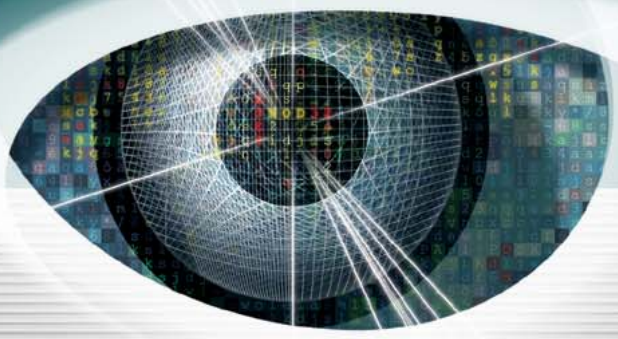


NOD32
antivirus system

Guide d'installation v2.7

Publication : janvier 2007

ESET, LLC

610 West Ash Street

Suite 1900

San Diego

California, 92101

U.S.A.

http://www.eset.com

NOD32 France :

Tél. : 01 55 89 08 85

http://www.eset-nod32.fr et http://www.nod32.fr

Support Technique

Tél. : 0 826 02 02 82 (coût de l'appel : 0,15 € TTC par minute)

Par e-mail:
support@eset-nod32.fr

Ce guide faisant l'objet de mises à jour régulières en fonction des évolutions applicatives de NOD32, la dernière version actualisée est toujours disponible en téléchargement (au format PDF et en couleur) sur notre site Internet http://www.eset-nod32.fr et http://www.nod32.fr **.**

Sommaire

CONFIGURATION APRES INSTALLATION

Introduction

Nouvel acquéreur ou déjà fidèle utilisateur/utilisatrice, nous vous remercions vivement de la confiance que vous accordez à NOD32 Antivirus System.

Bien que NOD32 soit simple à utiliser**,** ce guide vous aidera à en découvrir les multiples fonctionnalités et à maintenir ainsi le niveau de protection optimal.

NOD32 est bien davantage qu'un scanner antivirus, la détection des virus connus étant le strict minimum qu'un utilisateur soit en droit d'attendre de tout logiciel antivirus. NOD32 ne se contente pas d'exécuter cette tâche de manière plus fiable et plus rapide que ses concurrents, il identifie également bien d'autres types de codes malveillants et détient un taux record de détection des nouvelles menaces.

Le moteur d'analyse unique de NOD32 a été optimisé pour détecter et bloquer toutes les menaces évolutives, incluant Virus, Vers, Chevaux de Troie, et autres Malwares. De plus, depuis la version 2.5, il détecte également les logiciels espions (Spywares), publicitaires (Adwares), à risque, et les attaques de type Phishing.

Avec NOD32, vous êtes certain/certaine de bénéficier de la protection la plus avancée et complète possible. La technologie **ThreatSense**™, intégrée au puissant moteur de détection de NOD32, vous protège en temps réel des menaces actuelles et futures.

Conventions Utilisées dans ce Manuel

Afin de souligner les points les plus importants – nous avons utilisé un simple jeu d'icônes. Elles attireront votre attention sur les informations cruciales et les paramètres-clés.

Signification des icônes:

	**L'icône « Cochée » indique un paramètre que nous vous recommandons d'utiliser ou d'activer.**
	**L'icône « Info » souligne les informations ou faits importants concernant NOD32, afin de vous aider à optimiser l'utilisation du programme.**
	**Afin de vous aider à éviter tout dommage ou toute perte de données, l'icône "Danger" met l'accent sur un domaine où de potentiels problèmes peuvent survenir, ou une mauvaise configuration se présenter.**

Utilisation des icônes comme guides – leur présence insiste sur les secteurs de configuration les plus importants et leurs usages. Si une remarque est particulièrement importante, l'icône conserve le même dessin, mais est affichée en rouge.

Ce document utilise les conventions typographiques suivantes:

`C:\type.exe`

Utilisé pour le texte devant être saisi exactement comme présenté

`Ndntenst.exe`

Utilisé pour les noms des options dans les menus, des fichiers ou programmes, les messages à l'écran et les boîtes de dialogue.

Nom d'utilisateur

Utilisé pour les éléments tels que mot de passe et nom d'utilisateur.

Configuration Minimale Requise

Assurez-vous que l'ordinateur sur lequel vous souhaitez installer NOD32 répond à la configuration minimum requise ci-dessous:

- **Unité centrale:** processeur Pentium/Celeron/AMD 300MHz
- **Mémoire vive:** 32 Mo (98/ME), 64 Mo (NT4/2000), 128 Mo (XP/2003) de RAM
- **Espace disque:** 30 Mo d'espace libre sur le disque dur
- **Affichage:** carte vidéo VGA (SVGA 800x600 recommandée)

Veillez à ne pas installer plus d'UN scanner antivirus résident sur votre machine ; dans le cas contraire, votre système pourrait subir de sérieuses instabilités. Si vous installez NOD32 sur un ordinateur équipé d'un autre système antivirus, n'activez JAMAIS plus d'un scanner résident à la fois.

Si un autre programme antivirus a été préalablement installé sur votre ordinateur, son scanner résident (ou scanner à l'accès) peut entrer en conflit avec celui de NOD32. Généralement, les scanners résidents affichent une icône dans la barre des tâches (dans la partie proche de l'horloge système). Afin d'éviter d'importants dysfonctionnements, nous vous recommandons de désinstaller tout autre logiciel antivirus avant d'installer NOD32 v2.7 (y compris les versions antérieures à NOD32 v2.0).

Si la version d'évaluation de NOD32 est installée sur votre ordinateur, elle doit **impérativement** être désinstallée avant installation de la version commerciale de NOD32.

Si vous utilisez NOD32 version 2.5, la mise à niveau vers la version 2.7 sera assurée par le système de mise à jour automatique. En cas d'incident, nous vous invitons à effectuer une désinstallation complète de NOD32 v2.5, puis une réinstallation de NOD32 v2.7.

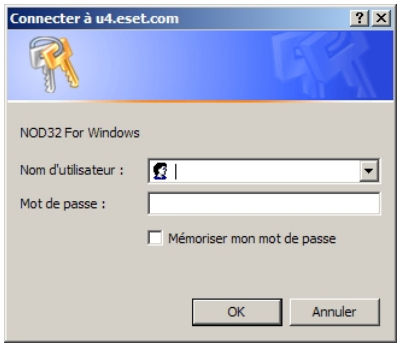
Voir détails de la procédure de désinstallation en **Annexe C** (page 52).

Instructions d'Installation pour Windows 95/98/ME et NT/2000/XP/2003

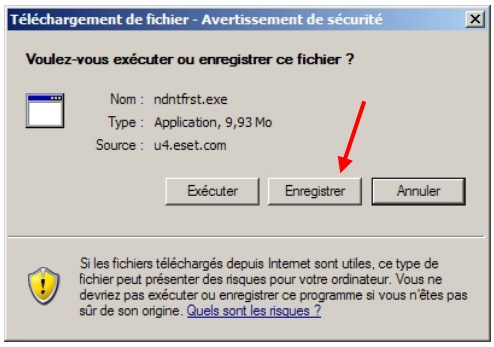
Pour installer NOD32 à partir du CD-ROM, insérez simplement le CD dans le lecteur. Si l'exécution automatique est désactivée pour ce lecteur et que la fenêtre répertoriant les versions de NOD32 disponibles sur le CD ne s'affiche pas automatiquement, double-cliquez sur le fichier **Menu** situé dans le répertoire principal du CD.

Pour installer une version téléchargée (recommandé, afin de bénéficier de la toute dernière version), téléchargez le fichier approprié à la version de votre système d'exploitation à l'adresse : http://www.eset.com/download/download.htm ou http://www.nod32.fr , en utilisant le **Nom d'utilisateur** et le **Mot de passe** qui vous ont été transmis par e-mail, dans le courrier de confirmation relatif à votre licence.

Sélectionnez la version à télécharger, afin que celle-ci corresponde à votre type de licence [monoposte → version standard OU multiposte → version Administrator], ainsi qu'à votre système d'exploitation, puis cliquez sur **Télécharger** (ou **Download**).

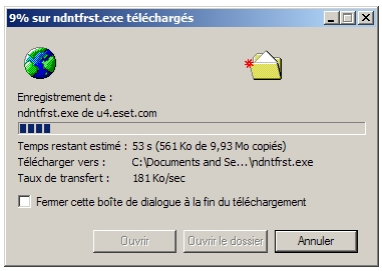


Effectuez un « copier/coller » du **Nom d'utilisateur** et du **Mot de passe**, de façon à les reporter avec exactitude dans les champs correspondants (vous pouvez utiliser les raccourcis clavier : 'Ctrl+C' pour copier, et 'Ctrl+V' pour coller). Cliquez sur OK.



A l'apparition de cette fenêtre, choisissez **Enregistrer**, puis sélectionnez l'emplacement où vous souhaitez enregistrer le fichier exécutable.

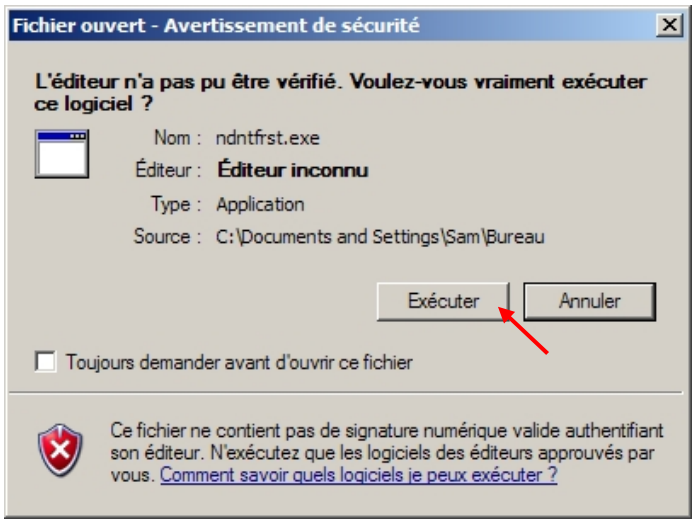
La fenêtre de progression du téléchargement s'affiche. Lorsqu'il est terminé, cliquez sur **Fermer** ou **Ouvrir le dossier**.



Enregistrez vos travaux et fermez toutes les applications en cours d'exécution avant de procéder à l'installation de NOD32.

Double-cliquez sur le fichier téléchargé pour lancer l'installation. Cliquez ensuite sur **Exécuter** dans la fenêtre ci-contre.

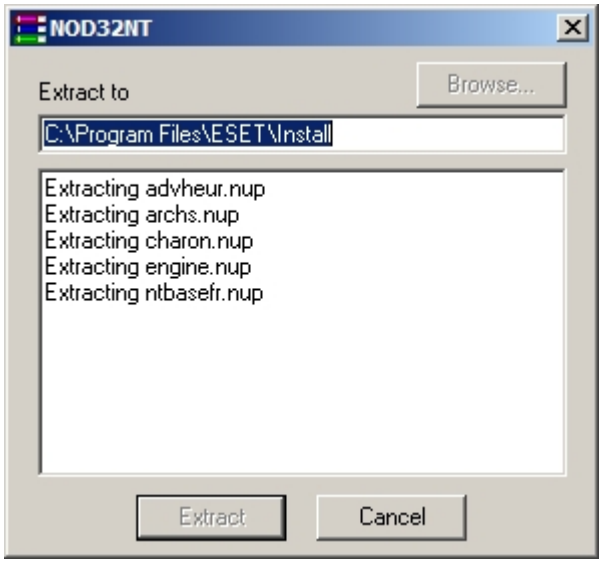
Pour les deux sources d'installation, à partir d'un CD ou d'un téléchargement, la suite des instructions est identique.



Depuis cette fenêtre, poursuivez en cliquant sur **Extract**.

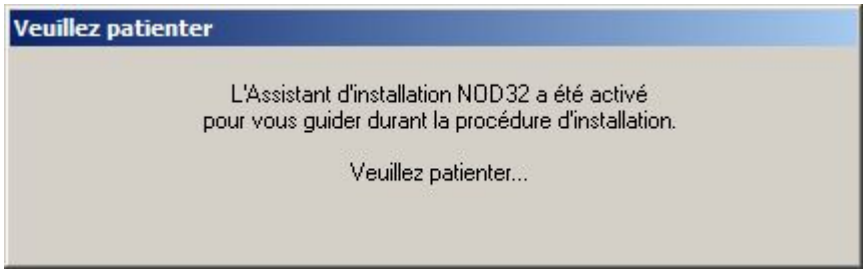
Le chemin du répertoire d'extraction peut être modifié dans le champ "**Extract to**" de la boîte de dialogue. Le changement n'affectera pas le répertoire d'installation final, seulement l'emplacement où les fichiers d'installation sont placés durant l'installation. Ces fichiers peuvent être supprimés à la fin de l'installation de NOD32.

Si vous installez NOD32 Antivirus System 64-bit sur un système compatible, le chemin d'extraction peut être différent : **C:\Program Files (x86)\ESET\Install**



Après avoir cliqué sur **Extract**, vous pourrez visualiser la liste des fichiers en cours de décompression sur le disque.

… ensuite, ce message apparaît durant quelques secondes :

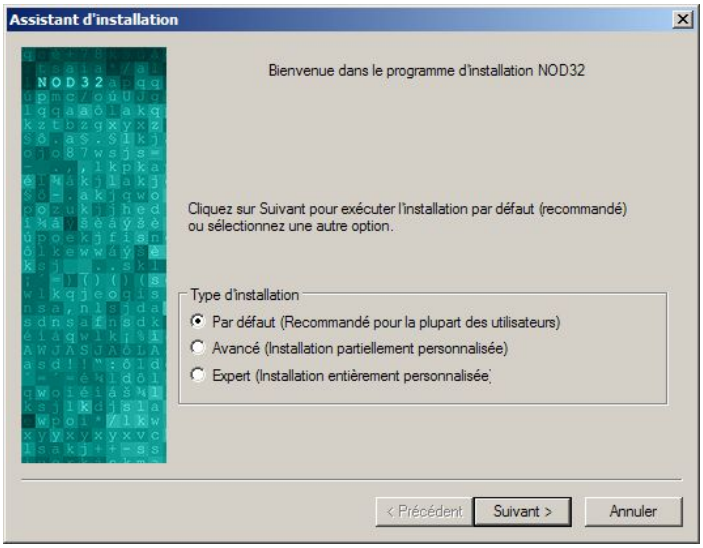


Dès que l'Assistant d'installation démarre, les trois types d'installation décrits ci-après vous sont proposés.

Choix du Type d'Installation de NOD32

Par défaut installe NOD32 avec les paramètres adaptés à un usage courant et prend la majorité des décisions concernant les paramètres d'installation à définir. Ce type d'installation est sélectionné par défaut* et est recommandé à la plupart des utilisateurs. (**La définition du terme "Par défaut" est disponible dans le Glossaire*)

Avancé 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.



Expert autorise une personnalisation et un contrôle total des différentes options disponibles via le processus d'installation, incluant le paramétrage SMTP de la messagerie pour l'envoi des alertes.

Ce guide décrit toutes les options d'installation pour chaque type. Elles sont clairement identifiées à leur type respectif : **Par défaut, Avancé** ou **Expert**, vous pouvez ainsi trouver facilement l'information pertinente.

Peu importe le type d'installation choisi, toutes les options sont modifiables après installation, **à l'exception** de la sélection du chemin d'installation, **de l'insertion de l'icône NOD32 sur le Bureau et de l'intégration du scanner à la demande dans le menu contextuel de la souris.**

Dans la plupart des cas, l'installation par défaut est donc plus simple et rapide.

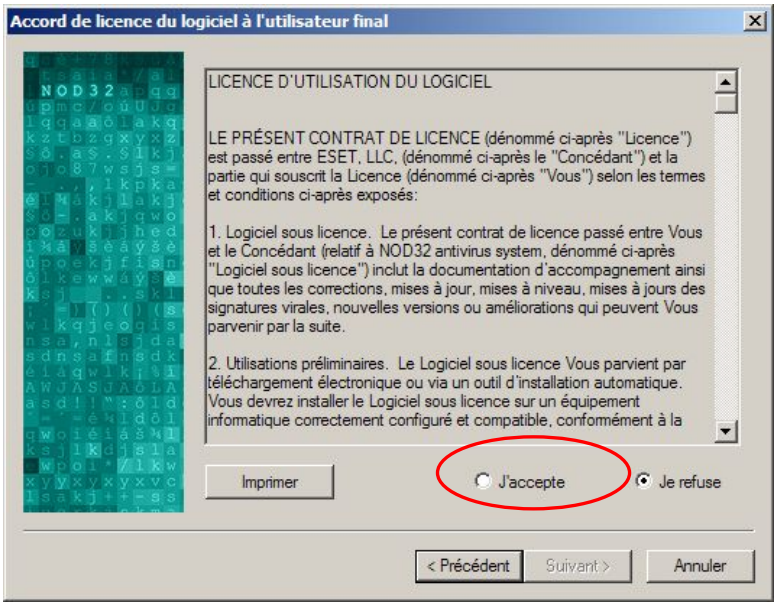
Un tableau récapitulatif des différentes options d'installation accessibles est disponible en **Annexe B** (page 51) **: Types d'installation.**

Si vous souhaitez modifier le chemin du répertoire d'installation sélectionné par défaut "**C:\Program Files\Eset**", l'installation doit être effectuée en mode **Avancé** ou **Expert**.

Accord de Licence à l'Utilisateur Final

Dans tous les types d'installation, l'écran suivant affichera le Contrat de licence. Veuillez en prendre connaissance, **cliquez sur** `J'accepte`, puis sur `Suivant>` pour poursuivre l'installation.

Vous êtes invité à lire attentivement les conditions d'utilisation de la licence. Si vous en refusez les termes, l'installation sera interrompue.



Vous pouvez également Imprimer le contrat de licence pour vous y référer ultérieurement.

Pour l'installation en mode Par défaut : voir directement la page 13

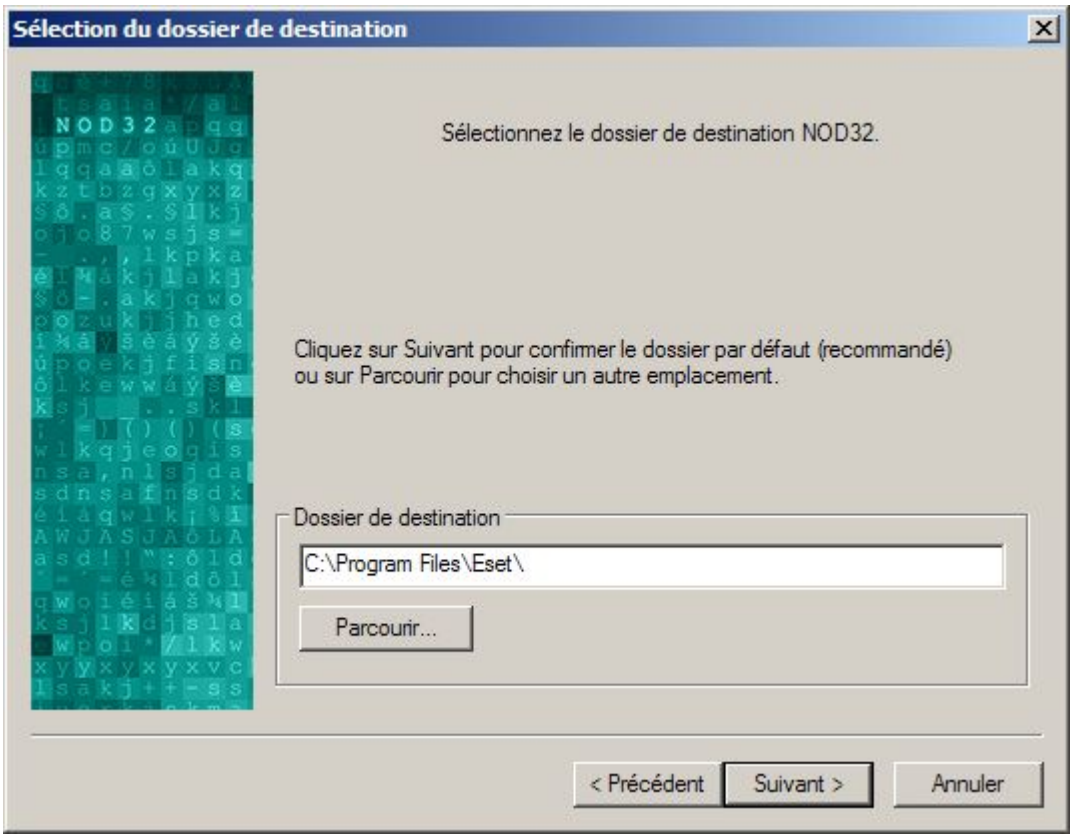
Pour l'installation en mode Avancé : continuer page suivante

Pour l'installation en mode Expert : continuer page suivante

Emplacement du Dossier de Destination du Programme

A ce stade, les modes d'installation **Avancé** et **Expert** vous permettent de modifier l'emplacement du dossier d'installation de NOD32.

