peut être configuré individuellement pour les modules de protection suivants :

- **Protection système** > Vérification automatique des fichiers de démarrage
- **Protection en temps réel** > Protection en temps réel du système de fichiers
- **Analyse de l'ordinateur** > Analyse de l'ordinateur à la demande

Les paramètres ThreatSense sont spécifiquement optimisés pour chaque module et leur modification peut grandement affecter le fonctionnement du système. Ainsi, changer les paramètres pour toujours analyser les fichiers exécutables compressés par un compresseur d'exécutables ou activer l'heuristique avancée dans le module de protection en temps réel du système de fichiers pourrait entraîner un ralentissement du système. Il est donc recommandé de laisser inchangés les paramètres par défaut de ThreatSense pour tous les modules, à l'exception du module Analyse de l'ordinateur.

4.1.3.1 Objets

La section **Objets** vous permet de définir les fichiers de l'ordinateur qui seront analysés pour y détecter les infiltrations.

- **Fichiers** - analyse tous les types de fichiers courants (programmes, images, musiques, vidéos, bases de données, etc.).
- **Liens symbolique** - (analyse à la demande seulement) analyse des types spéciaux de fichiers contenant une chaîne de caractères qui est interprétée et suivie par le système d'exploitation comme chemin vers un autre fichier ou dossier.
- **Fichiers courriel** - (non offert dans la protection en temps réel) analyse les fichiers spéciaux contenant le courriel.

- **Boîtes aux lettres** - (non offert dans la protection en temps réel) analyse les boîtes aux lettres de l'utilisateur dans le système. Une utilisation inappropriée de cette option pourrait entraîner un conflit avec votre client de messagerie. Pour plus de détails sur les avantages et désavantages de cette option, consultez cet article de la base de connaissances.
- **Archives** - (non offert dans la protection en temps réel) analyse les fichiers compressés dans des archives (.rar, .zip, .arj, .tar, etc.).
- **Archives à extraction automatique** - (non offert dans la protection en temps réel) analyse les fichiers contenus dans des fichiers d'archive à extraction automatique.
- **Fichiers exécutables compressés par un compresseur d'exécutables** – à la différence des types d'archives standard, ces fichiers se décompriment en mémoire, comme les compacteurs statiques standard (UPX, yoda, ASPack, FGS, etc.).

4.1.3.2 Options

Dans la section **Options**, vous pouvez choisir les méthodes utilisées lors de l'analyse du système pour y déceler des infiltrations. Les options suivantes sont disponibles :

- **Base de signature de virus** - les signatures de virus permettent de détecter et d'identifier de manière précise et fiable toute infiltration par son nom.
- **Heuristique** - l'heuristique utilise un algorithme qui analyse l'activité (malveillante) des programmes. Le principal avantage de la détection heuristique est la possibilité de détecter de nouveaux logiciels malveillants qui n'existaient pas précédemment ou ne figuraient pas sur la liste des virus connus (base des signatures de virus).
- **Heuristique avancée** - l'heuristique avancée désigne un algorithme heuristique unique développé par ESET et optimisé pour la détection de vers informatiques et de chevaux de Troie écrits dans des langages de programmation de haut niveau. La capacité de détection du programme augmente sensiblement grâce à l'heuristique avancée.
- **Spyware/logiciels publicitaires/à risque** - cette catégorie comprend les logiciels qui recueillent diverses données confidentielles sur les utilisateurs sans leur consentement, ainsi que les logiciels qui affichent des publicités.
- **Applications potentiellement indésirables** - ces applications ne sont pas conçues pour être malveillantes, mais peuvent avoir des répercussions négatives sur la performance de l'ordinateur. Ces applications exigent généralement le consentement de l'utilisateur avant leur installation. Si elles sont présentes sur votre ordinateur, votre système aura cependant un comportement différent (par rapport à son état avant l'installation). Les changements les plus significatifs concernent les fenêtres contextuelles, l'activation et l'exécution de processus cachés, l'utilisation accrue des ressources système, des changements dans les résultats de recherche et des applications communiquant avec des serveurs distants.
- **Applications potentiellement dangereuses** - cette catégorie inclut les logiciels commerciaux légitimes qui peuvent être exploités par des pirates, s'ils ont été installés à l'insu de l'utilisateur. Elle inclut des programmes tels que des outils d'accès à distance, raison pour laquelle cette option est désactivée par défaut.

4.1.3.3 Nettoyage

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

- **Ne pas nettoyer** - Les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche alors une fenêtre d'avertissement et vous laisse choisir une action.
- **Nettoyage standard** - Le programme tente de nettoyer ou de supprimer automatiquement tout fichier infecté. S'il n'est pas possible de sélectionner automatiquement l'action correcte, le programme propose différentes actions de suivi. Cette sélection s'affiche également si une action prédéfinie ne peut être menée à bien.
- **Nettoyage strict** - Le programme nettoie ou supprime tous les fichiers infectés (y compris les archives). Les seules exceptions sont les fichiers système. S'il n'est pas possible de les nettoyer, une fenêtre d'avertissement s'affiche avec une proposition d'action.

Avertissement : en mode de nettoyage Standard par défaut, le fichier d'archive n'est entièrement supprimé que si tous les fichiers qu'il contient sont infectés. Si l'archive contient aussi des fichiers légitimes, elle n'est pas supprimée. Si un fichier d'archive infecté est détecté en mode Nettoyage strict, le fichier entier est supprimé, même s'il contient également des fichiers intacts.

4.1.3.4 Extensions

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 de ThreatSense vous permet de définir les types de fichiers qui seront exclus de l'analyse.

Par défaut, tous les fichiers sont analysés, quelle que soit leur extension. N'importe quelle extension peut être ajoutée à la liste des fichiers exclus de l'analyse. Les boutons **Ajouter** et **Supprimer** permettent d'activer ou d'empêcher l'analyse des fichiers portant certaines extensions.

L'exclusion de fichiers de l'analyse peut parfois être utile lorsque l'analyse de certains types de fichiers empêche le fonctionnement approprié du programme utilisant ces extensions. Par exemple, il peut être judicieux d'exclure les extensions *.log*, *.cfg* et *.tmp*.

4.1.3.5 Limites

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

- **Taille maximale :** Définit la taille maximale des objets à analyser. Le module antivirus n'analysera que les objets d'une taille inférieure à celle indiquée. Il n'est pas recommandé de modifier la valeur par défaut et il n'y a généralement aucune raison de le faire. Cette option ne devrait être modifiée que par des utilisateurs expérimentés ayant des raisons précises d'exclure de l'analyse des objets de plus grande taille.
- **Durée maximale de l'analyse :** Précise la durée maximale pour l'analyse d'un objet. Si la valeur de ce champ a été définie par l'utilisateur, le module antivirus cessera d'analyser un objet une fois ce temps écoulé, que l'analyse soit finie ou non.
- **Niveau d'imbrication maximum :** Précise la profondeur maximale de l'analyse des archives. Il n'est pas recommandé de modifier la valeur par défaut (10). Dans des circonstances normales, il n'y a aucune raison de le faire. Si l'analyse prend fin prématurément en raison du nombre d'archives imbriquées, l'archive restera non vérifiée.
- **Taille maximale du fichier :** Cette option permet de préciser la taille maximale des fichiers contenus dans les archives qui doivent être analysés (après extraction). Si l'analyse d'une archive prend fin prématurément en raison de cette limite, cette dernière restera non vérifiée.

