

Security Task Manager

pour Windows XP, 2000, NT, ME, 98

Fournit des informations avancées sur les programmes et processus

© A. & M. Neuber GbR, 2003

Contenu

Possibilités de Security Task Manager	3
Utilisation de Security Task Manager	3
Types de processus	4
Taux de risques des processus	6
Afficher les détails de processus	9
Apprendre plus sur un processus	9
Terminer ou supprimer un processus	10
Utiliser le répertoire de quarantaine	10
Exporter la liste des processus	10
Imprimer la liste des processus	11
Ecrire un commentaire	11
Protéger votre ordinateur avec SpyProtector	11
Changer le langage de l'interface	12
Ajouter un fichier de langage	13
Contacter le team de Security Task Manager	13
Désinstaller Security Task Manager	13
Remarques sur la version d'évaluation (Shareware)	14
Passer de la version d'évaluation à la version enregistrée	14

Possibilités de Security Task Manager

Security Task Manager fournit des informations avancées sur les programmes et les processus lancés sur l'ordinateur. Pour chaque processus il affiche des informations supplémentaires par rapport au gestionnaire de tâches de Windows:

- ▶ Nom de fichier et chemin de répertoire
- ▶ Taux de risques pour la sécurité
- ▶ Description, date/heure de démarrage, icône du programme, type de processus
- ▶ Taux d'utilisation du processus (CPU)
- ▶ Fonctions cachées incluses (par ex. surveillance des entrées clavier, surveillance du navigateur, manipulation des programmes)

SpyProtector peut éliminer vos traces Internet, vous avertir des changements dans la base de registres et désactiver les surveillances du clavier et de la souris sur votre ordinateur.

Utilisation de Security Task Manager

Security Task Manager affiche tous les processus actifs sur votre ordinateur. Le taux vous renseigne sur les fonctions que contient un processus et qui peuvent altérer la sécurité. La liste des processus peut afficher les propriétés suivantes. Validez les éléments désirés dans le menu **Afficher** afin de choisir quelles propriétés seront affichées (colonnes).

▶ Nom

Affiche le nom du fichier, du service ou du pilote.

▶ Taux

Affiche de façon objective le taux de risques pour la sécurité. Plus la longueur de la barre rouge est grande, plus le processus contient de fonctions dangereuses. Les programmes avec un haut taux de risque ne sont pas forcément dangereux: ils utilisent peut-être seulement une propriété espion (Spyware). Cliquez sur un processus pour en apprendre plus sur lui. Vous pouvez ainsi évaluer la fiabilité de ce logiciel.

▶ CPU

Affiche le taux d'utilisation du processeur (CPU). Un programme actif occupe plus le processeur qu'un processus inactif.

▶ Mémoire

Affiche l'utilisation de la mémoire vive (RAM).

▶ Fichier

Affiche le nom du fichier et le chemin de répertoire.

▶ Type

Affiche le type de fichier. Le type de fichier peut être un programme, une icône de programme dans la barre de tâches, un plugin (BHO / Browser Helper Object), un pilote ou un service.

▶ Titre et Description

Affiche le titre et la description contenus dans le fichier. Pour une fenêtre Windows visible cela correspond au nom existant dans la barre de titre de la fenêtre.

▶ Fabricant et produit

Affiche le nom du fabricant et la description du produit contenus dans le fichier.

Cliquez avec le bouton droit sur un processus pour afficher un menu contextuel vous offrant la possibilité d'obtenir plus d'informations ou de stopper ce processus. Vous pouvez:



Afficher ses propriétés




Terminer le processus



Placer le processus en quarantaine

Astuces

- Cliquez sur le bouton  **Processus Windows** pour afficher également les processus internes de Windows. Ces processus appartiennent au système Windows. Les processus système Windows ne sont pas affichés par défaut.
- Un processus peut être un programme, un pilote, un service ou un PlugIn... ainsi que tout code exécutable qui serait actif dans la mémoire de l'ordinateur.

Types de processus

Security Task Manager distingue les sortes suivantes de processus. Cliquez dans le menu **Afficher** sur les types que vous voulez voir affichés dans les colonnes de la fenêtre principale.

Logiciels

- ▶ **Programme**: programme avec fenêtre visible ou programme invisible sans fenêtre.
- ▶ **Icône de la barre de tâches** : programme avec une icône dans la barre de tâches (à gauche de l'horloge). Un clic droit sur cette icône ouvre un menu contextuel qui peut vous permettre de récupérer certaines informations.