Lors d'une installation de type **Par défaut**, cet écran n'est pas affiché.



Excepté si vous avez une raison spécifique de modifier le chemin du dossier d'installation - par exemple, si vous souhaitez installer NOD32 sur un disque différent - nous vous recommandons de conserver le dossier par défaut.

Une fois le chemin indiqué, cliquez sur **Suivant>** pour continuer.

Configuration des Mises à Jour Automatiques

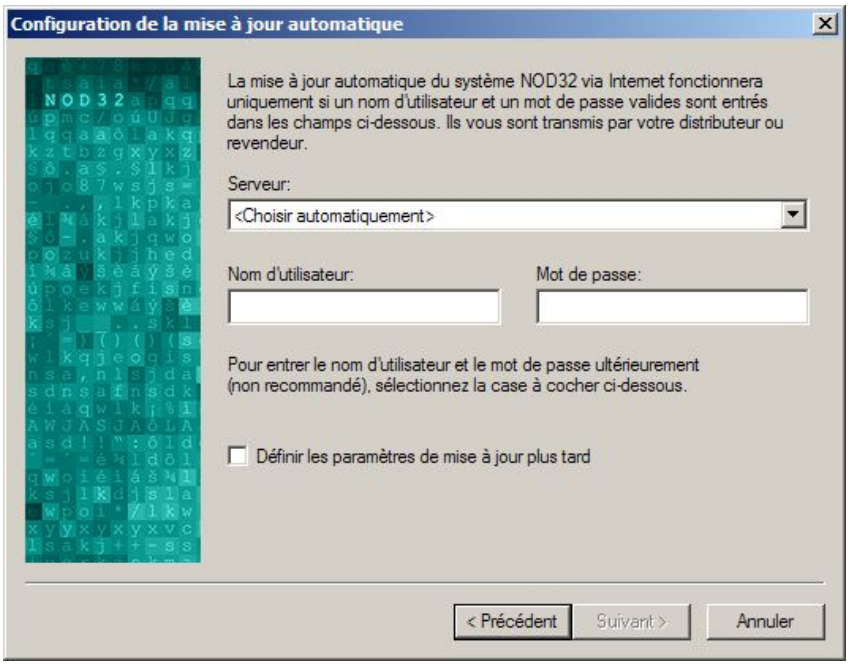
A ce niveau, les modes d'installation **Par défaut**, **Avancé** et **Expert** sont identiques.

Une fenêtre vous proposant de choisir le serveur de mise à jour s'affiche.

Nous vous recommandons vivement d'utiliser le paramètre **<Choisir automatiquement>**, qui garantit le mode d'obtention des mises à jour le plus fiable. Si vous ne saisissez pas votre **Nom d'utilisateur** et votre **Mot de passe** à ce stade de l'installation, NOD32 ne pourra pas bénéficier des mises à jour automatiques tant qu'ils ne seront pas renseignés.

Vous serez donc invité à fournir votre **Nom d'utilisateur** et votre **Mot de passe** pour permettre à NOD32 d'accéder aux serveurs de mises à jour d'Eset. Nous vous recommandons d'utiliser les fonctions *Copier* et *Coller*, afin d'éviter tout risque d'erreur lors du report de ces identifiants (sélectionnez le texte, cliquez sur Ctrl + C pour le Copier, puis Ctrl + V pour le Coller dans le champ approprié).

Si vous ne disposez pas de ces informations (fournies par e-mail après l'achat d'une licence et l'enregistrement de votre produit), cochez l'option **Définir les paramètres de mise à jour plus tard** pour poursuivre l'installation.



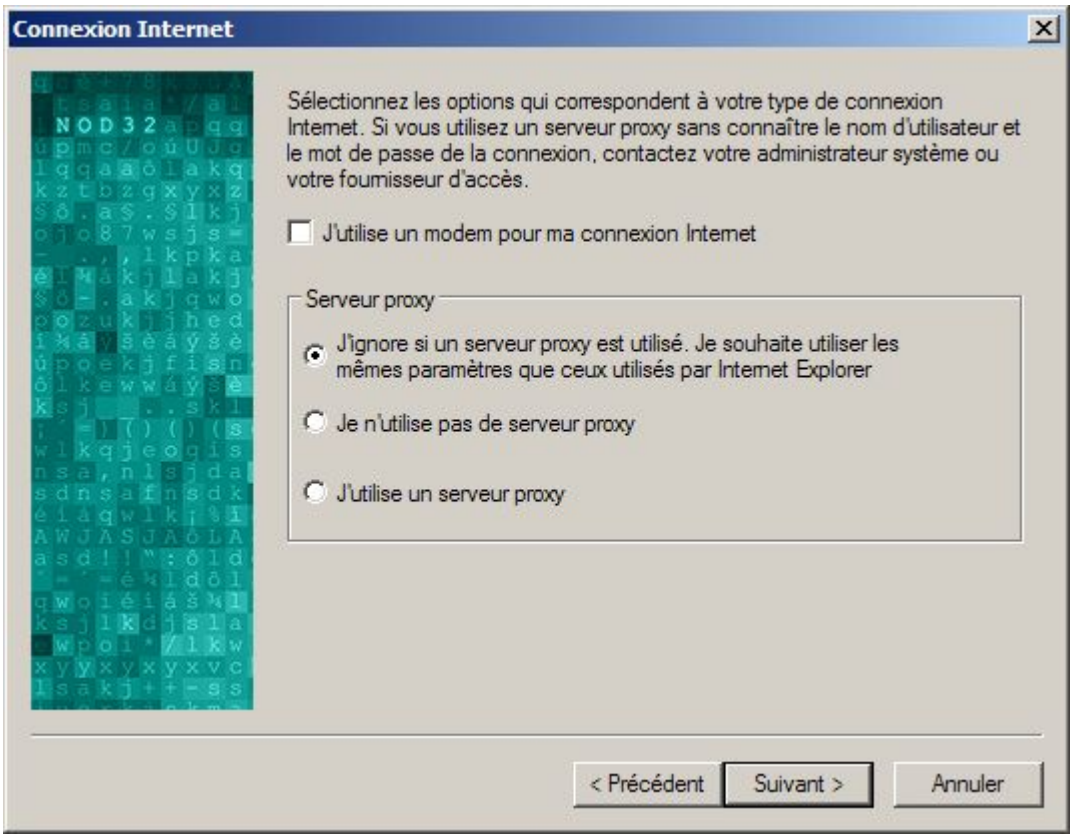
Rappel : tant que les identifiants ne seront pas saisis, la mise à jour de la base virale ne pourra pas s'effectuer et votre système ne sera pas protégé de manière optimale.

Configuration des Paramètres de Connexion à Internet

La fenêtre suivante est consacrée au paramétrage de votre connexion Internet.

Si vous utilisez un modem (pas à large bande ou interconnecté en réseau), cochez l'option **`J'utilise un modem pour ma connexion Internet`**, ce qui déclenchera le processus de mise à jour lorsqu'une connexion à Internet sera détectée.

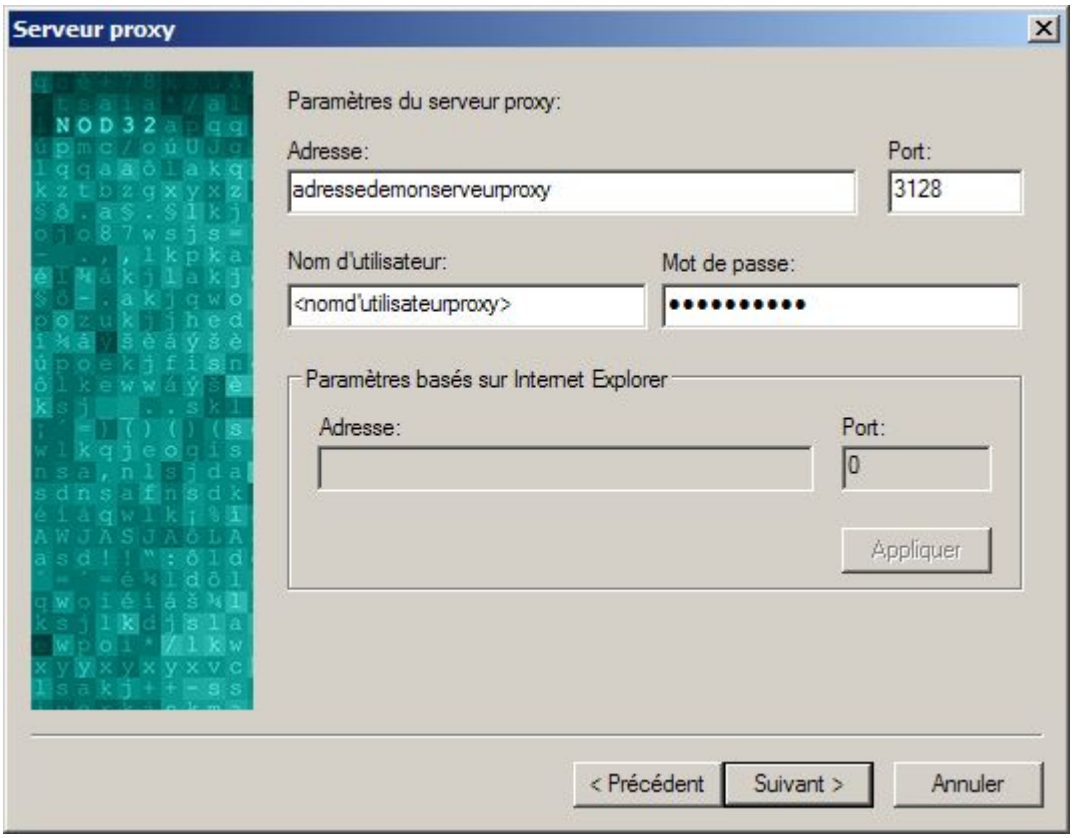
Cette fenêtre vous demandera également de préciser si vous utilisez un serveur Proxy. Si vous n'en utilisez pas ou n'êtes pas certain d'en utiliser un, acceptez le paramétrage par défaut, comme illustré ci-dessous, et NOD32 se chargera de détecter la configuration.



Serveur Proxy

Si vous êtes certain d'utiliser un serveur Proxy et que vous avez sélectionné l'option **J'utilise un serveur proxy**, la fenêtre ci-dessous s'ouvrira. Vous pourrez y spécifier les informations relatives au serveur Proxy.

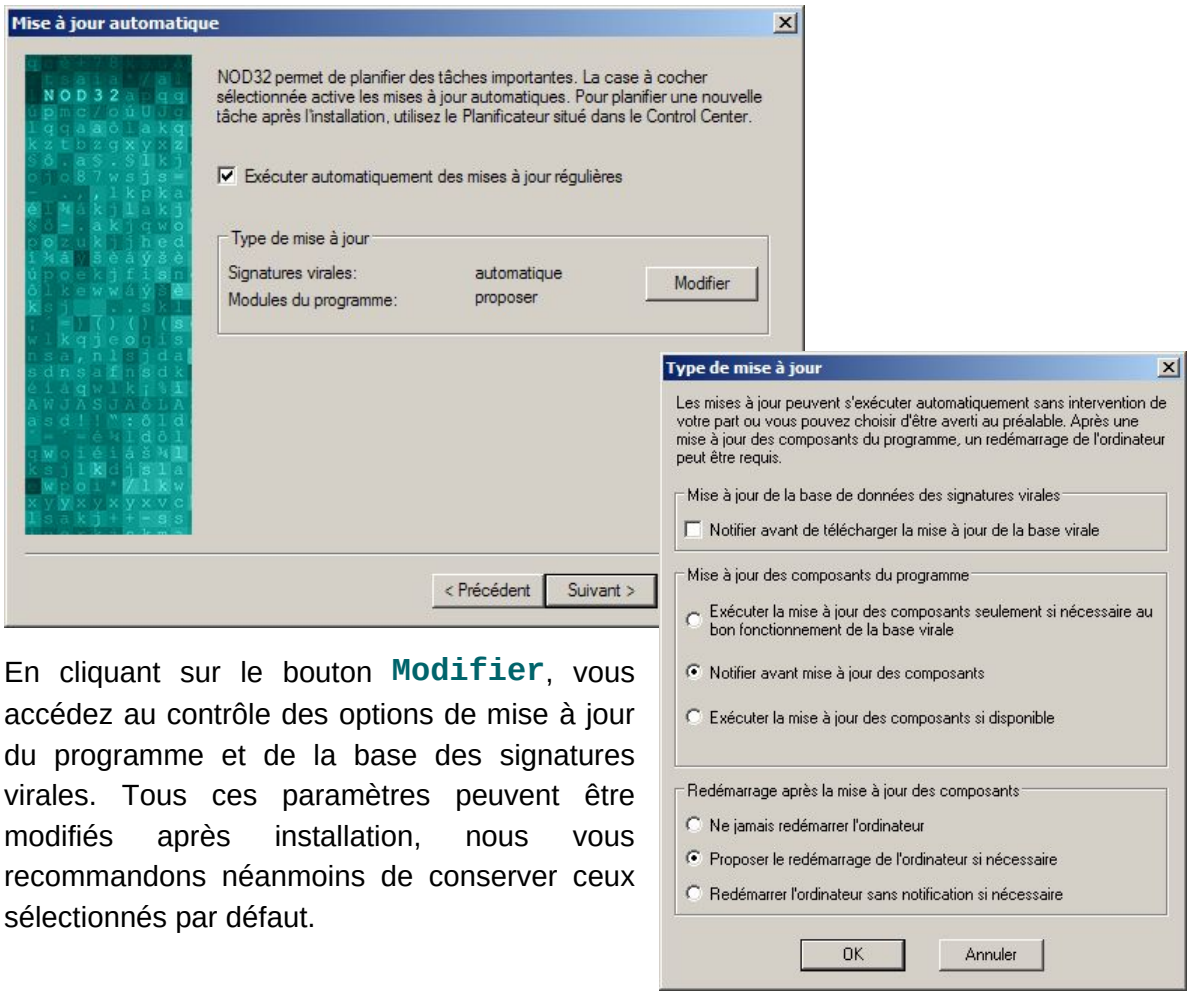
Le nom d'utilisateur et le mot de passe à saisir dans la fenêtre du **Serveur Proxy** sont uniquement nécessaires si votre Proxy requiert une authentification. Ils vous sont normalement communiqués par votre Administrateur ou fournisseur d'accès. Ne **PAS** saisir votre **Nom d'utilisateur** et votre **Mot de passe** NOD32 dans ces champs.



Lorsque vous avez terminé, cliquez sur **Suivant>** pour continuer l'installation.

Configuration de la Mise à Jour

Les modes d'installation **Avancé** et **Expert** vous permettent maintenant de configurer les options de mise à jour automatique.



En cliquant sur le bouton **Modifier**, vous accédez au contrôle des options de mise à jour du programme et de la base des signatures virales. Tous ces paramètres peuvent être modifiés après installation, nous vous recommandons néanmoins de conserver ceux sélectionnés par défaut.

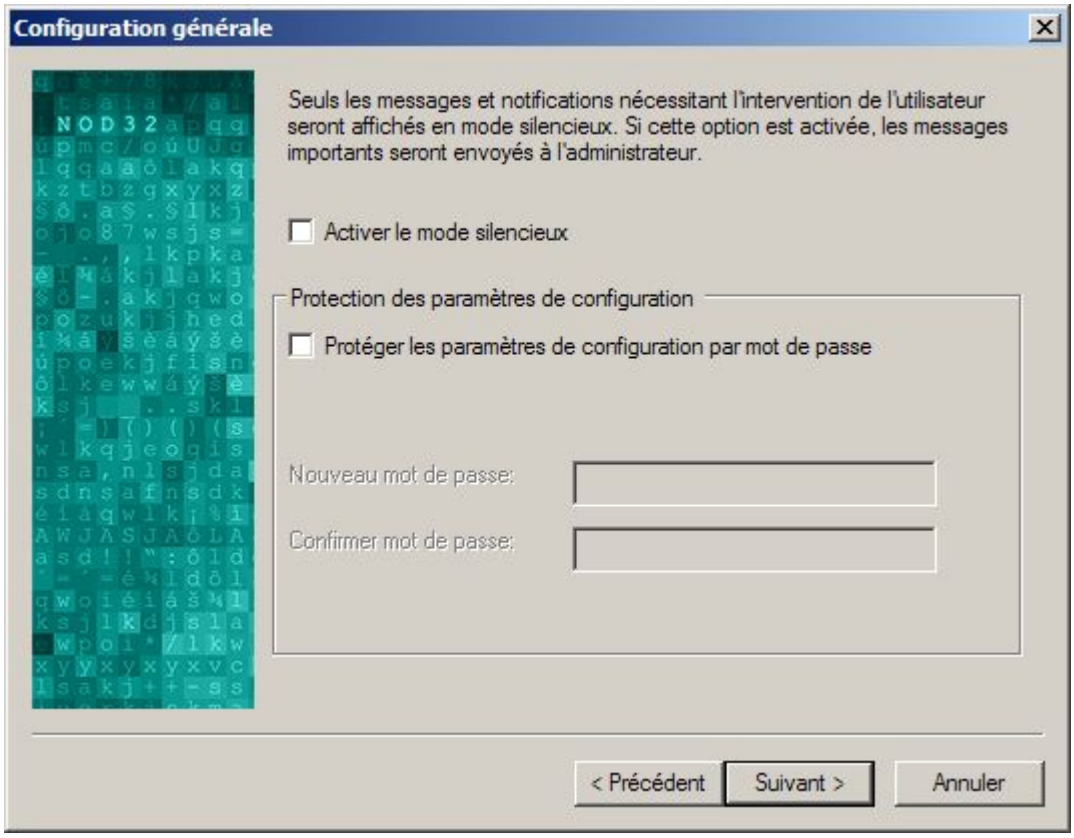
Eset délivre des mises à jour régulières afin d'actualiser l'ensemble de l'application et maintenir le niveau de protection de NOD32. Nous vous conseillons vivement de conserver l'option **Exécuter automatiquement des mises à jour régulières** activée, afin que votre ordinateur bénéficie de la meilleure protection possible.

