



manuel d'utilisation

AntiVirus Firewall

Un service de la gamme
securitoo.com

Sommaire

<u>À propos de ce guide</u>	1
<u>Explication des icônes</u>	1
1. <u>Installation de Securitoo AntiVirus Firewall</u>	3
1.1 <u>Avant de commencer</u>	3
1.2 <u>Procédure d'installation</u>	3
1.3 <u>Si vous devez désinstaller le logiciel Securitoo AntiVirus Firewall</u>	4
2. <u>Démarrage</u>	6
2.1 <u>Première utilisation de Securitoo AntiVirus Firewall</u>	6
2.2 <u>Que faire lorsque la fenêtre de contrôle d'application apparaît ?</u>	6
2.3 <u>Securitoo AntiVirus Firewall est-il actif et fonctionne-t-il correctement ?</u>	7
2.4 <u>Options d'accès à Securitoo AntiVirus Firewall</u>	9
3.  <u>Accueil</u>	12
4.  <u>AntiVirus</u>	13
4.1 <u>Profil de protection antivirus</u>	13
4.2 <u>Rechercher des virus</u>	14
4.3 <u>Suppression d'un virus de votre ordinateur</u>	14
<u>Comment l'Assistant de nettoyage supprime un virus</u>	14
<u>Suppression d'un virus lorsque l'Assistant de nettoyage échoue</u>	17
4.4 <u>Que faire si vous pensez avoir trouvé un nouveau virus ?</u>	18
4.5 <u>Demander à Securitoo AntiVirus Firewall d'ignorer/analyser certains fichiers</u>	18
5.  <u>Firewall</u>	20
5.1 <u>Profils du firewall</u>	20
5.2 <u>Utilisation du contrôle d'application</u>	21
5.3 <u>Personnalisation des profils du firewall</u>	23
<u>Création d'une nouvelle règle de firewall</u>	23
5.4 <u>Paramètres avancés</u>	26
<u>Interface approuvée</u>	26
<u>Filtre de paquets activé</u>	26
<u>Contrôle d'application activé</u>	26
6.  <u>Mise à jour automatique</u>	28


7.	 <u>Mon abonnement</u>	30
8.	<u>Comment Securitoo AntiVirus Firewall protège votre ordinateur</u>	31
	8.1 <u>Antivirus</u>	31
	8.2 <u>Firewall</u>	31
	8.3 <u>Comment se prémunir contre les virus et autres antiprogrammes</u>	32
	<u>Dépannage</u>	33
	<u>Installation</u>	33
	<u>Utilisation générale</u>	33
	<u>Antivirus</u>	33
	<u>Firewall</u>	33
	<u>Contrôle d'application</u>	34
	<u>Mise à jour automatique</u>	34
	<u>Mon abonnement</u>	34
	<u>Glossaire</u>	36
	<u>Support et maintenance</u>	38


À propos de ce guide


Ce guide fournit toutes les informations dont vous avez besoin pour installer et utiliser Securitoo AntiVirus Firewall.


Chapitre 1. [Installation de Securitoo AntiVirus Firewall](#) - Fournit les informations nécessaires pour installer Securitoo AntiVirus Firewall.


Chapitre 2. [Démarrage](#) – Présente des informations utiles pour les nouveaux utilisateurs et constitue une référence pour les utilisateurs plus expérimentés sur l'accès et la prise en mains de Securitoo AntiVirus Firewall.

Chapitre 3.  [Accueil](#) – Présente un aperçu rapide et détaillé des paramètres de sécurité et de l'état de Securitoo AntiVirus Firewall.

Chapitre 4.  [AntiVirus](#) – Explique comment vous pouvez activer ou désactiver la protection antivirus, sélectionner votre profil de protection antivirus et surveiller la réception de mises à jour des définitions de virus.

Chapitre 5.  [Firewall](#) – Explique comment vous pouvez modifier les profils du firewall, voir combien de connexions ont été autorisées ou refusées, et accéder à des paramètres avancés.

Chapitre 6.  [Mise à jour automatique](#) – Fournit des informations sur le service de mise à jour automatique, qui procure ce qu'il y a de plus récent en termes d'informations sur les virus, versions du logiciel et versions des profils.

Chapitre 7.  [Mon abonnement](#) – Explique comment vous pouvez vérifier l'état de votre abonnement.

Chapitre 8. [Comment Securitoo AntiVirus Firewall protège votre ordinateur](#) – Définit les menaces qui pèsent sur un ordinateur et explique comment Securitoo AntiVirus Firewall protège votre ordinateur contre ces menaces.




[Dépannage](#) – Résolution de certains problèmes courants.




[Glossaire](#) – Définition des termes.

[Support et maintenance](#) – Contacts pour l'assistance technique.


Explication des icônes

Les icônes suivantes apparaissent dans Securitoo AntiVirus Firewall:

	Activé	La fonction est activée et opère correctement.
	Question	Question pouvant exiger de prendre une décision.
	Info.	Informations complémentaires pour vous aider à utiliser Securitoo AntiVirus Firewall.

	Occupé	Veillez patienter.
	Avertissement	Une fonction de Securitoo AntiVirus Firewall est désactivée ou vos définitions de virus n'ont pas été mises à jour récemment.
	Erreur	Une erreur s'est produite. Lisez attentivement le message d'erreur.

Remarque : Certaines icônes ont une fonction différente dans la page *Mon abonnement*.

Pour plus d'informations, voir le chapitre 7.  *Mon abonnement* en page 30.

1. Installation de Securitoo AntiVirus Firewall

1.1 Avant de commencer

Configuration requise

Votre ordinateur doit répondre aux exigences suivantes pour que vous puissiez installer et exécuter Securitoo AntiVirus Firewall

Processeur :	Intel Pentium II ou supérieur
Système d'exploitation :	Microsoft® Windows® 95/98/ME/NT4.0 (SP6 requis)/2000/XP Les versions "serveur" de ces systèmes ne sont pas supportées
Mémoire :	Windows 98/ME/NT4.0 - 64 Mo RAM Windows 2000/XP - 128 Mo RAM
Espace disque :	30 Mo d'espace libre sur le disque dur (60 Mo pendant l'installation)
Écran :	Minimum 256 couleurs
Connexion Internet :	Une connexion Internet est requise pour valider votre enregistrement et recevoir des mises à jour
Navigateur :	Internet Explorer 3.0 ou supérieur

Préparation de votre ordinateur en vue de l'installation

Il n'est pas recommandé d'utiliser plusieurs antivirus et/ou firewall en même temps. Un conflit entre les logiciels antivirus pourrait endommager vos fichiers.

Suppression d'autres logiciels antivirus/firewall

Les antivirus et/ou firewall d'autres fournisseurs doivent être désinstallés séparément avant l'installation de Securitoo AntiVirus Firewall. Référez-vous à la documentation du fournisseur approprié pour la désinstallation de ces logiciels.

1.2 Procédure d'installation

Remarque : Si vous utilisez Windows NT 4.0, Windows 2000 ou Windows XP et avez plusieurs comptes, vous devez vous connecter comme administrateur pour pouvoir installer Securitoo AntiVirus Firewall.

Pour installer Securitoo AntiVirus Firewall, procédez comme suit :

1ère partie : Installation de Securitoo AntiVirus Firewall

1. Fermez tous les autres programmes et insérez votre CD Securitoo AntiVirus Firewall dans le lecteur de CD-Rom de l'ordinateur.



L'installation devrait démarrer automatiquement. Si elle ne démarre pas, accédez aux répertoires du CD et trouvez le fichier *install.exe*. Cliquez deux fois dessus pour lancer l'installation.

2. Choisissez la langue que vous souhaitez utiliser pour l'installation et cliquez sur **Suivant** pour continuer.
3. Lisez le contrat d'abonnement et, s'il vous agrée, cochez *J'accepte le contrat*. Cliquez sur **Suivant** pour continuer.
4. Choisissez le répertoire dans lequel vous souhaitez installer Securitoo AntiVirus Firewall. Cliquez sur **Suivant** pour continuer.
5. Les fichiers sont transférés vers votre ordinateur. Une fois le transfert terminé, passez à la deuxième partie de l'installation.

Remarque: Vous serez peut-être invité à faire redémarrer l'ordinateur. Sélectionnez *Redémarrage immédiat* (si vous sélectionnez *Redémarrage ultérieur*, l'installation ne sera pas achevée tant que vous n'aurez pas fait redémarrer l'ordinateur) et cliquez sur **Terminer**.

2e partie : Sélection des composants et validation de votre abonnement

1. Pour valider votre abonnement, assurez-vous que la connexion à Internet est active.
 - Entrez votre clé d'enregistrement. Cliquez sur **Suivant** pour continuer.

