Tuto Windows Defender

Activation/Désactivation, réglages, optimisation et utilisation

Wullfk

17/09/2015

Apprenez à paramétrer, optimiser et utiliser Windows Defender

PRÉSENTATION WINDOWS DEFENDER :

Windows Defender est l'Antivirus de Microsoft présent par défaut sur tous les systèmes Windows 8/8.1 et 10, c'est l'équivalent de **Microsoft Security Essentials (MSE)**

Comme il fait partie du Système, on ne doit pas chercher à le désinstaller. Sinon il y a de gros risque de rendre instable votre système.
Par contre, si on ne l'utilise pas ou plus, on peut toujours le désactiver.
(Ex : si l'on souhaite installer et utiliser un autre Antivirus)

Windows Defender possède deux grandes qualités :

1. Il est très simple et très facile à utiliser.
2. Il est très "léger" et consomme peu de ressources*.

*Ainsi, son utilisation sera particulièrement recommandée à ceux qui ont un PC qui dispose de peu de ressources, ainsi que pour les utilisateurs novices.

Le défaut de cette simplicité et légèreté, c'est que les réglages sont limités au stricte nécessaire, contrairement aux autres Antivirus qui fourmillent de multiples réglages, ce qui ne facilite pas la tâche pour les utilisateurs lambda.

Niveau efficacité, il faut bien admettre que ce n'est pas le mieux noté dans les comparatifs, mais il fait quand même ce qui lui est demandé.

Attention ! Sur Windows XP/Vista/7 Windows Defender est un simple Antimalware

ACTIVER WINDOWS DEFENDER :

Normalement par défaut Windows Defender est activé sur tout système récemment installé.

Si pour une raison quelconque ce n'est pas le cas, il suffit de cliquer sur le bouton **Démarrer**. Dans la zone de recherche, taper **Defender**.

Dans la liste des résultats, cliquer sur **Windows Defender**.

Si vous êtes invité à fournir un mot de passe administrateur ou une confirmation, faite le

Sur **Windows 8** par défaut **Windows Defender même activé n'apparait pas dans la zone de notification** (en bas près de l'horloge)

Un petit programme permet d'y remédier, voir ici : **Windows Defender dans le systray de Windows 8**

Sur **Windows 10** pas besoins de l'artifice précédemment cité pour Windows 8, dès que l'on a ouvert Windows Defender, son icône apparait dans la zone de notification.

Il se peut qu'après un redémarrage du PC l'icône de WD n'apparaisse plus dans la zone de notification, même si on a bien activé la protection en temps réel, on est alors obligé d'ouvrir Windows Defender pour que l'icône réapparaisse.

On va donc ajouter une clé manquante dans la base de registre

Avant toute modification du registre, faites-en une sauvegarde.

Pour y remédié je vous propose en téléchargement un fichier .reg

Show_Windows_Defender_notifcation_area_icon.reg

Et si vous désirez supprimer cette modification :

Hide_Windows_Defender_notifcation_area_icon.reg

DÉSACTIVER WINDOWS DEFENDER :

Lorsque l'on installe un autre Antivirus, normalement Windows Defender se désactive lui-même.

Ceci dit ce n'est pas toujours le cas, par exemple sur ma config **Windows 10 Pro 64Bits**, lorsque j'ai effectué la migration de **Windows 7 Pro 64Bits**, j'avais **AVG Free 2015**, hors après la mise à niveau je me suis rendu compte que Windows Defender était actif et ce même avec la présence d'**AVG**.

Une simple désactivation de la protection en temps réel de Windows Defender ne suffit pas, car au bout de certain temps celle-ci se réactive automatiquement.

Si l'on va dans les services Windows (*services.msc*) on peut par défaut constater que le service Windows Defender est en "Automatique" avec l'impossibilité de changer cet état (zone grisé).

