we protect your digital worlds

* Nous protégeons votre monde numérique

Guide pour le test et l'évaluation des solutions antivirus et de ESET Smart Security / NOD32 3.0

- Installation
- Considérations et conseils pour les tests optimums et réalistes des antivirus et des solutions ESET
- Méthodologie de test conseillée

we protect your digital worlds

* Nous protégeons votre monde numérique

we protect your digital worlds

* Nous protégeons votre monde numérique

Qui sommes nous ?

ESET développe des logiciels délivrant une protection instantanée et intelligente contre les menaces évolutives.

ESET est le pionnier et le leader en matière de détection proactive. Depuis plus de 20 ans, ESET a systématiquement effectué les meilleurs scores lors de comparatifs effectués tant en laboratoire qu' « in-the-Wild ». La technologie unique ThreatSense™ collecte les données émanant de tous les utilisateurs mondiaux et envoie un retour d'information anonyme sur les nouvelles menaces, rendant ESET plus efficace, tout en réduisant le nombre de faux positifs.

ESET Smart Security est une solution unique composée d'un pare-feu, d'un antispyware, d'un antispam et d'un antivirus. ESET Smart Security combine ainsi précision, vitesse et consommation minime en ressources système pour offrir la solution de protection la plus efficace actuellement. Prônant la légèreté et l'efficacité aux modules optionnels superflus, ESET Smart Security offre les analyses les plus rapides, ne ralentissant pas votre système ni votre réseau.

Vendues dans plus de 100 pays de part le monde, Les solutions d'ESET procurent sans le moindre effort une protection inégalée et une grande sérénité à ses utilisateurs.

Configuration minimale :

Système d'exploitation	Processeur	Mémoire vive (RAM)	Disque dur (espace libre)	Carte vidéo	Connexion Internet requise
Windows 2000, XP (32/64-bits)	400 MHz	128	40	SVGA (800x600)	Oui
Windows Vista (32/64-bits)	1 GHz	512			

Le moteur ThreatSense ™

Le moteur ThreatSense d'ESET NOD32 est un système intégré anti menaces (Antithreat™ system) utilisant une approche heuristique perfectionnée. Il comprend une émulation pour supprimer le chiffrement, le conditionnement et la compression; Une analyse du code pour examiner les fonctions du malware, et une description prédictive (détection générique) pour donner une identification précise des nouveaux types de malware. Cette technologie garantit des performances optimales en réduisant l'impact sur les performances système des analyses et émulations de fichiers. Par défaut, le système vérifie la présence de mises à jour toutes les heures. Les mises à jour incluent non seulement les signatures, mais aussi les améliorations du moteur et de la détection heuristique.

Le pare-feu d'ESET Smart Security

Le pare-feu d'ESET Smart Security fournit une protection pare-feu complète, multi-modes, bidirectionnelle, avec des services de détection des intrusions. Les trois modes opérationnels sont :

- **Mode normal.**- procure une protection non intrusive pour les utilisateurs ordinaires, ne demandant pas de connaissances approfondies des pare-feux.
- **Mode avancé.**- Procure une interface hautement configurable, pour les utilisateurs avancés.
- **Mode personnalisé (Disponible uniquement avec la Business Edition).**- Autorise l'administrateur à créer et déployer des configurations personnalisées de pare-feu.

Tous les modes fournissent un protocole de filtrage et une détection d'intrusion.
Une puissante caractéristique du pare-feu ESET est la possibilité de définir certains programmes comme « navigateurs» les plaçant au même niveau que des navigateurs connus tel que Microsoft Internet Explorer. Grâce à cette fonctionnalité, il est possible de définir ainsi n'importe quelle application (par exemple Microsoft Word), entrainant une analyse heuristique beaucoup plus rigoureuse du trafic relatif à cette application et de ses connections réseau.

L'antispam d'ESET Smart Security

Le module antispam procure une protection extrêmement fiable contre le spam, ses désagréments et contre les menaces véhiculées par courriels. Disposant de nombreuses caractéristiques communes avec les spams, la protection utilise une détection de type client/serveur pour offrir une technologie préventive continue, inaccessible aux solutions s'aidant de nombreux téléchargements pour la détection.

Installation

Si un antivirus est installé sur votre ordinateur, son module d'analyse peut interférer avec ESET Smart Security. Généralement, un module d'analyse résident affiche une icône dans la barre des tâches (à coté de l'horloge). Nous recommandons de supprimer tous les autres logiciels antivirus, y compris les anciennes versions de NOD32 avant d'installer ESET Smart Security, afin d'éviter tout problème.
NOTE : Si vous avez déjà installé une version beta ou une version d'essai d'ESET Smart Security, vous DEVEZ la désinstaller avant d'installer la version définitive d'ESET Smart Security

Il existe deux modes d'installation, offrant simplicité et souplesse.

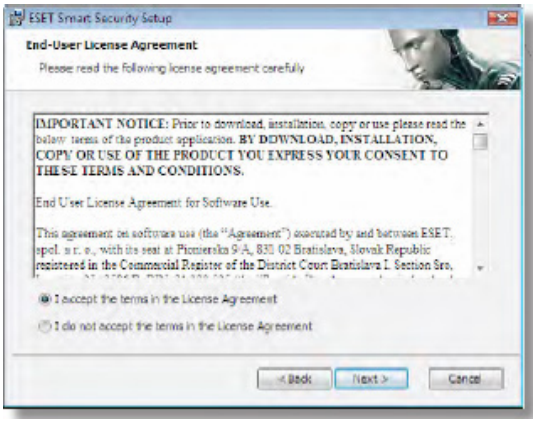
Installation typique. – Installe ESET Smart Security avec les options appropriées à la plupart des utilisateurs. Les paramètres utilisés allient une excellente sécurité, une facilité d'utilisation et un faible impact sur les ressources système.
Installation personnalisée. – Identique à l'installation typique, l'installation personnalisée autorise une personnalisation des paramètres des serveurs proxy, de quelques réglages du pare-feu et une protection par mot de passe de la configuration.