Fichiers DLL

- ▶ **Fichiers DLL** : lien de librairie dynamique (DLL / Dynamic Link Library) qui exécute un code de programme de la même façon qu'un programme. Un fichier DLL contient rarement des fonctions annexes utilisées par le programme principal.
- ▶ **ShellExecute**: fichier ayant démarré grâce à une boucle utilisant la commande « ShellExecute » dans la base de registres Windows. La commande « ShellExecute » lance un processus (Presque comme une DLL) quand n'importe quel programme Windows est démarré. Ce processus doit être examiné attentivement.


PlugIns Internet





PlugIns Internet (ou BHO / Browser Helpers Objects) : DLL qui permet aux développeurs de personnaliser et contrôler Internet Explorer. Alexa, GetRight, Go!Zilla et autres gestionnaires de téléchargement utilisent de tels PlugIns. Un PlugIn peut surveiller toutes vos activités Internet. Pour désactiver ces PlugIns, cliquez dans Internet Explorer sur le menu **Outils** puis choisissez **Options Internet**. Cliquez sur l'onglet **Avancés**. Désactivez la case **Activer les extensions tierce partie du navigateur (nécessite un redémarrage)**.


Services et pilotes


Services ou pilotes exécutant des fonctions système au niveau matériel (valable seulement dans la version complète).


 **Pilote de périphérique:** fanion de type de service indiquant un pilote de périphérique Windows NT qui contrôle des composants matériel (par ex. une carte graphique ou un scanner). Plusieurs modules logiciel (par ex. Pare-Feu, Anti-Virus) sont des pilotes de périphérique que l'utilisateur ne peut pas fermer.

 **Fichier pilote:** fanion de type de service indiquant un fichier de pilote système Windows NT.

 **Service (processus indépendant):** fanion de type de service indiquant un service Win32 qui tourne dans son propre processus. Un service Win32 démarre automat. au démarrage de Windows, est toujours lancé et ne dépend pas de l'utilisateur.

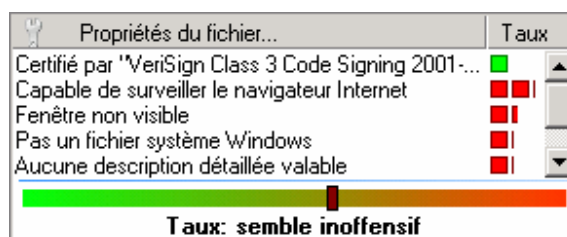
 **Service (processus indépendant en interaction avec le bureau):** fanion de type de service indiquant un service Win32 (par ex. Pare-Feu, Anti-Virus) qui tourne dans son propre processus et peut interagir avec le bureau. Un service Win32 démarre automatiquement au démarrage de Windows, il est toujours lancé et ne dépend pas de l'utilisateur.

 **Service (processus partagé):** fanion de type de service indiquant un service Win32 qui partage un processus avec d'autres services. Un service Win32 démarre automatiquement au démarrage de Windows, il est toujours lancé et ne dépend pas de l'utilisateur.

 **Service (processus partagé en interaction avec le bureau):** fanion de type de service indiquant un service Win32 qui partage un processus avec d'autres services et peut interagir avec le bureau. Un service Win32 démarre automatiquement au démarrage de Windows, il est toujours lancé et ne dépend pas de l'utilisateur.

Taux de risques des processus

Security Task Manager estime le taux de risques d'un processus selon des critères objectifs. Pour ceci Security Task Manager examine si un processus contient des appels critiques de fonctions ou des propriétés douteuses : chacun des résultats de ces recherches donne un certain nombre de points. La somme finale donne le taux de risques dans la colonne Taux de Security Task Manager (de 0 jusqu'à un maximum de 100 points).