Configuration Générale

Les modes d'installation **Avancé** et **Expert** vous proposent maintenant les options suivantes :

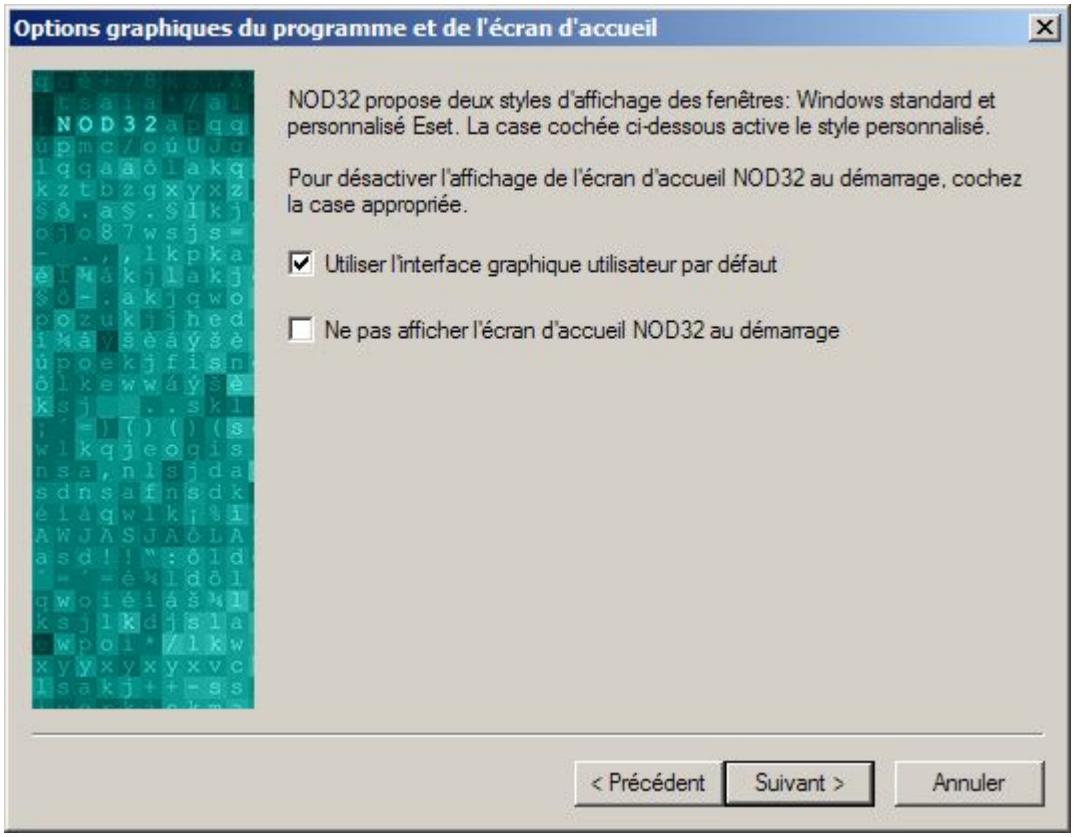
Activer le mode silencieux : cette option peut être sélectionnée si vous souhaitez que les messages ne requérant pas l'intervention de l'utilisateur soient envoyés directement à l'administrateur (défini ultérieurement).

Protéger les paramètres de configuration par mot de passe : si vous partagez un ordinateur avec d'autres utilisateurs et que vous ne souhaitez pas qu'ils puissent modifier la configuration de NOD32, vous pouvez définir un mot de passe (il doit être différent de votre **Mot de passe** NOD32). Vous serez ainsi le seul utilisateur à pouvoir modifier la configuration des paramètres.



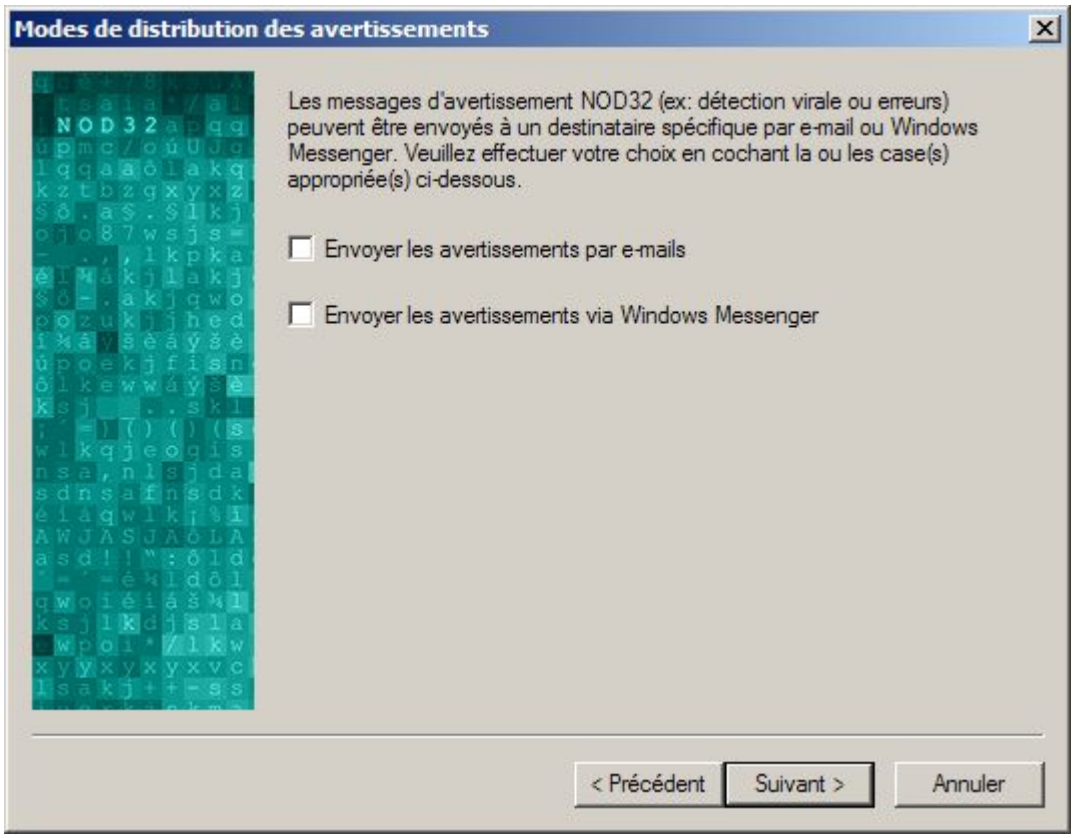
Options graphiques

A ce stade, le mode **Expert** vous propose d'utiliser l'interface standard de Windows ou celle de NOD32 (sélectionnée par défaut), et de désactiver l'affichage de "l'écran d'accueil" (petite fenêtre contenant des informations sur NOD32) qui apparaît à chaque démarrage de Windows.



Modes de distribution des avertissements

Si vous souhaitez envoyer des messages/notifications, par exemple à l'Administrateur, cette fenêtre vous offre 2 possibilités : envoyer les messages par e-mails et/ou via Windows Messenger. Si vous êtes particulier ou travailleur indépendant, vous n'avez pas besoin de cocher ces options.



>> SMTP / Options de la Messagerie

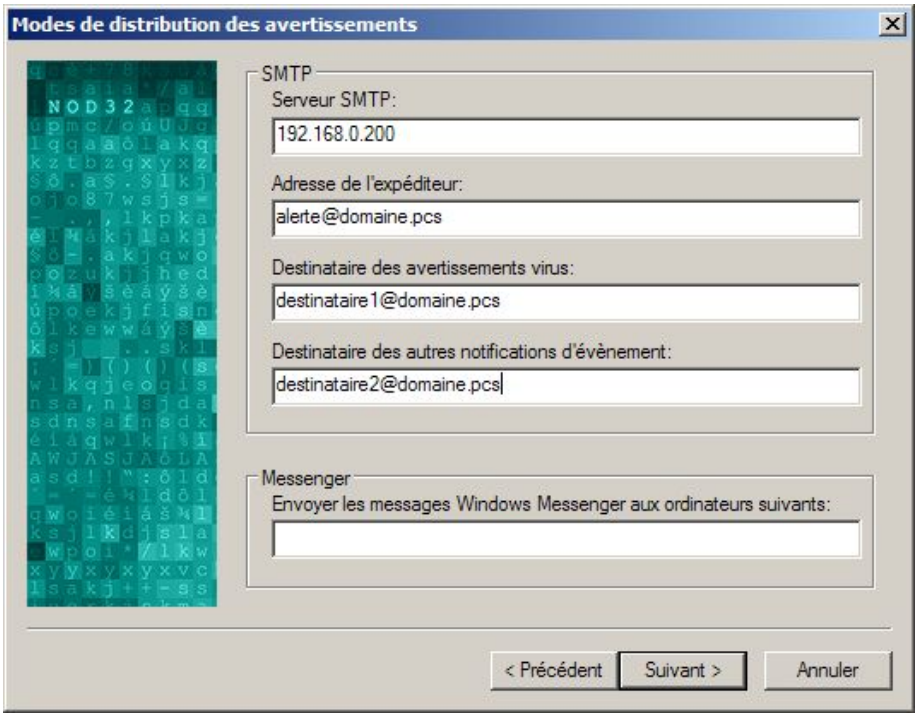
Le mode **Expert** vous permet de configurer les options d'alertes et de messagerie.

Si votre serveur SMTP requiert une authentification, vous pouvez avoir à configurer ces paramètres une fois l'installation de NOD32 terminée. A ce stade, vous pourrez seulement renseigner les informations concernant les adresses.

NOD32 offre plusieurs options pour l'envoi des messages, qui sont particulièrement utiles pour les ordinateurs en réseau, lorsqu'un administrateur doit surveiller plusieurs machines. Pour configurer ces options, les éléments suivants doivent être renseignés:

Adresse du Serveur SMTP, ou adresse du serveur de messagerie

Adresse(s) du ou des destinataire(s) par défaut, et adresse de l'expéditeur



***Note**: Les informations incluses dans la capture d'écran ci-dessus ont été ajoutées à titre d'exemple pour illustrer les différentes options. Les champs de ces options seront vides lorsque l'écran s'affichera.*

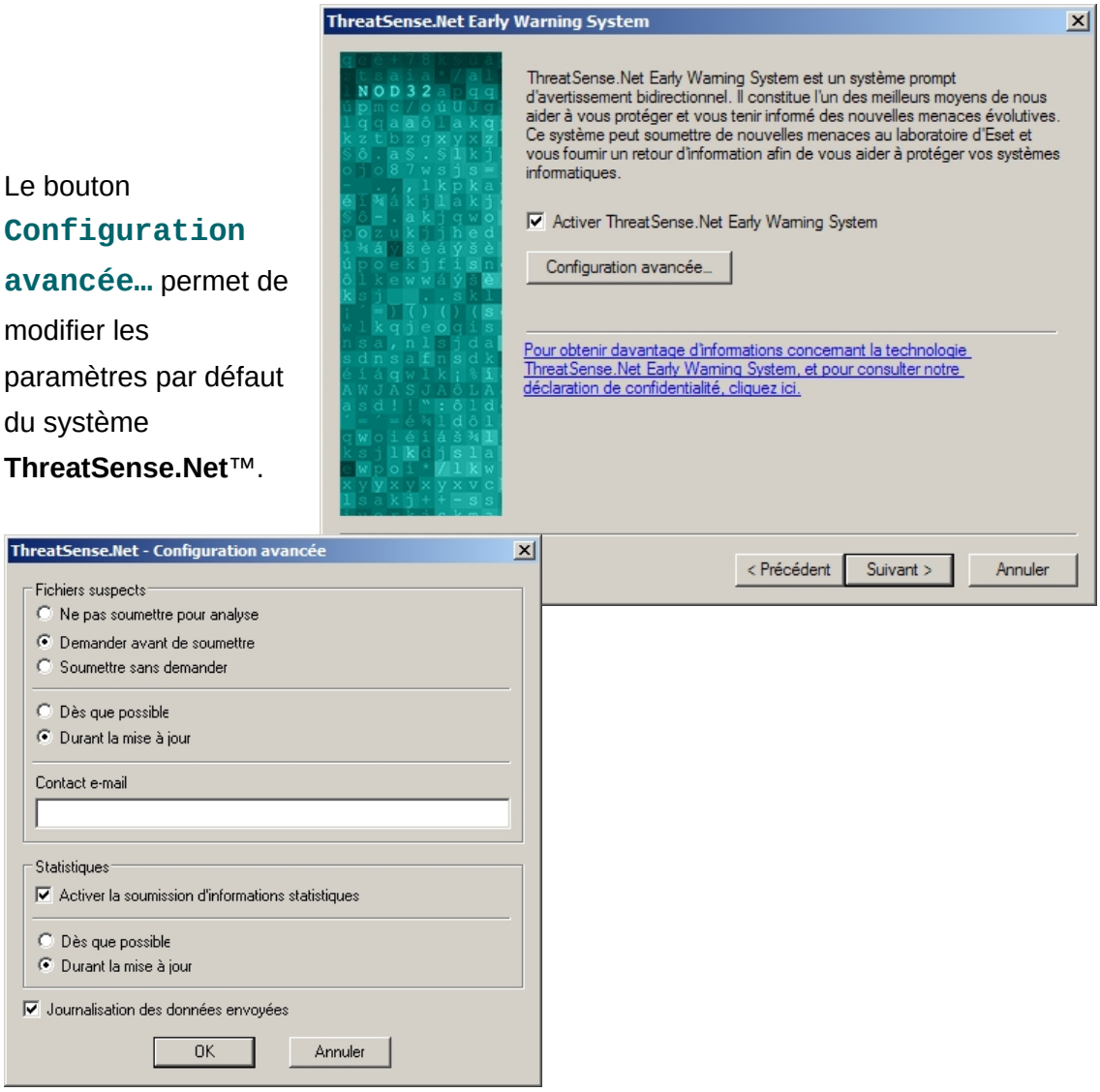
Si dans la boîte de dialogue précédent celle-ci (en page 19), aucune case n'a été sélectionnée, la fenêtre illustrée ci-dessus ne sera pas affichée. Si vous n'avez pas coché l'une des cases relatives à ces options dans la boîte de dialogue précédente, les champs appropriés seront grisés dans la fenêtre ci-dessus.

Le système ThreatSense.Net™

A ce niveau, les modes d'installation **Avancé** et **Expert** sont identiques.

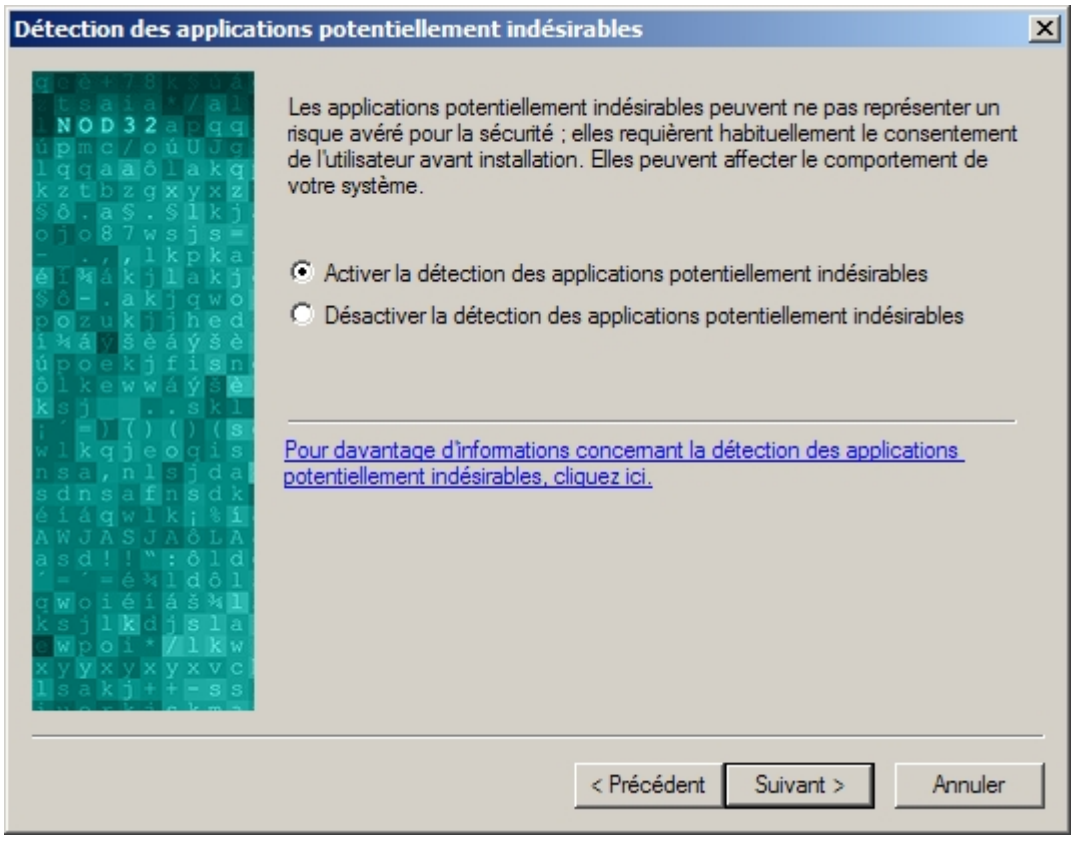
Le système **ThreatSense.Net**™ permet une soumission automatique des informations statistiques et des fichiers suspects aux laboratoires d'Eset pour y être analysés. Si vous choisissez d'activer le système **ThreatSense.Net**™, ce dernier collectera et enverra les données de manière totalement anonyme. Ces informations permettront à Eset d'être toujours plus réactif face aux nouvelles menaces (voir également page 47).

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



Détection des applications potentiellement indésirables

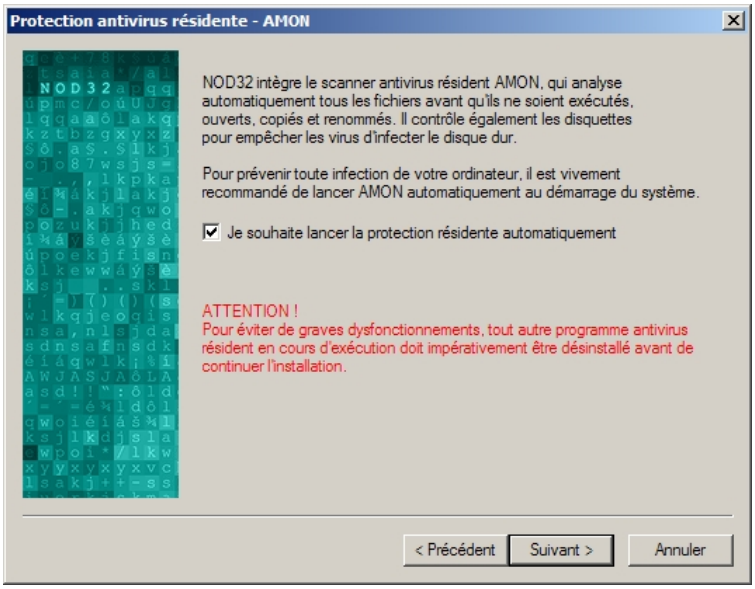
A ce niveau, les modes d'installation **Par défaut**, **Avancé** et **Expert** sont identiques.