Après avoir téléchargé ESET Smart Security, démarrer l'installation en double-cliquant sur le fichier.

Notez qu'ESET Smart Security ne supporte pas encore Windows NT et ne supportera jamais Windows 95/98/ME. Si vous utilisez l'une de ces versions, visitez notre site www.eset-nod32.fr pour télécharger l'antivirus ESET NOD 32 v2.7.

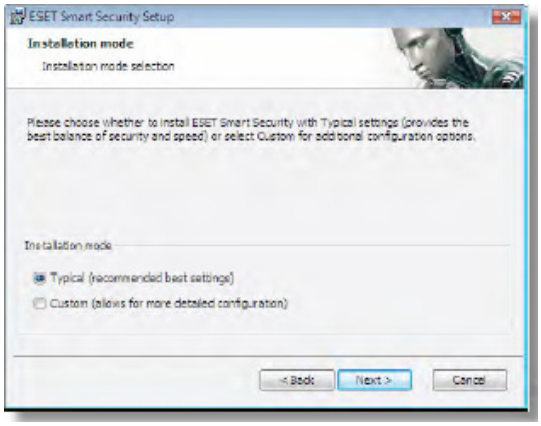
Les choix à l'installation d'ESET Smart Security

Au lancement d'ESET Smart Security, apparaissent un écran de bienvenue et un contrat de licence.



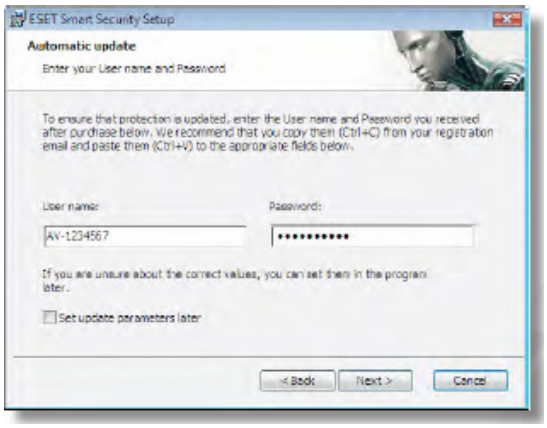
Après avoir lu et validé les conditions de licences, deux types d'installation sont proposés :

Par défaut installe NOD32 avec les paramètres adaptés à un usage courant et prend la majorité des décisions concernant les paramètres d'installation à sélectionner. Ce type d'installation est sélectionné par défaut (c'est-à-dire par l'application) et est recommandé à la plupart des utilisateurs.



Personnalisée permet de personnaliser l'installation, y compris de protéger les paramètres de configuration par mot de passe et d'activer le mode « silencieux » pour l'émission des messages d'avertissements.

Vous serez ensuite invité à fournir votre Nom d'utilisateur et votre Mot de passe pour pouvoir accéder au serveur de mises à jour d'ESET. Nous vous recommandons d'utiliser les fonctions Copier et Coller, afin d'éviter tout risque d'erreur lors de leurs reports (sélectionnez le texte, cliquez sur Ctrl + C pour Copier, puis Ctrl + V pour Coller les informations dans les champs appropriés).



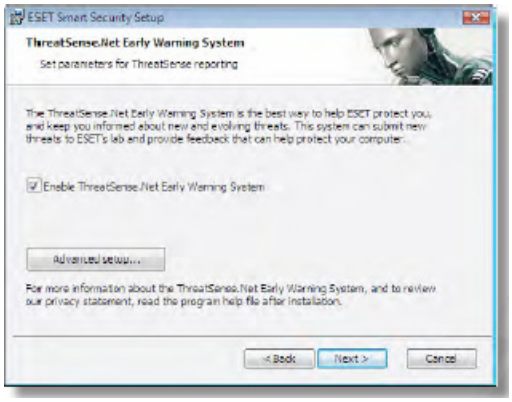
ThreatSense.Net

ThreatSense.Net étend encore la puissance de l'heuristique de ThreatSense® en soumettant automatiquement les fichiers suspectés d'être infectés au laboratoire d'ESET pour analyse approfondie. ThreatSense.Net aide à fournir davantage d'informations sur les nouvelles menaces.

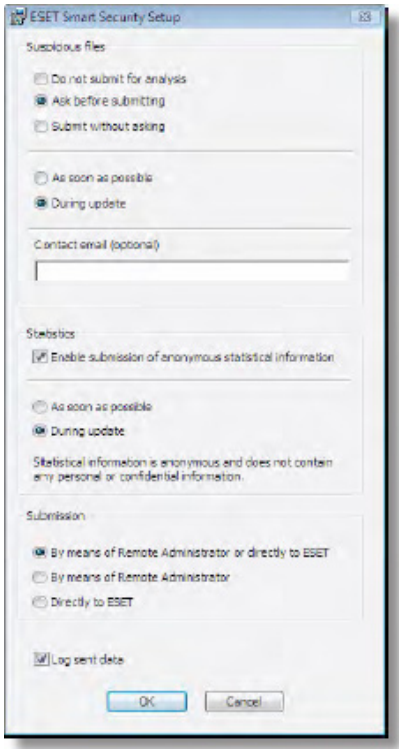
Deux options sont alors disponibles :

• Vous pouvez choisir d'activer ou non l'option ThreatSense.Net. Activer ou non cette fonction ne reduira en aucun cas la qualité de votre protection.

• Le bouton Configuration avancée... permet de modifier les paramètres par défaut du système **ThreatSense.Net™**.



Early Warning System de ThreatSense.Net collecte des informations relatives aux nouvelles menaces potentielles détectées. Les informations envoyées peuvent contenir un échantillon du fichier suspect, sa localisation sur votre disque dur, les informations qui lui sont relatives. Les informations ainsi collectées ne seront pas utilisées à des fins commerciales ni à aucune autre fin que l'analyse et la détection de nouvelles menaces.