Conseil : Vous pouvez suivre la progression de l'installation en cliquant deux fois sur  dans la barre d'état du système Windows, en bas à droite de l'écran. Cette icône sera remplacée par l'icône  une fois l'installation terminée.

2. Une fois que Securitoo AntiVirus Firewall a installé les fichiers nécessaires, vous êtes invité à faire redémarrer l'ordinateur. Sélectionnez *Redémarrage immédiat* (si vous sélectionnez *Redémarrage ultérieur*, l'installation ne sera pas achevée tant que vous n'aurez pas fait redémarrer l'ordinateur). Cliquez sur **OK** pour terminer.

Pour vous assurer que l'installation a réussi, consultez 2.3. [Securitoo AntiVirus Firewall est-il actif et fonctionne-t-il correctement ?](#)

Remarque : Lorsque l'installation est terminée, le contrôle d'application peut vous demander d'autoriser ou non l'accès à Internet par toute application. Pour obtenir des instructions, consultez 2.2 [Que faire lorsque la fenêtre de contrôle d'application apparaît ?](#)

1.3 Si vous devez désinstaller le logiciel Securitoo AntiVirus Firewall

Désinstallez Securitoo AntiVirus Firewall à l'aide de la fonction *Ajout/Suppression de programmes* du panneau de configuration Windows. Cette méthode assure la suppression sûre et complète du programme. Pour ce faire :

1. Ouvrez le menu Démarrer de Windows.
2. Sélectionnez *Paramètres -> Panneau de configuration -> Ajout/Suppression de programmes*.

3. Sélectionnez Securitoo AntiVirus Firewall et cliquez sur **Supprimer**.
4. Redémarrer l'ordinateur.

2. Démarrage

2.1 Première utilisation de Securitoo AntiVirus Firewall

Si vous utilisez Securitoo AntiVirus Firewall pour la première fois, consultez les sections suivantes, qui vous aideront à faire en sorte que Securitoo AntiVirus Firewall soit actif et vous protège de manière adéquate par rapport à vos besoins de sécurité.

- Section 2.2. [Que faire lorsque la fenêtre de contrôle d'application apparaît ?](#).
- Section 2.3. [Securitoo AntiVirus Firewall est-il actif et fonctionne-t-il correctement ?](#)
- Section 2.4. [Options d'accès à Securitoo AntiVirus Firewall](#).

2.2 Que faire lorsque la fenêtre de contrôle d'application apparaît ?

Lorsque Securitoo AntiVirus Firewall, est installé, la fonction de contrôle d'application peut intervenir lorsqu'une application tente de se connecter à Internet, selon votre profil d'utilisation du firewall.

Cette fonction permet de naviguer en toute sécurité et constitue une excellente défense contre les programmes malveillants tels que les chevaux de Troie (pour une définition de ce terme et d'autres concepts, voir le [Glossaire](#) en page 36). Au début, cependant, elle entraînera le blocage ou l'ouverture de connexions à une adresse particulière. Le nombre de demandes diminuera ensuite et vous ne verrez que rarement la fenêtre de contrôle d'application, à moins que vous n'installiez un nouveau logiciel ou qu'une application malveillante tente de se connecter à Internet à partir de votre ordinateur.

Exemple : Lancement du navigateur Internet pour la première fois après l'installation

1. Lancez votre navigateur Internet (par exemple Internet Explorer ou Netscape).



2. La fenêtre de contrôle d'application apparaît, vous demandant si la tentative de connexion "Internet Explorer" doit être autorisée ou refusée.


- Sélectionnez *Mémoriser cette connexion pour utilisation ultérieure*, car vous savez que votre navigateur Internet est une application sûre.
- Cliquez sur **Autoriser**, car vous savez que le navigateur que vous avez lancé vous-même est sûr (pour en savoir plus sur ce qui peut être considéré comme sûr ou non, voir 5.2 *Utilisation du contrôle d'application* en page 21).

Vous pouvez cliquer sur **Aide** pour en savoir plus sur le contrôle d'application.


Remarque : Si vous souhaitez désactiver le contrôle d'application, accédez au menu Firewall. Face à Contrôle d'application, cliquez sur **Changer**. Le message d'état changera de *Invite* en *Autoriser et connecter*.

Pour plus d'informations sur le contrôle d'application, voir 5.2 *Utilisation du contrôle d'application* en page 21.










2.3 Securitoo AntiVirus Firewall est-il actif et fonctionne-t-il correctement ?

Après avoir installé Securitoo AntiVirus Firewall ou chaque fois que vous l'utilisez, vous pouvez vérifier que Securitoo AntiVirus Firewall est actif et fonctionne correctement d'après l'icône  affichée dans la barre d'état de Windows (angle inférieur droit de l'écran) comme illustré ci-dessous :



Remarque : Sous Windows XP, les icônes peuvent être masquées. Pour afficher les icônes masquées, cliquez sur le bouton .

L'icône peut se présenter différemment ou non, selon l'état de Securitoo AntiVirus Firewall. Référez-vous à la liste des icônes ci-dessous pour connaître leur signification :

Icône	Signification	Que faire
	Securitoo AntiVirus Firewall fonctionne correctement. Votre ordinateur est protégé.	Utilisez normalement votre courrier électronique et votre navigateur Internet.
	Installation en cours. Votre ordinateur n'est pas encore protégé.	Attendez la fin de l'installation. L'icône  apparaît lorsque l'installation est terminée.
	Erreur. Une erreur s'est produite dans Securitoo AntiVirus Firewall.	Placez le pointeur de la souris sur l'icône  pour voir la raison de l'erreur. Au besoin, faites redémarrer l'ordinateur.
	Avertissement. Une fonction de protection a été désactivée ou vos définitions de virus ne sont plus à jour. Votre ordinateur n'est pas entièrement protégé.	Placez le pointeur de la souris sur l'icône  pour voir la bulle d'aide de l'icône d'état. Activez la fonction qui est actuellement désactivée ou accédez à Securitoo AntiVirus Firewall et vérifiez les mises à jour.
	Déchargé. Securitoo AntiVirus Firewall est désactivé et votre ordinateur n'est pas protégé.	Cliquez avec le bouton droit sur l'icône  et sélectionnez <i>Relancer</i> pour activer Securitoo AntiVirus Firewall.

Pas d'icône	Securitoo AntiVirus Firewall n'est pas installé. Votre ordinateur n'est pas protégé.	Faites redémarrer l'ordinateur et installez Securitoo AntiVirus Firewall.
-------------	--	---

2.4 Options d'accès à Securitoo AntiVirus Firewall

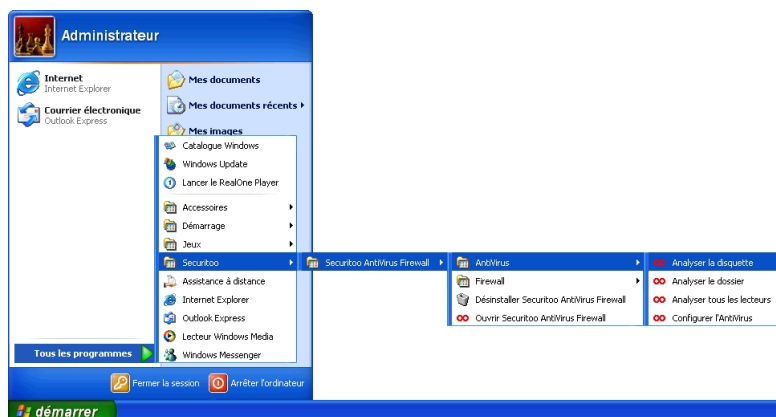
Il existe plusieurs façons d'accéder à Securitoo AntiVirus Firewall et de l'utiliser :

- Menu Démarrer de Windows
- Icône ☹
- Menu contextuel de Securitoo AntiVirus Firewall

Menu Démarrer de Windows

Pour ouvrir Securitoo AntiVirus Firewall, et accéder aux opérations de base :

1. Ouvrez le menu *Démarrer* de Windows.
2. Pointez *Programmes* et le sous-menu Securitoo AntiVirus Firewall.
3. Cliquez sur *Ouvrir Securitoo AntiVirus Firewall* pour commencer à utiliser Securitoo AntiVirus Firewall ou sélectionnez une autre option dans le sous-menu de Securitoo AntiVirus Firewall.



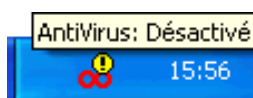
Icône ☹

Vous pouvez utiliser l'icône ☹ dans la barre d'état de Windows (angle inférieur droit de l'écran) pour ouvrir Securitoo AntiVirus Firewall, voir l'état du programme ou accéder à son menu contextuel.


