

# Découverte de Windows® Defender





Windows® Defender est le nom commercial de l'évolution de Windows® Antispyware. Windows® Defender est un logiciel de protection contre les menaces de sécurité (comme les logiciels espion) en provenance des réseaux informatique. Ce logiciel de protection est inclus dans la beta 2 de <u>Windows®</u> <u>Vista™</u> et le sera également dans la version finale de ce nouveau Système d'exploitation dont la sortie est toujours prévue pour le premier trimestre de 2007. <u>En savoir plus</u> sur les menaces de sécurité...

Il s'agit d'un **logiciel gratuit** téléchargeable depuis le site de Microsoft®, accessible avec une version authentique de Windows®. Selon l'éditeur, plus de 25 millions de clients l'utilisent. Windows® Defender est disponible pour toutes les versions de Windows®. Accéder au <u>site de téléchargement</u>... Pour les versions de Systèmes d'exploitation 64 bits, <u>cliquez ici</u>...

Ce logiciel, même s'il est encore en langue anglaise, est vraiment très simple d'emploi par le simple fait qu'il est déjà pré-configuré avec le maximum de sécurité et ceci dès l'installation. Si vous avez toutefois besoin d'informations, sachez qu'un newsgroup en langue anglaise est disponible. Accéder au newsgroup... Mais rien ne vous empêche de <u>me poser vos questions</u> auxquelles je répondrai volontiers.

Dans le cas où vous rencontriez un problème de localisation (lié au langage) ce <u>lien vous permettra de solutionner</u> votre problème.

Dès que Windows® Defender est installé, vous pouvez immédiatement rechercher tout logiciel non désiré qui pourrait être installé sur votre ordinateur. Vous pouvez programmer des balayages et choisir de les faire éradiquer ou être mis en quarantaine automatiquement. Si le logiciel potentiellement nocif essaye de s'exécuter ou de s'installer sur votre ordinateur, Windows® Defender vous informe sur la meilleure manière d'agir. Vous pouvez recevoir les dernières mises à jour automatiquement sans vous soucier de cette maintenance.

Autre avantage : il n'est pas nécessaire d'avoir des privilèges d'Administration pour utiliser Windows® Defender (General settings : Administrator options).

Et enfin, il faut savoir que Windows® Defender <u>ne remplace en aucun cas</u> un logiciel anti-virus.

#### On l'installe ?

Depuis la page de téléchargement communiquée plus haut, cliquez sur **Continue**. Si le déroulement ne se passe pas comme décrit, c'est que le site Microsoft® vient de s'apercevoir qu'il n'a jamais vérifié votre copie de Windows®. A ce titre, il vous propose d'installer un contrôle ActiveX pour effectuer cette vérification.

Une fois cette vérification effectuée, vous avez la possibilité de cliquez sur le bouton **Download** pour, cette fois, télécharger Windows® Defender.

Un avertissement de sécurité apparaît vous signalant le danger potentiel d'exécuter de tels logiciels en provenance de l'internet. Cliquez sur le bouton **Installer** (image 1) pour démarrer le téléchargement.

Offres spéciales pour les clients Windows original <del>»</del>





Inter	net Explorer - Avertis	sement d	e sécur 🗙
Voulez-	vous installer ce logiciel ?		
	Nom : <u>Windows Genuine Advanta</u> Éditeur : <u>Microsoft Corporation</u>	<u>ae</u>	
× Plus	s d' <u>o</u> ptions	Installer	Ne pas installer
<u>!</u>	Bien que les fichiers téléchargés depuis de fichier présente un danger potentiel approuvés par vous. <u>Quels sont les risc</u>	Internet puissent ê . N'installez que les <u>jues ?</u>	ètre utiles, ce type logiciels des éditeurs

Après avoir téléchargé le package MSI « WindowsDefender.msi » en quelques petites minutes, il ne vous reste plus qu'à exécuter son installation.

i	Téléc	hargement de fichier _ 🗖 🗙 <sub>mation page</sub> .
:	<b>3</b>	Téléchargement de fichier - Avertiss 🗙
ı.	Recherch	Voulez-vous exécuter ou enregistrer ce fichier ?
	Windows	Nom : WindowsDefender.msi
÷	Temps re	Type : Package Windows Installer, 5,49 Mo
	Téléchar	Source : download.microsoft.com
	Taux de	
r	🔽 Ferm	Exécuter Enregistrer Annuler
		Si les fichiers téléchargés depuis Internet sont utiles, ce type de fichier peut présenter des risques pour votre ordinateur. Vous ne devriez pas exécuter ou enregistrer ce programme si vous n'êtes pas sûr de son origine. Quels sont les risques ?