Certaines entreprises publicitaires ou ayant pour vocation de tracer vos activités se plaignent des moteurs de détection identifiant leurs programmes en tant que logiciels publicitaires (adware) ou expressément comme logiciels espions (spyware). NOD32 v2.7 intègre une détection spécifique des "Applications potentiellement indésirables", incluant certains logiciels publicitaires et autres applications n'étant pas nécessairement malveillantes. Bien que ces programmes ne présentent pas forcément un risque avéré pour la sécurité, certains logiciels publicitaires viendront étoffer le nombre de fichiers sur votre ordinateur et la consommation en mémoire, ce qui peut s'avérer agaçant, voire gênant, pour de nombreux utilisateurs.

Configuration d'AMON (Active MONitor): résident

Tous les modes d'installations comportent la fenêtre suivante.



AMON est le scanner « à l'accès », qui analyse constamment toutes les actions sur votre système. Le lancement automatique au démarrage de Windows est vivement conseillé. AMON étant la ligne de défense la plus importante du système de protection, il est crucial qu'il soit activé en permanence (et que la base des signatures virales soit à jour).

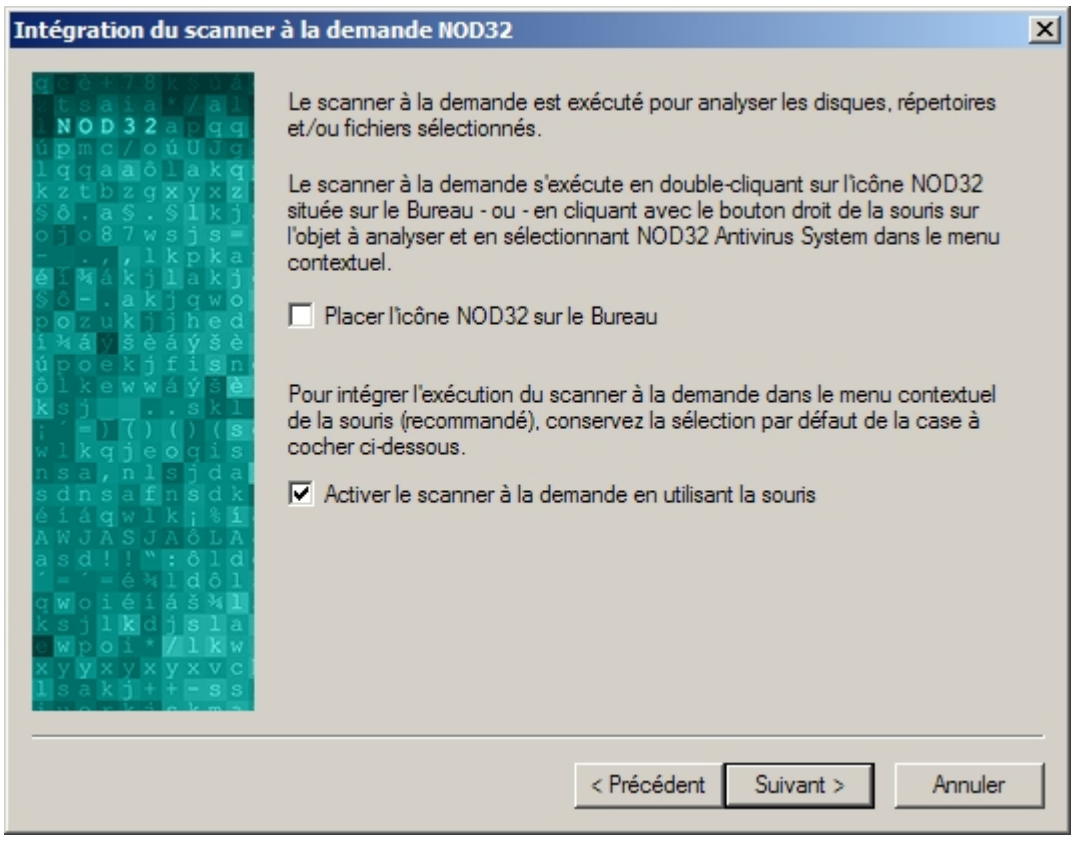
Sauf dans des conditions d'utilisation particulières ou en cas de nécessité absolue, AMON ne doit pas être désactivé ou arrêté.

ATTENTION ! Si l'option **Je souhaite lancer la protection résidente automatiquement** est décochée, AMON ne sera pas chargé en mémoire et votre ordinateur ne sera pas protégé en temps réel des virus et autres programmes malveillants.

Assurez-vous qu'aucun autre programme antivirus n'est en cours d'exécution sur votre ordinateur avant de cocher cette option, autrement votre système pourrait subir d'importantes instabilités, pouvant elles-mêmes conduire à la perte de données.

Options pour le Scanner à la Demande

La configuration de l'intégration de l'analyse **à la demande** dans le menu contextuel de la souris est disponible dans les modes d'installation **Expert/Avancé**



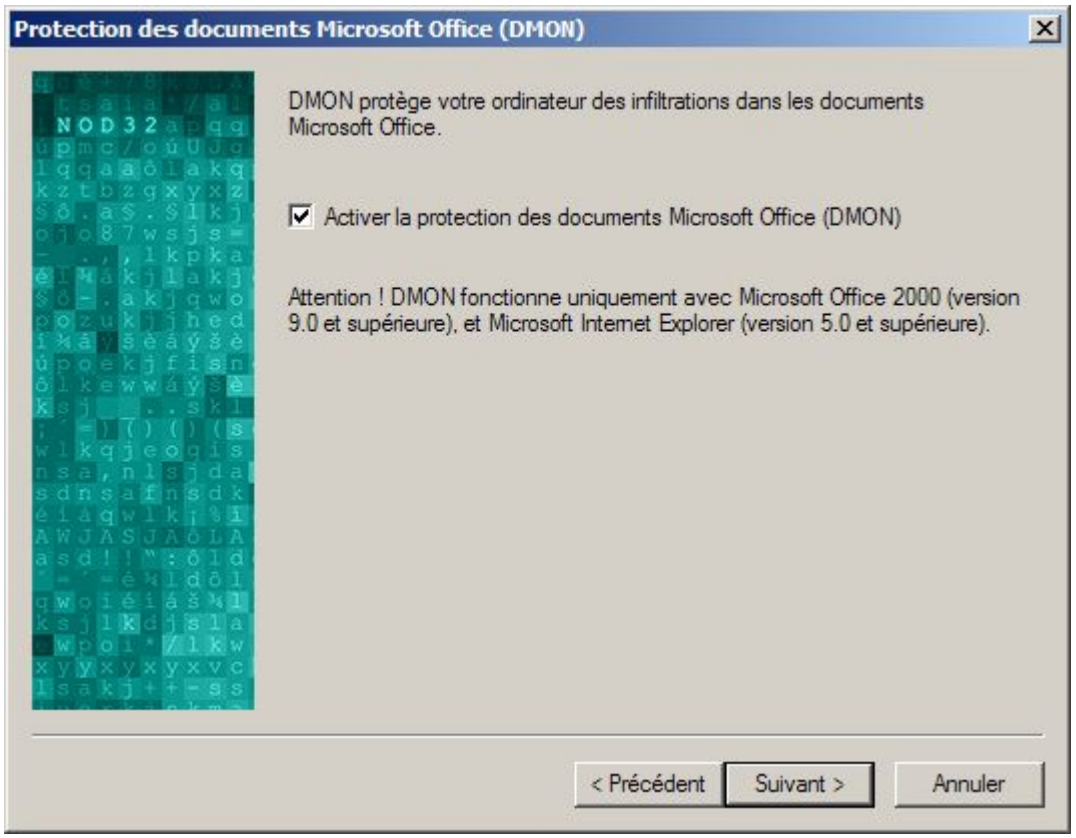
Pour permettre un accès plus rapide au Scanner à la demande NOD32, une icône peut être placée sur le **Bureau**. Si vous ne souhaitez pas activer cette option, laissez la case **Placer l'icône NOD32 sur le Bureau** décochée.

L'accès au Scanner à la demande NOD32 via le menu contextuel, correspondant à l'option **Activer le scanner à la demande en utilisant la souris**, vous permet d'analyser plus facilement un répertoire ou fichier avant de l'ouvrir, en effectuant un clic droit sur la cible et en sélectionnant **NOD32 Antivirus System** depuis le menu contextuel. L'intégration dans le menu contextuel peut être désactivée en décochant la case appropriée (**non recommandé**).

Aucune des deux options précitées ne peut être activée après installation si elle a été désactivée depuis cet écran. Le programme devra alors être réinstallé pour activer ces options.

Configuration de DMON (Document MONitor)

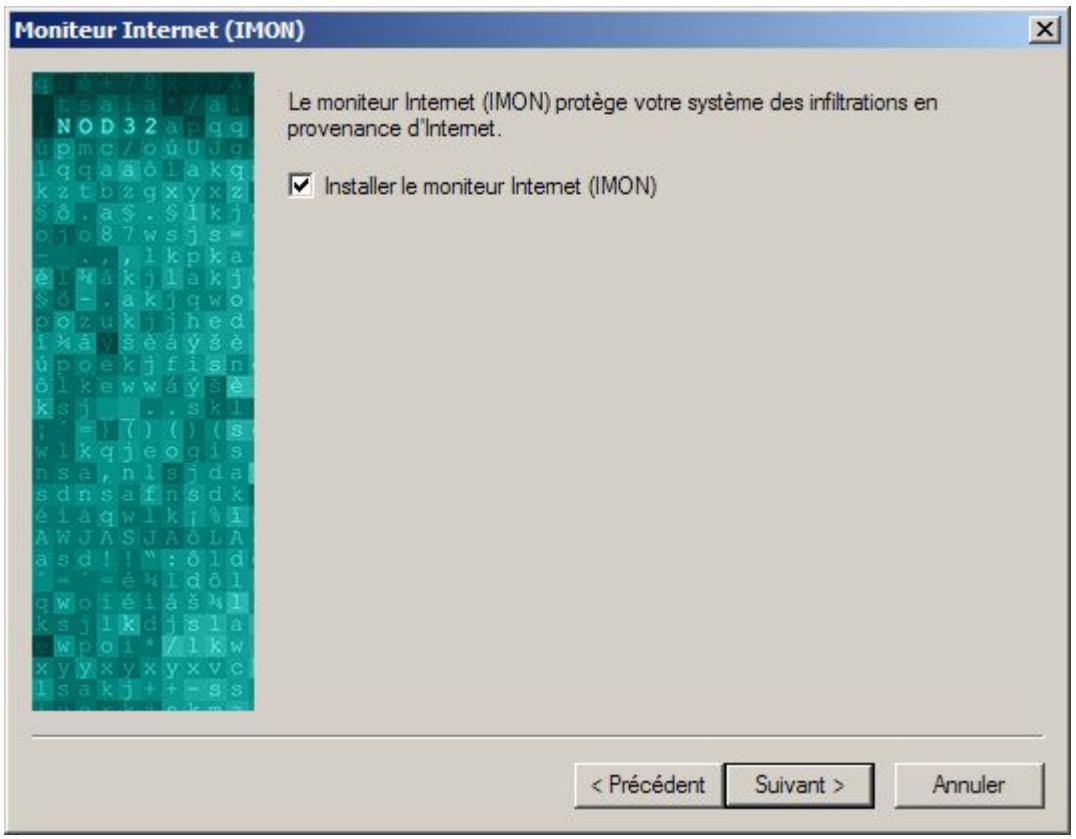
Les documents Microsoft Office (Word, Excel, etc.) peuvent également contenir des virus qui infectent d'autres fichiers lorsque les documents sont ouverts. DMON assure une protection contre ce type de menaces. Les plus récentes versions d'Internet Explorer permettent d'ouvrir les documents Microsoft Office depuis le navigateur, directement à partir d'Internet. DMON contrôlera ces documents et préviendra toute infection.



DMON est activé par défaut dans tous les types d'installation, mais vous pouvez toutefois le désactiver dans les modes **Avancé** et **Expert**.

NOTE : la protection des documents traités avec des Suites bureautiques autres que MS Office est pleinement assurée par AMON.

Configuration du Moniteur Internet (IMON)



IMON (**I**nternet **MON**itor) protège votre ordinateur des menaces en provenance d'Internet, dans les e-mails ou lors de la navigation. Pour permettre l'analyse des e-mails utilisant le protocole POP3, ainsi que celle du trafic Internet, nous vous recommandons d'installer le moniteur IMON.

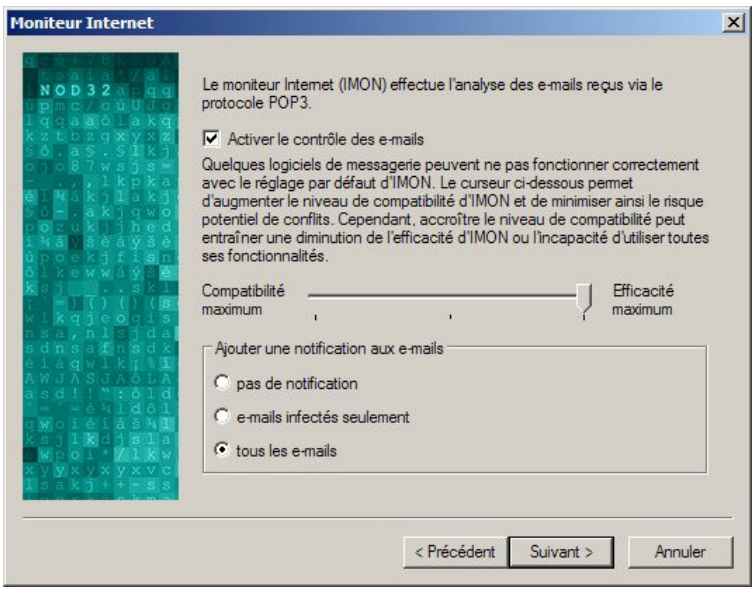
IMON est activé par défaut dans tous les types d'installation, mais vous pouvez le désactiver si nécessaire dans les modes **Avancé** et **Expert**.

Si IMON est désactivé, le module AMON préviendra toujours l'ouverture de pièces jointes infectées, enregistrées à partir des e-mails et d'Internet. Toutefois, il est vivement recommandé d'activer IMON lors de vos séances de navigation et lorsque vous téléchargez/consultez vos e-mails.

IMON – Configuration pour le Courrier Electronique

Pour activer le contrôle des e-mails, laissez la case correspondante cochée.

Une notification, attestant que le message a été analysé par NOD32, peut être ajoutée à la fin de chaque e-mail ou aux e-mails infectés seulement. L'accès à ces options est disponible dans les modes **Avancé** et **Expert**.



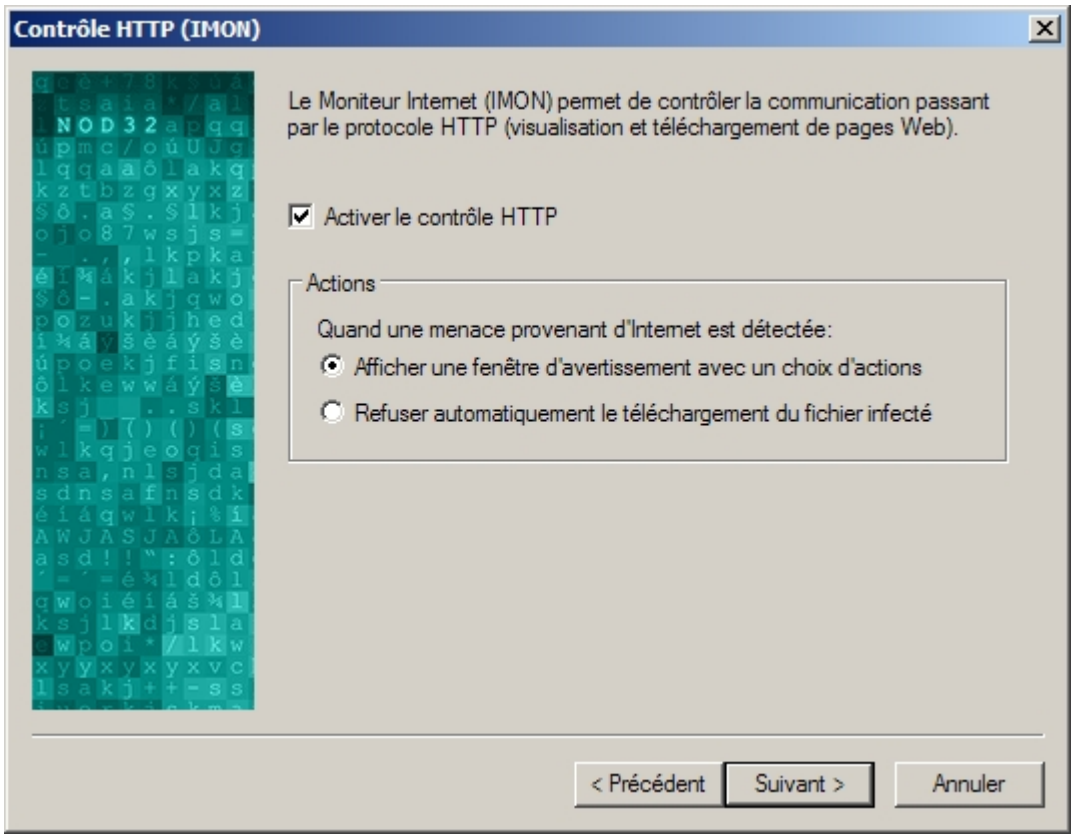
IMON fonctionne avec la majorité des logiciels de messagerie POP3. Toutefois, dans de rares cas, des phénomènes d'incompatibilité peuvent survenir. Si cette situation se présente, vous pouvez augmenter le niveau de compatibilité d'IMON en déplaçant le curseur vers la gauche, afin d'en assurer le bon fonctionnement.

Attention ! Augmenter la compatibilité d'IMON peut entraîner la désactivation de certaines fonctionnalités, ou une réduction de son niveau d'efficacité.

Lorsque NOD32 est installé sur un serveur, l'installation du moniteur IMON n'est généralement pas recommandée. Pour de plus amples informations techniques à ce sujet, nous vous invitons à contacter votre revendeur ou distributeur local.

IMON - Configuration HTTP

IMON contrôle également le trafic Internet et vous protège ainsi des infiltrations véhiculées par votre navigateur.

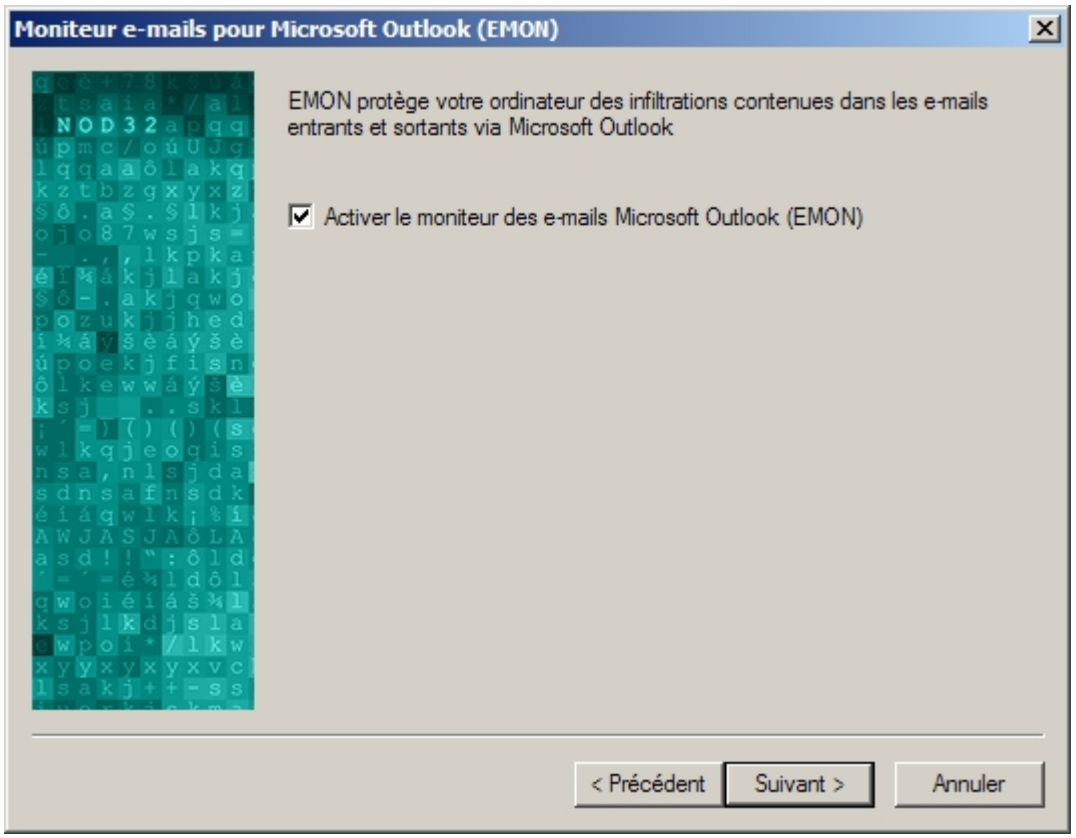


En cas de tentative d'infiltration, l'option sélectionnée par défaut dans la fenêtre ci-dessus déclenchera l'affichage d'une fenêtre d'avertissement, vous offrant le choix des actions disponibles. IMON peut également être configuré de manière à refuser automatiquement le téléchargement du fichier infecté.