Pour ouvrir Securitoo AntiVirus Firewall, cliquez deux fois sur l'icône ☹ avec le bouton gauche de la souris.

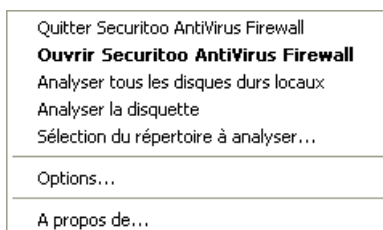
Bulle d'aide de l'icône d'état Securitoo AntiVirus Firewall

Placez le pointeur de la souris sur l'icône pour voir la bulle d'aide de l'icône d'état Securitoo AntiVirus Firewall. Cette bulle d'aide permet de voir instantanément si Securitoo AntiVirus Firewall a un problème, comme dans l'exemple ci-dessous où la protection antivirus a été désactivée.



Menu contextuel de Securitoo AntiVirus Firewall

Cliquez sur l'icône  avec le bouton droit de la souris pour accéder au menu contextuel Securitoo AntiVirus Firewall, qui contient une liste des commandes les plus utilisées. À partir de ce menu, vous pouvez ouvrir Securitoo AntiVirus Firewall ou lancer immédiatement une détection de virus.



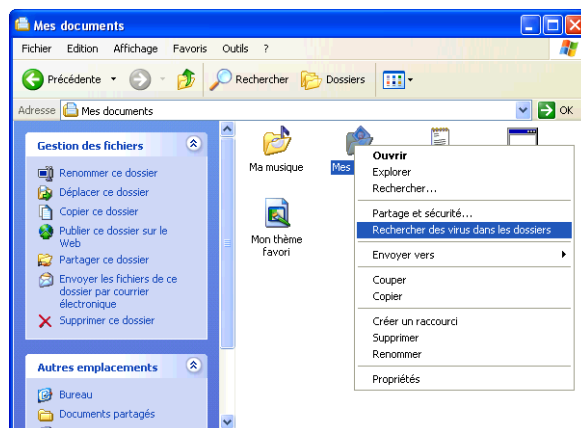
Pour mieux comprendre chaque option du menu, consulter le tableau ci-dessous:

Sélection	Explication
Ouvrir Securitoo AntiVirus Firewall	Ouvre Securitoo AntiVirus Firewall.
Quitter Securitoo AntiVirus Firewall	Décharge les produits de la mémoire. Cette opération est parfois nécessaire pour l'installation de certains logiciels ou pour effectuer des tâches pour lesquelles les performances sont critiques. Ne laissez pas inutilement votre ordinateur dans cet état, car il n'est pas protégé.
Analyser tous les disques durs locaux	Securitoo AntiVirus Firewall analyse tous les disques durs disponibles sur votre ordinateur.
Analyser la disquette	Securitoo AntiVirus Firewall analyse toute disquette présente dans le lecteur A:.
Sélection du répertoire à analyser...	Securitoo AntiVirus Firewall analyse la cible de votre choix. L'arborescence des répertoires apparaît. Sélectionnez le répertoire cible et cliquez sur OK pour commencer l'analyse.
Options...	Ouvre les options avancées
A propos de...	Affiche des informations concernant Securitoo AntiVirus Firewall.

Menu contextuel de Securitoo AntiVirus Firewall

Vous pouvez analyser des disques, dossiers et fichiers à la recherche de virus avec l'Explorateur Windows. Pour ce faire :

1. Placez le pointeur de la souris sur le disque, dossier ou fichier à analyser et cliquez avec le bouton droit de la souris.
2. Dans le menu contextuel, sélectionnez Rechercher des virus dans les dossiers. La fenêtre *Analyse manuelle* apparaît et l'analyse commence.



Si un virus est détecté, voir 4.3 [Suppression d'un virus de votre ordinateur](#) en page 14.




Remarque : Lorsque vous effectuez une analyse, Securitoo AntiVirus Firewall utilise les paramètres d'analyse définis dans votre profil antivirus actuel.

3. Accueil

La page *Accueil* présente un aperçu rapide et détaillé des paramètres de sécurité et de l'état de Securitoo AntiVirus Firewall.



Sur la page *Accueil*, vous pouvez :

- Sélectionner votre profil d'antivirus et surveiller l'état de la protection antivirus. Pour plus d'informations et des instructions, voir 4.  *AntiVirus* en page 13.
- Sélectionner votre profil de firewall. Pour plus d'informations et des instructions, voir 5.  *Firewall* en page 20.
- Activer et désactiver les mises à jour automatiques et afficher des informations sur les mises à jour reçues sur votre ordinateur. Pour plus d'informations et des instructions, voir 6.  *Mise à jour automatique* en page 28.

4. AntiVirus

Sur la page du menu AntiVirus, vous pouvez :



- Sélectionner votre profil d'antivirus (pour plus d'informations, voir 4.1 [Profil de protection antivirus](#) en page 13).
- Voir quand vous avez reçu des mises à jour des définitions de virus et quand vos fichiers de définitions de virus ont été créés par le laboratoire Securitoo.
- Voir le nombre de fichiers analysés par Securitoo AntiVirus Firewall et combien de virus ont été supprimés.
- Analyser manuellement des fichiers (pour plus d'informations, voir 4.2 [Rechercher des virus](#) en page 14).

4.1 Profil de protection antivirus

Les profils de protection antivirus permettent de changer instantanément votre niveau de protection en fonction de vos besoins. Les profils sont automatiquement mis à jour pour garantir votre protection contre les formes les plus récentes de programmes malveillants et d'attaques via Internet.

Si vous changez les paramètres d'un profil (dans la fenêtre Paramètres avancés du menu AntiVirus), son nom sera changé en Personnalisé. Pour restaurer votre profil de protection antivirus, voir [Modification du profil de protection antivirus](#) ci-dessous.

Modification du profil de protection antivirus

Vous pouvez changer de profil à tout moment selon la protection dont vous avez besoin. Un changement de profil modifie le niveau des actions automatisées et des rapports.

Pour changer votre profil, dans la section Profil de l'AntiVirus :

1. Cliquez sur **Modifier**.
2. Sélectionnez un profil dans la liste déroulante. Lisez attentivement la description de chaque profil avant de l'activer.

3. Cliquez sur **OK** pour utiliser le profil sélectionné.

4.2 Rechercher des virus

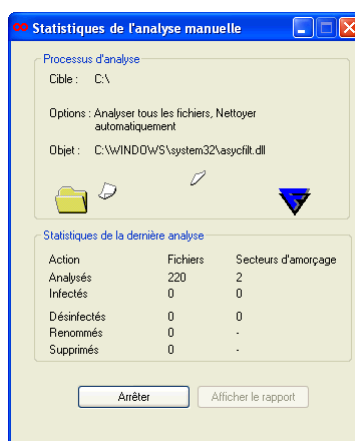
Lorsque la protection antivirus est activée, votre ordinateur est protégé. L'ouverture ou la fermeture d'un fichier entraîne automatiquement la recherche de virus dans ce fichier.

Si vous suspectez un certain fichier de contenir un virus, vous pouvez l'analyser ou analyser votre ordinateur à la recherche de virus. Pour effectuer une analyse vous-même, procédez comme suit :

1. Cliquez sur **Rechercher des virus**.
2. Dans le menu, choisissez d'analyser tous les disques durs locaux, une disquette ou un dossier (encore appelé *répertoire*) que vous spécifiez.

Analyser tous les disques durs locaux
Analyser la disquette
Sélection du répertoire à analyser...

3. La fenêtre *Statistiques de l'analyse manuelle* apparaît, affichant les statistiques de l'analyse. Cliquez sur **Arrêter** pour interrompre l'analyse à tout moment.



4. A la fin de l'analyse, un rapport est généré. Cliquez sur **Afficher le rapport** pour visualiser le rapport dans votre navigateur Web. Si un virus est détecté, voir 4.3 [Suppression d'un virus de votre ordinateur](#) en page 14.

Remarque : Lorsque vous effectuez une analyse, Securitoo AntiVirus Firewall utilise les paramètres définis dans votre profil de protection antivirus actuel. Pour sélectionner un autre profil, voir 4.1 [Profil de protection antivirus](#) en page 13.