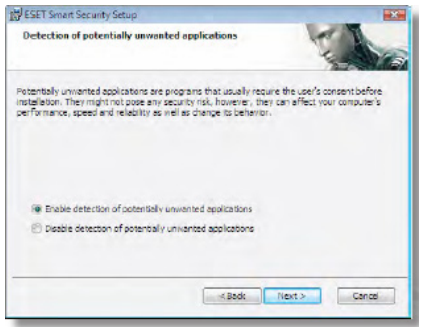


Par défaut, ESET Smart Security est configuré pour demander une validation avant de soumettre les fichiers suspects au laboratoire d'ESET, où ils seront analysés en détail. Il est à noter que les fichiers avec des extensions particulières, comme .doc ou .xls ne sont jamais envoyés, même si une menace y est détectée. Vous pouvez ajouter d'autres extensions à cette liste de fichiers exclus lors de l'envoie.

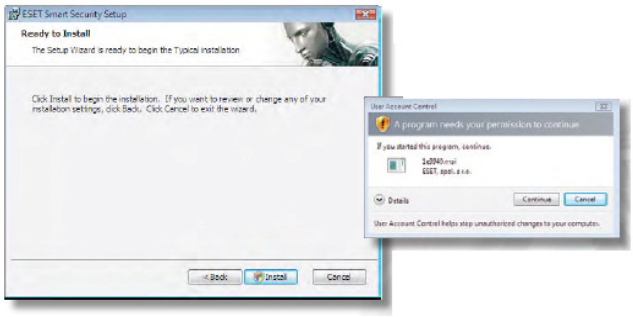
Les paramètres avancés de ThreatSense.net permettent de déterminer quand et comment les fichiers et les données sont soumis au laboratoire d'ESET.

Détection des applications potentiellement dangereuses

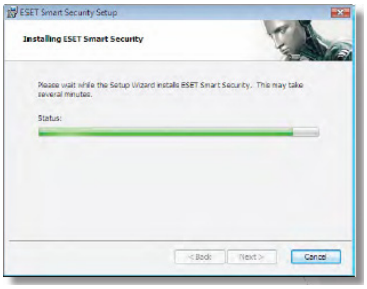
Des applications potentiellement dangereuses, comme certains types de publicités, certains utilitaires de contrôle distant, etc. peuvent être détectés. Ces programmes ne sont pas nécessairement malveillants, et ne sont pas toujours considérés comme des chevaux de Troie. Cependant, notre expérience montre que certains utilisateurs, principalement dans le milieu des affaires, veulent les détecter. Il est donc nécessaire de choisir si ces applications seront détectées ou non.



Le produit est maintenant prêt à être installé.



Une barre de progression permet aux utilisateurs de suivre la progression de l'installation d'ESET Smart Security.



Une fois l'installation terminée, il n'est pas nécessaire de redémarrer l'ordinateur pour qu'ESET Smart Security soit active et protège totalement le système. Néanmoins le système peut vous le proposer.

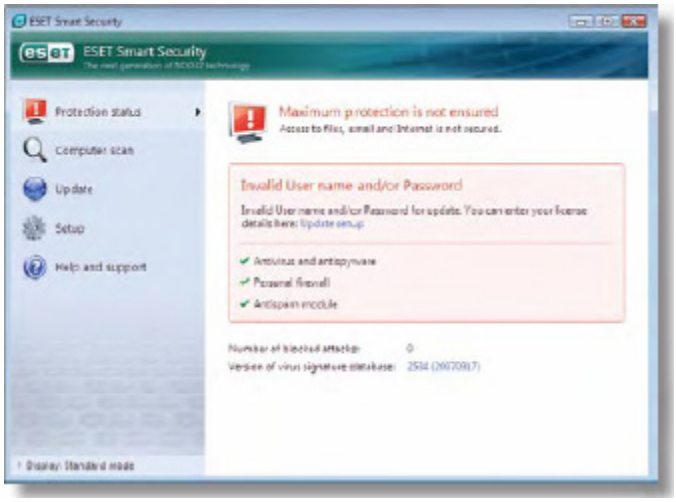
Mise en place du mode « protection réseau »

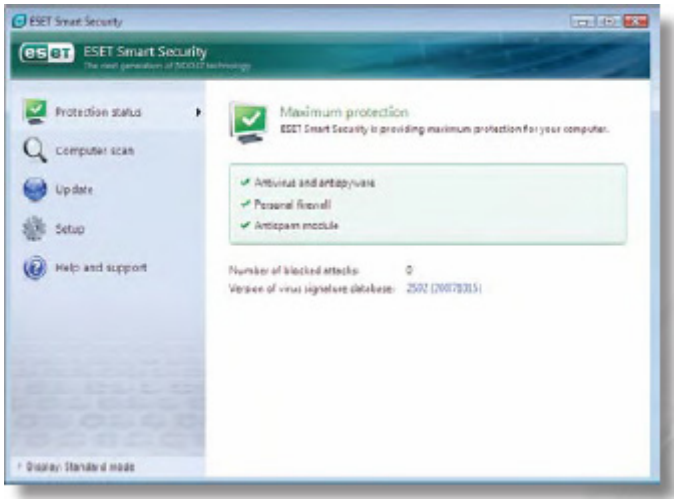
Dans le cas ou l'ordinateur est connecté à un réseau, une nouvelle fenêtre apparaît alors.
Le pare-feu peut être configuré pour une protection stricte ou pour autoriser le partage. La protection stricte est recommandée pour les ordinateurs individuels qui sont sur un réseau public partagé, comme un réseau public sans fil. Les utilisateurs dans un environnement réseau, au domicile ou au bureau, peuvent décider de partager les ressources et la visibilité de leur système avec les autres utilisateurs de ce réseau.