Un des moyens pour modifier le démarrage automatique du service Windows Defender, c'est d'effectuer un **démarrage en mode sans échec** (**MSE**) (cf : Démarrer en mode sans échec par la touche F8 (Compatible Windows 10) ou Démarrer en mode sans échec sous Windows 10)

Retourner dans les services Windows :

Démarrer >> **Exécuter** >> **services.msc** >> **service Windows Defender** >> **Propriétés** >> Type de démarrage : mettre sur "***Désactiver***", arrêter le service, et cliquer sur "**Appliquer**" pour valider la modification.

Fermer le gestionnaire des services Windows, et redémarrer en mode normale, à présent Windows Defender est bien désactivé.

Autre solution, **réservée aux versions Pro / Intégrale / Entreprise de Windows 8/8.1 et 10.**

Passer par **la Stratégie de groupe** :

- **Démarrer >> Exécuter >> gpedit.msc**
- **Configuration ordinateur** >> **Modèles d'administration >> Composants Windows >>** cliquer sur : **Windows Defender.**
- Cliquer sur : **Protection en temps réel.**
- Clic droit sur : **Désactiver la protection en temps réel >> Modifier >>** cocher "*Activer*" **>> Appliquer >> OK**
- Fermer **l'Éditeur de stratégie de groupe locale.**

Il n'y a pas besoins de redémarrer, la modification est directement effective.

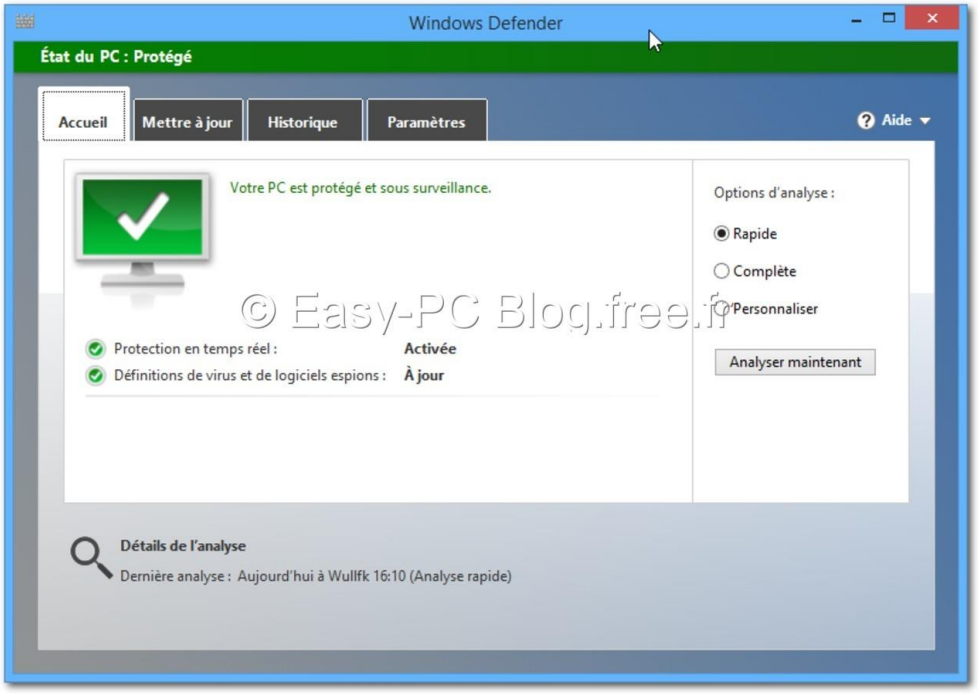
Pour d'autres réglages via **la stratégie de groupe** (entre autre pour ceux qui n'arriveraient plus à faire fonctionner Windows Defender) (cf : Activer-Désactiver Windows Defender via la stratégie de groupe)

RÉGLAGES DE WINDOWS DEFENDER :