4.1.3.6 Autres

Lorsque l'optimisation Smart est activée, les paramètres optimaux sont utilisés pour assurer le niveau d'analyse le plus efficient tout en conservant la vitesse d'analyse la plus élevée. Les différents modules de protection effectuent une analyse intelligente, utilisant pour ce faire différentes méthodes d'analyse qui seront appliquées à différents types de fichiers. L'optimisation Smart n'est pas définie de façon rigide dans le produit. L'équipe de développement d'ESET y apporte continuellement des modifications qui seront ensuite intégrées dans votre ESET NOD32 Antivirus par l'entremise des mises à jour régulières. Si l'optimisation Smart est activée, seuls les paramètres définis par l'utilisateur dans le moteur ThreatSense utilisé pour ce module particulier seront appliqués au moment d'effectuer une analyse.

Analyser le flux alternatif de données (analyse à la demande seulement)
Les flux de données alternatifs (fourchettes de ressource/données) utilisés par le système de fichier sont des associations de fichiers et de dossiers qui sont invisibles pour les techniques ordinaires de détection de virus. De nombreuses infiltrations tentent d'éviter la détection en se faisant passer pour des flux de données alternatifs.

4.1.4 Une infiltration est détectée

Les infiltrations peuvent utiliser différents points d'entrée pour attaquer votre système, y compris les pages Web, les dossiers partagés, le courriel ou les supports amovibles (USB, disques externes, CD, DVD, disquettes, etc.).

Si votre ordinateur montre des signes d'une infection par logiciel malveillant, si, par exemple, vous remarquez un ralentissement, des blocages fréquents, etc., nous vous recommandons d'effectuer les opérations suivantes :

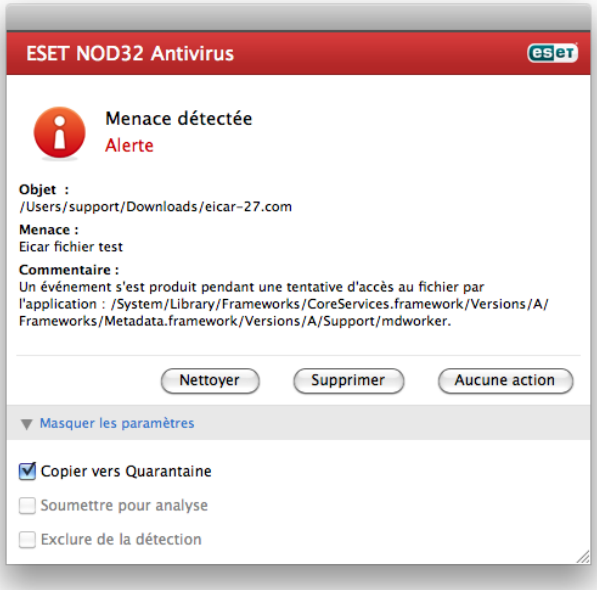
1. Ouvrez ESET NOD32 Antivirus et cliquez sur **Analyse de l'ordinateur**.
2. Cliquez sur **Analyse intelligente** (pour plus de détails, consultez la rubrique Analyse intelligente 13).
3. Lorsque l'analyse est terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés.

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

À titre d'exemple général de la façon dont les infiltrations sont traitées dans ESET NOD32 Antivirus, supposons qu'une infiltration est détectée par la protection en temps réel du système de fichiers qui utilise le niveau de nettoyage par défaut. Le

programme tentera alors de nettoyer ou de supprimer le fichier. Si aucune action n'est prédéfinie pour le module de protection en temps réel, vous serez invité à sélectionner une option dans une fenêtre d'avertissement. Les options **Nettoyer**, **Supprimer** et **Aucune action** sont généralement disponibles. Il n'est pas recommandé de sélectionner **Aucune action** car les fichiers infectés seraient alors conservés tels quels. La seule exception concerne les situations où vous êtes sûr que le fichier est inoffensif et a été détecté par erreur.

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



Suppression de fichiers dans des archives En mode de nettoyage par défaut, l'archive entière 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 aussi des fichiers sains. Cependant, soyez prudent si vous choisissez **Nettoyage strict** car dans ce mode, l'archive sera supprimée si elle comprend au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

4.2 Mise à jour du programme

Des mises à jour régulières de ESET NOD32 Antivirus sont nécessaires pour conserver le niveau maximal de sécurité. Le module de mise à jour veille à ce que le programme soit toujours actualisé en effectuant la mise à jour la base des signatures de virus.

En cliquant sur **Mettre à jour** à partir du menu principal, vous pourrez obtenir l'état actuel des mises à jour, y compris la date et l'heure de la dernière mise à jour réussie et si une nouvelle mise à jour est requise. Pour lancer manuellement le processus de mise à jour, cliquez sur **Mettre à jour la base des signatures de virus**.

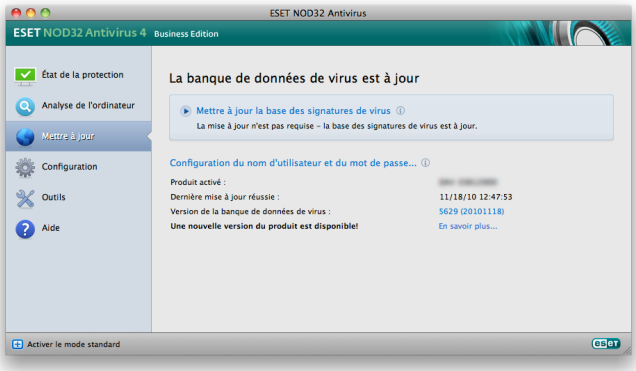
Dans des circonstances normales, lorsque les mises à jour sont téléchargées correctement, le message **La base des signatures de virus est à jour** s'affiche dans la fenêtre Mettre à jour. Si la base des signatures de virus ne peut pas être mise à jour, il est recommandé de vérifier les paramètres de mise à jour 18 - la cause la plus courante de cette erreur est une entrée incorrecte de données d'authentification (nom d'utilisateur et mot de passe) ou une configuration incorrecte des paramètres de connexion 24.

La fenêtre Mettre à jour contient également les informations sur la version de la base des signatures de virus. Cet indicateur numérique est un lien actif vers le site Web d'ESET qui permet de voir toutes les signatures ajoutées pendant cette mise à jour.