La boite de dialogue « paramétrage avancé » permet de désactiver ce pop-up, et de valider un choix permanent pour tous les réseaux (Ce pop-up peut être réactivé à tout moment par : Paramétrages>pare-feu Personnel > Changer la protection…).

Mise à jour et maintenance d'ESET Smart Security

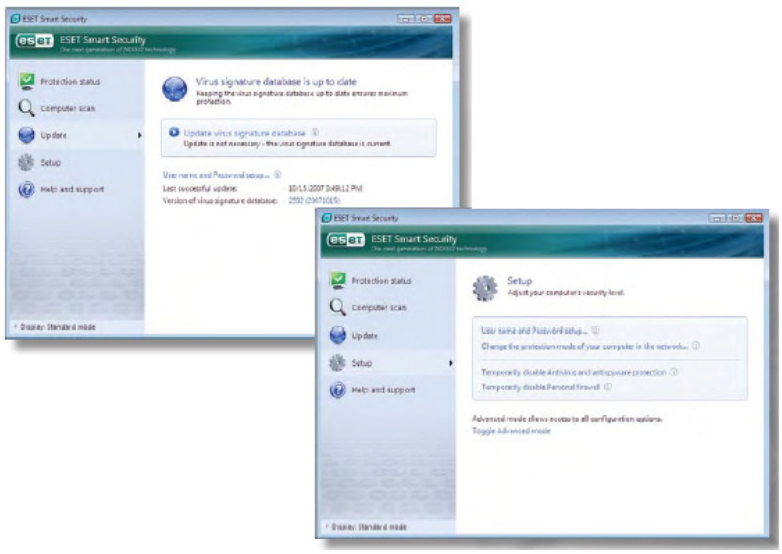
Si le nom d'utilisateur ou le mot de passe sont erronés, ou s'ils n'ont pas été saisis lors de l'installation, les mises à jour ne sont pas actives, et l'écran d'état affiché à droite signale le problème. De plus une alerte apparaîtra, accompagnée d'un changement de couleur de l'icône présente dans la barre de tâches, s'il n'y a pas eu de mises à jour depuis plus d'un jour.





Une fois l'installation et le paramétrage correctement réalisés, ESET Smart Security se mettra automatiquement à jour et le statut de protection sera affiché.

La section Mise à jour contient des informations importantes pour les mises à jour du programme. Il est essentiel que le programme soit régulièrement mise à jour pour fournir une protection maximale contre les menaces les plus récentes.



• Mettre à jour la base de signature virale

Cliquez ici pour mettre à jour la base virale immédiatement (sans attendre la prochaine mise à jour automatique). L'écran principal de la section « mise à jour » affiche l'état actuel des mises à jour. Il est important que ce dernier affiche toujours : «La base de signature virale est à jour ». Dans le cas contraire, le programme ne dispose pas des dernières mises à jour, ce qui augmente le risque d'infection. Il est alors recommandé de mettre à jour les bases virales dès que possible.

• Configuration du nom d'utilisateur et du mot de passe

Affiche une fenêtre permettant ses paramètres d'authentification (nom d'utilisateur et mot de passe). Le nom d'utilisateur et le mot de passe sont envoyés à l'adresse Email de l'utilisateur après l'enregistrement de sa licence.

• Dernière mise à jour réussie

Montre la date de la dernière mise à jour. Une date récente doit être affichée, indiquant que la base des signatures de virus est à jour.

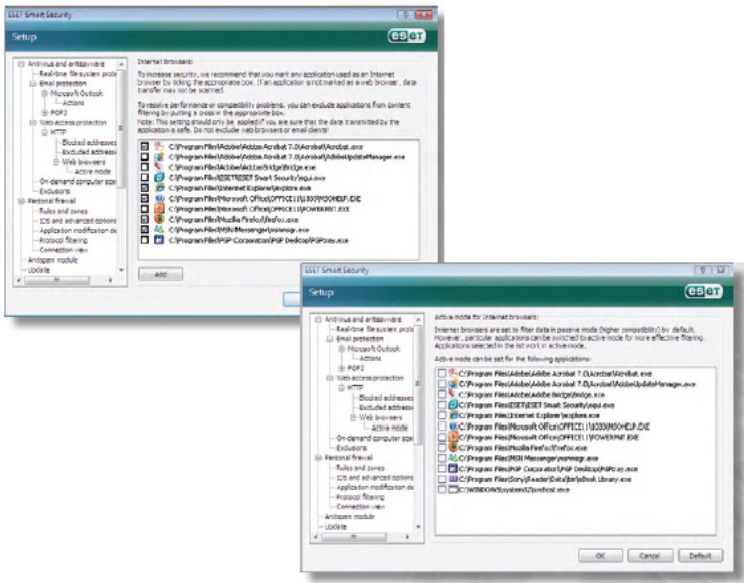
Procédure de mise à jour

Après avoir cliqué sur « mettre à jour la base virale », le processus de téléchargement débute. Une barre d'état montre la progression de la mise à jour et le temps de téléchargement restant. Cliquez sur Annuler pour interrompre le téléchargement. ESET Smart Security est conçu pour se mettre automatiquement à jour. Il n'y a généralement pas de raison de forcer une mise à jour, mais il est toutefois possible de l'initier manuellement.

Considérer des applications comme des navigateurs

Il est possible de considérer diverses applications comme des navigateurs Internet afin d'accroître le niveau de protection. Une fois cette fonction active, un ensemble de règles heuristiques plus strictes et plus restrictives est appliqué au trafic entre Internet et l'application. Les applications sont automatiquement ajoutées à la liste si elles ont un composant réseau, et certaines applications sont automatiquement considérées comme des navigateurs. Nous recommandons de laisser ESET Smart Security optimiser cette fonction, mais il est possible d'ajouter ou de retirer des applications manuellement.