4.3 Suppression d'un virus de votre ordinateur

Comment l'Assistant de nettoyage supprime un virus

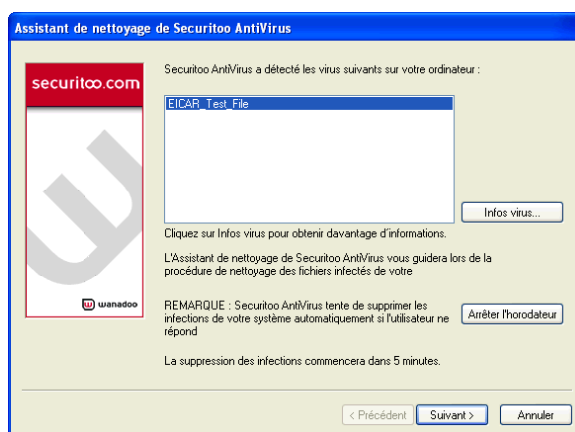
L'Assistant de nettoyage de Securitoo AntiVirus Firewall apparaît si :

- un virus a été détecté lors d'une analyse.
- un virus a été détecté et votre profil de protection antivirus est réglé pour afficher toutes les anomalies découvertes et vous les signaler avant la désinfection.
- un virus a été détecté durant une analyse automatisée (option Protection automatique activée) et Securitoo AntiVirus Firewall n'a pas pu supprimer le virus lui-même.

L'Assistant vous aide à éradiquer le virus en plusieurs étapes, comme suit.

Étape 1 - Virus détecté

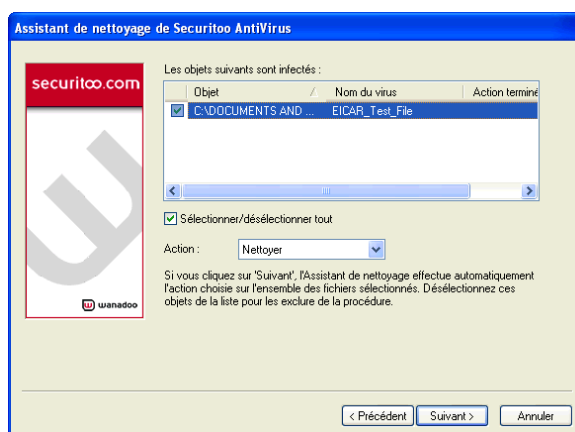
Le nom du virus détecté est affiché, comme illustré ci-dessous. Pour poursuivre la désinfection, cliquez sur **Suivant**.



Remarque : Pour plus d'informations sur le virus, cliquez sur son nom, puis sur **Infos** sur les virus. Si le virus est récent, il n'est peut-être pas décrit. Consultez le site Internet de Securitoo <http://www.securitoo.com/> pour obtenir les informations les plus récentes.

Étape 2 - Action exécutée

La liste des fichiers infectés s'affiche.



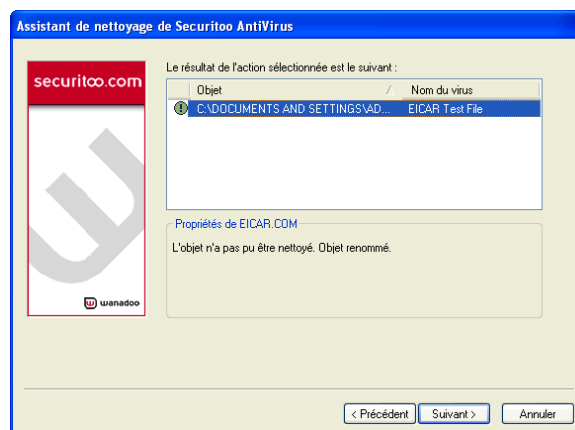
Dans la zone Action, sélectionnez l'opération à exécuter sur les fichiers infectés. Ces actions sont brièvement décrites dans le tableau ci-dessous.

Action	Explication
Nettoyer	L'Assistant de nettoyage désinfecte le fichier. Remarque : Si l'Assistant de nettoyage ne parvient pas à désinfecter le fichier, il tente de le renommer automatiquement.
Supprimer	L'Assistant de nettoyage supprime le fichier qui contient le virus. Toutes les informations contenues dans le fichier sont perdues. Avertissement : Si vous sélectionnez Supprimer, l'objet infecté est également supprimé.
Renommer	L'Assistant de nettoyage renomme le fichier de sorte qu'il ne soit pas possible de l'exécuter automatiquement. Cela empêche l'activation du virus.

Une fois que vous avez sélectionné l'action à effectuer, cliquez sur **Suivant** et l'Assistant de nettoyage applique automatiquement l'action choisie à tous les objets sélectionnés.

Étape 3 - Résultats de l'action

Les résultats de l'action s'affichent. Si vous avez choisi une action qui a échoué, vous pouvez revenir en arrière et répéter l'étape 2 pour choisir une autre action.



Si le nettoyage et la suppression échouent, vous pourrez éventuellement choisir de renommer le fichier. C'est généralement une bonne option pour les exécutables (.exe) infectés, car elle change l'extension en une extension de fichier qui n'est pas autorisée à s'exécuter automatiquement.

Notez que, si le nettoyage a échoué, il se peut que l'Assistant de nettoyage l'ait déjà automatiquement renommé (voir le tableau des actions ci-dessus). Dans ce cas, une note à cet effet apparaît dans le champ *Propriétés*.

Remarque : Si un nouveau virus est découvert, si les définitions de virus ne sont plus à jour ou si vous recevez une fausse alerte, le nettoyage ou la suppression peuvent échouer. Pour des instructions sur ce qu'il faut faire dans ce cas, voir [Suppression d'un virus lorsque l'Assistant de nettoyage échoue](#) en page 17.

Si l'opération a réussi, cliquez sur **Suivant** pour continuer.

Étape 4 - Vérifier et terminer

Un rapport de nettoyage sera généré après la fin du processus de nettoyage. Si vous ne souhaitez pas obtenir de rapport, ne cochez pas la case Créer le rapport. Notez que le rapport de nettoyage n'est pas généré pour les virus trouvés lors d'une analyse automatisée.

Cliquez sur **Terminer** pour quitter l'Assistant de nettoyage.




Le rapport de nettoyage s'affiche dans le navigateur Web par défaut et contient des liens vers les descriptions de virus correspondantes dans la base de données des virus du Web Club.

Remarque : Si le virus a été détecté dans un fichier qui était verrouillé par un autre processus au moment où l'Assistant de nettoyage a tenté de le supprimer, une fenêtre apparaîtra pour demander de faire redémarrer l'ordinateur. Si cette fenêtre apparaît, enregistrez tous vos documents ouverts et suivez les instructions affichées.

Suppression d'un virus lorsque l'Assistant de nettoyage échoue

Si l'Assistant de nettoyage n'a pas pu nettoyer ou supprimer le fichier, une des conditions suivantes est probablement à l'origine de cet échec :

- **La base de données des définitions de virus n'est plus à jour.** Vérifiez que vous possédez les fichiers de définition les plus récents et réessayez (voir 6.  [Mise à jour automatique](#) en page 28).
- **Fausse alerte.** Tout est fait pour que Securitoo AntiVirus Firewall évite de déclarer infecté un fichier inoffensif, mais la nature complexe des fichiers fait qu'une fausse suspicion est toujours possible.
- **Un nettoyage manuel est nécessaire.** Dans certains cas, vous devez exécuter un outil qui nettoie le fichier et supprime le virus. C'est souvent le cas pour des virus plus modernes utilisant des techniques avancées pour se cacher et s'attacher à vos fichiers.
- **Vous avez découvert un nouveau virus.** Un nouveau type de virus peut avoir infecté votre ordinateur. Pas de panique. Vos fichiers sont en sécurité, puisque Securitoo AntiVirus Firewall a détecté et arrêté le virus avant qu'il fasse des dégâts.

Si vous êtes certain que le fichier est sans danger, vous pouvez ignorer les avertissements. Vous pouvez configurer la protection automatique et l'analyse manuelle pour qu'elles ignorent ce fichier lors de prochaines analyses. Pour ce faire, voir 4.5 [Demander à l'antivirus d'ignorer/analyser certains fichiers](#) en page 18.


Comment supprimer manuellement le virus

1. Essayez de nettoyer le fichier vous-même. Pour supprimer plus facilement le virus, vous pouvez, au choix :
 - Consulter le site Internet de Securitoo <http://www.securitoo.com/> pour obtenir des informations sur le virus. Ces informations vous aideront à supprimer le virus et peuvent comprendre un lien vers l'outil nécessaire pour ce faire.
 - **Utilisateurs avancés** : Accédez directement à <ftp://ftp.europe.f-secure.com/anti-virus/tools/> pour trouver un outil de nettoyage adapté.
Les outils contiendront toutes les instructions à suivre pour supprimer le virus de votre système.
2. Si vous avez essayé d'utiliser l'Assistant de nettoyage sans succès, que votre base de données des définitions de virus est à jour et que les outils de nettoyage proposés sur le site Web de F-Secure n'apportent pas de solution, suivez les instructions de la section 4.4 *Que faire si vous pensez avoir trouvé un nouveau virus ?* en page 18.