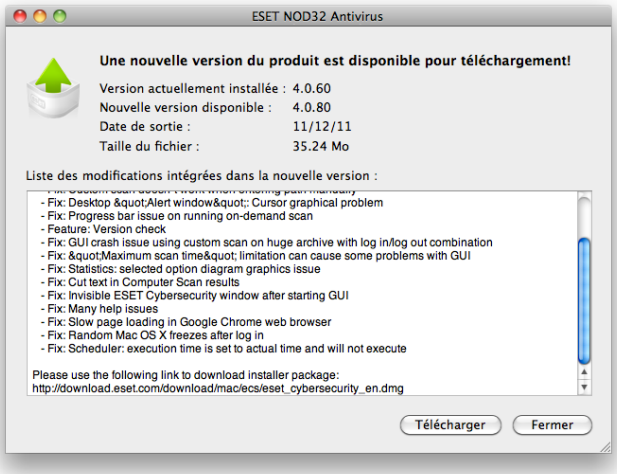
REMARQUE : Votre nom d'utilisateur et votre mot de passe vous seront fournis par ESET après l'achat de ESET NOD32 Antivirus.

4.2.1 Mise à niveau vers une nouvelle version

Pour profiter de la protection maximale, il est important d'utiliser la version la plus récente de ESET NOD32 Antivirus. Pour rechercher une nouvelle version, cliquez sur **Mettre à jour** dans le menu principal sur la gauche. Si une nouvelle version est disponible, un message *Une nouvelle version de ESET NOD32 Antivirus est disponible* s'affiche dans la partie inférieure de la fenêtre. Cliquez sur **En savoir plus...** pour afficher une nouvelle fenêtre contenant le numéro de la nouvelle version et la liste des changements.



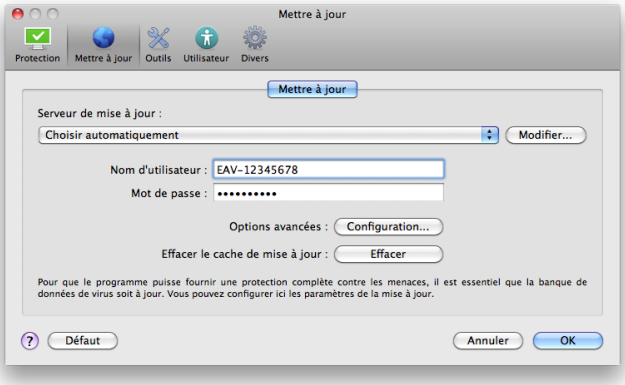
Cliquez sur **Télécharger** pour télécharger la version la plus récente. Cliquez sur **Ok** pour fermer la fenêtre et télécharger la mise à niveau plus tard.



Si vous avez cliqué sur **Télécharger**, le fichier sera téléchargé dans le dossier de téléchargement (ou dans le dossier par défaut défini par votre navigateur). Lorsque le téléchargement du fichier est terminé, lancez le fichier et suivez les instructions d'installation. Votre nom d'utilisateur et votre mot de passe seront automatiquement transférés dans la nouvelle version. Il est recommandé de rechercher des mises à niveau régulièrement, particulièrement en cas d'installation de ESET NOD32 Antivirus à partir d'un CD/DVD.

4.2.2 Configuration des mises à jour

La section de la configuration des mises à jour permet de préciser l'information sur 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 à **Choisir automatiquement** pour s'assurer que tous les fichiers de mise à jour sont automatiquement téléchargés du serveur ESET ayant le plus faible trafic réseau.



La liste des serveurs de mise à jour disponibles est accessible par le menu déroulant **Serveur de mise à jour**. Pour ajouter un nouveau serveur de mise à jour, cliquez sur **Modifier...** Entrez ensuite l'adresse du nouveau serveur dans le champ **Serveurs de mise à jour** puis cliquez sur le bouton **Ajouter**. L'authentification d'accès aux serveurs de mise à jour est fondée sur le **nom d'utilisateur** et le **mot de passe** qui ont été générés et envoyés à l'utilisateur après l'achat.

Pour activer l'utilisation du mode de test (téléchargement des mises à jour avant diffusion), cliquez sur le bouton **Configuration...** adjacent à **Options avancées**, puis activez la case à cocher **Activer les mises à jour avant diffusion**. Pour désactiver l'affichage de notifications dans la barre d'état système après la réussite de chacune des mises à jour, activez la case à cocher **Ne pas afficher de notification de réussite de la mise à jour**.

Pour supprimer toutes les données de mises à jour stockées de façon temporaire, cliquez sur le bouton **Effacer** adjacent à **Effacer le cache de mise à jour**. Utilisez cette option si vous éprouvez des problèmes au moment de la mise à jour.

4.2.3 Comment créer des tâches de mise à jour

Les mises à jour peuvent être déclenchées manuellement en cliquant sur **Mettre à jour la base des signatures de virus** dans la principale fenêtre d'information qui s'affiche après avoir cliqué sur **Mettre à jour** dans le menu principal.

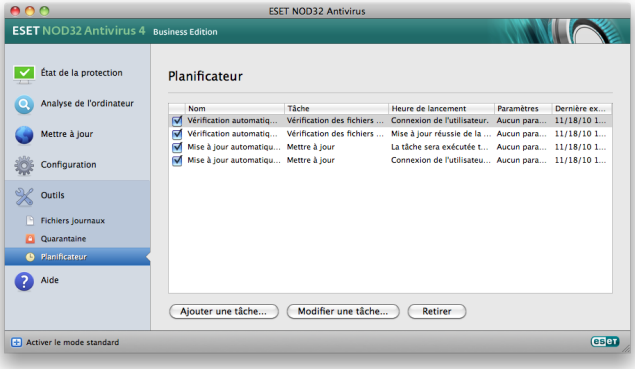
Les mises à jour peuvent également être exécutées comme tâches planifiées. Pour configurer une tâche planifiée, cliquez sur **Outils** > **Planificateur**. Par défaut, les tâches suivantes sont activées dans ESET NOD32 Antivirus :

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

Chacune des tâches de mise à jour susmentionnées 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 de détails sur la création et la configuration des tâches de mise à jour, consultez la rubrique Planificateur 18

4.3 Planificateur

Le **Planificateur** est disponible si le mode Avancé est activé dans ESET NOD32 Antivirus. Le Planificateur se trouve dans le menu principal de ESET NOD32 Antivirus, sous **Outils**. Le **Planificateur** contient une liste de toutes les tâches planifiées avec leurs propriétés de configuration telles que la date prédéfinie, l'heure et le profil d'analyse utilisé.