Le contrôle du flux HTTP est activé par défaut, mais peut être désactivé ou modifié dans les modes d'installation **Avancé** et **Expert**.

EMON – Configuration pour le Courrier Electronique

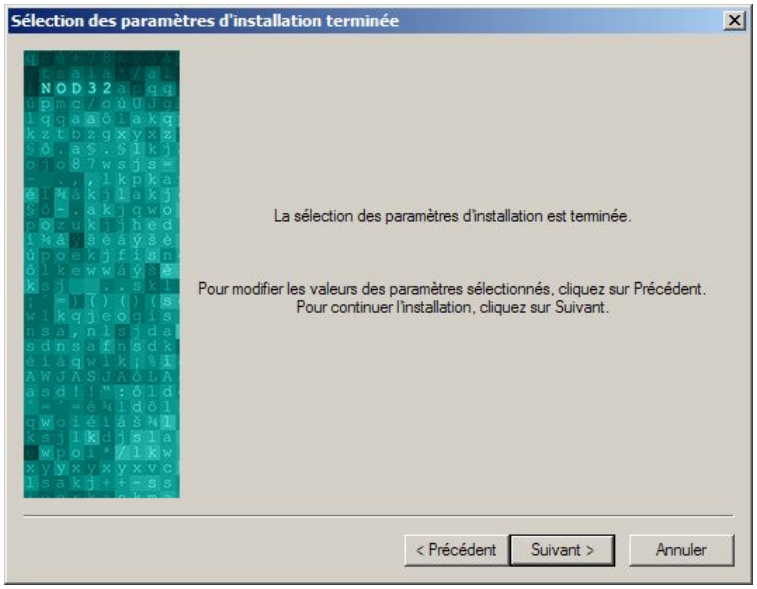
EMON, module résident, analyse vos e-mails entrants et sortants via les logiciels de messagerie compatibles MAPI (l'interface MAPI est utilisée : par Microsoft Outlook - lors de la réception des e-mails à partir d'un serveur de messagerie Microsoft Exchange via le protocole Exchange).



Même si aucune interface MAPI n'est utilisée sur votre ordinateur, EMON sera installé. Les e-mails entrants via le protocole POP3 **seront analysés par IMON**.

Compléter la Configuration de l'Installation

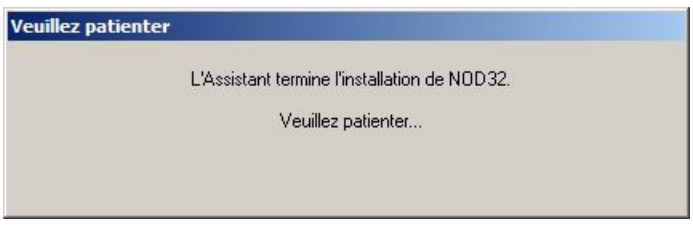
A ce point, tous les modes d'installation affichent la même fenêtre. C'est le dernier stade vous permettant de modifier les paramètres sélectionnés précédemment, avant que les fichiers ne soient copiés et la configuration prise en compte.



Si vous souhaitez modifier un ou plusieurs paramètre(s) de configuration, cliquez sur le bouton **< Précédent**. **Si vous avez activé le lancement automatique du module AMON, assurez-vous qu'aucun autre résident antivirus (scanner à l'accès) n'est actif sur votre ordinateur avant de terminer l'installation.**

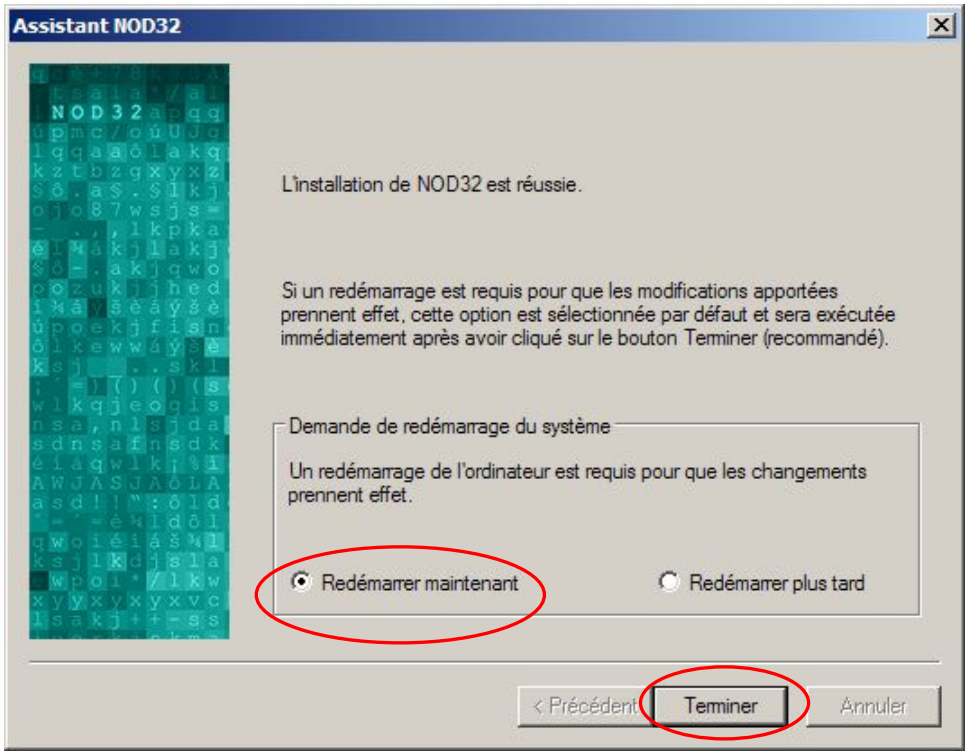
Pour compléter l'installation avec les paramètres de configuration sélectionnés, cliquez sur **Suivant >**.

Durant la procédure de prise en compte de la configuration, ce message est affiché:



Une fois l'installation complétée, un redémarrage de votre ordinateur sera requis.

Enregistrez vos travaux et fermez les applications en cours d'exécution, si ce n'est déjà fait, puis cliquez sur **Terminer** pour redémarrer votre système.



Si vous ne souhaitez pas redémarrer votre ordinateur immédiatement, choisissez **Redémarrer plus tard**. NOD32 peut alors ne pas fonctionner correctement, et votre ordinateur ne sera pas protégé des infiltrations virales avant que vous ne le redémarriez et n'effectuiez la première mise à jour.

Une fois votre PC redémarré, ouvrez le Control Center en cliquant sur l'icône, située dans la barre des tâches. Cliquez ensuite sur le module **Mise à jour**, puis lancez la procédure de mise à jour en cliquant sur **Mettre à jour.** Lorsque la mise à jour est terminée, cliquez sur le module **NOD32**, puis sur **Analyse approfondie,** afin d'effectuer une analyse en profondeur de votre ordinateur.

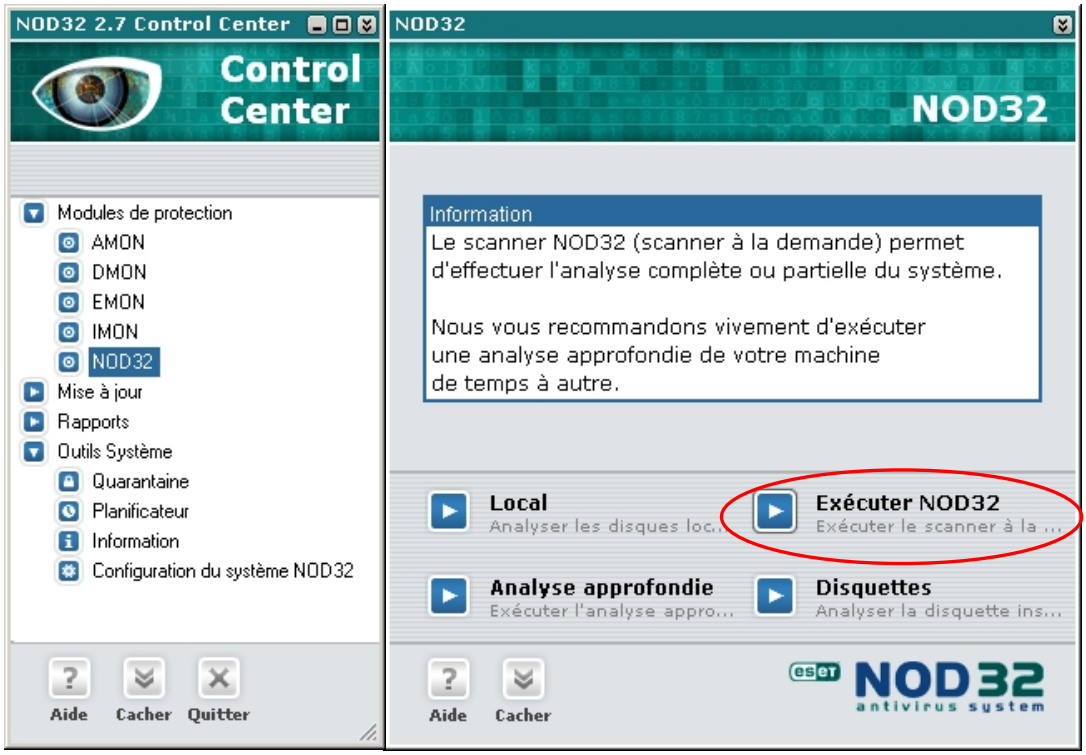
CONFIGURATION APRES L'INSTALLATION

Profils pour les analyses à la demande

Les premiers paramètres que vous pouvez souhaiter examiner sont les profils d'analyse par défaut de NOD32. Ils vous permettent d'analyser exactement ce que vous souhaitez et quand vous le souhaitez, le Planificateur de tâches supportant également ces profils. Un profil est constitué par l'ensemble des paramètres sélectionnés pour une analyse. Par exemple, vous pouvez visualiser en page 33 les paramètres de l'onglet **`Configuration`**, sélectionnés par défaut en utilisant le *[Profil du Control Center] (standard),* puis en page 45, ceux sélectionnés via le *[Profil du Control Center - Analyse approfondie]*.

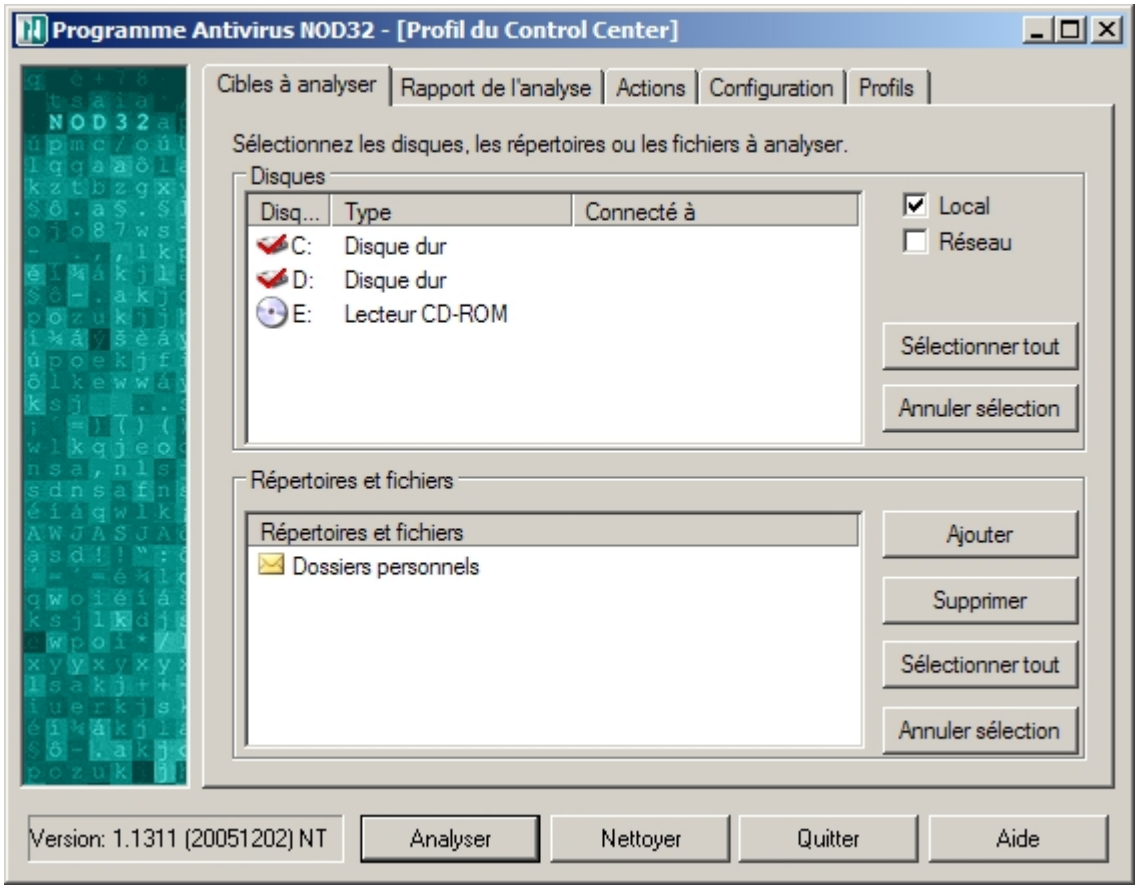
Ouvrez le Control Center NOD32 en cliquant sur l'icône , située dans la barre des tâches.

Dans la section *Modules de protection*, cliquez sur NOD32



… puis, dans la fenêtre qui apparaît sur la droite, cliquez sur **`Exécuter NOD32.`**

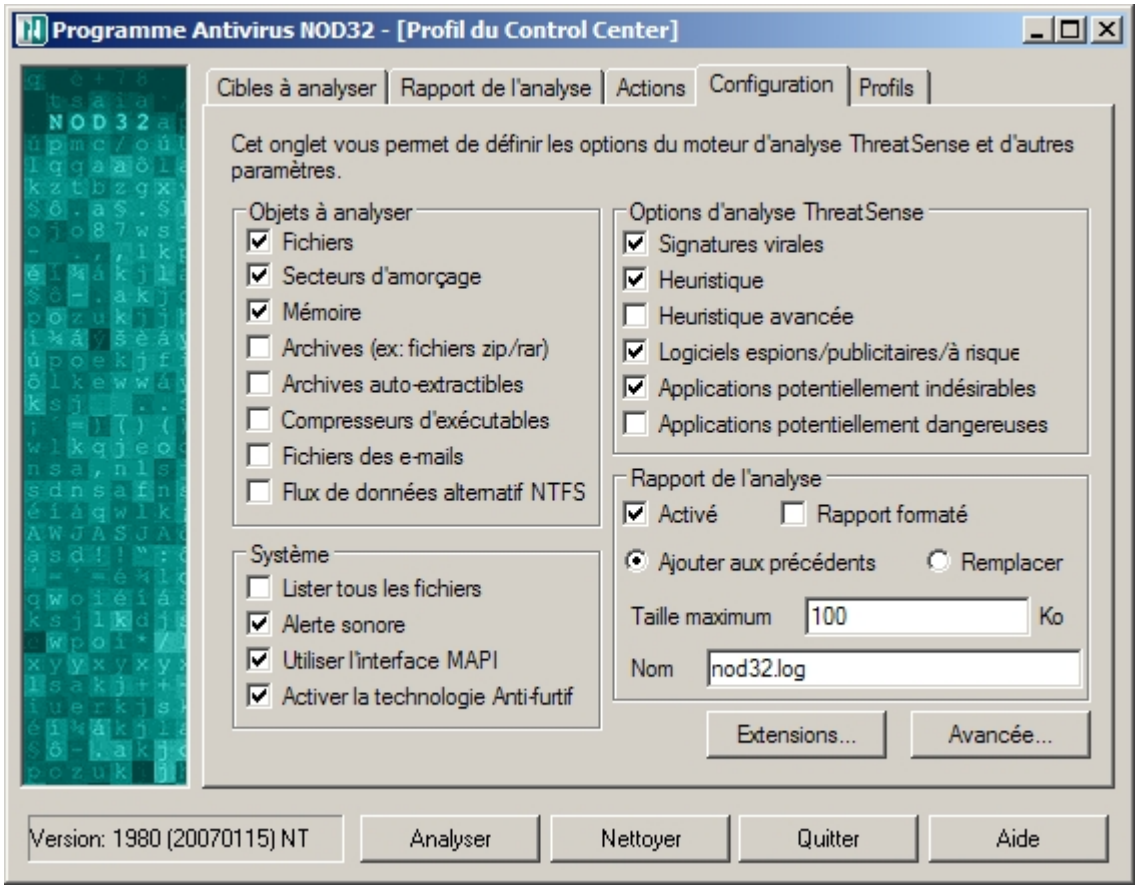
Après quelques secondes, l'onglet **Cibles à analyser** s'ouvre :

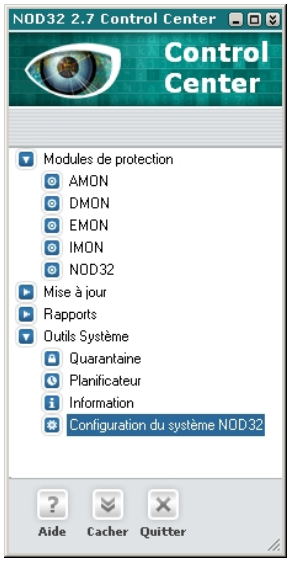


Cette fenêtre répertorie les cibles à analyser. Vous pouvez sélectionner les disques, supports amovibles, etc., à analyser, et également ajouter les répertoires et fichiers de votre choix.

Les cibles sélectionnées affichent un sigle rouge en forme de « V » sur leurs icônes respectives.