4.4 Que faire si vous pensez avoir trouvé un nouveau virus ?

Si Securitoo AntiVirus Firewall vous avertit que vous avez un fichier infecté par un virus, mais ne peut pas vous donner le nom du virus ni le nettoyer ou le supprimer, il se peut qu'il s'agisse d'un tout nouveau virus. Tant que vous n'avez pas la certitude que le virus potentiel a été supprimé ou qu'il s'agissait d'une fausse alerte, n'essayez pas d'utiliser le fichier.

Pour supprimer le virus, procédez comme suit :

1. Vérifiez que votre base de données de définitions de virus est à jour. Un fichier de définitions plus récent peut indiquer à Securitoo AntiVirus Firewall comment traiter le virus et le supprimer de votre ordinateur.
2. Si vous avez déjà les définitions de virus les plus récentes (voir 6.  *Mise à jour automatique* en page 28), vérifiez sur le site de F-Secure s'il existe des outils que vous pouvez utiliser pour supprimer manuellement le virus (<http://www.f-secure.com/v-descs/> ou <ftp://ftp.europe.f-secure.com/anti-virus/tools/>).
3. Si ces mesures échouent, envoyez le fichier à F-Secure VirusLab. Pour des instructions, visitez : <http://www.f-secure.com/support/technical/general/samples.shtml>.

4.5 Demander à l'antivirus d'ignorer/analyser certains fichiers

Dans certains cas, vous souhaitez demander à l'antivirus d'ignorer certains types de fichiers ou des fichiers spécifiques. Par exemple :

- Vous êtes certain qu'un fichier n'est pas infecté, mais recevez des fausses alertes.
- Votre ordinateur possède des ressources limitées et l'analyse de tous les fichiers par l'antivirus ralentirait l'ordinateur de manière insupportable.
- Le fichier est d'un type qui n'est jamais infecté par un virus.

Certains profils règlent déjà l'analyse automatisée de manière à analyser certains types de fichiers. Ces réglages offrent un bon équilibre entre la nécessité d'analyser les fichiers contenant généralement des virus et la limitation de l'impact sur le temps processeur et la mémoire.

Avertissement : Si vous demandez à l'antivirus d'ignorer certains fichiers, ces fichiers restent exposés à une attaque virale future et cela limite la possibilité de détecter et de nettoyer des virus. Cet usage n'est donc recommandé que dans des cas extrêmes.

Réglage de la protection en temps réel ou de l'analyse manuelle pour analyser certains fichiers

Pour demander à la protection en temps réel ou à l'analyse manuelle d'analyser certains fichiers :

1. Ouvrez la fenêtre principale de Securitoo AntiVirus Firewall.
2. Sélectionnez le menu AntiVirus et cliquez sur Paramètres avancés. Dans les onglets Protection en temps et Analyse manuelle, assurez-vous que l'option Fichiers avec ces extensions est cochée.

Réglage de la protection en temps réel ou de l'analyse manuelle pour ignorer certains fichiers

Pour demander à la protection en temps réel ou à l'analyse manuelle d'ignorer certains fichiers :

1. Ouvrez la fenêtre principale de Securitoo AntiVirus Firewall.
2. Sélectionnez le menu AntiVirus et cliquez sur **Paramètres avancés**. Dans les onglets Protection en temps et Analyse manuelle, assurez-vous que :
 - l'option Exclure les fichiers avec ces extensions est cochée, puis entrez les extensions de fichiers dans la zone de texte.
 - l'option Exclure les objets (fichiers, dossiers...) est cochée. Cliquez sur **Sélectionner** pour parcourir les fichiers à exclure et les ajouter à la liste des fichiers à exclure.

5. Firewall



Sur la page du menu Firewall, vous pouvez :

- Sélectionner votre profil de protection Internet (pour plus d'informations, voir 5.1 [Profils de Protection](#) Internet en page 20).
- Changer l'état du contrôle d'application. Pour ce faire, cliquez sur **Modifier** face à l'état actuel du contrôle d'application.
- Vérifier combien d'applications sont autorisées à se connecter à Internet. Pour changer les droits de connexion d'une application, voir [Modification des droits de connexion d'une application](#) en page 21.
- Changer votre configuration d'alerte. Pour ce faire, cliquez sur **Modifier** face à l'état actuel.
- Voir combien d'alertes vous avez reçues depuis la date spécifiée. Cliquez sur **Afficher** pour voir une liste des alertes.
- Vérifier combien de paquets ont été éliminés. Les paquets dangereux connus sont toujours éliminés par le firewall, mais vous pouvez aussi affecter cette fonction en personnalisant les règles du firewall (voir 5.3 [Personnalisation des profils du firewall](#) en page 23).
- Vérifier quand vous avez reçu la dernière alerte du firewall. Cliquez sur **Détails** pour afficher les détails de la dernière alerte et les cinq protocoles et hôtes (adresses IP) les plus fréquemment bloqués.

5.1 Profils de Protection Internet

Les profils du firewall permettent de changer instantanément le niveau de protection en fonction de vos besoins ; ils sont automatiquement mis à jour afin de garantir votre protection contre les formes les plus récentes des programmes malveillants et attaques Internet.

Modification du profil du firewall

Vous pouvez changer de profil à tout moment selon la protection dont vous avez besoin. Un changement de profil modifie le niveau des actions automatisées et des rapports.

Pour changer votre profil, dans la section Profil du Firewall :

1. Cliquez sur **Modifier**.
2. Sélectionnez un profil dans la liste déroulante. Lisez la description de chaque profil avant de l'activer.
3. Cliquez sur **OK** pour utiliser le profil sélectionné.

Pour personnaliser un profil, voir 5.3 [Personnalisation des profils du firewall](#) en page 23.

5.2 Utilisation du contrôle d'application

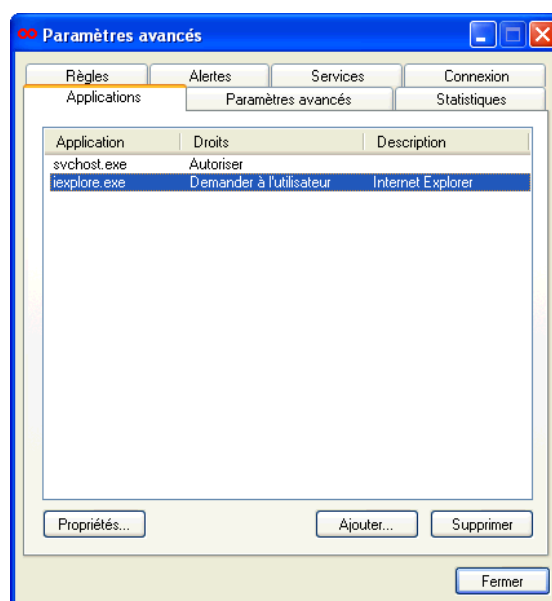
Le contrôle d'application est une fonction de Securitoo AntiVirus Firewall qui vérifie toutes les applications se connectant à Internet à partir de votre ordinateur. Le contrôle d'application vous demande si la tentative de connexion de l'application doit être autorisée ou refusée, comme décrit sous 2.2 [Que faire lorsque la fenêtre de contrôle d'application apparaît ?](#) en page 6. Autorisez les applications connues et sûres à se connecter à Internet ; si une application n'est pas sûre, refusez-lui de se connecter.

Un fichier intitulé Journal des actions enregistre toutes les connexions et leurs propriétés pour vous permettre de voir où votre ordinateur s'est connecté. Pour y accéder, cliquez sur **Paramètres avancés**, puis sur l'onglet *Connexion*.

Modification des droits de connexion d'une application

Si vous souhaitez changer les droits de connexion ou les propriétés d'une application, procédez comme suit :

1. Accédez au menu Firewall et cliquez sur **Modifier** face à *Applications autorisées/refusées*.
2. La page *Paramètres avancés* s'ouvre.



3. Sélectionnez l'application dont vous souhaitez changer les propriétés (les droits actuels sont indiqués dans la colonne Droits). Cliquez sur **Propriétés**.
4. Sélectionnez Refuser, Invite ou Autoriser. Cliquez sur **OK** pour retourner à la page Applications.
5. Les nouveaux droits de l'application apparaissent dans la colonne Droits face au nom de l'application. Cliquez sur **Fermer** pour terminer.