Nous recommandons de ne pas désactiver cette fonction pour les navigateurs Internet, afin de ne pas compromettre la sécurité du système. Les applications considérées comme navigateurs filtrent le trafic en mode passif pour une plus grande compatibilité. Ce fonctionnement peut être changé en mode actif pour accroître le degré de protection. Si des problèmes de compatibilité (trafic bloqué ou fonctionnement incorrect) se produisent, il suffit de revenir au mode passif.



Analyse du système

Cliquez sur l'icône Analyse de l'ordinateur, pour faire apparaître une fenêtre permettant de choisir entre Analyse Standard et Analyse personnalisée. L'Analyse Standard est une méthode facile à utiliser permettant de lancer rapidement une analyse de l'ordinateur qui va détecter et nettoyer tous les fichiers infectés automatiquement.
L'avantage principal de cette analyse est sa facilité d'utilisation, sans recourir à des options et paramètres complexes. L'analyse standard contrôle tous les fichiers des disques locaux (à l'exception des fichiers email et archives), et répare ou supprime automatiquement toutes les infections détectées. Pour plus d'informations sur le nettoyage, reportez vous à la section « Nettoyage » de l'aide d'ESET Smart Security.

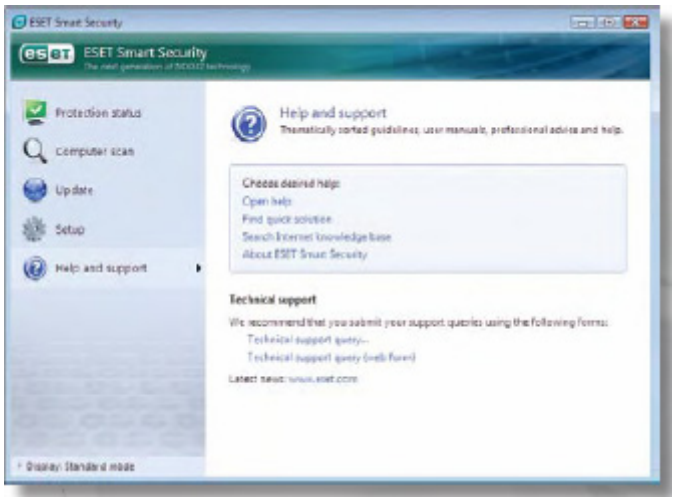
L'analyse personnalisée est la solution idéale pour configurer le paramétrage en détail, tel que des cibles ou des méthodes spécifiques. Ces configurations peuvent ensuite être sauvegardées dans des profils d'analyse pour être réutilisées.
Deux méthodes sont disponibles pour sélectionner les cibles de l'analyse, utiliser la sélection rapide dans un menu déroulant, ou utiliser l'arborescence qui liste tous les disques disponibles sur l'ordinateur. Il est aussi possible de choisir entre trois niveaux de nettoyage en cliquant sur « Configuration> Nettoyage ». Si vous voulez seulement analyser l'ordinateur sans aucune action, choisissez l'option « Analyse sans nettoyage ».

L'utilisation de l'analyse personnalisée est adaptée aux utilisateurs expérimentés ayant déjà utilisé des programmes antivirus.

Tant que l'analyse se poursuit, un indicateur vous indique l'avancée du programme. Quand l'analyse est terminée, les résultats sont affichés et il est possible d'obtenir un fichier de rapport détaillé.

Aide et support

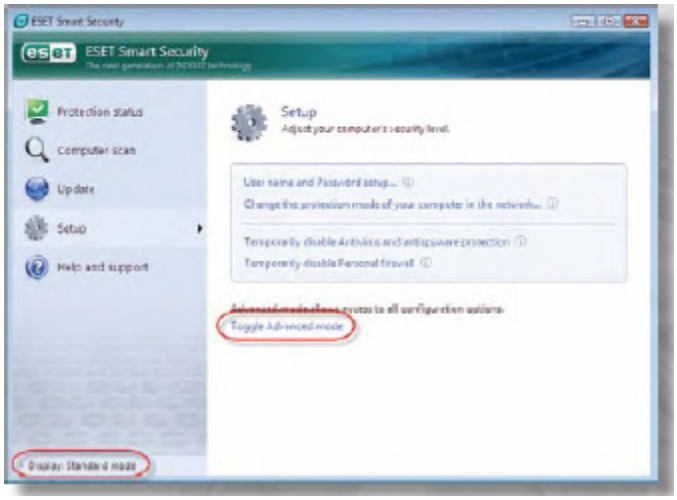
La section d'aide et de support fournit des informations claires et pratiques sur le produit, ainsi que des conseils sur la façon de soumettre des requêtes.



Mode avancé

Utilisation de l'interface « Mode Avancé »

L'interface standard d'ESET Smart Security donne accès aux paramètres basiques, suffisant à la plupart des utilisateurs. Il est cependant possible d'utiliser un Mode Avancé qui fournit une vue plus détaillée de l'état de la protection.