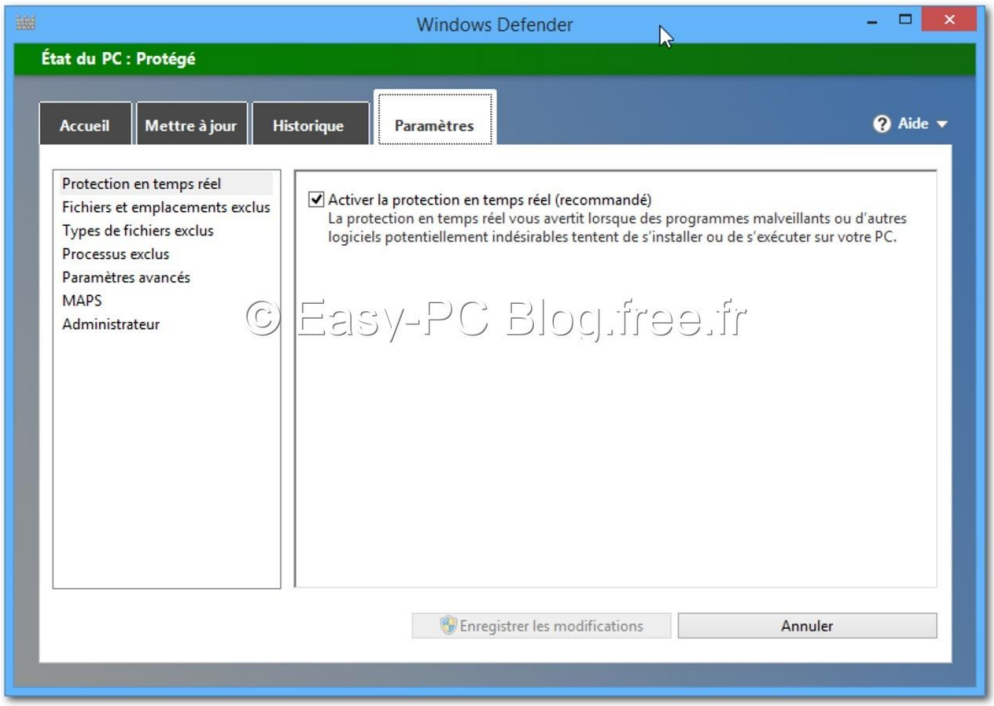
Pour ouvrir Windows Defender, cliquer sur son icône se trouvant dans la barre de notification.

Note : *Les réglages présents si dessous concernent Windows Defender sur Windows 8.1*

La fenêtre principale "**Accueil**" s'ouvre !

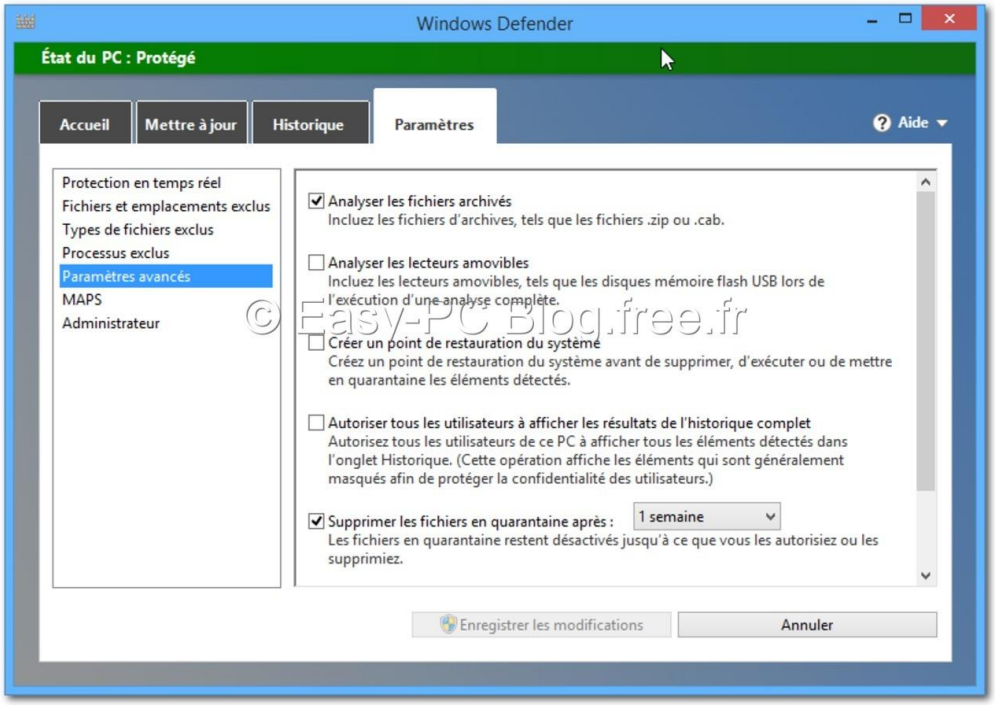


Cliquer sur l'onglet "**Paramètres**"