Security Task Manager examine les processus en cherchant les fonctionnalités suivantes (classés selon leur dangerosité):

- *Capable d'enregistrer les entrées clavier*: le processus surveille chaque entrée clavier. Ceci est réalisé à l'aide d'une fonction de boucle. Les programmes sérieux n'utilisent pas une telle fonction de boucle.
- *Fichier est caché*: le fichier est caché pour l'explorateur de Windows. Ne prenez pas un fichier avec l'attribut caché pour un fichier inoffensif !
- *Pilote de clavier pouvant enregistrer les entrées clavier*: pilote de clavier pouvant lire toutes les entrées que vous faites au clavier.
- *Peut manipuler d'autres programmes*: le processus peut manipuler n'importe quel programme ou opération du système Windows. Une boucle est établie pour faire ceci. Une boucle est une fonction interne Windows qui peut, par exemple, simuler une fausse liste de fichiers (en manipulant la commande DIR). Ainsi le programme qui démarre le processus n'est pas visible par d'autres programmes tels que les logiciels Anti-Virus.
- *Capable de surveiller le navigateur Internet*: un PlugIn (BHO / Browser Helper Object) est une DLL qui permet aux développeurs de personnaliser et contrôler Internet Explorer. Alexa, GetRight, Go!Zilla et autres gestionnaires de téléchargement utilisent de tels PlugIns. Ces PlugIns peuvent surveiller toutes vos activités Internet. Pour désactiver ces PlugIns, cliquez dans Internet Explorer sur le menu **Outils** puis choisissez **Options Internet**. Cliquez sur l'onglet **Avancés**. Désactivez la case **Activer les extensions tierce partie du navigateur (nécessite un redémarrage)**.


- *Démarre au démarrage de programmes*: ce fichier est démarré par une boucle utilisant la commande « ShellExecute » dans la base de registres Windows. La commande « ShellExecute » lance un processus (Presque comme une DLL) quand n'importe quel programme Windows est démarré. Ce processus doit être examiné attentivement.
- *Ecoute sur le port <N°>*: le processus peut recevoir des informations depuis Internet. Les pirates informatiques (Hackers) utilisent de tels procédés pour prendre le contrôle de l'ordinateur. Vous pouvez empêcher ce genre d'attaques avec un bon Pare-Feu.
- *Envoie vers <nom d'ordinateur> sur port <N°>*: le processus se connecte à un nom d'ordinateur ou à une adresse IP et peut lui envoyer n'importe quelle information. Vous pouvez empêcher ce genre d'attaques avec un bon Pare-Feu.
- *Programme inconnu écoute ou envoie*: un port est ouvert afin de recevoir ou envoyer des informations sur le réseau ou Internet. Il faut déterminer de quel programme il s'agit. Vous pouvez empêcher ce genre d'attaques avec un bon Pare-Feu.
- *Surveille le démarrage des programmes*: le processus surveille quand et quels programmes sont démarrés ou fermés.
- *Fenêtre non visible*: le programme n'a aucune fenêtre visible et est lancé en tâche de fond. Dans le meilleur des cas, il s'agit par exemple d'un pilote logiciel de périphérique.
- *Démarre quand Windows démarre*: le programme est démarré à chaque démarrage de Windows car il écrit une clé d'auto-démarrage dans la base de registres.
- *Aucune description détaillée valable*: plusieurs descriptions standard importantes sont manquantes dans le fichier. Chaque fichier contient par défaut des champs internes pour ces descriptions.
- *Pas un fichier système Windows*: le fichier ne fait pas partie du système Windows. Les fichiers système Windows sont vérifiés et protégés spécialement par Windows.
- *Aucune description de programme*: aucune description n'a été trouvée dans le fichier. Chaque fichier contient par défaut des champs internes pour ces descriptions.
- *Fonctions: Internet, surveillance, enregistrement d'entrées, caché, manipulation*. Le fichier contient des appels de fonction avec les propriétés ci-dessus. Mais cela n'a pas beaucoup d'influence sur le taux de risques car ces fonctions n'entrent peut-être pas en action.

- *Fonctions: pas déterminable.* Aucun appel de fonction dangereuse n'a été trouvé dans le fichier. Mais ces fonctions peuvent avoir été intégrées de façon cachée.
- *Fabricant inconnu:* le fabricant du logiciel n'a pas été trouvé dans les champs de description du fichier. Chaque fichier contient par défaut un champ interne contenant le nom du développeur du logiciel.