Par défaut, les tâches planifiées suivantes s'affichent dans le Planificateur :

- Mise à jour automatique régulière
- Mise à jour automatique après ouverture de session utilisateur
- Vérification automatique des fichiers de démarrage
- Vérification automatique des fichiers de démarrage après la mise à jour réussie de la base des signatures de virus
- Maintenance des journaux (après avoir activé l'option **Afficher les tâches système** dans la configuration du planificateur)

Pour modifier la configuration d'une tâche planifiée existante (tant par défaut que définie par l'utilisateur), cliquez avec le bouton droit sur la tâche, puis sur **Modifier...** ou sélectionnez la tâche à modifier, puis cliquez sur le bouton **Modifier...**.

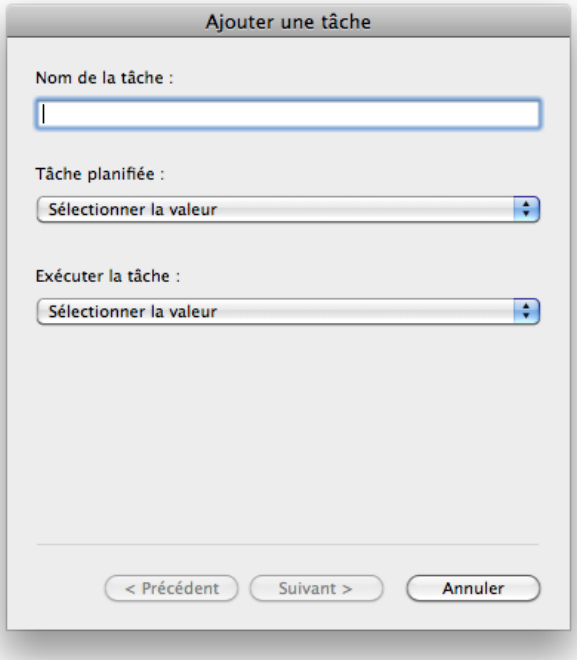
4.3.1 Pourquoi planifier des tâches

Le planificateur gère et lance les tâches planifiées qui ont été préalablement définies et configurées. La configuration et les propriétés de ces tâches comprennent des informations telles que la date et l'heure ainsi que des profils particuliers à utiliser pendant l'exécution de ces tâches.

4.3.2 Création de nouvelles tâches

Pour créer une nouvelle tâche dans le Planificateur, cliquez sur le bouton **Ajouter une tâche...** ou cliquez avec le bouton droit et sélectionnez **Ajouter...** dans le menu contextuel. Cinq types de tâches planifiées sont disponibles :

- **Exécuter l'application**
- **Mettre à jour**
- **Maintenance des journaux**
- **Analyse de l'ordinateur à la demande**
- **Contrôle des fichiers de démarrage du système**



Puisque la mise à jour est l'une des tâches planifiées les plus souvent utilisées, nous expliquerons comment ajouter une nouvelle tâche de mise à jour.

Dans le menu déroulant **Tâche planifiée**, sélectionnez **Mettre à jour**. Entrez le nom de la tâche dans le champ **Nom de la tâche**. Sélectionnez la fréquence de la tâche à partir du menu déroulant **Exécuter la tâche**. Les options suivantes sont disponibles : **Défini par l'utilisateur**, **Une fois**, **Plusieurs fois**, **Quotidiennement**, **Chaque semaine** et **Déclenchée par un événement**. Selon la fréquence sélectionnée, vous serez invité à choisir différents paramètres de mise à jour. On peut ensuite définir l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée. Les trois options suivantes sont disponibles :

- **Attendre le prochain moment planifié**
- **Exécuter la tâche le plus rapidement possible**
- **Exécuter la tâche immédiatement si le temps écoulé depuis la dernière exécution dépasse l'intervalle spécifié** (l'intervalle peut être défini immédiatement à l'aide de la zone de liste déroulante **Intervalle minimum pour la tâche**).

Dans l'étape suivante, une fenêtre sommaire avec l'information sur la tâche planifiée actuelle est affichée. Cliquez sur le bouton **Terminer**.

La nouvelle tâche planifiée sera ajoutée à la liste des tâches planifiées.

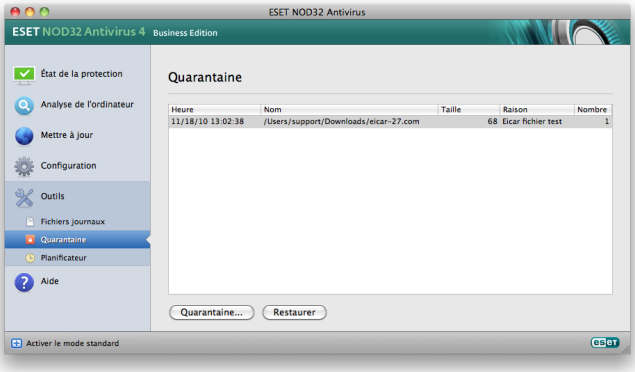
Le système contient, par défaut, les tâches planifiées essentielles pour assurer le fonctionnement approprié du produit. Ces tâches ne devraient pas être modifiées et elles sont masquées par défaut. Pour modifier cette option et pour rendre ces tâches visibles, ouvrez

Configuration > **Entrée des préférences de l'application...** > **Outils** > **Planificateur** et sélectionnez l'option **Afficher les tâches système**.

4.4 Quarantaine

La quarantaine vise principalement à stocker en toute sécurité les fichiers infectés. Ces fichiers doivent être mis en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer ou s'ils sont détectés par erreur par ESET NOD32 Antivirus.

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



Les fichiers stockés dans le dossier de quarantaine peuvent être visualisés dans un tableau indiquant la date et l'heure de mise en quarantaine, le chemin de l'emplacement d'origine du fichier infecté, sa taille en octets, la raison (ajoutée par l'utilisateur, par ex.) et le nombre de menaces (s'il s'agit d'une archive contenant plusieurs infiltrations, par ex.). Le dossier de quarantaine contenant les fichiers mis en quarantaine (*/Library/Application Support/Eset/cache/esets/quarantine*) reste dans le système même après la désinstallation ESET NOD32 Antivirus. Les fichiers en quarantaine sont stockés sous une forme chiffrée sécuritaire et peuvent être restaurés de nouveau, après l'installation de ESET NOD32 Antivirus.

4.4.1 Mise de fichiers en quarantaine

ESET NOD32 Antivirus envoie automatiquement les fichiers supprimés en quarantaine (si l'utilisateur n'a pas annulé cette option dans la fenêtre d'alerte). Au besoin, vous pouvez mettre manuellement en quarantaine tout fichier suspect en cliquant sur le bouton **Quarantaine...**. Il est également possible d'utiliser le menu contextuel à cette fin. Cliquez, pour ce faire, avec le bouton droit de la souris dans la fenêtre **Quarantaine**, choisissez le fichier à mettre en quarantaine, puis cliquez sur le bouton **Ouvrir**.