Dans l'onglet **Configuration**, vous pouvez modifier les paramètres par défaut pour sélectionner vos préférences personnelles concernant les éléments qui doivent être analysés par le scanner à la demande. Vous pouvez ajouter ou exclure certains types de fichiers, si désiré, et également paramétrer l'envoi des messages d'avertissement vers une autre machine ou l'administrateur, via le bouton **Avancée…**

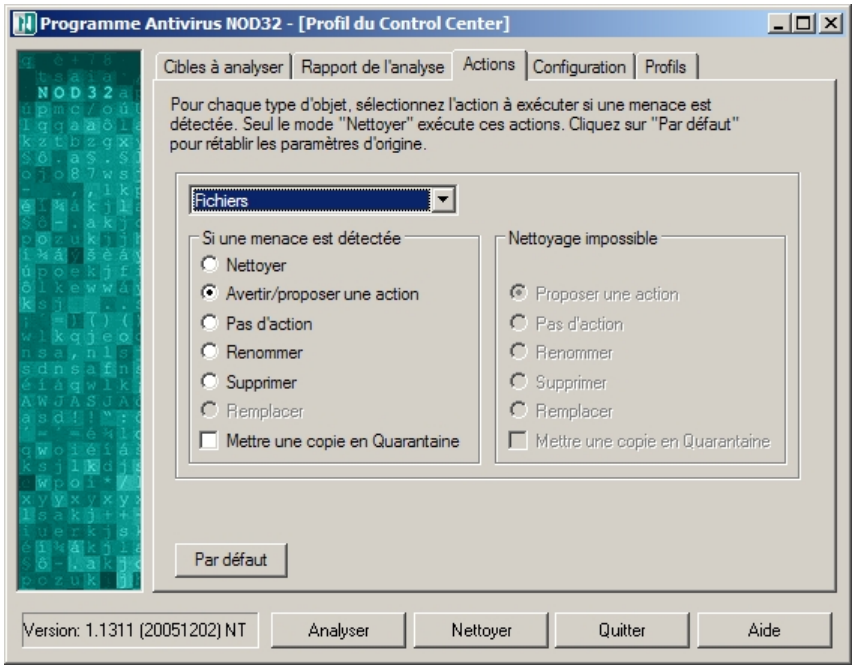




Les détails de la configuration des notifications (messages d'avertissement) doivent être renseignés depuis la section **Configuration du système NOD32** → **Configuration** → onglet **Notifications**.

Dans l'onglet **Actions**, vous pouvez maintenant modifier les actions par défaut à exécuter en cas d'attaques virales.

Vous pouvez sélectionner une action différente par type d'objets. La liste des types d'objets disponibles dépend elle-même des Objets à analyser qui ont été sélectionnés dans l'onglet **Configuration** :



> Fichiers
> Secteurs d'amorçage
> Mémoire
> Archives
> Archives auto-extractibles
> Compresseurs d'exécutables
> Fichiers des e-mails
> Flux de données alternatif NTFS

Pour la majorité des types d'objets, vous pouvez mettre les fichiers infectés ou suspects en Quarantaine, ce qui signifie qu'une copie de ces fichiers sera placée dans un dossier créé à cet effet (**C:\Program Files\ESET\infected**). La copie peut alors être envoyée à Eset pour analyse approfondie, si nécessaire.

NOTE : le répertoire **infected** est créé automatiquement lors de la première mise en Quarantaine. La copie mise en Quarantaine est sauvegardée dans un format encrypté, rendant impossible toute exécution accidentelle.

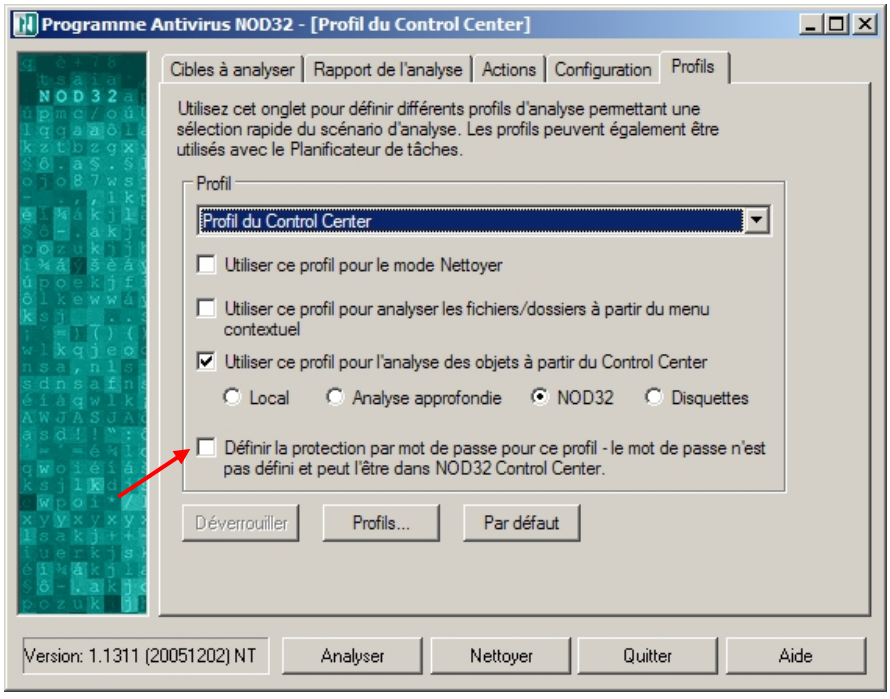
Si vous choisissez l'option **Nettoyer**, la liste d'actions alternatives devient alors accessible dans la colonne de droite **Nettoyage impossible**. L'action secondaire choisie est uniquement appliquée lorsqu'un fichier s'avère impossible à nettoyer pour des raisons techniques.

Voir la rubrique **Traitement des alertes et incidents d'origine virale**, en page 46, pour davantage d'information.

Le dernier onglet de la section est dédié aux **Profils**. Un profil est constitué d'un ensemble de paramètres. Par défaut, le programme utilisera le profil du Control Center, mais si vous avez effectué des changements dans les onglets précédents, vous pouvez maintenant les enregistrer sous le profil en cours d'utilisation ou décider d'en créer un nouveau.

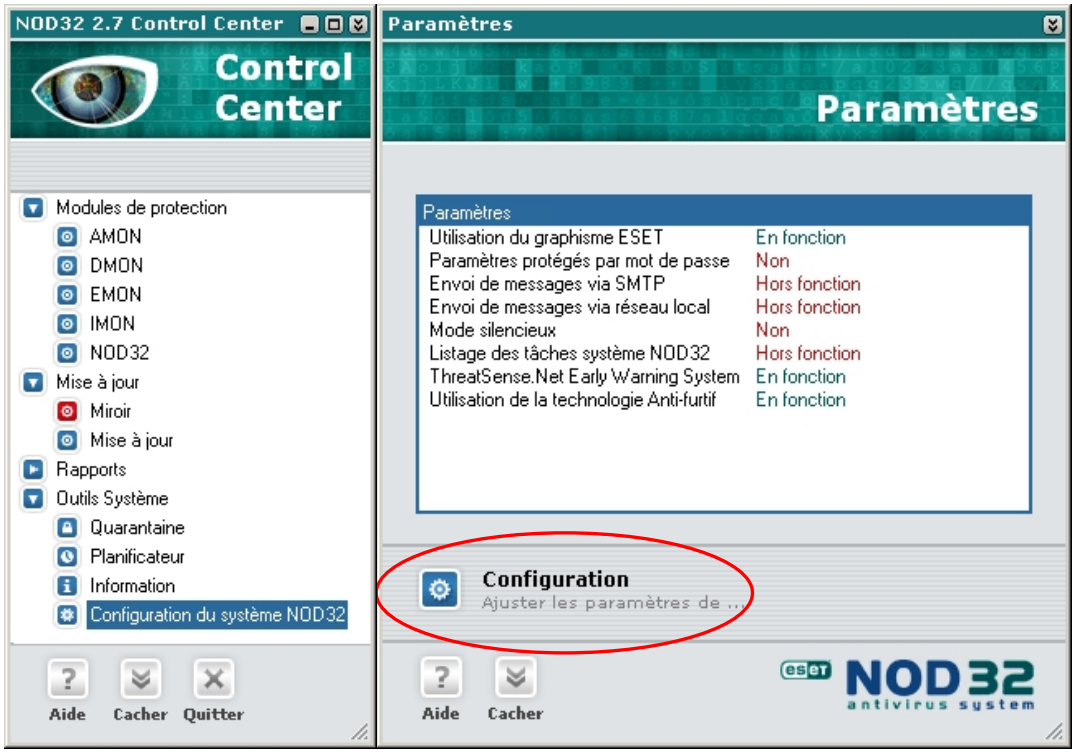
Le profil d'origine pour l'analyse depuis le menu contextuel (accessible via le menu déroulant) peut également être modifié et sauvegardé. Ce profil est dédié à l'analyse rapide de fichiers ou dossiers individuels, en effectuant directement un clic droit sur la cible choisie et en sélectionnant **NOD32 Antivirus System** dans le menu contextuel qui apparaît alors. Cette option est particulièrement conviviale lorsque vous souhaitez analyser rapidement un élément avant de l'ouvrir.

Si vous souhaitez que le profil en cours d'utilisation ou de modification soit également utilisé pour l'analyse via le menu contextuel, ou à partir du Control Center, cochez la ou les case(s) appropriée(s) après avoir sélectionné le profil désiré.



En fonction des besoins, vous pouvez créer un profil différent pour analyser certains supports spécifiques. Pour créer un nouveau profil, cliquez sur le bouton **Profils** → **Nouveau**, entrez alors le nom du nouveau profil, puis validez. Vous pouvez alors sélectionner les paramètres de votre choix au fil des différents onglets et les sauvegarder sous ce nouveau profil.

Chaque profil peut être protégé par un mot de passe (option pointée par une flèche rouge en page 35). Cette fonctionnalité s'avère très utile si vous partagez votre ordinateur avec plusieurs autres utilisateurs et que vous ne souhaitez pas qu'ils puissent modifier vos paramètres NOD32. Pour définir votre mot de passe, ouvrez la fenêtre principale du Control Center, en cliquant sur l'icône située dans la barre des tâches. Cliquez sur **Configuration du système NOD32**,



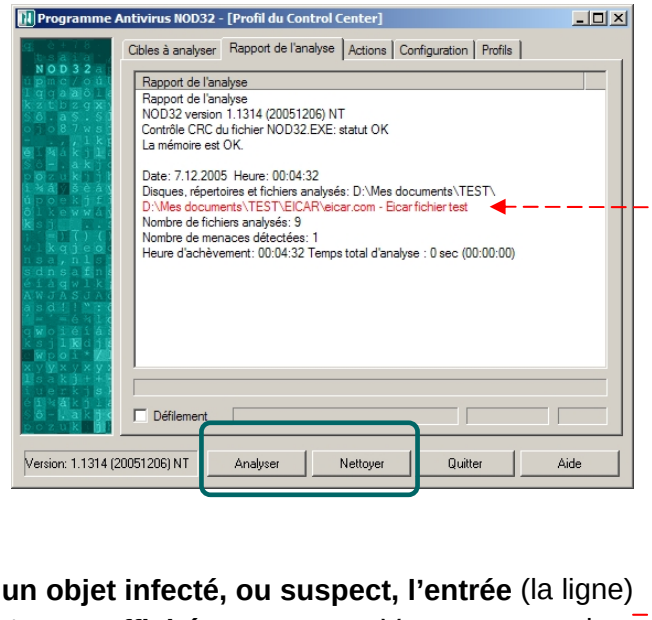
… puis sur **Configuration** dans la fenêtre de droite. Dans l'onglet **Général** qui s'ouvre, dans la section **Protection des paramètres de configuration**, cliquez sur **Configuration**. Choisissez un mot de passe différent de celui de qui vous a été envoyé avec votre **Nom d'utilisateur**. En cas d'oubli du mot de passe qui protège les paramètres de configuration, vous pouvez déverrouiller NOD32 en téléchargeant notre outil de déverrouillage à l'adresse : http://www.eset.sk/unlock.exe.

NOTE : le module **Miroir**, présent sous la section **Mise à jour** de la capture d'écran ci-dessus, est uniquement disponible dans la version multipostes (Administrator) de NOD32. Ce module est dédié à la mise à jour des stations de travail en réseau. La couleur rouge de l'icône indique que le Miroir est désactivé.

Enfin, l'onglet **Rapport de l'analyse** affiche les résultats détaillés de l'analyse, mais également sa progression.

Bouton Analyser

Cliquer sur le bouton **Analyser** aura pour effet de lancer une analyse des supports sélectionnés dans l'onglet **Cibles**. Vous verrez ensuite la liste des fichiers analysés s'afficher dans la fenêtre. Par défaut, seuls les fichiers faisant l'objet d'un commentaire particulier inscrit en **bleu** sont listés (voir page 38). Pour lister tous les fichiers analysés, cochez l'option **Lister tous les fichiers** depuis l'onglet **Configuration**.



Si le scanner à la demande détecte un objet infecté, ou suspect, l'entrée (la ligne) **du rapport** correspondant à cet objet **sera affichée en rouge**. Vous pouvez alors choisir de cliquer sur le bouton **Nettoyer** (ce qui aura pour effet de relancer une analyse complète en appliquant les options sélectionnées dans l'onglet *Actions*), ou plus simplement d'effectuer un clic droit sur l'entrée du rapport inscrite en rouge et sélectionner **Nettoyer** (si applicable) dans le menu contextuel. Cette dernière méthode est la plus rapide.

Bouton Nettoyer

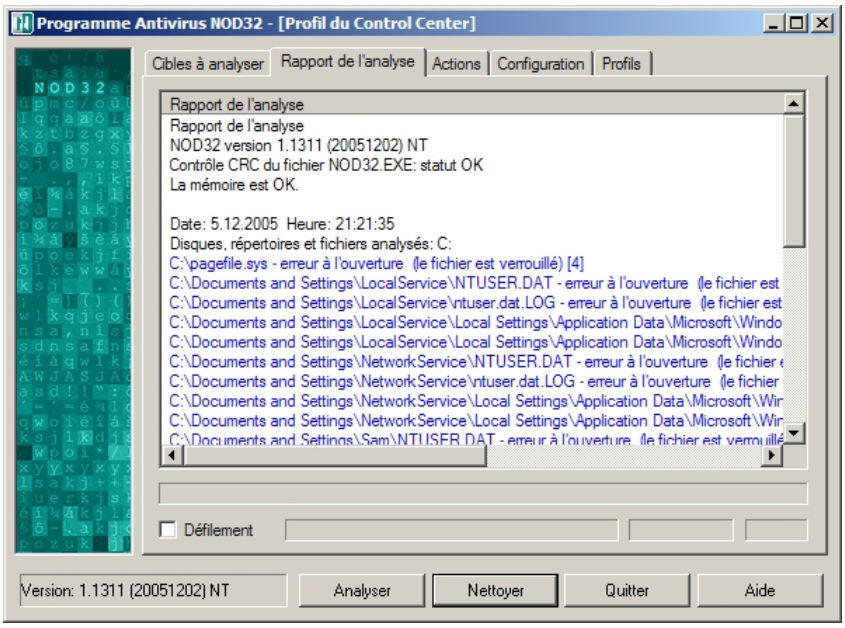
Ce bouton a également pour effet de lancer une analyse des supports sélectionnés, mais les actions choisies dans l'onglet Actions (Nettoyer, Proposer une action, Pas d'action, Supprimer, Remplacer, Mettre une copie en quarantaine) sont alors appliquées automatiquement.

Une fois l'analyse lancée, les boutons **Analyser** et **Nettoyer** se transforment respectivement en **Pause** et **Arrêter**, dans l'hypothèse où vous souhaiteriez suspendre temporairement ou mettre un terme à l'analyse.

NOTE : le mode **Analyser** permet d'effectuer une analyse sans interruption, même en cas de détection d'une ou plusieurs infiltration(s). Aucune action n'est appliquée et les objets infectés sont uniquement listés en rouge dans la fenêtre Rapport de l'analyse. A l'inverse, le mode **Nettoyer** suspend l'analyse - si l'action sélectionnée dans l'onglet Actions ne peut être exécutée ou si elle requiert une intervention de l'usager - tant que l'utilisateur n'a pas sélectionné une action alternative.

Analyse

Le déroulement de l'analyse via le bouton **Analyser** ne requiert pas de surveillance en temps réel. Ce mode est fort pratique, il vous permet par exemple de lancer une analyse avant de partir déjeuner, puis de visualiser son résultat et la liste des entrées à votre retour. L'analyse peut prendre de quelques secondes à plusieurs minutes, en fonction du nombre de cibles à analyser et de la profondeur de l'analyse. **Les objets infectés sont inscrits en rouge** et leur chemin d'accès est indiqué. Vous savez ainsi où ces fichiers sont localisés sur votre ordinateur.



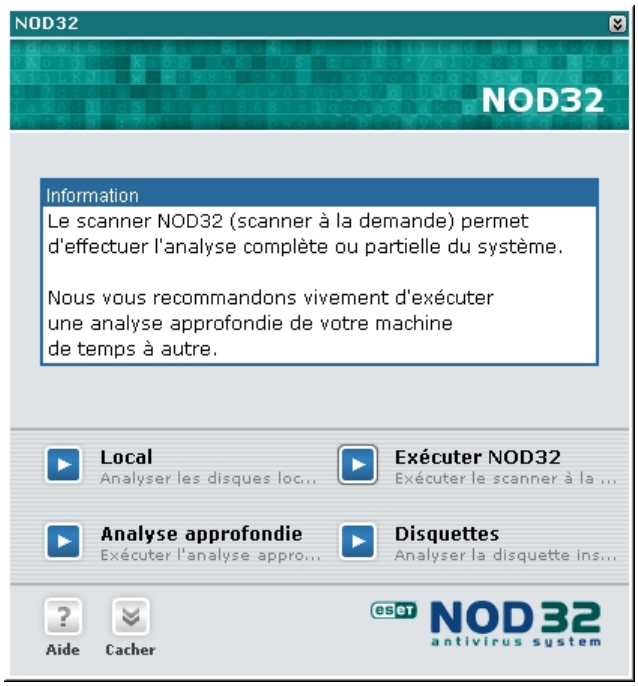
Dans la capture d'écran ci-dessus, vous pouvez noter la présence de **C:\pagefile.sys** – erreur à l'ouverture (le fichier est verrouillé) [4]. Sur les ordinateurs dont le système de mise en veille prolongée est actif, vous noterez également l'élément **C:\hiberfil.sys**. La présence de ces deux fichiers dans le rapport est parfaitement normale, ils sont verrouillés car utilisés exclusivement par votre système d'exploitation. Aucune autre application, pas même NOD32, n'a l'autorisation d'y accéder.

A tout moment, vous pouvez consulter les précédents **Rapports du scanner NOD32** via le Control Center, sous la section **Rapports**.

Le **Rapport des menaces** détectées, ainsi que le **Rapport** relatif aux évènements (comme les Mises à jour, les erreurs de connexion, etc.) sont également disponibles.

Analyse à la Demande

Lorsque vous souhaitez réaliser une analyse de votre ordinateur, d'un support, tel un CD, etc., rendez-vous dans le Control Center, puis sous la section **Modules de protection**, cliquez sur **NOD32**. La fenêtre suivante apparaît alors sur la droite.



Cliquez au choix sur :

Exécuter NOD32 pour ouvrir la fenêtre *Cibles à analyser* du scanner à la demande, comme décrit dans les pages précédentes, et modifier les paramètres d'analyse si vous le désirez.