Quels sont les éléments pouvant être considérés comme "fiables" ?

- Une application connue que vous avez lancée vous-même.
- Des services Windows se connectant à Internet.

Des services Microsoft Windows sûrs

Certains services Microsoft Windows exigent un accès au réseau pour fonctionner. La plupart des services sont automatiquement autorisés mais le contrôle d'application peut vous demander d'autoriser ou non les services ci-dessous, en particulier sur les plates-formes Windows NT 4.0, Windows 2000 et Windows XP. Autorisez ces services à accéder au réseau, faute de quoi certaines fonctionnalités Windows risquent de ne pas fonctionner.

Liste des applications :

Remarque : %Winnt% se réfère au répertoire d'installation de Windows, généralement C:\Winnt\ ou C:\Windows

Exécutable	Emplacement	Description	Trafic réseau
SVCHOST.EXE	%Winnt%\System32\	Processus hôte générique pour les services Win32	udp/67 out, udp/68 in, udp/137 out
SPOOLSV.EXE	%Winnt%\System32\	Sous-système de spoule	udp/137 out, udp/138 out
LSASS.EXE	%\Windows%\System32\	Exécutable LSA et DLL Serveur	udp/137 out
SERVICES.EXE	%Winnt%\System32\	Application Services et Contrôleur	udp/67 out, udp/68 in, udp/137 out
WINLOGON.EXE			udp/137 out

Quels sont les éléments pouvant être considérés comme "non fiables" ?

Les applications reçues d'une source non fiable doivent toujours être traitées comme suspectes. Les applications reçues d'une source fiable sans accord préalable doivent toujours être traitées comme suspectes.

- Toute application que vous n'avez pas installée vous-même ou que vous ne connaissez pas.
- Toute application considérée comme fiable, mais qui tente de se connecter sans que vous l'ayez lancée.
- Toute connexion ne contenant pas de nom cible (adresse Web sous forme de texte) propre.

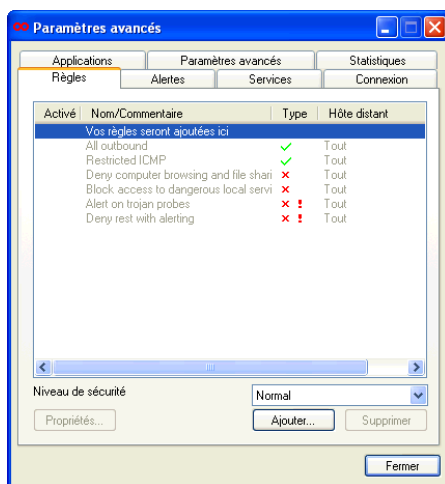
5.3 Personnalisation des profils du firewall

Dans certains cas, vous souhaitez ajouter, modifier ou supprimer les règles définissant que faire de certaines connexions. Ces situations se produisent lorsque vous souhaitez :

- Vous connecter à un nouveau serveur de jeux sur un ordinateur particulier.
- Autoriser les connexions en général, mais bloquer une connexion à un site ou à un ordinateur particulier que vous ne considérez pas comme fiable.

Pour personnaliser vos paramètres de firewall :

1. Cliquez sur **Paramètres avancés** sur la page relative au menu Firewall. La fenêtre Paramètres avancés s'ouvre.
2. Dans le menu déroulant Niveau de sécurité, sélectionnez le profil à personnaliser.
3. Cliquez sur l'onglet Règles (s'il n'est pas encore sélectionné).



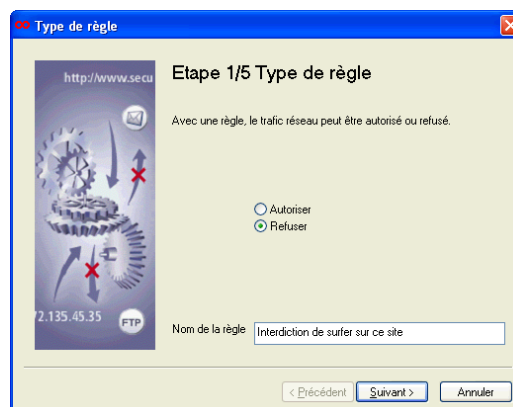
- Pour modifier une règle existante, sélectionnez-la dans la liste et cliquez sur **Propriétés**.
- Pour ajouter une règle, cliquez sur **Ajouter**.
- Pour supprimer une règle, sélectionnez-la dans la liste et cliquez sur **Supprimer**.

Remarque : Il n'est pas possible de modifier ni de supprimer les règles prédéfinies. Vous pouvez uniquement ajouter des règles ou changer/supprimer des règles que vous avez créées vous-même.

Création d'une nouvelle règle du firewall

Étape 1 – Type de règle

Donnez un nom descriptif à la règle et choisissez d'autoriser ou refuser la connexion.



Étape 2 - Spécifiez la (les) cible(s)

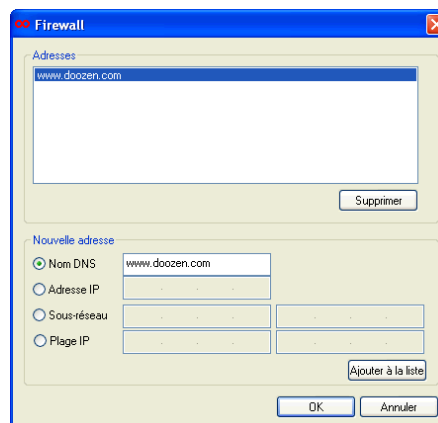
Choisissez si cette règle s'applique à toutes les connexions en cours ou à certaines connexions uniquement.



Vous pouvez :

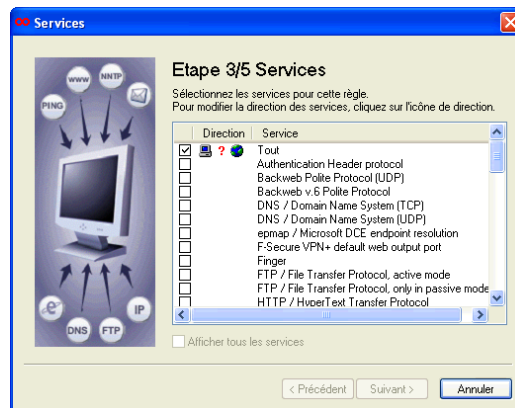
- Cocher **Toute adresse IP** pour appliquer la règle à toutes les connexions Internet et cliquer sur **Suivant** pour passer à l'étape 3 ou
- Désélectionner **Toute adresse IP** et cliquer sur **Modifier** pour ouvrir une nouvelle fenêtre où vous pouvez entrer les détails des cibles.
- Les cibles peuvent être énumérées dans un ordre quelconque et peuvent être n'importe quel nom DNS, adresse IP, sous-réseau (au format de masque de réseau binaire) ou plage d'adresses IP. Par exemple :
 - Nom DNS : www.un.domaine.org
 - Adresse IP : 192.168.5.16
 - Sous-réseau : 192.168.88.0/29
 - Plage IP : 192.168.1.1-192.168.1.63

Cliquez sur **Ajouter à la liste** pour ajouter la nouvelle cible à la liste de cibles auxquelles s'applique la règle. Pour supprimer une adresse cible, sélectionnez-la dans la liste et cliquez sur **Supprimer**. Pour modifier les propriétés d'une cible, sélectionnez-la dans la liste. Cliquez sur **OK** pour retourner à la page Hôte(s) distant(s) et cliquez sur **Suivant** pour continuer.



Étape 3 - Choisissez le service et la direction de la règle

Dans la liste des services disponibles, choisissez le service auquel cette règle s'appliquera. Si vous voulez que la règle s'applique à tous les services, sélectionnez *Tous* dans le haut de la liste. Vous pouvez sélectionner autant de services individuels que vous le souhaitez.



Pour les services choisis, sélectionnez la direction dans laquelle s'applique la règle en cliquant sur le point d'interrogation rouge qui apparaît. Continuez à cliquer pour faire défiler les options disponibles en boucle. Pour des exemples, consultez le tableau ci-dessous.

Sélection	Terme	Explication
	Non défini	La direction n'a pas encore été définie. Cliquez sur le graphique pour définir une direction.
	Entrant	Le service sera autorisé /refusé s'il provient d'Internet en direction de votre ordinateur.
	Sortant	Le service sera autorisé /refusé s'il provient de votre ordinateur en direction d'Internet.
	Les deux	Le service sera autorisé /refusé dans les deux directions, qu'il provienne de votre ordinateur ou s'y dirige.

Étape 4 - Choisissez la connexion et l'option de création de rapports

Vous pouvez choisir d'être informé ou non chaque fois que la règle est appliquée à une tentative de connexion.