4.4.2 Restaurer depuis la quarantaine

Les fichiers mis en quarantaine peuvent aussi être restaurés à leur emplacement d'origine. Pour ce faire, utilisez le bouton **Restaurer**. L'option Restaurer est aussi disponible à partir du menu contextuel, après avoir cliqué avec le bouton droit sur un fichier indiqué dans la fenêtre **Quarantaine**, puis sur **Restaurer**. Le menu contextuel offre également l'option **Restaurer vers...** qui permet de restaurer des fichiers vers un emplacement autre que celui d'où ils ont été supprimés.

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 jugé infecté par erreur (par l'analyse heuristique du code, par ex.) et mis en quarantaine, envoyez ce fichier au laboratoire d'ESET. Pour soumettre un fichier mis en quarantaine, cliquez sur ce dernier avec le bouton droit de la souris, puis, dans le menu contextuel, sélectionnez **Soumettre le fichier pour analyse**.

4.5 Fichiers journaux

Les fichiers journaux contiennent tous les événements importants qui ont eu lieu et donnent un aperçu des menaces détectées. La consignation représente un puissant outil pour l'analyse système, la détection de menaces et le dépannage. Elle est toujours active en arrière-plan, sans interaction de l'utilisateur. Les données sont enregistrées en fonction des paramètres actifs de verbosité. 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.

Les fichiers journaux sont accessibles à partir de la fenêtre principale de ESET NOD32 Antivirus en cliquant sur **Outils** > **Fichiers journaux**. Sélectionnez le type de journal souhaité à l'aide du menu déroulant **Journal** au haut de la fenêtre. Les journaux suivants sont disponibles :

1. **Menaces détectées** – cette option permet de consulter toutes les données sur les événements liés à la détection d'infiltrations.
2. **Événements** – cette option permet aux administrateurs système et aux utilisateurs de résoudre des problèmes. Toutes les actions importantes exécutées par ESET NOD32 Antivirus sont enregistrées dans les journaux des événements.
3. **Analyse de l'ordinateur** - les résultats de toutes les analyses effectuées sont affichés dans cette fenêtre. Double-cliquez sur n'importe quelle entrée pour afficher les détails de l'analyse à la demande correspondante.

Vous pouvez copier les données affichées dans chacune des sections dans le Presse-papiers en sélectionnant l'entrée souhaitée, puis en cliquant sur

Copier.

4.5.1 Maintenance des journaux

La configuration de journalisation pour ESET NOD32 Antivirus est accessible à partir de la fenêtre principale du programme. Cliquez sur **Configuration** > **Entrée des préférences de l'application...** > **Outils** > **Fichiers journaux**. Vous pouvez préciser les options suivantes pour les fichiers journaux :

- **Supprimer automatiquement les anciens enregistrements** - les entrées de journal plus anciennes que le nombre de jours précisé seront automatiquement supprimées.
- **Optimiser automatiquement les fichiers journaux -** les fichiers journaux sont automatiquement défragmentés en cas de dépassement du pourcentage indiqué d'entrées non utilisées.

Pour configurer le **filtre par défaut pour les entrées journal**, cliquez sur le bouton **Modifier...** et sélectionnez ou désélectionnez les types de journaux, au besoin.

4.5.2 Filtrage des journaux

Les journaux stockent des données sur les événements système importants. La fonctionnalité de filtrage des journaux permet d'afficher des entrées sur un type d'événement particulier.

Les types de journaux les plus fréquemment utilisés sont indiqués ci-dessous :

- **Avertissements critiques** - erreurs système critiques (échec de démarrage de la protection antivirus, par ex.)
- **Erreurs** - messages d'erreur comme « *Erreur de téléchargement de fichier* » et erreurs critiques
- **Avertissements** - messages d'avertissement
- **Entrées informationnelles** - messages d'information concernant les mises à jour réussies, les alertes, etc.
- **Dossiers des diagnostics** - données nécessaires pour régler finement le programme et toutes les entrées décrites ci-dessus.

4.6 Interface utilisateur

Les options de configuration de l'interface utilisateur incluses dans ESET NOD32 Antivirus vous permettent d'ajuster l'environnement de travail selon vos besoins. Ces options de configuration sont accessibles dans **Configuration** > **Entrée des préférences de l'application...** > **Utilisateur** > **Interface**.

Dans cette section, l'option du mode Avancé permet aux utilisateurs de basculer vers le mode Avancé. Le mode Avancé affiche des paramètres plus détaillés et des commandes supplémentaires pour ESET NOD32 Antivirus.

Pour activer la fonctionnalité de l'écran de démarrage, sélectionnez l'option **Afficher l'écran de démarrage au lancement**.

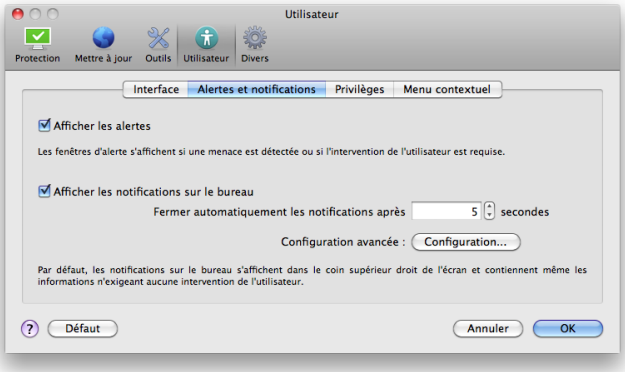
Dans la section **Utiliser le menu standard**, vous pouvez sélectionner les options **En mode standard**/**En mode avancé** pour permettre l'utilisation du menu standard dans la fenêtre du programme principal dans chacun des modes d'affichage.

Pour activer l'utilisation des infobulles, sélectionnez l'option **Afficher les infobulles**. L'option **Afficher les fichiers masqués** permet d'afficher et de sélectionner les fichiers masqués dans la configuration des **Cibles à analyser** de l'**Analyse de l'ordinateur**.

4.6.1 Alertes et notifications

La section **Alertes et notifications** permet de configurer la façon dont ESET NOD32 Antivirus traitera les messages d'alerte et les notifications système.

Désactiver l'option **Afficher les alertes** annulera toutes les fenêtres d'alerte et n'est approprié que dans des situations précises. Nous recommandons à la majorité des utilisateurs de garder l'option par défaut (activée).



Sélectionner l'option **Afficher les notifications sur le bureau** activera les fenêtres d'alerte qui n'exigent aucune interaction utilisateur pour s'afficher sur le bureau (par défaut, dans le coin supérieur droit de votre écran). Vous pouvez définir la durée pendant laquelle la notification s'affichera en ajustant la valeur de **Fermer automatiquement les notifications après** X **secondes**.