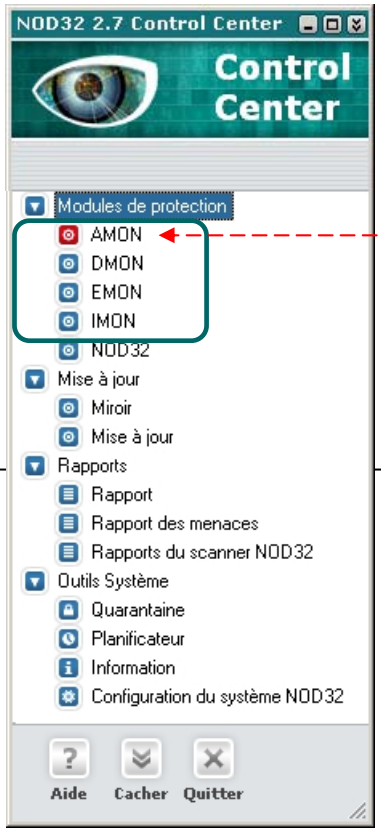
Disquettes pour démarrer instantanément l'analyse de toute disquette.

Analyse approfondie pour analyser directement votre système encore plus en profondeur qu'avec le niveau d'analyse standard (le temps d'analyse est en revanche un peu plus long). Le jeu de paramètres sélectionnés par défaut assure le meilleur niveau de détection possible.

NOTE : Une analyse approfondie du système est vivement recommandée après une première installation de NOD32, tout particulièrement si vous suspectez votre ordinateur d'être infecté. Elle est également conseillée périodiquement et/ou en cas de doute (par exemple, si votre système présente un comportement inhabituel pouvant être imputable aux méfaits d'un malware).

Local pour analyser directement tous vos disques locaux.

Analyse à l'Accès (AMON)



Lorsque vous ouvrez, copiez, renommez un fichier, AMON vérifie automatiquement et en temps réel l'intégrité de ce fichier. AMON, résident en mémoire, surveille constamment - en tâche de fond - toutes les actions entreprises par l'utilisateur et le système. Il est ainsi toujours prêt à bloquer les attaques et vous en avertir.

Si AMON est désactivé (chargé en mémoire mais inactif) ou arrêté (non chargé en mémoire), l'icône précédent le nom AMON dans le Control Center s'affiche respectivement en rouge ou en grisé. Dans les deux cas, l'icône de NOD32 située dans la barre des tâches s'affiche en rouge. Cela signifie que votre ordinateur n'est PAS protégé en temps réel. Pour réactiver ou démarrer la protection résidente, veuillez vous reporter à l'aide en ligne, en cliquant sur **Aide** depuis la fenêtre principale du module AMON.

Analyse des documents Office (DMON)

DMON est un plug-in complémentaire à AMON, permettant d'analyser les documents Microsoft Office et les fichiers téléchargés automatiquement par Internet Explorer (par exemple, les éléments ActiveX Microsoft).

DMON fonctionne uniquement avec les applications qui supportent l'interface antivirus API Microsoft, comme MS Office 2000 (version 9.0 et supérieures), ou MS Internet Explorer (version 5.0 et supérieures).

NOTE : la protection des documents traités avec des Suites bureautiques autres que MS Office est pleinement assurée par AMON.

Analyse des E-mails (EMON)

EMON est un module résident, qui analyse les e-mails entrants et sortants via les logiciels de messagerie compatibles MAPI. Cette interface est utilisée par MS Outlook et par les serveurs de messagerie MS Exchange. EMON est compatible avec toutes les versions de MS Outlook.

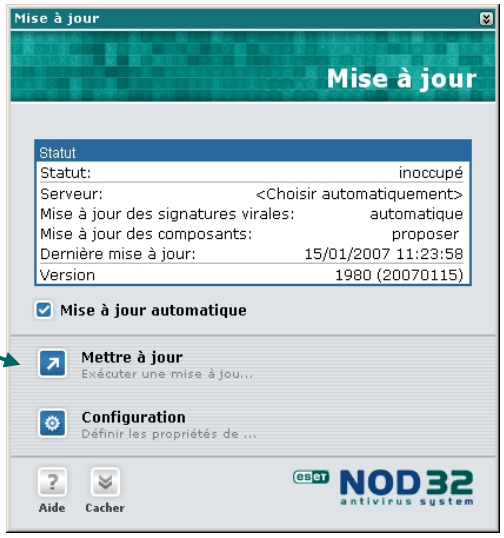
Analyse du Trafic Internet (IMON)

IMON contrôle - en permanence et en tâche de fond - tous vos e-mails entrants, mais aussi le flux Internet lorsque vous visitez des sites et y téléchargez des fichiers.

Pour davantage d'informations concernant AMON, DMON, IMON, EMON, ou le Scanner à la demande NOD32, veuillez vous reporter à l'aide en ligne intégrée au logiciel, en cliquant sur le bouton Aide depuis le Control Center. Vous pouvez également consulter notre FAQ (Questions les plus fréquemment posées) sur le site Internet d'Eset (en anglais - http://www.eset.com/support/faq.htm) ou de votre distributeur local (pour la France : http://www.eset-nod32.fr ou http://www.nod32.fr).

Les scanners « à l'accès » se chargent en mémoire et interceptent toutes les requêtes émises par le système d'exploitation au système de fichiers. De cette manière, ils assurent l'analyse des fichiers avant qu'ils ne soient ouverts, et par conséquent, évitent au système d'être infecté.

Mise à Jour

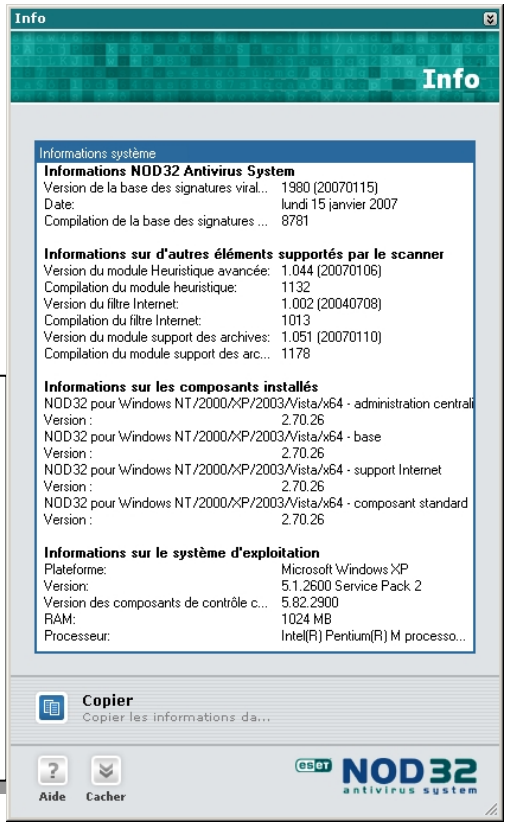


Par défaut, NOD32 vérifie automatiquement la disponibilité de nouvelles mises à jour pour la base des signatures de virus et les composants du programme. Vous pouvez également vérifier manuellement l'éventuelle disponibilité d'une mise à jour, en cliquant sur le bouton **Mettre à jour**, situé dans la fenêtre principale *Mise à jour*.

La sous-fenêtre *Statut* affiche les informations concernant la dernière date de mise à jour et le numéro de version de la base des signatures virales (également communément dénommée : base virale). Si vous souhaitez vérifier que vous disposez bien de la dernière version de la base virale, le numéro le plus récent est indiqué en haut de la page : http://www.eset.com/support/info.php. Vous y trouverez également la liste des signatures ajoutées à chaque mise à jour.

Pour modifier la procédure de mise à jour, cliquez sur le bouton **Configuration**.

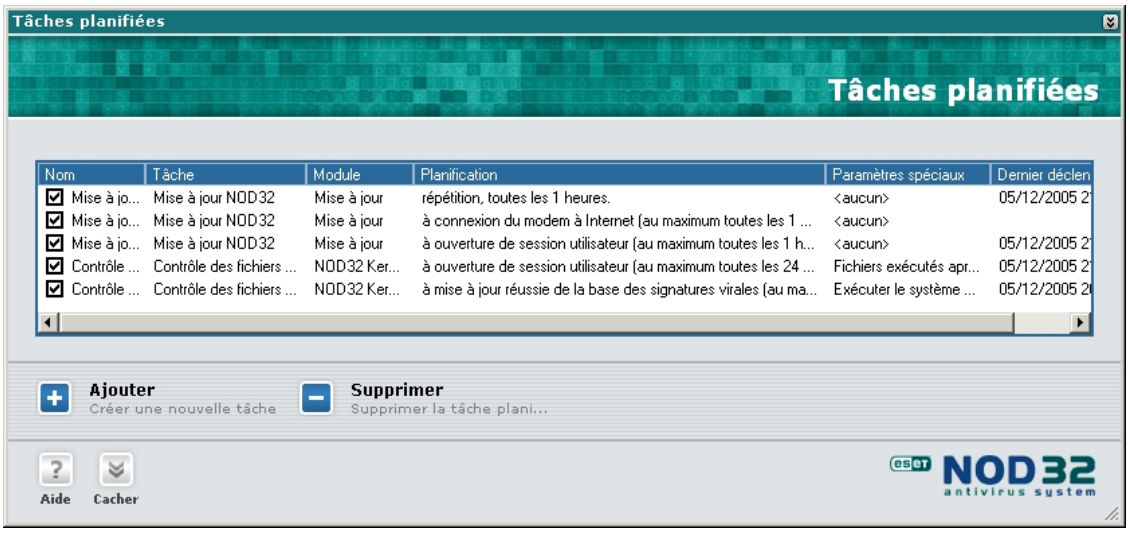
Pour obtenir l'ensemble des informations sur la version de NOD32 installée, cliquez sur **Information**, sous la section **Outils Système,** depuis la fenêtre principale du Control Center. Le détail des versions de la base virale et des composants installés, ainsi que les informations relatives à votre système y figurent.



De nouvelles mises à jour de la base virale sont publiées chaque jour, en moyenne. Les mises à jour (mises à niveau) des composants du programme vous parviennent également par Internet, via le processus de mise à jour standard. Ces mises à niveau sont publiées lorsque des modifications ont été apportées à l'application.

Mise à Jour à partir d'un Modem

Si vous utilisez un modem standard, NOD32 vérifiera si une mise à jour est disponible dès qu'il détectera la connexion de votre modem à Internet, puis toutes les heures (à la condition que vous restiez connecté). Les options de planification des mises à jour sont accessibles depuis la fenêtre principale du Control Center, sous la section **Outils Système** → **Planificateur**.



Le premier élément de la liste sera vérifié si vous bénéficiez d'une connexion permanente (par exemple, DSL ou T1) et êtes donc constamment connecté. Le premier et le second seront vérifiés si votre ordinateur est raccordé via un modem standard, à la condition que vous ayez sélectionné les paramètres appropriés lors de l'installation.

Mise à Jour à partir d'un Miroir

Concerne exclusivement la version multipostes [Administrator], pour la mise à jour des stations de travail en réseau.

Les utilisateurs possédant une licence multipostes de NOD32 et souhaitant utiliser le module additionnel **Miroir,** inclus dans la version Administrator (module permettant de créer une copie des fichiers de mise à jour sur un ordinateur du réseau accessible aux autres ordinateurs), peuvent consulter le document :

Guide d'administration réseau NOD32 (GuideAdmin-NOD32-RES.pdf) disponible à l'adresse :

http://www.eset-nod32.fr/telechargement-documentation-nod32.htm

Technologie ThreatSense™

La technologie **ThreatSense**™de NOD32 intègre un puissant système de détection proactif, basé sur une méthode d'analyse comportementale, dénommée *heuristique*.

>> Heuristique

L'analyse heuristique de NOD32 est une suite complexe d'algorithmes, particulièrement puissante, **permettant de détecter les nouveaux codes malveillants dont les signatures ne sont pas encore répertoriées dans la base virale**. De ce fait, **la sécurité de votre ordinateur est assurée en temps réel** et n'est plus tributaire du temps de réaction - si infime soit-il - nécessaire à la publication des signatures appropriées.

>> Heuristique Avancée

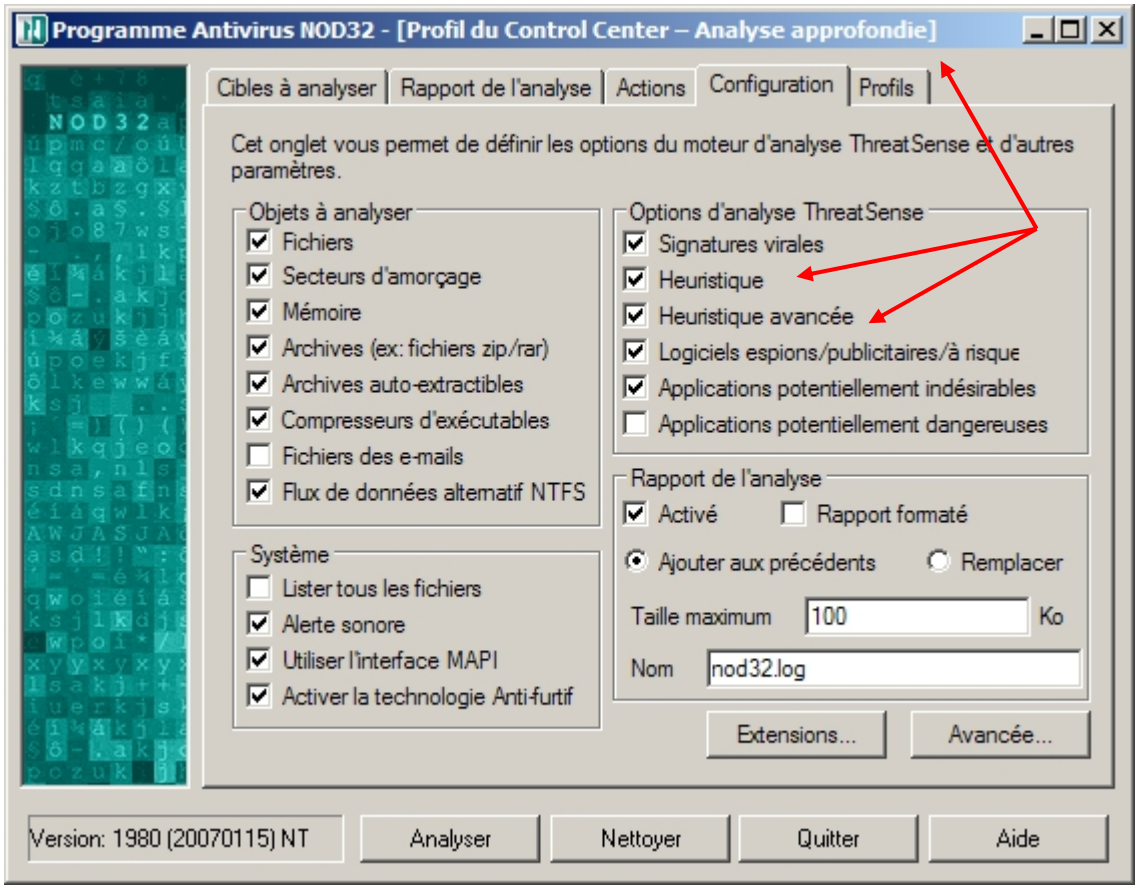
L'heuristique avancée étend les capacités de détection de l'heuristique standard, en identifiant un plus grand nombre de nouvelles menaces (vers, chevaux de Troie et Spywares). Toutefois, nous vous signalons que cette méthode peut augmenter les temps d'analyse et déclencher occasionnellement une fausse alerte (c'est-à-dire que NOD32 suspecte alors un objet de contenir un code malicieux, qui est en fait inoffensif).

L'heuristique avancée est activée par défaut pour les modules AMON, DMON, IMON, EMON et le Scanner à la demande NOD32 (uniquement via le bouton **`Analyse approfondie`**). Pour vérifier le statut de l'heuristique avancée de chacun des modules, cliquez sur le bouton **`Configuration`** dans la fenêtre principale du module concerné.

Nous vous recommandons fortement de laisser l'**`Heuristique avancée`** activée dans les modules AMON, DMON, EMON & IMON.

Pour davantage d'informations, veuillez consulter la rubrique d'**Aide** en ligne accessible via le Control Center et/ou consulter la FAQ sur le site Internet d'Eset (en anglais - http://www.eset.com/support/nodfaq2.htm) ou de votre distributeur local (pour la France: http://www.eset-nod32.fr et http://www.nod32.fr).

Nous vous conseillons également d'exécuter périodiquement une **Analyse approfondie** de votre ordinateur via le bouton dédié à cet effet dans la fenêtre NOD32 du Control Center (méthode recommandée aux utilisateurs inexpérimentés). Vous pouvez également créer un profil personnalisé, en sélectionnant toutes les cibles locales et tous les paramètres, y compris l'heuristique avancée. L'exécution des analyses approfondies peut être programmée via le **Planificateur**.



Traitements des Alertes et Incidents d'Origine Virale

Règles de base recommandées si une menace est détectée

- Les chevaux de Troie peuvent uniquement être supprimés puisqu'ils n'infectent pas d'autres fichiers et contiennent seulement leur propre code (instructions de programmation).
- Les vers contenus dans les pièces jointes des e-mails devraient également être supprimés dans la mesure où ils ne contiennent que du code viral.
- Si le contrôle HTTP du moniteur Internet IMON détecte une tentative d'infiltration, choisissez de mettre fin à la connexion afin de prévenir son enregistrement sur le disque dur.

Même si vous êtes certain qu'il est sans danger de supprimer un fichier infecté sans nuire au bon fonctionnement de votre système d'exploitation, nous vous recommandons de mettre une copie dudit fichier en Quarantaine avant sa suppression. Gardez à l'esprit que la plupart des virus se recopient dans les dossiers système, tels que **windows** ou **windows\system32**, pour troubler l'utilisateur. Si vous avez la moindre hésitation à supprimer un fichier, que vous ne trouvez pas sa description sur notre site ou sur Internet, veuillez nous envoyer ce fichier suspect (voir procédure page 47).

NOTE :

AMON peut rapporter une erreur en nettoyant ou supprimant un fichier infecté situé dans un dossier temporaire. Ceci peut se produire lorsque le fichier a été supprimé automatiquement entre temps. Si tel est le cas, veuillez fermer la fenêtre d'avertissement et effectuer une Analyse approfondie de votre ordinateur avec le Scanner à la demande NOD32, afin de vous assurer que votre système ne contient aucun virus.

Occasionnellement, vous pouvez voir apparaître une alerte où le nom de l'infiltration est « inconnue » ou « probablement inconnue… ». Ce type d'alertes se produit lorsqu'un module de NOD32 a détecté dans un fichier des caractéristiques similaires à celles d'un code malveillant, mais qu'aucune signature virale ne lui correspond dans la base pour en vérifier le nom. Cette situation est commune à toutes les nouvelles menaces (détectées par l'heuristique) qui n'ont pas encore été identifiées.

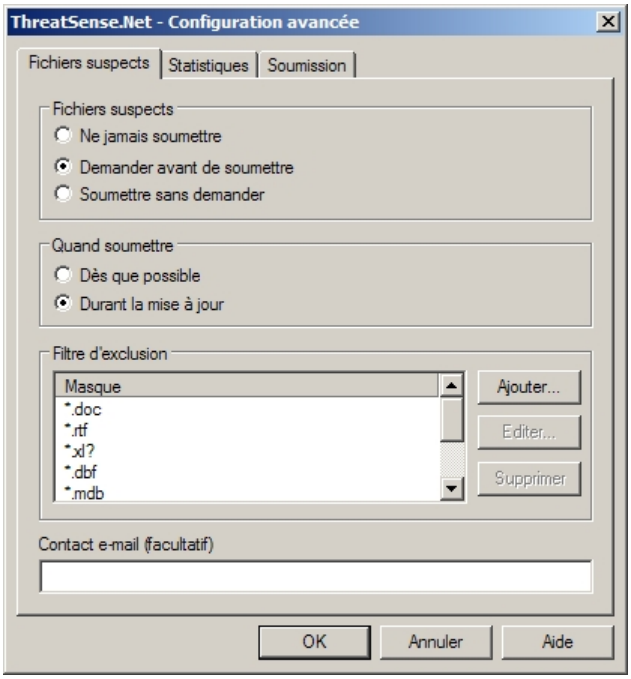
NOD32 détient un taux impressionnant de détection de virus et autres malwares encore inconnus, grâce à la sensibilité et la puissance de sa technologie **ThreatSense**™. Les menaces inconnues étant chaque jour plus nombreuses, ESET éprouve toujours un vif intérêt à recevoir les échantillons (copies) de ces fichiers suspects pour analyse.