# Image 2

Deux choix s'offrent à vous (image 2) :

- Exécuter directement le téléchargement et l'installation dans la foulée sans conserver une copie du package WindowsDefender.msi sur votre disque
- Enregistrer ce package sur votre disque et l'exécuter plus tard.

Cliquer sur le bouton **Exécuter** afin de provoquer le démarrage de l'installation.







Image 3

Cliquez sur le bouton **Next** pour passer à l'étape suivante (Image 3).

A tout moment, vous pouvez interrompre l'installation en cliquant sur le bouton **Cancel**.





🖥 Windows Defender		×
Windows Defender License Agree	ment	
Please read the following license agr	eement carefully.	
MICROSOFT PRE-RELEASE SOFTWARE LICENSE TER	45	
MICROSOFT WINDOWS DEFENDER BETA 2 SOFTWAR	le la	
FOR MICROSOFT WINDOWS 2000, WINDOWS XP, A	ID WINDOWS SERVER 2003	
These license terms are an agreement between Microsoft read them. They apply to the pre-release software name also apply to any Microsoft:	Corporation (or based on where you live, d above, which includes the media on whi	one of its affiliates) and you. Please ch you received it, if any. The terms
• updates,		
• supplements,		
<ul> <li>Internet-based services, and</li> </ul>		
support services (if any)		-
• I accept the terms in the license agree	ement	
• I do not accept the terms in the licens	se agreement	
	< <u>B</u> ack <u>N</u> e	ext > Cancel

Après avoir coché l'option d'acceptation (Image 4) des termes de la licence d'utilisation, cliquez sur le bouton Next pour passer à l'étape suivante.





Image 5

Deux options d'installation (Image 5) à savoir :

## 1. Use recommended settings

- Installation automatiques des mises à jour,
  - Protection « renforcée »,
- Devenir membre\*, standard ou avancé, de Microsoft Spynet.

SpyNet est une communauté qui apporte des informations aux utilisateurs sur les spywares pour les identifier et les partager. Cette communauté rapporte des menaces potentielles identifiées par Windows® Defender en temps réel et participe à la mise à jour du système pour vous aider et vous protéger contre de nouvelles menaces. La communauté de SpyNet rassemble l'information, telle que le nom de fichier et l'action que la communauté a choisi de prendre dans un rapport au sujet du dossier en question. Quand Windows® Defender envoie le rapport à la Communauté de SpyNet, il envoie également l'information standard de l'ordinateur, telle que votre paramétrage de région et de langue. <u>Aucune information personnelle</u> n'est rassemblée.

\* Vous pouvez modifier ceci à partir du paramétrage logiciel





## 2. Install definition updates only

Les mises à jour sont automatiques,

Sélectionnez l'option de votre choix puis, cliquez de nouveau sur le bouton **Next**...

🞼 Windows De	efender			×
Setup Type Choose the se	tup type that best suits	your needs.		
Please select a	a setup type.			
Complete				
	All program features ( space.)	will be installed. (R	equires the most di	sk
Custom	Choose which program they will be installed.	n features you war Recommended for	nt installed and whe advanced users.	re
		< <u>B</u> ack	<u>N</u> ext >	Cancel

## Image 6

Si vous désirez choisir le répertoire d'installation de Windows® Defender, sélectionnez l'option **Custom** (image 6) puis, cliquez sur le bouton **Next**...





🞼 Windows Defender	×
Custom Setup	
Select the program features you want installed.	
Click on an icon in the list below to change how a feature is	installed.
Windows Defender	Feature Description Helps protect user from spyware and other potentially unwanted software. This feature requires 9509KB on your hard drive.
Install to: G:\Program Files\Windows Defender\	<u>C</u> hange
<u>H</u> elp <u>Space</u> < <u>B</u> ack	<u>N</u> ext > Cancel

Pour modifier le répertoire d'installation, cliquez sur le bouton **Change** (image 7) puis, suivez les indications et validez votre choix en cliquant sur le bouton OK. Cliquez ensuite sur le bouton **Next** pour passer à l'étape suivante...