4.6.1.1 Configuration avancée des alertes et notifications

Afficher seulement les notifications exigeant une intervention de l'utilisateur
Cette option permet de basculer l'affichage de messages nécessitant l'intervention de l'utilisateur.

Afficher uniquement les notifications exigeant une intervention de l'utilisateur lors de l'exécution d'applications en mode plein écran
Cette option est utile lorsque vous travaillez sur des présentations, jouez à des jeux ou faites d'autres activités qui exigent tout l'écran.

4.6.2 Privilèges

Les paramètres utilisés par ESET NOD32 Antivirus peuvent avoir d'importantes répercussions sur la sécurité dans votre organisation. Des modifications non autorisées pourraient mettre en danger la stabilité et la protection de votre système. Vous devez donc pouvoir choisir quels utilisateurs auront la permission de modifier la configuration du programme.

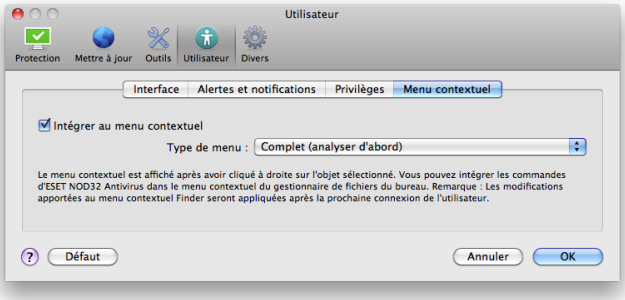
Pour préciser les utilisateurs privilégiés, ouvrez **Configuration** > **Entrée des préférences de l'application...** > **Utilisateur** > **Privilèges**.

Il est essentiel que le programme soit correctement configuré pour garantir la sécurité maximale du système. Tout changement non autorisé peut faire perdre des données importantes. Pour afficher une liste des utilisateurs privilégiés, sélectionnez-les simplement à partir de la liste des **utilisateurs** du côté gauche, puis cliquez sur le bouton **Ajouter**. Pour retirer un utilisateur, sélectionnez simplement son nom dans la liste des **utilisateurs privilégiés** du côté droit puis cliquez sur le bouton **Retirer**.

REMARQUE : Si la liste des utilisateurs privilégiés est vide, tous les utilisateurs du système auront la permission de modifier les paramètres du programme.

4.6.3 Menu contextuel

L'intégration du menu contextuel peut être activée dans la section **Configuration** > **Entrée des préférences de l'application...** > **Utilisateur** > **Menu contextuel** en cochant la case **Intégrer au menu contextuel**.



4.7 ThreatSense.Net

Le système d'avertissement anticipé ThreatSense.Net s'assure que ESET est continuellement avisé des nouvelles infiltrations, et ce, dès qu'elles se produisent. Le système d'avertissement anticipé bidirectionnel n'a qu'un objectif - améliorer la protection que nous vous offrons. Le meilleur moyen d'être sûr de voir les nouvelles menaces dès qu'elles apparaissent est d'être en contact permanent avec le plus grand nombre de nos clients et de les utiliser comme des éclaireurs pour les menaces. Deux options sont offertes :

1. Vous pouvez décider de ne pas activer le système d'avertissement anticipé ThreatSense.Net. Vous ne perdrez aucune fonctionnalité du logiciel et vous continuerez à recevoir la meilleure protection que nous pussions vous offrir.
2. Vous pouvez configurer le système d'avertissement anticipé ThreatSense.Net pour qu'il envoie des données anonymes concernant de nouvelles menaces et l'endroit où se trouve le code menaçant. Ce fichier peut être envoyé à ESET pour une analyse détaillée. Étudier ces menaces aidera ESET à mettre à jour sa base de données de menaces et améliorera la capacité de détection de menaces du programme.

Le système d'avertissement anticipé ThreatSense.Net recueille sur votre ordinateur des données concernant de nouvelles menaces détectées. Ces données comprennent un échantillon ou une copie du fichier dans lequel la menace est apparue, le chemin du fichier, le nom du fichier, la date et l'heure, le processus par lequel la menace est apparue sur votre ordinateur et de l'information sur le système d'exploitation de votre ordinateur.

Bien qu'il soit possible que cela entraîne la divulgation de certaines données connexes à vous ou à votre

ordinateur (noms d'utilisateur dans un chemin de dossiers, etc.) au laboratoire d'ESET, vous devez savoir que ces données ne seront utilisées à AUCUNE autre fin autre que celle de nous aider à répondre immédiatement aux menaces.

La configuration de ThreatSense.Net est accessible depuis la fenêtre de configuration avancée, dans **Outils** > **ThreatSense.Net**. Sélectionnez l'option **Activer le système d'avertissement anticipé ThreatSense.Net** pour l'activer puis cliquez sur le bouton **Configuration...** adjacent à l'en-tête Options avancées.

4.7.1 Fichiers suspects

L'option Fichiers suspects permet de configurer la manière dont les menaces sont soumises pour analyse au laboratoire d'ESET.

Si vous trouvez un fichier suspect, vous pouvez le soumettre à notre laboratoire pour analyse. S'il contient une application malveillante, il sera ajouté à la prochaine mise à jour de la base des signatures de virus.

Soumission de fichiers suspects - Vous pouvez choisir d'envoyer ces fichiers **Pendant la mise à jour**, ce qui signifie qu'ils seront soumis au laboratoire d'ESET pendant une mise à jour régulière de la base de données de signature de virus. Vous pouvez également choisir de les envoyer **Dès que possible** - ce paramètre est approprié si une connexion Internet permanente est disponible.

Si vous ne voulez soumettre aucun fichier, sélectionnez l'option **Ne pas soumettre**. Choisir de ne pas soumettre de fichier pour analyse n'aura aucun effet sur la soumission des renseignements statistiques configurée dans une section distincte.

Le système d'avertissement anticipé ThreatSense.Net recueille de l'information anonyme sur votre ordinateur, à propos des menaces nouvellement détectées. Ces données peuvent inclure le nom de l'infiltration, la date et l'heure de détection, la version du produit de sécurité d'ESET ainsi que des données sur la version du système d'exploitation de votre ordinateur et ses paramètres régionaux. Les statistiques sont généralement envoyées au serveur d'ESET une ou deux fois par jour.