Pour la **Protection en temps réel** si ce n'est déjà fait laisser cocher "**Activer la protection en temps réel (recommandé)**"

- Cliquer sur "**Paramètres avancés**"

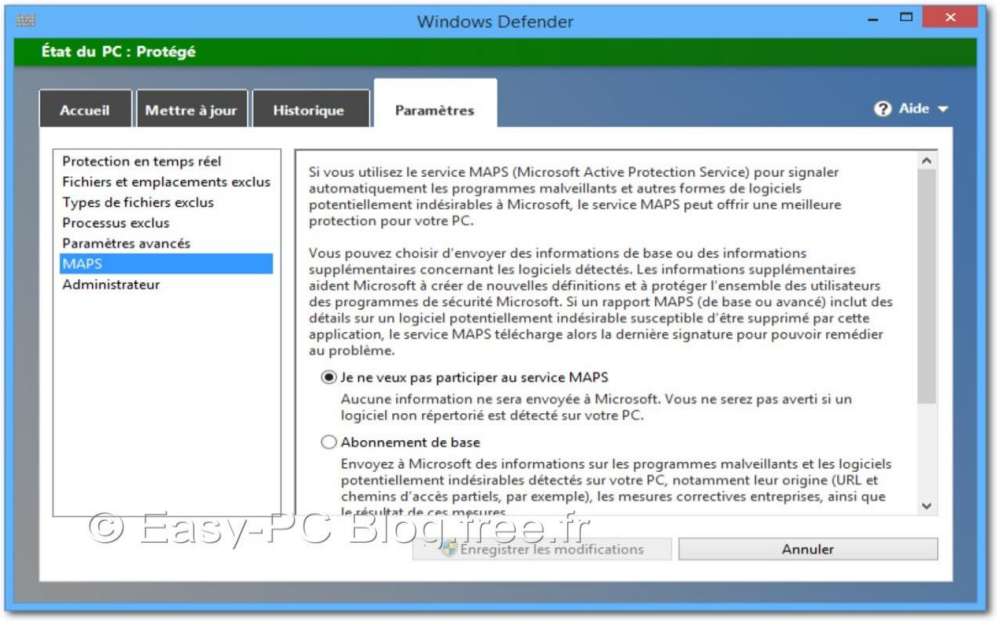


Laisser cochés les paramètres par défaut et profitez-en pour cocher aussi "**Analyser les lecteurs amovibles**"

Pour la "**création d'un point de restauration du système**", je vous conseille de ne pas cocher cette fonctionnalité, car sinon si vous allez créer un point de restauration qui comportera les éventuelles infections, et ce n'est pas le but, **on crée un point de restauration sur un système propre**.

Valider les changements effectués en cliquant sur "**Enregistrer les modifications**"

- Cliquer maintenant sur "**MAPS**"



Sur ce paramètre, trois choix possible:

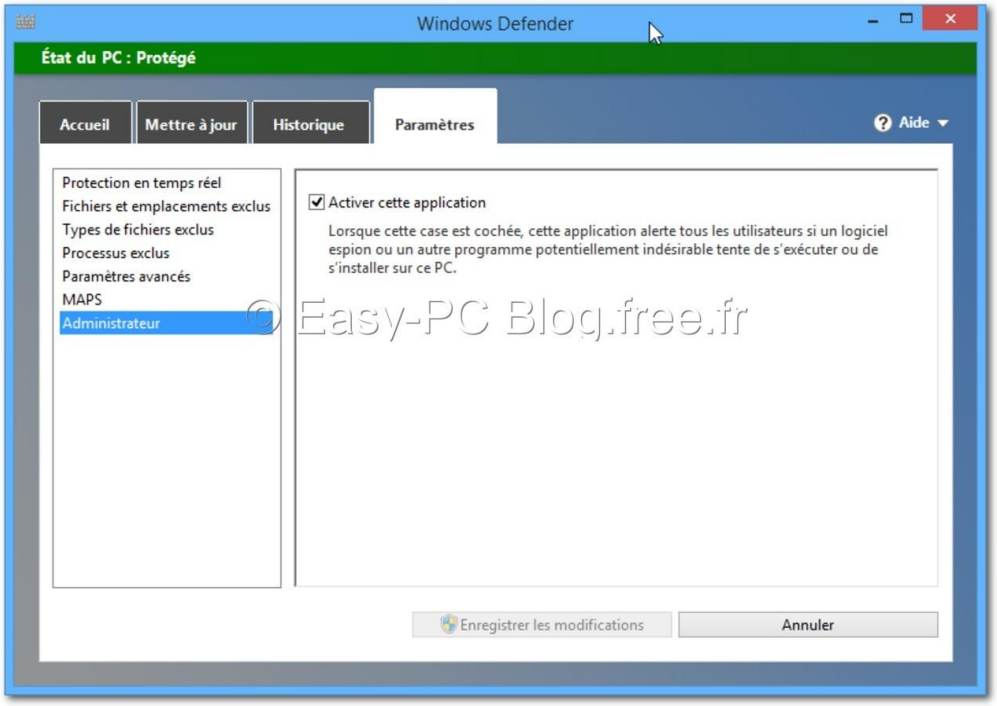
1. **Je ne veux pas participer au service MAPS (par défaut)**
2. **Abonnement de base**
3. **Abonnement avancé**

Pour une meilleur protection, je vous conseils de cocher "**Abonnement de base**"
Enregistrer les modifications

- Cliquer à présent sur "**Administrateur**"

Vérifier que la fonctionnalité "**Activer cette application**" est bien cochée.

N'oublier pas d'**Enregistrer les modifications**



Voilà on a fait le tour des principaux réglages de Windows Defender.

MISES À JOUR :

Normalement, Windows Defender se met automatiquement à jour !

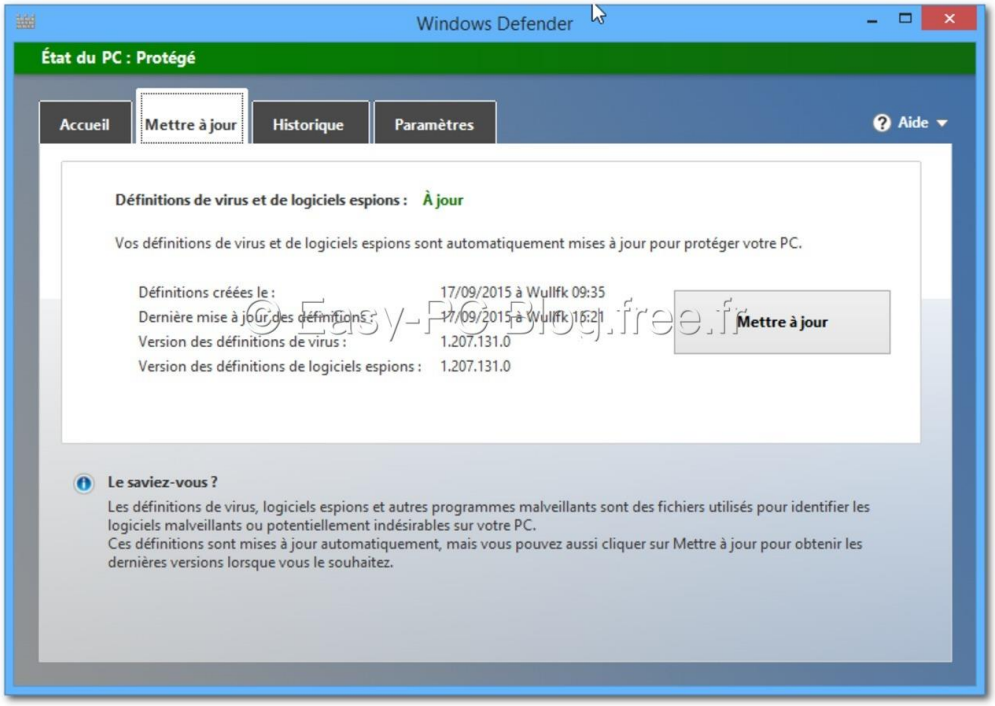
Mais au besoin, on peut effectuer cette mise à jour manuellement.