- *Aucune alerte* : vous ne recevrez aucune information lorsque la règle est appliquée à une connexion.
- *Enregistrer* : des données concernant la connexion sont enregistrées dans un fichier.
- *Enregistrer et afficher* : des données sont enregistrées et une fenêtre de notification s'affiche par exemple lorsque la connexion est autorisée/refusée.

Étape 5 - Vérifier et accepter la règle

Vous pouvez maintenant vérifier la règle. Cliquez sur **Précédente** pour revoir la règle et apporter des modifications éventuelles.



Si vous êtes satisfait de votre nouvelle règle, cliquez sur **Terminer**. Votre nouvelle règle sera ajoutée en haut de la liste des règles actives sur l'onglet Règles des paramètres avancés.

5.4 Paramètres avancés

Remarque : Cette section concerne uniquement les utilisateurs avertis. La modification des réglages peut désactiver le firewall.

Pour accéder aux paramètres avancés du firewall, cliquez sur **Paramètres avancés** dans la page relative au menu Firewall. Cliquez sur l'onglet Paramètres avancés dans la fenêtre qui apparaît.

Les éléments suivants doivent être pris en considération lors de la personnalisation des paramètres avancés du firewall.

Interface approuvée

Cette option peut être utilisée si l'ordinateur où est installé Securitoo AntiVirus Firewall sert de passerelle réseau, p. ex. si le partage de connexion Internet est activé dans Windows. L'interface réseau utilisée pour le réseau local peut être réglée sur « Interface approuvée » de sorte qu'aucune règle du firewall ne s'y applique.

Remarque : Cette interface réseau sera laissée complètement ouverte et n'est pas protégée.

Filtre de paquets activé

Le filtrage de paquets est la fonction principale du firewall ; si vous le désactivez, Securitoo AntiVirus Firewall sera grandement inefficace contre tous les types d'attaques réseau.

Contrôle d'application activé

Ne désactivez pas le contrôle d'application dans la fenêtre Paramètres avancés. La désactivation du contrôle d'application augmente le risque d'attaques basées sur un logiciel et ne doit se faire qu'à des fins de dépannage, etc.

Si vous souhaitez désactiver le contrôle d'application, accédez au menu Firewall et changez l'état du contrôle d'application de *Demander à l'utilisateur* en *Autoriser automatiquement*.

6. Mise à jour automatique

Le service de mise à jour automatique s'active de manière transparente à l'arrière-plan chaque fois que vous vous connectez à Internet et veille à ce que vous receviez les mises à jour les plus récentes sur votre ordinateur.



Dans la section Mise à jour automatique, vous pouvez :

- Cliquer sur **Activer** ou **Désactiver** les mises à jour automatiques.
- Voir quand a eu lieu le dernier contrôle de mise à jour et/ou quand aura lieu le prochain.

Si vous souhaitez vérifier personnellement que vous possédez les définitions de virus les plus récentes, cliquez sur **Vérifier maintenant**. Si vos définitions ne sont pas à jour, les versions les plus récentes sont alors téléchargées.

Remarque : Si vous utilisez un modem ou une liaison RNIS pour vous connecter à Internet, cette connexion doit être active pour que le contrôle de mise à jour puisse avoir lieu.

Remarque pour les utilisateurs de routeurs RNIS ou de systèmes à numérotation automatique : Par défaut, les mises à jour automatiques sont programmées une fois par heure. Cela signifie qu'une connexion à Internet sera ouverte une fois par heure si vous avez un routeur RNIS ou un système similaire de numérotation automatique (et chaque connexion vous coûtera de l'argent). Si vous souhaitez empêcher votre routeur RNIS d'établir automatiquement la connexion, désactivez la fonction Mises à jour automatiques et utilisez le bouton **Vérifier maintenant** pour vérifier les mises à jour.

- Vérifiez la dernière mise à jour des trois éléments ci-dessous.
 - **Définitions de virus** - Base de données de protection antivirus, fréquemment mise à jour. Ces mises à jour automatiques sont effectuées de manière

transparente à l'arrière-plan, sans intervention de votre part, et s'activent chaque fois que vous vous connectez à Internet.




- **Profils de sécurité** – Divers niveaux de paramètres de sécurité. Pour une protection maximale de votre ordinateur, les profils sont mis à jour chaque fois que de nouveaux types d'attaques sont découverts.
- **Logiciel** - Les mises à jour du logiciel Securitoo AntiVirus Firewall sont téléchargées à l'arrière-plan.

7. Mon abonnement

La page Mon abonnement affiche des informations concernant votre abonnement personnel.



Sur cette page, vous pouvez :

- Consulter l'état de votre abonnement. La date d'échéance de votre abonnement est indiquée, ainsi que l'état actuel et une des icônes d'état suivantes :
 -  Valide Votre abonnement est valide.
 -  Bientôt à expiration Votre abonnement est valide mais vient bientôt à expiration.
 -  Expiré Votre abonnement a expiré.

8. Comment Securitoo AntiVirus Firewall protège votre ordinateur

8.1 AntiVirus

On appelle "antiprogrammes" diverses formes de programmes ou fichiers tels que virus, vers, chevaux de Troie, blagues et canulars développés dans le but de nuire à votre ordinateur.



L'antivirus détecte et supprime les virus et autres programmes informatiques malveillants de votre ordinateur. Chaque fois qu'il y a accès à un fichier, que ce soit à partir du disque dur de votre propre ordinateur, d'une unité de stockage externe ou d'Internet, la fonction antivirus de Securitoo AntiVirus Firewall vérifie que le fichier ne contient pas de virus.

Un logiciel de protection antivirus combiné au chargement automatique des définitions virus les plus récentes garantit la meilleure protection possible contre les virus. Le laboratoire de recherche Securitoo publie et met à jour régulièrement les définitions de virus, les profils et le logiciel Securitoo AntiVirus Firewall, que le programme télécharge rapidement et automatiquement chaque fois que vous vous connectez à Internet.

Securitoo AntiVirus Firewall utilise plusieurs moteurs de détection de virus afin d'assurer une protection sans faille contre les virus. Parmi ceux-ci, le moteur de détection heuristique protège particulièrement contre les virus nouveaux et inconnus.

8.2 Firewall

Chaque fois que votre ordinateur est connecté à Internet, il constitue une cible pour les attaques de sources inconnues à travers le réseau Internet. Dans certains cas, ces attaques ne sont pas agressives, mais sont des messages inoffensifs parvenus à votre ordinateur par accident. Dans d'autres cas, en revanche, une personne ou un ordinateur inconnu tente délibérément d'accéder à votre ordinateur et à vos fichiers.

La sécurité de votre ordinateur peut être compromise de diverses manières, notamment :

- Des services laissés ouverts par inadvertance peuvent facilement être trouvés et utilisés à mauvais escient par des personnes extérieures.



Le firewall protège votre ordinateur pendant que vous êtes connecté à Internet. Cette fonction n'autorise que les connexions de/vers votre ordinateur définies dans votre profil sélectionné. Tout autre trafic est rejeté, ce qui réduit sensiblement les possibilités pour l'intrus de visualiser/modifier les informations sur votre ordinateur.

- Votre ordinateur diffuse des informations le concernant. Lorsqu'il est connecté à Internet, quiconque sait comment lire ces informations peut les utiliser pour déployer une attaque contre vous.



Le firewall empêche votre ordinateur de diffuser sur Internet des informations sur lui-même et bloque toute connexion sortante qui tente de laisser filtrer

des informations vous concernant ou concernant votre ordinateur.

- Certains chevaux de Troie se cachent à l'intérieur de logiciels qui sont normalement fiables. Ils utilisent une connexion ou une application que vous croyez sûre pour transférer des données à votre sujet ou celui de votre ordinateur.



Le firewall identifie les tentatives de chevaux de Troie de transférer des données et empêche la connexion, protégeant ainsi vos données en permanence contre les attaques.