Propriétés partagées (risques réduits):

- *Fichier signé Microsoft:* ce fichier a été signé par Microsoft. Vous pouvez faire confiance à ce fichier autant que vous faites confiance à Microsoft (?!?).
- *Fichier signé Verisign:* ce fichier a été signé par VeriSign. Vous pouvez faire confiance à ce fichier autant que vous faites confiance à Verisign.
- *Certifié par <autorité d'enregistrement> pour la compagnie <fabricant>:* ce fichier a été signé par une autorité d'enregistrement. Vous pouvez faire confiance à ce fichier autant que vous faites confiance à cette autorité d'enregistrement et au fabricant du logiciel.
- *Commentaire personnalisé:* vous pouvez écrire votre propre commentaire et évaluer votre propre taux de risques; cette dernière option influencera le taux de risques affiché: « dangereux » changera le taux sur 100, « pas dangereux » changera le taux sur 0, « ne sais pas ou sans opinion » laissera le taux qui a été déterminé automatiquement.

Astuces


- Les programmes avec un haut taux de risque ne sont pas forcément dangereux: ils utilisent peut-être seulement une propriété espion (Spyware).
- Cliquez sur le bouton  **Processus Windows** pour afficher également les processus internes Windows. Ces processus appartiennent au système Windows. Les processus système Windows ne sont pas affichés par défaut.

Afficher les détails de processus

Cliquez sur un processus pour afficher plus d'informations sur celui-ci. Les propriétés suivantes sont affichables:

- ▶ Nom: affiche le nom du logiciel ou du pilote.
- ▶ Taux : affiche objectivement le taux de risques du processus. Plus la barre rouge est longue, plus le processus contient de fonctions dangereuses et plus le taux de risques est grand. Les programmes avec un haut taux de risque ne sont pas forcément dangereux: ils utilisent peut-être seulement une propriété espion (Spyware). Cliquez sur un processus pour en apprendre plus sur lui. Vous pouvez ainsi évaluer la fiabilité de ce logiciel.
- ▶ Fichier: affiche le chemin de répertoire et le nom du fichier.
- ▶ Type: affiche le type de fichier. Le type de fichier peut être un programme, une icône de programme dans la barre de tâches, un plugin (BHO / Browser Helper Object) , un pilote ou un service.
- ▶ Titre et Description: affiche le titre et la description contenus dans le fichier. Pour une fenêtre Windows visible cela correspond au nom existant dans la barre de titre de la fenêtre.
- ▶ Fabricant et produit: affiche le nom du fabricant et la description du produit contenus dans le fichier.

Astuces

- Cliquez sur le bouton  **Processus Windows** pour afficher également les processus internes de Windows. Ces processus appartiennent au système Windows. Les processus système Windows ne sont pas affichés par défaut.
- Cliquez dans le menu **Afficher** sur les types que vous voulez voir affichés dans les colonnes de la fenêtre principale.

Apprendre plus sur un processus

1 Cliquez sur le processus que vous voulez examiner.

2 Cliquez sur le bouton  **Google** dans la barre d'outils.

Une page d'information WEB est affichée chez « www.neuber.com/taskmanager » dans laquelle vous pouvez donner votre opinion sur ce logiciel/pilote ou lire les commentaires des autres utilisateurs. Vous pouvez rechercher d'autres informations sur ce processus via « Google.com » depuis cette même page WEB.

Astuces

- Votre navigateur Internet transmet des informations (par ex. version de Windows, langage, ...). Security Task Manager n'effectue jamais une connexion à Internet.
- « Google.com » est un des moteurs de recherche le plus utilisé et le plus efficace.

Terminer un processus

1 Cliquez sur le processus que vous voulez terminer.

2 Cliquez sur le bouton **Supprimer**.

3 Sélectionnez une des options suivantes:

▶ **Fin du processus:**

Le processus sera enlevé de la mémoire. Si le processus écrit une clé dans la base de registres dans la section de démarrage automatique (Autostart), il sera alors à nouveau actif au prochain démarrage de Windows.

▶ **Mettre fichier en quarantaine:**

Le processus sera enlevé de la mémoire. En plus Security Task Manager met le fichier correspondant dans le répertoire de quarantaine et efface les entrées correspondantes dans la base de registres (section de démarrage automatique / Autostart). Le fichier et les entrées de la base de registres sont sauvegardées; vous pouvez ainsi restaurer le processus n'importe quand.

Astuces

- Terminer un processus peut engendrer une instabilité du système ou même le bloquer. les logiciels ayant besoins de programmes additionnels de type Adware peuvent ne plus fonctionner. Sauvegardez auparavant vos documents ouverts !