(Ex: lorsque l'on n'a pas allumé et utilisé son PC depuis plusieurs jours, et que l'on veut que les mises à jour se fassent immédiatement)

Pour faire manuellement les mises à jour, Ouvrir **Windows Defender**, et cliquer en haut de la fenêtre sur "**Mettre à jour**"

Dans la nouvelle fenêtre qui s'ouvre, à droite cliquer sur "**Mettre à jour**"

Et laisser faire Windows Defender pour qu'il puisse effectuer sa mise à jour.



EFFECTUER UNE ANALYSE :

Dans la fenêtre "**Accueil**" à droite, sous la mention "**Options d'analyse**" vérifier que l'option "**Rapide**" soit bien cochée, et cliquer sur "**Analyser maintenant**".

Comme son nom l'indique, cette analyse rapide ne prend que quelques minutes!

On peut aussi faire une analyse complète.

Dans ce cas, sous la mention "**Options d'analyse**" il faut cocher "**Complète**"
Mais, attention ! Cette option d'analyse va prendre beaucoup plus de temps !

Donc, on choisira cette analyse complète, que si l'on a vraiment de gros soupçons d'infections.

⚠ Il est fortement recommandé d'effectuer une analyse complète au moins une fois par mois.

À PROPOS DU CENTRE DE MAINTENANCE DE WINDOWS ET DE WINDOWS DEFENDER

Sur Windows 8/8.1, **Le Centre de maintenance de Windows** est symbolisé par une petite icône qui s'affiche en bas à droite de l'écran, à côté de l'horloge Windows.

Cette icône prend la forme d'un **petit drapeau triangulaire blanc** qui s'affiche souvent et brièvement au démarrage du pc.

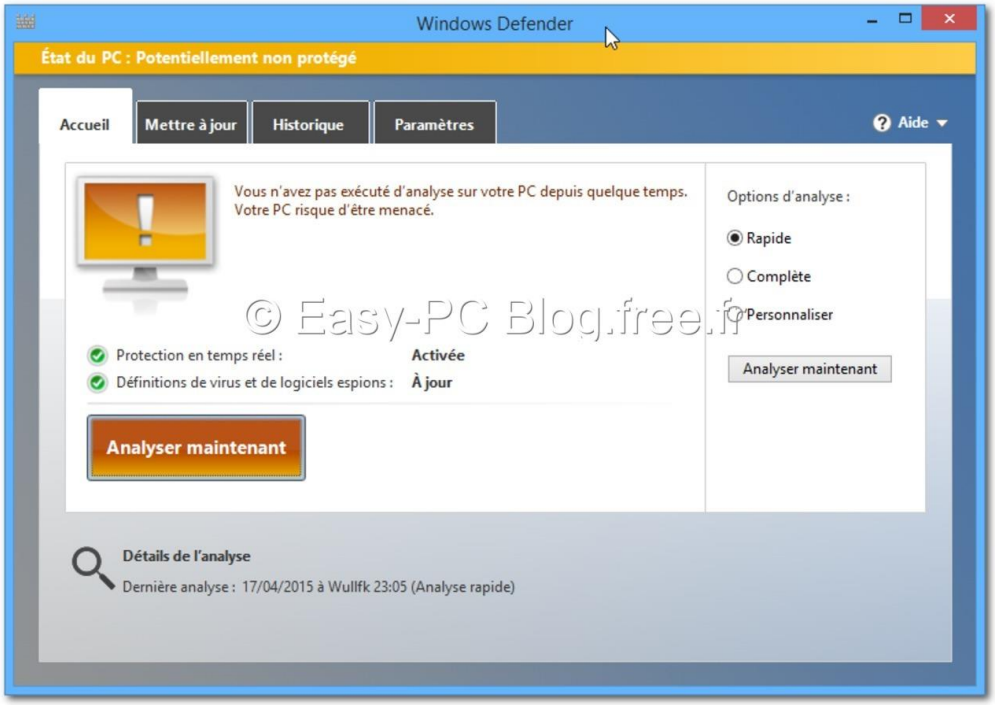
Sur Windows 10, **l'icône est de forme carrée translucide** et quand on passe le pointeur de la souris dessus, la plupart du temps si le système est OK on peut lire "**Aucune nouvelle notification**"