Voici un exemple de données statistiques envoyées :

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463
[1].zip
```

Soumission des informations statistiques anonymes - Vous pouvez définir à quel moment les informations statistiques seront soumises. Si vous choisissez de les envoyer **Dès que possible**, les données statistiques seront envoyées dès leur création. Ce choix convient si une connexion Internet permanente est disponible. Si l'option **Pendant la mise à jour** est sélectionnée, toute l'information statistique sera soumise pendant la mise à jour suivant la collecte des données.

Si vous ne voulez pas envoyer de données statistiques anonymes, vous pouvez sélectionner l'option **Ne pas soumettre**.

Distribution de la soumission - Vous pouvez choisir la façon dont les fichiers et les données statistiques seront soumis à ESET. Sélectionnez l'option **Serveur d'administration à distance ou ESET** pour les fichiers et statistiques devant être soumis par tout moyen disponible. Sélectionnez l'option **Serveur d'administration à distance** pour soumettre les fichiers et les données statistiques au serveur d'administration à distance qui les soumettra ensuite au laboratoire d'ESET. Si l'option **ESET** est sélectionnée, tous les fichiers suspects et données statistiques seront envoyés directement au laboratoire d'ESET par le programme.

Filtre d'exclusion - Cette option permet d'exclure certains fichiers/dossiers de ceux qui seront soumis. Ainsi, il est utile d'exclure des fichiers qui peuvent comporter des données confidentielles, tels que des documents ou des feuilles de calcul. Les types de fichiers les plus courants sont exclus par défaut (*.doc*, etc.). Vous pouvez cependant ajouter tout type de fichier à la liste des fichiers exclus.

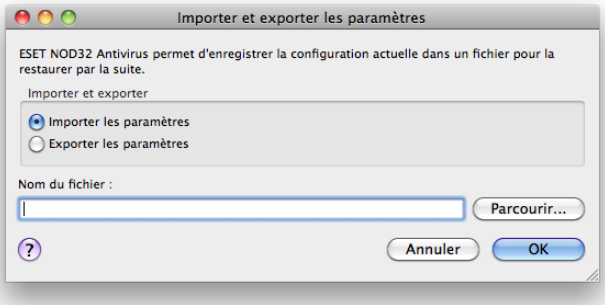
Adresse courriel du contact (facultative) - Votre adresse courriel peut également être envoyée avec tout fichier suspect et pourra être utilisée pour communiquer avec vous si nous avons besoin de plus d'information pour l'analyse. Veuillez noter que vous ne recevrez pas de réponse d'ESET sauf si d'autres renseignements sont requis.

5. Utilisateur chevronné

5.1 Importer et exporter les paramètres

L'importation et l'exportation des configurations de ESET NOD32 Antivirus sont disponibles en mode Avancé, sous **Configuration**.

L'importation et l'exportation utilisent des fichiers d'archives pour enregistrer la configuration. Les fonctions d'importation et d'exportation sont utiles si vous devez faire une copie de sauvegarde de la configuration actuelle de ESET NOD32 Antivirus pour pouvoir l'utiliser par la suite. L'option d'exportation des paramètres est aussi pratique pour les utilisateurs qui veulent utiliser la configuration préférée de ESET NOD32 Antivirus sur plusieurs systèmes - ils peuvent alors importer facilement le fichier de configuration et transférer les paramètres voulus.



5.1.1 Importer les paramètres

Il est très facile d'importer une configuration. Du menu principal, cliquez sur **Configuration** > **Importer et exporter les paramètres...**, puis sélectionnez l'option **Importer les paramètres**. Entrez ensuite le nom du fichier de configuration ou cliquez sur le bouton **Parcourir...** pour parcourir les fichiers et trouver le fichier de configuration que vous voulez importer.

5.1.2 Exporter les paramètres

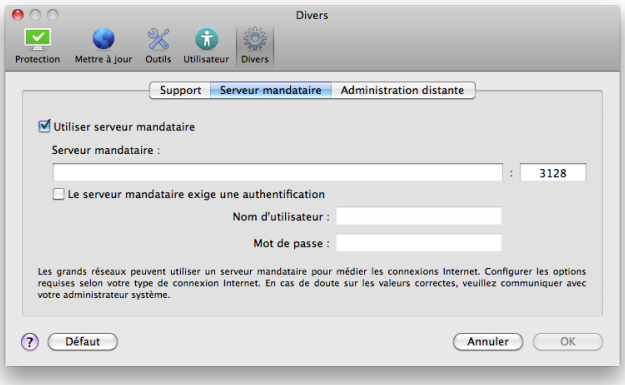
La procédure d'exportation d'une configuration est très semblable à la procédure d'importation. Du menu principal, cliquez sur **Configuration** > **Importer et exporter les paramètres...** Sélectionnez alors l'option **Exporter les paramètres** et entrez le nom du fichier de configuration. Utilisez le navigateur pour sélectionner l'emplacement sur votre ordinateur où enregistrer le fichier de configuration.

5.2 Configuration du serveur mandataire

Les paramètres du serveur mandataire peuvent être configurés sous **Divers** > **Serveur mandataire**. La sélection du serveur mandataire à ce niveau définit les paramètres de serveur mandataire globaux pour l'ensemble de ESET NOD32 Antivirus. Les paramètres définis ici seront utilisés par tous les modules exigeant une connexion Internet.

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

Si la communication avec le serveur mandataire exige une authentification, cochez la case **Le serveur mandataire exige une authentification** et entrez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants.



5.3 Blocage des supports amovibles

Les supports amovibles (comme les CD ou clés USB) peuvent contenir du code malveillant et représenter un risque pour votre ordinateur. Pour bloquer les supports amovibles, cochez l'option **Activer le blocage des supports amovibles**. Pour permettre l'accès à certains types de supports, décochez les supports voulus.

5.4 Administration à distance

ESET Remote Administrator (ERA) est un outil utilisé pour gérer la politique de sécurité et pour obtenir un aperçu de la sécurité globale d'un réseau. Elle est particulièrement utile pour les grands réseaux. ERA augmente non seulement le niveau de sécurité, mais il offre une facilité d'utilisation tout en gérant ESET NOD32 Antivirus sur les postes de travail clients.

Les options de configuration de l'administration à distance sont accessibles à partir de la fenêtre principale de ESET NOD32 Antivirus. Cliquez sur **Configuration > Entrée des préférences de l'application... > Divers > Administration à distance**.

Activez l'administration à distance en sélectionnant l'option **Connecter au serveur d'administration à distance**. Vous pourrez alors accéder aux options décrites ci-dessous :

Intervalle de connexion au serveur - fréquence à laquelle ESET NOD32 Antivirus se connectera au serveur ERA Server . Si la valeur est **0**, les données sont envoyées toutes les 5 secondes.

Remote Administrator Server - Adresse réseau et numéro de port du serveur (où est installé ERA Server) - ce champ contient un port de serveur prédéterminé, utilisé pour la connexion réseau. Il est recommandé de laisser le paramètre de port par défaut sur *2222*.

Le serveur d'administration à distance exige une authentification - Mot de passe pour la connexion au serveur ERA Server, si requis.

En temps normal, seul le serveur **primaire** doit être configuré. Si vous utilisez plusieurs serveurs ERA sur le réseau, vous pouvez choisir d'en ajouter un autre, soit une connexion ERA Server **secondaire**. Il sera alors utilisé comme solution de secours. Si le serveur primaire devient inaccessible, ESET NOD32 Antivirus communiquera alors automatiquement avec le serveur ERA Server secondaire. ESET NOD32 Antivirus tentera également de rétablir la connexion avec le serveur primaire. Une fois la connexion réactivée, ESET NOD32 Antivirus basculera automatiquement vers le serveur primaire. La configuration de deux profils de serveur d'administration à distance est plus appropriée pour les clients mobiles qui utilisent des portables qui se connectent tant à partir du réseau local que d'un réseau extérieur.

6. Glossaire

6.1 Types d'infiltrations