Utiliser le répertoire de quarantaine

Le répertoire de quarantaine travaille comme la poubelle de Windows (recycle bin). Lorsque vous placez un fichier en quarantaine, le fichier est renommé et déplacé dans un répertoire isolé. La clé correspondante d'auto-démarrage est effacée (base de registres). Ainsi le processus ne pourra redémarrer. Une restauration du processus est possible à tout moment.

Restauration de processus

1 Cliquez sur le bouton  **Quarantaine** dans la barre d'outils.

2 Dans le répertoire de quarantaine cliquez sur le processus que vous voulez restaurer.

3 Cliquez sur le bouton **Restaurer**.

Exporter la liste des processus

1 Dans le menu **Fichier** cliquez sur **Exporter sous...**

2 Choisissez le type de fichier:


▶ Fichier texte (*.txt)

▶ Fichier WEB (*.html)

Imprimer la liste des processus

- 1 Dans le menu **Fichier** cliquez sur **Imprimer**.
- 2 Choisissez une imprimante et corrigez éventuellement les propriétés nécessaires (par ex. recto-verso).

Astuces

- Cliquez sur le bouton  **Processus Windows** pour afficher également tous les processus internes de Windows. Ces processus appartiennent au système de Windows. Les processus systèmes de Windows ne sont pas visibles par défaut.
- Sauvegardez régulièrement la liste des processus. Vous trouverez ainsi plus facilement de nouveaux processus. Une sauvegarde de la liste des processus peut servir à des fins de démonstration.

Ecrire un commentaire

Vous pouvez écrire vos propres remarques sur chaque processus. Elle sera visible dans les propriétés du processus. Vous pouvez également re-évaluer la dangerosité du processus afin de changer la valeur de taux de risques.

Pour écrire un commentaire

- 1 Clic droit sur le processus concerné.
- 2 Cliquez sur **Commentaire...** dans le menu contextuel qui apparaît ensuite.
- 3 Entrez votre commentaire et éventuellement votre opinion sur la dangerosité de ce processus. Le taux de risque affiché changera sur la valeur 0 si vous choisissez "Pas dangereux" et sur 100 si vous optez pour "Dangereux". Le choix de "Ne sais pas ou sans opinion" laissera le taux qui a été déterminé automatiquement.

Protéger votre ordinateur avec SpyProtector

Pour lancer SpyProtector, cliquez sur l'icône  14:58 dans la barre de tâches.

SpyProtector contient les outils suivants pour protéger votre ordinateur des surveillants d'entrées clavier (keyloggers), logiciels espions (Spyware) et chevaux de Troie (Trojans):

Effacer les divers historiques

Validez cette option pour éliminer les traces d'activités Internet (cookies, cache, historique, URLs tapées) dans Internet Explorer. Vous pouvez également effacer la liste des fichiers récemment utilisés (par ex. Word, ACDSee, PDF, WinZip, Mediaplayer) ainsi que la liste des programmes récemment lancés depuis le menu Démarrer.



Désactiver la surveillance du clavier

Validez cette option pour bloquer la plupart des moniteurs d'entrées clavier (keyloggers) pour la session Windows en cours. La redirection de toutes les entrées clavier par un moniteur d'entrées clavier est bloquée. Une telle redirection du clavier est obtenue au moyen d'une fonction de boucle. Même des utilitaires clavier telle qu'une macro ou un programme inscrivant du texte automatiquement (autotext) n'utilisent pas une telle mauvaise boucle.



Désactiver les autres surveillances

Validez une ou plusieurs de ces options pour bloquer les programmes qui surveillent les éléments suivants pour la session Windows en cours:

Entrées de clavier (indirectes)

Cela désactive la surveillance des messages internes Windows messages (par ex. entrées clavier) par d'autres programmes.

Activités de la souris

Cela désactive la surveillance des mouvements et clics de la souris.

Macro

Cela désactive la surveillance des activités de l'utilisateur. Cette méthode est souvent utilisée par les programmes macros mais généralement pas par les moniteurs d'entrées clavier (keyloggers).

Démarrage et fermeture de programmes

Les démarrages et fermetures de programme sont surveillés. Les programmes d'apprentissage (tutoriaux, CBT) utilisent souvent ce genre de surveillance pour interagir avec le programme à apprendre.

Attention: Quelques programmes sérieux (par ex. quelques programmes macro) utilisent cette "mauvaise" fonction de boucle. Si vous constatez qu'un programme ne fonctionne plus, réactivez alors l'option correspondante et redémarrez votre ordinateur.