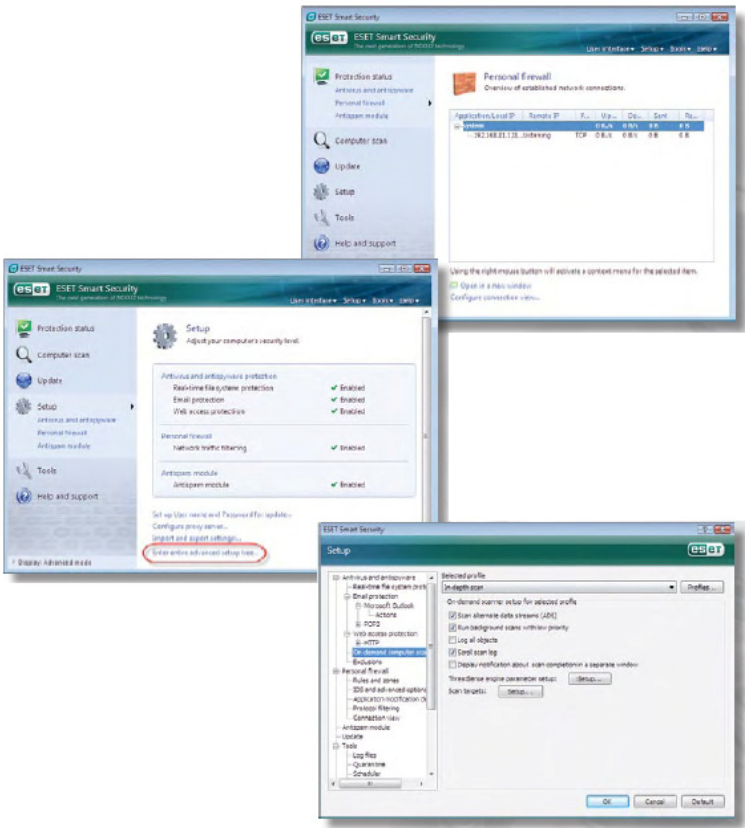


Le Mode Avancé n'est recommandé que pour les utilisateurs habitués aux logiciels de sécurité, car il permet des changements importants dans la configuration. Le Mode Avancé permet une flexibilité totale d'ESET Smart Security. Le mode avancé est accessible en cliquant sur le choix du mode d'affichage dans le coin inférieur gauche de l'écran.

En mode avancé, l'onglet « Etat de la protection » affiche beaucoup plus de détails utiles aux utilisateurs avertis. Les onglets « analyse de l'ordinateur » et « mise à jour » sont les mêmes dans les deux modes.

En mode avancé, l'onglet configuration donne accès à toutes les options de configuration d'ESET Smart Security.

Le mode avancé présente également un nouvel onglet, l'onglet Outils. Cet onglet comprend une méthode manuelle pour soumettre un fichier suspect au laboratoire ESET, la zone de quarantaine, un accès aux fichiers logs et les options relatives à la programmation des tâches.



En basculant en mode avancé, vous aurez accès à l'intégralité des paramètres ESET. C'est ici que les anciens utilisateurs d'ESET NOD32 retrouveront leurs habitudes, offrant une solution fiable et facile d'utilisation. La flexibilité et la qualité d'ESET Smart Security permettent aux utilisateurs avancés d'ajuster les paramètres à leur convenance. Le Mode Standard rend ESET Smart Security approprié et facile à utiliser pour les utilisateurs moins techniques ou simplement désireux d'une protection efficace et simple.

* Nous protégeons votre monde numérique

Tester ESET Smart Security

ESET Smart Security est plus que la juxtaposition de différents éléments. L'intégration entre les modules antivirus, antispyware, pare-feu et antispam permet au système de prendre des décisions plus pertinentes à tous les niveaux. ESET Smart Security réalise cela avec la combinaison du plus haut niveau de précision, de performance et de protection dynamique disponible. Nous recommandons de ne tester la solution qu'avec tous les composants activés. Des composants comme le pare-feu ne sont pas initialement conçus pour fonctionner seul, et reposent sur leur intégration avec le moteur d'analyse antivirus ThreatSense.

Tester un produit antivirus ne consiste pas à analyser quelques fichiers pour vérifier s'ils contiennent des virus. Le test doit être mené d'une manière rigoureuse et méthodique pour s'assurer des résultats obtenus. Ce guide pointe les critères les plus importants à tester, et donne des conseils pour tester les différents types d'analyses antivirus.

Tester un antispam requiert une importante collection d'échantillons de spams ainsi qu'un système qui simule la manière dont les spams sont envoyés.

Tester un pare-feu est une procédure complexe qui suppose une connaissance approfondie des protocoles réseaux. Les tests classiques « de fuite » ne correspondent en général pas à des situations du monde réel. En réalité, ce type de test conduit à tort les gens à penser qu'un système est efficace/sécurisé ou non suivant qu'il le passe avec succès ou pas.

Le but d'ESET Smart Security n'est pas de déléguer des tâches de sécurité spécifiques à chacun de ses modules, mais plutôt de créer une sécurité globale par une approche en profondeur des processus de défense. Dans certains scénarios, une fonction généralement traitée par le pare-feu peut être traitée par la partie antivirus du logiciel. C'est la raison pour laquelle il est primordial de faire les tests dans un environnement complet et réel. Le véritable test du produit est aussi bien de voir comment il protège le système comme un tout, que la qualité de l'expérience de l'utilisateur.

Considérations et conseils pour les tests de logiciels antivirus et plus particulièrement la gamme ESET

Quelques considérations sur les tests d'une analyse à la demande

• Vitesse d'analyse et impact sur les performances

Pendant les tests d'analyse à la demande, la rapidité de l'analyse et son impact sur les performances sont des points très importants (moins importants, bien entendu, que la détection des virus). Usuellement, il y aura un impact sur les performances lors de l'analyse d'un fichier, et un système normal contient des centaines ou des milliers de fichiers. Une analyse ralentissant la machine de manière significative, la rendant parfois inopérante, n'est pas acceptable. Il est important que tout impact sur les performances soit d'une durée minime. De ce fait, l'analyse doit être effectuée efficacement et utiliser le moins de ressources système possible.

• Paramètres de l'analyse

Les outils d'analyse à la demande ont généralement une série d'options que l'on peut définir, et le testeur doit spécifier celles qui seront utilisées. Suivant qu'on utilise la meilleur configuration ou celle par défaut, il y aura des différences sur les résultats du test et sur ses performances comme sa vitesse, etc… Les tests doivent être faits dans les conditions où un utilisateur normal utiliserait le produit sur sa machine : les fichiers infectés ne doivent pas être renommés, ou modifiés, et doivent être sur l'un des disques locaux (sauf si le test doit porter sur une analyse de disques réseau).

• Action après détection

Les outils d'analyse à la demande proposent généralement une série d'options relatives à la manière de traiter les fichiers jugés infectés. L'action à entreprendre peut avoir un impact sur le système. Pour la plupart des tests, un simple rapport dans un fichier log est suffisant.