Vous avez maintenant rassemblé toutes les informations nécessaires à l'installation de Windows® Defender. Cliquez maintenant sur le bouton **Ins-tall** (Image 8) pour débuter l'installation du produit sur votre ordinateur.





L'installation démarre (image 9) puis, au bout de quelques minutes votre produit est prêt à l'utilisation.





Windows Defender	(Beta 2)	
🎦 🏠 Home 🏓 Scan	- 🤗 History 🥸 Tools 🕢  -	<b>Window</b> Defender
No unwanted or harmful s	oftware detected.	
Your computer is running norma	ily.	
7		
Status		
Last scan:	Today at 07:58. Quick scan.	
Scan schedule:	Daily at 02:00.	
Real-time protection:	Un. 1.14.1315.1 built op.08/03/2006 ⇒t.10-06	
Signature version:		

Windows® Defender possède une interface dépouillée (image 10) et simple d'utilisation. Cliquez sur **Tools** pour procéder aux premiers paramétrages.







Depuis ce masque (Image 11), vous avez ici accès au paramétrage de Windows® Defender, vous avez la possibilité de joindre la communauté Spynet, accès aux objets en quarantaine...

Cliquez sur General Settings.





Windows Defende	· (Beta 2)	<u> ×</u>
🕤 🏈 Home 🏓 Scan	+ 🤗 History 🔇 Tools 🕐  +	Windows Defender
General Settings		-
Automatic scanning		
Automatically scan my c	mputer (recommended)	
Scan freguency:	Daily	
<u>Time of day:</u>	19:00	
Type of scan	Full system scan	
I Apply actions on determined of the second sec	cted items after scanning	
Windows Defender will displ	ay the following actions by default for software with these aler	t levels:
High alert items	Signature default	
Medium alert items	Signature default	
Low alert items	Signature default	
Note: If you enabled Windows Det as part of the automatic sca	ender to apply actions after completing an automatic scan, th ining processes.	en items marked "Remove" will be removed
		<u>S</u> ave <u>C</u> ancel

\* Dans **Automatic scanning**, choisissez la fréquence de consultation (**Scan frequency**) du système : Quotidiennement ou un jour en particulier ; Quotidiennement est un bon réglage (image 12).

Dans **Time of day**, sélectionnez l'heure qui vous convient pour laquelle votre machine est en fonctionnement.

Dans **Type of scan**, choisissez si Windows® Defender effectuera un contrôle total du système ou rapide. Ce dernier est axé principalement sur les zones où les spywares sont susceptibles de s'installer ; c'est un bon réglage. En cas de doute, lancer une consultation **Full system scan**.

Pour que votre système soit continuellement à jour, cochez la case **Check** for updated definitions before scanning (Alt+k).

Pour appliquer les actions définies dans Default actions lors d'alertes, cochez la case **Apply actions on detected items after scanning**.

\* En règle générale, il est recommandé de conserver les réglages pré-définis.







Ensuite, vous allez configurer la manière dont Windows® Defender réagit en temps réel (image 13).

Windows Defender (Beta 2)	
💬 🏠 Home 🏓 Scan  + 🧭 History 🥸 Tools 🕐  +	Window Defender
Real-time protection options	
✓ Tum on real-time protection (recommended)	
Choose which security agents you want to run. Understanding real-time protection options	
✓ Auto Start	
System Configuration	
✓ Internet Explorer Add-ons	
Internet Explorer Configurations	
✓ Internet Explorer Downloads	
Services and Drivers	
Application Execution	
Application Registration	
Windows Add-ons	
Choose when Windows Defender should notify you.	
When changes are detected from software that has not vet been classified.	
When changes are detected from allowed software.	
Advanced options	
Scan inside ambives	
<ul> <li>Jee heuristics to detect suspicious files</li> </ul>	
Do not scan the following files or paths:	
	Saus Canad
	Save Cancel

Image 13

Sous **Real-Time Protection options**, cochez la case **Turn on Real-Time Protection (recommended)**. Divers agents, tous aussi importants les uns que les autres, surveillent les points d'entrée sur la machine. C'est la raison pour laquelle je vous recommande de tous les sélectionner.