Pour Envoyer un Echantillon Viral à Eset

NOD32 intègre un système bidirectionnel d'avertissement "précoce", **ThreatSense.Net**™ Early Warning System, qui permet de faire évaluer les fichiers qui ont été considérés par les scanners de NOD32 comme suspects. Ce système assiste l'utilisateur afin qu'il puisse soumettre, s'il le souhaite, de tels fichiers aux analystes du Laboratoire d'ESET. **ThreatSense.Net**™ est activé par défaut, mais une confirmation de l'utilisateur est requise avant tout envoi. Le processus peut être entièrement automatisé ou désactivé si désiré.

Ce système collecte et soumet également des données statistiques anonymes relatives aux infiltrations détectées, permettant à ESET d'analyser et évaluer la gravité et la virulence des menaces… et par conséquent de mieux protéger votre environnement informatique.

Le panneau de configuration de **ThreatSense.Net**™ EWS est accessible depuis : **Control Center** → **Outils Système** → **Configuration du système NOD32.** Dans la fenêtre de droite intitulée **Paramètres,** cliquez sur **Configuration**, puis dans celle qui s'ouvre alors, cliquez sur l'onglet **ThreatSense.Net**. Cliquez sur **Paramètres avancés…** pour accéder aux paramètres de la fenêtre ci-contre.



Le "*Filtre d'exclusion*" permet de sélectionner les extensions des fichiers qui ne devront jamais être envoyées et ce, dans le but de prévenir toute divulgation accidentelle de vos données privées et confidentielles. Les extensions les plus courantes (telles celles des documents Word, Excel, etc.) figurent dans la liste par défaut. Vous pouvez ajouter ou supprimer des extensions si désiré.

Les informations émises par le système **ThreatSense.Net**™ sont totalement anonymes. Si vous choisissez de saisir votre adresse de messagerie dans le champ *Contact e-mail* (saisie facultative), elle pourra être utilisée pour vous contacter si des informations complémentaires sont nécessaires à l'analyse d'un fichier suspect. Dans le cas contraire, vous ne recevrez aucun courriel d'ESET.

>> Envoi manuel

Si vous souhaitez soumettre manuellement un fichier suspect à ESET, cochez tout d'abord la case **Mettre une copie en Quarantaine** avant de lancer toute autre action (nettoyage, suppression, changement de nom…). La procédure de mise en quarantaine sauvegarde une copie du fichier sous une forme encryptée et non exécutable, ainsi le fichier ne risque pas d'être exécuté accidentellement lors de son déplacement ou son envoi.

Les fichiers mis en quarantaine sont stockés par défaut dans C:\Program Files\ESET\infected (ce dossier est créé lors de la première mise en quarantaine). **Il est bien entendu inutile d'envoyer des fichiers manuellement s'ils ont déjà été considérés comme suspects par NOD32 et envoyés automatiquement.**

Pour soumettre manuellement un fichier en quarantaine, ouvrez le Control Center, puis dans la section **Outils Système**, cliquez sur **Quarantaine**. Dans la fenêtre de droite, effectuez un clic gauche sur l'entrée ciblée de manière à la surligner, puis cliquez sur le bouton **Soumettre pour analyse** disponible en bas à droite de la fenêtre.

Pour davantage d'informations sur la manière d'envoyer manuellement un fichier suspect, veuillez consulter les instructions (en anglais) fournies à l'adresse : http://eset.zftp.com/submit.htm.

Annexe A : Dépannage

Question : Mon **Nom d'utilisateur** et mon **Mot de passe** ne fonctionnent pas.

Réponse : Si une boîte de dialogue apparaît vous demandant votre **Nom d'utilisateur** et votre **Mot de passe**, c'est probablement qu'ils ont été saisis de manière incorrecte durant la procédure d'installation, ou que votre licence NOD32 a expiré. Si vous êtes certain que votre licence est toujours en cours de validité, cliquez sur le module Mise à jour → Configuration, pour saisir à nouveau votre **Nom d'utilisateur** et votre **Mot de passe**, tels qu'ils vous ont été envoyés par votre distributeur dans l'e-mail de confirmation relatif à votre licence.

Votre **Nom d'utilisateur** et votre **Mot de passe** sont sensibles à la casse, c'est-à-dire au respect de la saisie des lettres majuscules, minuscules et des caractères spéciaux. Ils doivent donc être saisis impérativement à l'identique de ceux qui figurent dans l'e-mail envoyé par votre distributeur. Afin d'éviter tout risque d'erreur lors de leurs reports, nous vous recommandons vivement d'utiliser les fonctions « Copier » et « Coller » : sélectionnez l'une des valeurs à l'aide de votre souris, puis appuyez simultanément sur les touches **Ctrl + C** pour Copier, placez votre curseur dans la zone où vous souhaitez coller la valeur copiée, puis appuyez simultanément sur les touches **Ctrl + V** pour Coller.

Si les solutions décrites ci-dessus se révèlent infructueuses, veuillez consulter la FAQ sur www.eset-nod32.fr ou contacter le Support technique de votre distributeur local (pour la France : support@eset-nod32.fr).

Question : J'obtiens le message ci-dessous…

Réponse : Cet avertissement est affiché par l'application Microsoft Outlook (et non par NOD32), lorsque NOD32 tente d'accéder au fichier MAPI32.DLL et que MS Outlook n'est pas défini comme client de messagerie à utiliser par défaut.

Options :

Si vous utilisez Microsoft Outlook comme logiciel de messagerie principal pour recevoir vos e-mails et qu'il n'est pas défini comme client de messagerie par défaut, vous pouvez modifier cet état de la manière suivante : dans Internet Explorer, sélectionnez Outils → Options Internet → Programmes → changez l'application sélectionnée par défaut dans le champ Messagerie, en la remplaçant par Microsoft Outlook.

Si Microsoft Outlook est installé mais que vous ne l'utilisez pas : envisagez une désinstallation de MS Outlook.

Si vous utilisez Microsoft Outlook, mais ne souhaitez pas le définir comme client de messagerie par défaut : vous pouvez empêcher NOD32 d'accéder au fichier MAPI32.DLL. Depuis le Control Center, sous la section Modules, sélectionnez NOD32 → ouvrez le Scanner à la demande NOD32 en cliquant sur **Exécuter NOD32**. Dans l'onglet Configuration, décochez la case **Utiliser l'interface MAPI**, située sous la section Système.

Question : Puis-je utiliser IMON avec tous les logiciels de messagerie ?

Réponse : Si votre logiciel de messagerie utilise le protocole POP3, il devrait fonctionner avec IMON, sans paramétrage particulier. Si votre logiciel de messagerie utilise le protocole IMAP, ou tout autre protocole n'étant pas encore supporté par IMON, votre système sera toujours protégé par le module AMON à l'ouverture des pièces jointes.

Question : Mon problème n'est pas listé dans ce manuel, que dois-je faire ?

Réponse : Pour toute question supplémentaire, vous pouvez vous reporter à l'Aide en ligne intégrée à NOD32, consulter la FAQ (Questions les plus fréquemment posées) générale sur le site www.eset.com (en anglais), consultez également celle de votre distributeur local (pour la France : www.eset-nod32.fr).

Si vous ne trouvez pas la solution recherchée dans les sources d'information mentionnées ci-dessus, veuillez contacter le Support technique de votre distributeur local (pour la France : support@eset-nod32.fr).

Annexe B : Types d'installation

Déf. = Installation de type Par défaut (recommandé à la plupart des utilisateurs)
Ava. = Installation de type Avancé (partiellement personnalisable)
Exp. = Installation de type Expert (totalement personnalisable)
Post = Options pouvant être configurées après installation

Option	Valeur par défaut	Déf.	Ava.	Exp.	Post
Dossier de destination de NOD32	C:\Program Files\Eset		●	●	
Mode silencieux / Protection des paramètres par mot de passe	Désactivé / Désactivé		●	●	●
Type d'interface utilisateur / Ecran d'accueil	Personnalisé Eset / Oui			●	●
Envoi d'avertissements par e-mails ou Windows Messenger	Désactivé			●	●
Serveur de mise à jour, Nom d'utilisateur et Mot de passe	Auto, -aucun-, -aucun-	●	●	●	●
Paramètres connexion Internet et Proxy	Utiliser IE, pas de Proxy	●	●	●	●
Configuration de la mise à jour automatique	Chaque heure ou à la connexion du modem		●	●	●
Lancement auto de la protection résidente (AMON) au démarrage du système	Win9x Oui, NT/2000/XP/2003 Non	●	●	●	●
Placer l'icône de NOD32 sur le Bureau	Oui		●	●	
Activer l'analyse à la demande via la souris	Oui		●	●	
Installation des services DMON, IMON	Oui		●	●	●
Activer l'analyse/le nettoyage des e-mails	Oui		●	●	●
Installation des services EMON	Si Outlook est installé		●	●	●
Activer l'analyse du trafic HTTP	Oui		●	●	●
ThreatSense.Net™ Early Warning System	Oui	●	●	●	●

Annexe C : Désinstaller NOD32

Fermez tous les documents ouverts et toutes les applications en cours d'exécution.

Depuis la barre des tâches de Windows, cliquez sur **Démarrer** → **Tous les programmes** → pointez le curseur de votre souris sur le dossier **Eset**, puis dans le sous-menu qui s'affiche, cliquez sur **Désinstallation**.

Une fenêtre de dialogue vous demandera alors de confirmer votre choix. Pour accepter la désinstallation, cliquez sur **OK**.

La procédure de désinstallation peut prendre quelques instants et une fois terminée, vous invite à redémarrer votre ordinateur. Validez le redémarrage.

Votre ordinateur est maintenant prêt pour une nouvelle installation de NOD32, si vous le désirez.

Glossaire

Adware	Logiciel publicitaire
Adresse IP	Chaque ordinateur sur Internet se voit attribuer une adresse IP, c'est un peu comme le numéro de téléphone de votre ordinateur. Une adresse IP est formatée de la manière suivante : xx.xxx.xxx.xx (ex : 83.114.567.55). Votre navigateur Internet compose ces numéros afin de localiser d'autres ordinateurs sur le Web. Les adresses IP correspondent à des noms plus compréhensibles, comme par exemple www.eset.com, par l'intermédiaire d'un service DNS (Domain Name Service).
AMON	Scanner à l'accès – analyse tous les fichiers de votre ordinateur, dès que vous tentez d'y accéder.
Archives	Fichiers compressés pouvant être utilisés pour réduire la taille des données et ainsi préserver un espace disque précieux, ou permettre l'envoi plus rapide de fichiers en pièces jointes via Internet. A titre d'exemple, les fichiers en .zip et .rar sont des archives.
Base virale	Egalement dénommée « Base de données des signatures virales » – correspond à l'ensemble des définitions des virus connus. Chaque jour, en moyenne, Eset fournit une mise à jour des signatures correspondant aux derniers virus répertoriés.
Cheval de Troie	Est un programme destiné à exécuter des actions dérobées et généralement à caractère malicieux, auxquelles l'utilisateur ne s'attend pas et qu'il ne souhaite pas. Contrairement à un virus, le cheval de Troie ne se réplique (reproduit) pas. Toutefois, un virus peut parfaitement contenir un cheval de Troie.
C:\	Est la lettre standard la plus fréquemment attribuée au disque dur principal d'un ordinateur.
Cache	Le Cache est un fichier sur lequel vos lecteurs enregistrent une copie des objets auxquels vous avez accédez récemment. Si le même objet est appelé à nouveau, votre système peut éviter une nouvelle requête en utilisant la copie du Cache, et gagner ainsi un temps considérable.

Connexion modem	Souvent dénommée « Connexion d'accès à distance » - signifie que l'ordinateur est relié à Internet par l'intermédiaire d'un modem et d'une ligne téléphonique standard. La vitesse de téléchargement est beaucoup plus lente qu'avec une connexion à large bande.
Compresseurs d'exécutables	Ils compressent un programme, pratiquement comme un compresseur comme Pkzip le fait. Les compresseurs attachent alors leurs propres informations descriptives / de chargement, qui décompressent le programme avant de reprendre son exécution normale au point d'entrée du programme. Ces compresseurs sont souvent utilisés par les concepteurs de virus pour tenter de tromper les scanners antivirus.
DMON	Scanner à l'accès spécifiquement dédié à l'analyse des documents Microsoft Office.
FAI	Fournisseur d'Accès à Internet – société qui vous fournit votre connexion Internet.
HTTP	HyperText Transfer Protocol – communication standard Internet, identifiable par la chaîne « http:// » au début de toutes les adresses des pages Web (l'ajout d'un « s » à la fin, soit https://, signifie une forme sécurisée et chiffrée). Le HTTP est ce qui permet aux navigateurs Internet de fonctionner.
IMON	Scanner du trafic Internet – analyse les e-mails entrants, le flux http (y compris les téléchargements de fichiers).
IMAP	Internet Message Access Protocol – protocole permettant à un client d'accéder et de manipuler du courrier électronique sur un serveur. Cela permet la manipulation de dossiers de messagerie (boîtes à lettres) à distance, d'une manière fonctionnellement équivalente aux boîtes à lettres locales.
Large bande	Canal de transmission à haute vitesse, haut débit. Les connexions à large bande sont véhiculées par des câbles coaxiaux ou en fibre optique qui ont une bande passante plus large que les lignes téléphoniques conventionnelles, donnant la possibilité de supporter vidéo, voix, et données simultanément.
Malware	Programmes / codes malveillants

MAPI	Messaging Application Programming Interface – Système de Microsoft Windows qui autorise les logiciels de messagerie à travailler ensemble pour la distribution du courrier. Tant que les applications en questions sont compatibles MAPI (MAPI activé), elles peuvent partager les messages entre elles.
Mémoire (système)	La zone de mémoire utilisée par le système pour s'exécuter, ainsi que tous les programmes chargés. Egalement, certaines mémoires système sur le disque dans un fichier « swap » (sorte de Cache) et le reste de la RAM. Les virus tentent de se charger eux-mêmes dans la mémoire système de manière à rester actifs tant que l'ordinateur est en fonctionnement.
Mot de passe	Par exemple, votre **Mot de passe** personnel attribué par Eset pour accéder aux serveurs d'Eset fournissant les mises à jour, mises à niveau et téléchargements. Dans NOD32, vous pouvez également définir un mot de passe (qui doit être différent de celui permettant l'accès aux serveurs d'Eset) pour protéger l'accès aux paramètres de configuration.
Nom d'utilisateur	Votre **Nom d'utilisateur** personnel attribué par Eset pour accéder aux serveurs d'Eset fournissant les mises à jour, mises à niveau et téléchargements.
PCU	Program Component Upgrade (Mise à niveau des composants du programme) – Périodiquement, Eset publie de nouvelles versions de NOD32. Elles vous sont délivrées automatiquement* via Internet et mettent à niveau (à jour) la version installée sur votre machine. * à la condition que les paramètres d'installation par défaut n'aient pas été modifiés.
POP3	Version 3 du « Post Office Protocol ». Le protocole POP3 permet à un ordinateur client de récupérer le courrier électronique sur un serveur POP3 via une connexion (temporaire) TCP/IP ou autre. Le POP3 ne gère pas l'envoi des e-mails, qui est assuré par le protocole SMTP ou autre. IMAP et POP3 sont les méthodes les plus courantes de récupération des e-mails.

Proxy (serveur)	Serveur conçu spécifiquement pour réduire la quantité de bande passante utilisée, ou pour contrôler l'accès à un autre service. Un Proxy est un « attrapeur » (il stocke une copie du contenu téléchargé par son intermédiaire pour un accès ultérieur plus rapide) ou/et un « passe à travers » (il fournit simplement une passerelle vers d'autres services, les sites Internet par exemple). En règle générale, les utilisateurs particuliers n'utilisent pas de Proxy.
Par défaut	Se dit d'une donnée ou d'une valeur attribuée automatiquement par le programme en l'absence d'une indication explicite de la part de l'utilisateur et qui représente habituellement le choix ou le réglage le plus probable, compte tenu du contexte.
RAM	Random Access Memory – Terme désignant la mémoire système qui peut être utilisée par les programmes pour exécuter les tâches nécessaires lorsque l'ordinateur est en service ; un circuit mémoire intégré qui permet de stocker les informations et d'y accéder ultérieurement plus rapidement qu'à partir du disque dur.
ROM	Read Only Memory – mémoire dont le contenu est accessible en lecture mais non modifiable ; utilisée principalement par les systèmes BIOS et les puces CMOS (ces derniers indiquent à la machine comment démarrer et trouver le disque dur, ainsi que le chargement de tous les paramètres de base, tel que la détection du matériel).
Secteurs d'amorçage (de Boot)	Le secteur d'amorçage est le premier secteur sur une disquette. Sur un disque dur, c'est le premier secteur de la partition. Il contient des informations concernant le disque ou la partition, comme le nombre de secteurs, plus une petite quantité de code de programmation.
SMTP	Simple Mail Transfert Protocol – Permet les échanges de courriers électroniques entre serveurs. Le dialogue SMTP se passe généralement en tâche de fond sous le contrôle de l'agent de transfert des messages (MTA), tels Sendmail ou Outlook Express par exemple.
Signature de virus *(Signature virale)*	Une signature est une suite d'éléments binaires commune à chacune des copies d'un virus ou d'un ver particulier, et utilisée par les logiciels antivirus pour détecter leur présence.

Spyware (logiciel espion)	Logiciel qui espionne les usages et les transfère à des tiers, comme des publicitaires par exemple. En général, le pistage se fait à l'insu de l'utilisateur. Certains Spywares peuvent ralentir de manière significative votre ordinateur ou causer des crashs système.
Téléchargement	Transfert d'un fichier d'Internet vers votre machine. Exemple : téléchargement d'une mise à jour à partir du site d'Eset.
ThreatSense.Net™	Le système de détection "précoce" ThreatSense.net™ vous assiste lors de la soumissions d'informations, relatives aux menaces encore inconnues, auprès du laboratoire d'ESET. Cette source d'informations à pour but de mieux nous aider à mieux vous protéger.
UC	Unité Centrale – également connue sous le nom de processeur ou microprocesseur. Les 80386, 80486, Pentium, sont des exemples d'unités centrales développées par Intel, mais il existe de nombreux autres types d'UC.
URL	Uniform Resource Locator – La structure d'une adresse Internet. C'est-à-dire, la partie http, le nom de domaine ou l'adresse IP et la section finale ([.com], [.fr], [.org], [.net], [.gov], etc). Exemple d'URL : http://www.eset.com
Ver	Sous-ensemble de virus qui tout comme eux se répliquent, mais sans nécessiter un fichier hôte (le fichier du Ver contient tout ce qui lui faut pour se répliquer lui-même). Les Vers requièrent généralement un système en réseau, tel le courrier électronique, pour se reproduire.
Virus	Un virus informatique est un programme qui s'autoréplique. Il contient un code qui se copie lui-même et peut infecter d'autres programmes en les modifiant ou en affectant leur environnement.