Mise en garde quand la base de registres est modifiée

Validez cette option pour obtenir un message d'avertissement si un programme essaie d'écrire son nom dans la base de registres dans la section démarrage automatique. Le logiciel est démarré secrètement avec une telle entrée à chaque démarrage de Windows. Tous les programmes dangereux ont besoin d'une telle clé pour être actifs lorsque l'ordinateur redémarre !

Changer le langage

Security Task Manager reconnaît automatiquement la langue utilisée par défaut dans Windows (Français, Anglais, Allemand, ...).

Pour changer de langage:

1. Dans le menu **Afficher** cliquez sur cliquez sur **Langage**
2. Choisissez ensuite le langage désiré.

Astuce

- Le logiciel peut facilement être transcrit dans une autre langue. Traduisez simplement le fichier lgs_english.txt dans le dossier du programme et envoyez-le à info@neuber.com. Vous recevrez gratuitement un code d'enregistrement en récompense de votre travail.

Ajouter un fichier de langage

Vous pouvez télécharger des fichiers additionnels de langage:

- 1 Allez sur www.neuber.com/taskmanager/download.html
- 2 Vous voyez dans cette page tous les langages existants.
- 3 Copiez la dernière version du logiciel dans le répertoire de Security Task Manager. Par exemple c:\program files\Security Task Manager
- 4 Changez le langage et redémarrez Security Task Manager.

Astuce

- Divers langages sont déjà contenus par défaut dans Security Task Manager.

Contacter le team de Security Task Manager

Contact technique:

Adresse: Alexander and Matthias Neuber GbR
PF 11 05 25
D-06019 Halle
Germany
fax: (+49) 0700-11 777 000
Internet: www.neuber.com/taskmanager
WWW:
email: info@neuber.com

L'enregistrement est effectué par le service d'enregistrement international Sharelt (Greensburg/U.S.A, Köln/Germany, London/UK, Roissy/France, Upplands Väsby/Sweden).

Vous trouverez une version allemande sous <http://www.neuber.com/taskmanager>

Désinstallation de Security Task Manager

- 1 Cliquez sur **Démarrer-Paramètres-Panneau de configuration**.
- 2 Double-cliquez sur **Ajout/Suppression de programmes**.
- 4 Cliquez sur **Security Task Manager**.
- 3 Cliquez sur le bouton **Supprimer** pour désinstaller Security Task Manager de votre ordinateur.

Astuce

- Vous pouvez aussi lancer uninstal.exe dans le répertoire de Security Task Manager.

Remarques au sujet de la version d'évaluation

Security Task Manager est distribué en tant que Shareware. Le principe du Shareware est une méthode de distribution basée sur l'honneur, et n'est pas un type de logiciel. Vous êtes libres de l'utiliser pour une période d'évaluation de 30 jours. Si vous trouvez ce programme utile et convivial, et que vous décidez de continuer à utiliser Security Task Manager, il vous sera alors demandé de l'enregistrer pour seulement \$29 (ou 29 EURO). Vous recevrez alors un code d'enregistrement qui vous permet de libérer le shareware. Le code d'enregistrement supprimera les messages d'avertissement et les limitations du logiciel, et restera valable pour toutes les futures mises à jour.

En tant qu'utilisateur enregistré, vous disposez de:

- Licence légale pour le logiciel
- Votre propre code d'enregistrement vous permettant de libérer la version Shareware
- Mises à jour gratuites à vie
- Utilisation libre du logiciel SpyProtector
 - Spyprotector élimine vos traces Internet, vous avertit si des clés de la base de registre (zones de lancement automatique) sont modifiées et désactive les surveillances clavier et souris.
- Support technique libre (via email ou mail)

Cliquez sur **A propos...** dans le menu **Aide** pour vérifier si votre version est enregistrée.

Comment libérer la version Shareware

- 1 Cliquez sur **Entrer le code d'enregistrement...** dans le menu **ENREGISTREMENT**.
- 2 Entrez le code d'enregistrement exactement comme vous l'avez reçu dans la boîte de dialogue.
- 3 Cliquez sur le bouton **Libérer**.

Astuces

- Si vous avez des questions contactez-nous.
- Vous pouvez obtenir votre code d'enregistrement pour \$29 (ou 29 Euro).