Au démarrage du PC, cette icône s'affiche, en déplaçant le pointeur de la souris au-dessus de l'icône, on pourra souvent lire cette notification : "**Centre de maintenance. Aucun problème détecté**"

Néanmoins, le **Centre de maintenance** et **Windows Defender** force un peu à la paranoïa !

En effet, **si l'utilisateur n'a pas effectué d'analyse depuis longtemps**, le Centre de maintenance risque bien de se manifester par des notifications alarmantes !

De même, si on ouvre **Windows Defender**, un message du genre "**l'analyse n'a pas été faite depuis longtemps**" peut apparaitre.



Dans ce cas, et après avoir bien pris connaissance des avertissements du **Centre de maintenance** et de **Windows Defender**, deux solutions s'offre à vous :

1. Ne pas tenir compte de ces avertissements. (Pas recommandé)
2. Ouvrir **Windows Defender** et lancer une **analyse rapide.**

ÉLARGIR LE DOMAINE D'ACTION DE WINDOWS DEFENDER SUR WINDOWS 10

Vers la fin de l'année 2015 Microsoft a annoncé que ses produits de sécurité à vocation professionnelle vont bénéficier d'une nouvelle fonctionnalité qui stoppera également les logiciels potentiellement indésirables et les adwares. La fonctionnalité a été d'abord mise à la disposition des entreprises. Pour les protéger contre les applications indésirables, Microsoft a ajouté la nouvelle fonctionnalité de l'opt-in à la solution d'entreprise System Center Endpoint Protection (SCEP) et Forefront Endpoint Protection (FEP).

cette nouvelle fonctionnalité peut également être activée sur toute version "**professionnelle"** ou **"familiale"** de l'Os. Après une modification de registre, **Windows Defender va proteger le système contre les logiciels potentiellement indésirables tels que les adwares, les barres d'outils et autres logiciels tiers indésirables**. Voici comment faire.

Avant toute modification du registre, faites en une sauvegarde.

Ouvrir le bloc note de Windows et copier/coller le texte suivant :

```
Windows Registry Editor Version 5.00
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\MpEngine]
"MpEnablePus"=dword:00000001
```

- Nommez le fichier "**Defender.reg**" et enregistrez le fichier sur le bureau.
- Pour lancer la modification sur la base de registre, double-cliquez sur **Defender.reg** puis acceptez l'élévation de droits "administrateur" pour qu'elle soit effectuée.
- Redémarrez l'ordinateur.

Source : cnetfrance

Fichier .reg disponible en téléchargement : **Defender.reg**

INFORMATIONS

Toutes les captures d'écran proviennent de ma machine virtuelle (VM) **Windows 8.1 Pro 32Bits** sur **VirtualBox**

Si **CCleaner** est installé sur votre poste, voilà ce qu'il convient de faire :

- Ouvrir **CCleaner**
- Si ce n'est pas déjà fait, cliquer en haut à gauche sur le bouton "***Nettoyeur***"
- Cliquer en haut sur le bouton "***Applications***"
- Dans la liste des options de nettoyage, sous la mention "*Utilitaires*" décocher bien la case se trouvant devant "*Windows Defender*"

Si vous avez des problèmes concernant la compréhension de ce tuto, je vous invite à poser vos questions sur le forum Zebulon

Merci à ***Le Novice °¿°*** *membre actif sur le forum Zebulon, pour m'avoir fournis la base, et sans qui ce tuto n'aurait pas existé*