Quelques considérations sur les tests d'analyse à l'accès

• Impact sur les performances système

De part le fait qu'un outil d'analyse à l'accès se charge au démarrage du système et analyse chaque fichier accédé, il peut avoir une incidence négative très importante sur les performances du système. Idéalement, cette incidence devrait être minimale. Souvent, la perte de performance la plus significative est à l'ouverture d'une application : le temps d'ouverture d'une application avec l'outil d'analyse actif comparé au temps nécessaire sans ce même outil est un bon indicateur de son impact sur les performances.

• Action après détection

L'action entreprise par défaut est aussi importante. Est-ce qu'on empêchera le virus de s'ouvrir en refusant l'accès au fichier, ou est-ce que le virus aura le temps de s'ouvrir et d'infecter le système pendant que l'antivirus rapportera sa découverte ? Pendant le test, il est généralement conseillé de se contenter de créer le rapport étant donné qu'il y aura un nombre inhabituel de virus dans le système et que d'autres actions pourraient interférer avec le test.

• Stabilité du système

Il faut noter que la stabilité du système peut être affectée par un logiciel antivirus mal configuré. Des comportements inhabituels d'applications ou des problèmes système peuvent survenir par interférence avec un outil d'analyse à l'accès.

Heuristique

L'heuristique est une technologie utilisée pour détecter des menaces pour lesquelles aucune signature traditionnelle n'est encore répertoriée. ESET est depuis longtemps reconnu comme le leader de la détection proactive des menaces, sans utiliser de bases virales.

Heuristique avancée

L'heuristique avancée étend les possibilités de l'heuristique et permet à ESET Smart Security de détecter un grand nombre de nouvelles menaces. Par défaut, l'heuristique avancée est désactivée dans les composants d'ESET Smart Security. Nous recommandons de l'utiliser avec précaution dans l'analyse à l'accès car elle peut ralentir fortement le temps d'analyse et produire de temps à autre un faux-positif.

Nous recommandons d'exécuter périodiquement une analyse approfondie de votre machine, avec l'heuristique avancée activée. Ce type d'analyse est la plus minutieuse et la plus efficace et devrait être exécutée à peu près chaque semaine. On l'exécute en choisissant Analyse d'ordinateur > analyse personnalisée et en s'assurant que le profil « approfondie» a été sélectionné.

Quelques considérations pour tester l'analyse heuristique

Les antivirus disposant de capacités heuristiques essayent d'identifier des virus nouveaux ou modifiés pour donner à l'utilisateur une protection accrue dans les premières périodes d'une attaque. Ces outils d'analyse peuvent être difficiles à tester ; on peut porter une attention particulière aux points suivants :

- **Agressivité de l'analyse**

ESET NOD32 a deux niveaux d'analyse heuristique, le Mode Standard et le Mode Avancé. Le Mode Avancé est beaucoup plus agressif, en ce sens qu'il suspectera davantage certains types de fichiers. Ce mode donne une vision plus juste des possibilités du scanner heuristique, car il est utilisé par défaut dans tous les modules d'intervention critique de NOD32.

- **Faux-positifs**

Une analyse agressive peut accroître le nombre de faux-positifs. Ceci est dû à une grande suspicion attachée aux objets analysés. Il peut être désagréable d'identifier chaque fichier sain comme infecté, mais l'analyse heuristique peut conduire à cette éventualité, comme d'ailleurs des produits non heuristiques peuvent se tromper sur les signatures.

- **Niveau de mise à jour**

Pour tester la détection heuristique, l'échantillon choisi doit comporter des virus inconnus du produit au moment du test, sinon les capacités heuristiques ne seront pas testées.

- **Version du produit**

Notons que les capacités heuristiques sont mises à jour aussi fréquemment que les signatures de virus classiques. C'est pourquoi tester de vieilles versions (en termes de semaines ou de mois) ne reflète pas les capacités heuristiques réelles du produit. Dans l'idéal, le produit testé devra être la dernière version, sans mise à jour des signatures de virus.

- **Tester sur une longue période**

Il est possible de tester les capacités heuristiques sur un échantillon volumineux en « gelant » un produit (c'est-à-dire en ne mettant pas à jour la base des signatures) pendant un certain temps, et en testant l'heuristique sur les virus apparus depuis la dernière mise à jour.

Il est important de noter que les implications statistiques d'un échec de recherche heuristique ne sont pas les mêmes que l'échec de détection de virus après mise à jour. En effet, l'échantillon testé est en général assez petit comparé à la liste de tous les virus dans la nature (parce que très peu, parfois même un seul, aura été libéré). Ne tester qu'un ou deux virus inconnus ne fournit pas un bon indicateur des capacités d'un scanner heuristique.

On peut s'attendre aussi à ce que les vieux virus soient détectés à la fois par les mises à jour et par l'heuristique une fois qu'ils sont connus, puisque la détection heuristique est améliorée à chaque mise à jour des bases virales. Cela peut rendre moins précis les résultats des tests.

Un antivirus testé est-il meilleur s'il détecte plus de virus injectés ?

Non, ce n'est pas si simple que ça, car un produit doit être fréquemment mis à jour pour détecter les virus les plus récents ; un produit qui détecte tous les virus apparus le mois dernier, mais pas ceux du mois en cours est inutile. Les tests de produits antivirus sont faits pour montrer que le produit atteint un niveau constant de détection, détectant de préférence tous les virus qu'un utilisateur ne verra vraisemblablement jamais. Malheureusement, il y a quelques problèmes qui surgissent fréquemment quand on teste des produits antivirus. Les plus significatifs sont brièvement détaillés ci-dessous :

- **Méthodologie de test incorrecte**
- **Tester sur des virus modifiés ou spécialement créés**
- **Tester sur des fichiers infectés renommés**
- **Tester sur des virus endommagés ou non viables**
- **Tester sur des fichiers sains (parce qu'ils ont déjà été détectés par erreur par un autre produit).**
- **Tester avec de mauvais paramétrages**
- **Tester avec des paramètres subjectifs**
- **Tester sur un PC après une simple désinstallation d'un autre antivirus testé avant (il faudrait repartir à chaque fois d'une image propre)**

La plupart de ces problèmes peuvent être facilement évités en testant les fonctionnalités des échantillons avant de les confronter au produit. La partie « Sélection d'échantillon » de ce guide répond à cette préoccupation essentielle. Les paramètres subjectifs sont, par exemple, le fait que le testeur croit que le produit antivirus va détecter les cookies, ou le lancement de tests peu virulents qui ne tiennent pas compte des performances du produit pendant qu'il détecte des virus ou assure la sécurité.