8.3 Comment se prémunir contre les virus et autres antiprogrammes

Securitoo AntiVirus Firewall constitue la meilleure ligne de défense contre les virus en bloquant les virus connus avant qu'ils infestent votre ordinateur. Cependant, vous pouvez aussi contribuer à la protection de votre ordinateur :

- Tenez à jour votre système d'exploitation et vos applications et appliquez les correctifs les plus récents dès qu'ils sont disponibles. Procurez-vous les mises à jour directement auprès du fournisseur (exemple : Microsoft, etc..).
- Lorsque vous téléchargez des fichiers, enregistrez-les toujours sur votre disque dur avant de les ouvrir ou de les exécuter. En enregistrant un fichier téléchargé, vous permettez à Securitoo AntiVirus Firewall de le vérifier.
- La plupart des vers utilisent des messages électroniques pour se diffuser et visent les utilisateurs de Microsoft Outlook ou Outlook Express. Si vous devez utiliser une version d'Outlook, cherchez, téléchargez et installez régulièrement les correctifs de sécurité Outlook publiés par Microsoft.
- Lorsque vous recevez par courrier électronique des annonces non sollicitées ou si un message reçu d'un ami vous paraît bizarre, n'ouvrez pas les pièces jointes et ne cliquez pas sur les liens contenus dans le message. Si vous souhaitez voir le contenu d'une pièce jointe, enregistrez cette dernière sur votre disque dur avant de l'ouvrir plutôt que de l'ouvrir directement depuis votre logiciel de messagerie. Securitoo AntiVirus Firewall peut ainsi vérifier si la pièce jointe ne contient pas de virus.
- Évitez les fichiers provenant de groupes de news publics et de systèmes de conversation en ligne tels qu'IRC et ICQ.
- Évitez de transférer les annonces de virus ou messages en chaîne que vous recevez.

Dépannage

Installation

Q. Échec de l'installation. Pourquoi ?


R. S'il n'y avait pas de connexion Internet, Securitoo AntiVirus Firewall n'a pas pu valider votre abonnement. Assurez-vous que vous avez une connexion Internet et réinstallez Securitoo AntiVirus Firewall.

Utilisation générale

Q. Securitoo AntiVirus Firewall est très lent et/ou ne s'ouvre pas. Quel est le problème ?

R. Internet Explorer 3.0 (ou plus récent) n'est peut-être pas installé. Vérifiez si Internet Explorer est installé et contrôlez le numéro de version (Internet Explorer est disponible sur le site web de Microsoft).

Q. Je ne vois pas l'icône de Securitoo AntiVirus Firewall dans la barre d'état du système en bas à droite de l'écran.

R. Sous Windows XP, les icônes peuvent être masquées. Pour afficher les icônes masquées, cliquez sur le bouton . Si vous n'utilisez pas Windows XP, installez Securitoo AntiVirus Firewall.



AntiVirus

Q. Securitoo AntiVirus Firewall ne peut pas désinfecter/supprimer/renommer un fichier infecté sur mon ordinateur. Que dois-je faire ?

R. Voir [Suppression d'un virus lorsque l'Assistant de nettoyage échoue](#) en page 17.



Firewall

Q. (Je pense que) je suis attaqué par un pirate via Internet. Que dois-je faire ?

R. Ouvrez le menu Firewall et sélectionnez le profil *Bloquer tout*. Pour plus d'informations sur la sélection d'un profil de firewall, voir 5.3 [Personnalisation des profils du firewall](#) en page 23.

Contrôle d'application

- Q. Comment puis-je changer les droits de connexion Internet de l'application ? Comment puis-je autoriser une application à se connecter à Internet si je l'ai bloquée précédemment ?**
- R. Voir [Modification des droits de connexion d'une application](#) en page 13.
- Q. Mon programme de messagerie (ou un autre programme tel que le navigateur Internet) ne fonctionne plus.**
- R. Vous avez peut-être accidentellement refusé au programme de se connecter. Voir [Modification des droits de connexion d'une application](#) en page 13 pour des informations sur la façon d'autoriser le programme à se connecter.
- Q. Quels programmes/applications puis-je autoriser à se connecter à Internet ?**
- R. Voir [Quels sont les éléments pouvant être considérés comme "fiables" ?](#) et [Quels sont les éléments pouvant être considérés comme "non fiables" ?](#) en page 22 pour vous aider à décider quelles applications autoriser (ou non) à se connecter.




Mise à jour automatique

- Q. Que se passe-t-il si mon ordinateur n'est pas connecté lorsqu'une mise à jour automatique des virus doit avoir lieu ?**
- R. La prochaine fois que vous êtes en ligne, Securitoo AntiVirus Firewall téléchargera la mise à jour la plus récente des virus.
- Q. À quelle fréquence faut-il mettre à jour les bases de données de définitions de virus ?**
- R. Les bases de données de définitions de virus sont automatiquement mises à jour si la fonction Mise à jour automatique est activée. Si vous voulez mettre à jour manuellement les bases de données, faites-le au moins une fois par semaine.
- Q. J'essaie de vérifier manuellement s'il y a des mises à jour des bases de données de définitions de virus (en cliquant sur Vérifier maintenant) mais rien ne se passe.**
- R. Si vous utilisez un modem ou avez une connexion RNIS, vous devez vous connecter manuellement à Internet avant de cliquer sur **Vérifier maintenant**.



Mon abonnement

- Q. Je suis en train d'installer un logiciel, mais Securitoo AntiVirus Firewall m'informe que ce logiciel contient un virus et je ne peux donc pas achever l'installation.**
- R. Si vous êtes sûr que le logiciel ne contient pas de virus, vous pouvez effectuer une des opérations suivantes :
- Choisissez un profil d'antivirus moins strict (pour les instructions, voir [Modification du profil de protection antivirus](#) en page 13), ou

- Cliquez avec le bouton droit sur l'icône  dans la barre d'état du système (en bas à droite de l'écran) et choisissez *Quitter Securitoo AntiVirus Firewall*. N'oubliez pas de recharger les produits après l'installation.

Glossaire

Application

Programme logiciel écrit pour un usage spécifique. Généralement, les applications se lancent manuellement.

Contrôle d'application

Contrôle d'application est une fonction de Securitoo AntiVirus Firewall qui vérifie automatiquement si une application est autorisée à se connecter à Internet à partir de votre ordinateur en comparant l'application à une liste des logiciels sûrs (pré-approuvés) et des logiciels malveillants connus (chevaux de Troie, etc.).

DoS (*Deny of Service* - Refus de Service)

Tentative explicite d'agresseurs d'empêcher les utilisateurs légitimes d'accéder à un service en rompant les connexions, en inondant un réseau ou en empêchant un individu d'accéder au réseau.

DNS (*Domain Name System* - Système de Nom de Domaine)

DNS est la façon dont les noms de domaines Internet sont localisés et convertis en adresses IP (Internet Protocol). Un nom de domaine est un « pointeur » facile à retenir menant à une adresse Internet. Par exemple, l'adresse Internet www.un.domaine.org est un nom DNS.

Heuristique

Méthode exploratoire de résolution de problèmes utilisant des techniques d'auto-apprentissage.

Antiprogramme

Programmes ou fichiers développés dans le but de nuire. Cela comprend les virus informatiques, les vers et les chevaux de Troie.

Paquet

Unité de données acheminée entre une origine et une destination sur Internet. Lorsqu'un fichier (par exemple un message électronique) est envoyé d'un endroit à un autre sur Internet, il est divisé en paquets d'une taille appropriée pour assurer un routage efficace. Une fois tous les paquets parvenus à destination, ils sont assemblés pour reconstituer le fichier d'origine.

Profil

Attributs préconfigurés définissant votre niveau de sécurité. Les profils sont automatiquement mis à jour pour garantir votre protection contre les formes les plus récentes de programmes malveillants et d'attaques via Internet.

Sous-réseau

Section d'un réseau. Les ordinateurs situés dans le même sous-réseau sont généralement proches les uns des autres physiquement et ont des adresses IP qui commencent par les deux ou trois mêmes chiffres.

Cheval de Troie

Programme qui effectue intentionnellement une action à laquelle l'utilisateur ne s'attend pas.

Virus

Programme qui se répand en se reproduisant.

Base de données des définitions des virus

Base de données utilisée pour détecter des virus. Chaque fois qu'un nouveau virus est trouvé, la base de données doit être mise à jour afin que Securitoo AntiVirus Firewall puisse le détecter.

Ver

Programme capable de se répliquer par l'insertion de copies dans les ordinateurs reliés en réseau.

Support et maintenance

Toutes les documentations et questions fréquentes relatives à Securitoo AntiVirus Firewall sont disponibles sur le site Internet de Securitoo à l'adresse <http://www.securitoo.com/>

Vous pouvez également contacter notre service d'assistance technique au numéro qui vous a été communiqué lors de votre abonnement.

Configuration minimale requise :

- Processeur Pentium IV - 400Mhz
- Windows 95 / 98 / Me /
NT4 Workstation / 2000 Pro / XP
- 64 Mo de mémoire vive (RAM) pour
Windows 95 / 98 / Me et NT4 (128 Mo
pour Windows 2000 et XP)
- 30 Mo d'espace disponible
sur disque dur
- Connexion Internet.

www.securitoo.com