Une infiltration est un morceau de logiciel malveillant qui tente de s'introduire dans l'ordinateur d'un utilisateur 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 comme ceci : après l'exécution du fichier infecté, le virus s'active lui-même (avant l'application originale) et exécute une tâche prédéfinie. Ce n'est qu'après cela que l'application originale pourra s'exécuter. Un virus ne peut pas infecter un ordinateur à moins qu'un utilisateur exécute ou ouvre lui-même (accidentellement ou délibérément) le programme malveillant.

L'activité et la gravité des virus varient. 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 véritables dommages : ils ne servent qu'à ennuyer l'utilisateur et à démontrer les compétences techniques de leurs auteurs.

Il est important de noter que les virus sont (par rapport aux chevaux de Troie et aux spyware) de plus en plus rares, parce qu'ils ne sont pas commercialement très attrayants pour les auteurs de programmes malveillants. En outre, le terme « virus » est souvent utilisé de façon inappropriée pour couvrir tout type d'infiltrations. On tend aujourd'hui à le remplacer progressivement par le terme plus précis « 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 répand par un réseau. La différence de base entre un virus et un ver est 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). Ils se répandent par l'entremise des adresses courriel enregistrées dans votre liste de contacts ou exploitent les failles de sécurité de diverses 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 même 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 des programmes. De par sa nature, il est qualifié pour 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 parce qu'ils contiennent probablement du code malicieux.

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 ont été définis comme une catégorie d'infiltrations ayant comme particularité de se présenter comme des programmes utiles pour duper ensuite les utilisateurs qui acceptaient de les exécuter. De nos jours, les chevaux de Troie n'ont plus besoin de se déguiser. Ils n'ont qu'un objectif : trouver la manière la plus facile de s'infiltrer pour accomplir leurs desseins malveillants. « 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 en mesure de télécharger d'autres infiltrations sur Internet.
- injecteur – type de cheval de Troie conçu pour déposer d'autres types de logiciels malveillants sur des ordinateurs infectés.
- porte dérobée – application qui communique à distance avec les pirates et leur permet d'accéder à un système et d'en prendre le contrôle.

- enregistreur de frappe (« keystroke logger ») – programme qui enregistre chaque touche sur laquelle l'utilisateur appuie avant d'envoyer l'information aux pirates.
- composeur – programme destiné à se connecter à des numéros surfacturés. Il est presque impossible qu'un utilisateur remarque qu'une nouvelle connexion a été créée. 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. Si un fichier est identifié comme cheval de Troie sur votre ordinateur, nous vous recommandons 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 Logiciels publicitaires

L'expression « logiciels publicitaires » désigne les logiciels soutenus par la publicité. Les programmes qui affichent des publicités entrent donc dans cette catégorie. Souvent, les logiciels publicitaires ouvrent automatiquement une nouvelle fenêtre contextuelle contenant de la publicité dans un navigateur Internet ou modifient la page de démarrage de ce dernier. Ils sont généralement associés à des programmes gratuits et permettent à leurs créateurs de couvrir les frais de développement de leurs applications (souvent utiles).

En eux-mêmes, les logiciels publicitaires ne sont pas dangereux; tout au plus dérangent-ils les utilisateurs par l'affichage de publicités. Le danger tient au fait qu'ils peuvent aussi inclure des fonctions d'espionnage (comme les spyware).

Si vous décidez d'utiliser un logiciel gratuit, soyez particulièrement attentif au programme d'installation. La plupart des programmes d'installation vous avertiront en effet qu'ils installent en plus un programme publicitaire. Souvent, vous pourrez désactiver cette installation supplémentaire et n'installer que le programme, sans logiciel publicitaire.

Certains programmes refuseront cependant de s'installer sans leur logiciel publicitaire ou verront leurs fonctionnalités limitées. Cela signifie que les logiciels publicitaires peuvent souvent accéder au système d'une manière « légale », dans la mesure où les utilisateurs ont accepté qu'ils soient installés. Dans ce cas, mieux vaut jouer la carte de la prudence. Si un logiciel publicitaire est détecté sur votre ordinateur, il est préférable de le supprimer, car le risque est grand qu'il contienne du code malveillant.

6.1.5 Spyware

Cette catégorie englobe toutes les applications qui envoient des données confidentielles sans le consentement des utilisateurs et à leur insu. Ces applications utilisent des fonctions de traçage pour envoyer diverses données statistiques telles qu'une liste des sites Web consultés, les adresses courriel de la liste de contacts de l'utilisateur ou une liste des touches de frappe utilisées.

Les auteurs de ces spyware 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 données récupérées ne seront pas utilisées à des fins frauduleuses. Les données récupérées par les spyware peuvent être des codes de sécurité, des codes secrets, des numéros de compte bancaire, etc. Les spyware 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 spyware au cours de l'installation d'un programme afin de les inciter à acquérir la version payante qui en est dépourvue.

Parmi les produits logiciels gratuits bien connus qui contiennent des spyware, on trouve les applications clients de réseaux P2P (poste-à-poste). Spyfalcon ou Spy Sheriff (et beaucoup d'autres) appartiennent à une sous-catégorie particulière de spyware : ils semblent être des programmes antispyware alors qu'ils sont en réalité eux-mêmes des spyware.

Si un logiciel publicitaire est détecté sur votre ordinateur, il est préférable de le supprimer, car le risque est grand qu'il contienne du code malveillant.

6.1.6 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 vous offre l'option de détecter de telles menaces.

La classification « applications potentiellement dangereuses » désigne les logiciels commerciaux légitimes. Elle inclut également les programmes d'accès à distance, les applications de craquage de mots de passe ou les enregistreurs de frappe.

Si vous découvrez qu'une application potentiellement dangereuse est présente et fonctionne sur votre ordinateur (sans que vous l'ayez installée), consultez votre administrateur réseau et supprimez l'application.

6.1.7 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 exigent généralement le consentement de l'utilisateur avant leur installation. Si elles sont présentes sur votre ordinateur, votre système se comportera différemment (par rapport à son état avant l'installation). Les changements les plus significatifs sont :

- l'apparition de nouvelles fenêtres qui n'existaient pas auparavant
- des processus cachés qui sont activés et exécutés
- une plus grande utilisation des ressources système
- la modification des résultats de recherche
- le fait que l'application communique avec des serveurs distants.