Puis, sous **Choose when Windows Defender should notify you**, cochez la case appropriée (la première convient très bien).





Windows Defender (Beta 2)	
💽 🏐 奣 Home 🏓 Scan   🗸 🧐 History 🏠 Tools 👔   +	<b>Windows</b> Defender
<ul> <li>When changes are detected from software that has not yet been classified.</li> <li>When changes are detected from allowed software.</li> </ul>	<u>-</u>
Advanced options	
Scan inside amhives	
Use heuristics to detect suspicious files	
Do not scan the following files or paths:	
Administrator options	<u>H</u> emove
✓ Use Windows Defender	
When Windows Defender is on, all users are alerted if spyware or other potentially unwanted softw on the computer. Windows Defender will check for new definitions, regularly scan the computer, a software detected by a scan.	ware attempts to run or install itself and automatically remove hamful
Allow users who do not have administrative rights to scan the computer, choose actions to ap software, and review all Windows Defender activities.	ply to potentially unwanted
	<u>Save</u> <u>Cancel</u>

Si vous désirez que tous les utilisateurs de la machine sur laquelle s'exécute Windows® Defender puissent utiliser le produit et recevoir des alertes, laisser les 2 cases cochées dans **Administrative options** (image 14).

Depuis Software Explorer (image 15), vous avez un œil sur les différents logiciels chargés en mémoire, ceux qui démarrent automatiquement...





Windows Defend	ler (Beta 2)	
💽 🂮 🏫 Home 🏓 Sc	an   🚽 🤗 Histor	y 🔅 Tools 🕐 I+ 🛛 🕂 Windows' Defender
🔊 Software Exp	lorer	
Explore and manage key areas or Category: Startup Programs	f your computing expe	rience. <u>Using Software Explorer</u>
Name	Classification	Adobe Acrobat
Système d'exploitation Micro	Allowed	
Système d'exploitation Micro	Allowed	File Name: reader_sl.exe Display Name: Adobe Acrobat
Système d'exploitation Micro	Allowed	Description: Adobe Acrobat SpeedLauncher
Watson Subscriber for SEN	Allowed	Digitally Signed By: NOT SIGNED
Windows Defender	Allowed	File Type: Application File Path: G:\Program Files\Adobe\Acrobat 7.0\Reader\reader_sl.exe File Size: 29696 Bytes
Adobe Systems Incorpora	ted	File Version: 7.0.5.2005092300 Date Installed: 23/09/2005 22:05:26
Adobe Acrobat	Allowed	Startup Type: All Users Startup Folder Location: E:\Documents and Settings\All Users\Menu Démarrer\Programmes\Démarra Classification: Allowed
Integrated Technology Ex	press, Inc.	Ships With OS: No SpyNet Voting: Not applicable
RaidMgr Application	Not yet classified	▼
1		
Defeat		
netresn		<u>rx</u> emove <u>Disable</u> Enable

... ceux qui écoutent la carte réseau ainsi que leurs niveaux de classification associés.

Ce document vous a donné un premier aperçu de l'installation et du fonctionnement de Windows® Defender. A vous maintenant, de procéder à la mise en pratique de ces informations.

Et puis, n'oubliez pas que vous pouvez toujours me joindre pour obtenir des renseignements supplémentaires.

## Infos annexes :

Questions fréquentes (en anglais) : <a href="http://www.microsoft.com/athome/security/spyware/software/about/fag.mspx">http://www.microsoft.com/athome/security/spyware/software/about/fag.mspx</a>

Notions essentielles de sécurité :

http://www.microsoft.com/france/securite/gpublic/protect/windowsxpsp2/default.ms px





Maintenez les défenses de votre ordinateur : http://www.microsoft.com/france/securite/gpublic/update/msupdate\_keep\_current. mspx Logiciels de sécurité : http://www.microsoft.com/france/securite/gpublic/downloads/default.mspx Virus et vers : http://www.microsoft.com/france/securite/gpublic/viruses/default.mspx Les logiciels espions : http://www.microsoft.com/france/securite/gpublic/spyware/default.mspx