Quelques règles fondamentales pour tester votre antivirus

• Les fichiers doivent avoir leur extension réelle, et pas d'extensions renommées.

ESET Smart Security est un produit très sophistiqué optimisé pour être utilisé au quotidien, et non pour des tests académiques. Cela signifie qu'il fonctionne de façon optimale dans les conditions où un utilisateur s'en servirait – en analysant un système avec de vrais virus actifs, en bloquant de vrais spams, en évitant une intrusion, quelle que soit la partie du produit qui accomplit la tâche. Analyser un fichier qui n'a pas son extension légitime – par exemple, le fichier myscreensaver.exe renommé myscreensaver.ex? – donnera des résultats imprévisibles et souvent inexacts. L'extension .ex? n'est pas exécutable dans un système normal, et ESET NOD32 peut légitimement ignorer ce fichier comme étant une menace très faible, bien que, par défaut, le scanner à la demande d'ESET Smart Security analyse tous les fichiers. Bien entendu, avec l'extension correcte, un virus serait reconnu comme une menace pour le système.

• Les fichiers doivent être sur un disque local

Sauf si l'on teste spécifiquement l'antivirus sur des unités en réseau, les fichiers infectés doivent être sur un disque local. Dans le cas contraire, les valeurs portant sur la rapidité d'analyse et l'impact sur le système seront erronés. ESET Smart Security est extrêmement rapide et a un impact minimum sur le système pendant l'analyse ; Cette vitesse ne sera pas mesurée correctement à travers un réseau, parce qu'elle sera limitée par la connexion réseau.

• Les paramétrages doivent être contrôlés

Certains tests sont menés avec le paramétrage par défaut, d'autres avec le paramétrage optimal. Les membres de l'équipe d'ESET pourront vous aider à déterminer les paramétrages à utiliser pour un test parfait.

• Les virus doivent être réels

On doit utiliser des échantillons sans altération, qui pourront être vérifiés comme virus après reproduction.

• Fichiers endommagés

On ne doit pas tester les fichiers endommagés, réguliers ou sans danger, même s'ils ont été étiquetés à tort « fichiers tests », y compris les fichiers simulateurs de virus – ce ne sont pas des virus, et ils ne doivent pas être testés comme tels. ESET est fier de détecter seulement des malware réels, et ne souhaite pas entrer dans le jeu de détection des fichiers inoffensifs simplement pour passer les tests.

Guide des tests du produit

• Les virus testés doivent être des variantes existantes.

Les virus doivent être conservés, sans transformation, dans leur état habituel « In-the-Wild », et doivent être des virus existant réellement. ESET ne veut être en aucun cas responsable de la création de nouveaux virus, ou de l'altération de virus pour créer des variantes, y compris à l'occasion de tests. Altérer un virus (en supposant qu'il est ensuite reproductible) crée effectivement un nouveau virus. En conséquence, nous considérons ces pratiques comme contraire à notre éthique et à notre professionnalisme, et nous ne participerons pas à des tests basés, en totalité ou en partie, sur des virus altérés ou spécialement créés.

• On doit utiliser des fichiers normaux pour tester les faux-positifs

Les fichiers sains utilisés pour tester les faux-positifs doivent être des fichiers normaux, pouvant exister dans le système d'un utilisateur de base, et non des fichiers spécifiquement créés pour ressembler à des virus dans le but de piéger les logiciels antivirus.

• Intégrité des statistiques

La sélection d'échantillons doit être faite sur une bonne base, car le nombre d'échantillons utilisés est très important. Tester 2 ou 3 ou même 10 ou 15 échantillons n'est pas statistiquement satisfaisant. La « Wildlist » contient 250 à 270 virus dans sa liste de base (la plus significative) des virus couramment en liberté. Plus l'échantillon testé sera petit, plus il y aura des erreurs statistiques sur les résultats. Le nombre de chevaux de Troie qui ne sont pas des virus oblige à porter ce nombre à des centaines de milliers pour que le test soit significatif.

• Virus manqués

Tout virus qu'un produit manque, ou ne détecte pas correctement, ou tout fichier sain qu'un logiciel détecte par erreur doit être rendu disponible aux auteurs du produit pour vérification, et, éventuellement, réparation. Si ESET Smart Security omet de détecter ou de réparer un malware quelconque, signalez-le à ThreatSense.net.

Que doit-on tester dans un produit antivirus, en plus de la détection de virus ?

Il y a un point primordial dans les tests de logiciels antivirus, et plusieurs autres de moindre importance. Le point le plus important du test d'un logiciel antivirus est sa détection des virus « réels » ; il y a cependant différents types d'analyses, et il faut avoir une certaine connaissance de ces différences pour les tester.

Tester des suites ou des solutions intégrées demande toute l'expertise pour tester un antivirus, plus un ensemble de connaissances pour tester les antispam et les pare-feux.

ESET, LLC.
610 West Ash Street, Suite 1900
San Diego, CA 92101
U.S.A.
www.eset.com

Distributeur exclusif pour la France :
ATHENA Global Services
20 allée Louis Calmanovic
93320 Les Pavillons-sous-bois
www.eset-nod32.fr