

**McAfee®**  
**VirusScan USB**  

---

**Guide de l'utilisateur**



---

# Table des matières

<b>McAfee VirusScan USB</b>	<b>3</b>
Caractéristiques .....	4
<b>Installation et mise à jour de VirusScan USB</b>	<b>5</b>
Installation de VirusScan USB .....	6
Mise à jour de VirusScan USB .....	8
<b>Réglage des options d'analyse</b>	<b>9</b>
Définition des types de fichiers analysés .....	11
Définition des emplacements à analyser .....	12
Désactivation de la surveillance en temps réel.....	13
Lancement d'une analyse à l'insertion .....	14
Désactivation de la détection de logiciel antivirus .....	15
Affichage des messages d'information.....	15
<b>Utilisation des alertes</b>	<b>17</b>
A propos des alertes.....	17
<b>Analyse de votre périphérique USB</b>	<b>19</b>
Analyse de votre périphérique USB.....	20
Interruption d'une analyse .....	21
Reprise de l'analyse .....	21
Annulation d'une analyse .....	21
<b>Exploitation des résultats d'analyse</b>	<b>23</b>
Visualisation des résultats d'une analyse.....	24
Suppression d'un fichier infecté .....	25
Visualisation du résumé de la dernière analyse .....	26
Visualisation du résumé du programme VirusScan USB.....	26
<b>Protection de votre ordinateur</b>	<b>27</b>
Téléchargement d'un logiciel antivirus pour votre ordinateur .....	27
<b>Renouvellement de votre abonnement à VirusScan USB</b>	<b>29</b>
Renouvellement de votre abonnement à VirusScan USB.....	29
<b>Questions fréquentes</b>	<b>31</b>
Une menace a été détectée. Que faire ?.....	31

Dois-je être connecté à Internet pour lancer une analyse ?.....	31
VirusScan USB analyse-t-il les fichiers compressés (.zip) ? .....	32
Comment faire pour obtenir une aide supplémentaire de McAfee ?.....	32
<b>Glossaire</b>	<b>33</b>
<hr/>	
<b>Glossaire</b>	<b>34</b>
<hr/>	
<b>A propos de McAfee</b>	<b>37</b>
<hr/>	
Copyright.....	38
<b>Index</b>	<b>40</b>
<hr/>	

---

## CHAPITRE 1

# McAfee VirusScan USB

VirusScan USB offre une protection antivirus complète, fiable et à jour pour votre périphérique USB. Géré par notre moteur d'analyse McAfee primé, VirusScan USB protège le contenu de votre périphérique USB contre les virus et les chevaux de Troie.

## Contenu de ce chapitre

Caractéristiques .....4

## Caractéristiques

VirusScan USB propose les fonctionnalités suivantes :

### Surveillance en temps réel

Lorsqu'il est activé, VirusScan USB surveille constamment votre périphérique USB, à la recherche de changements de fichiers (par exemple, lorsqu'un nouveau fichier est ajouté au périphérique ou qu'un fichier s'y trouvant est modifié). Si la fonction de surveillance en temps réel détecte un changement de fichier, VirusScan USB analyse le fichier concerné, à la recherche d'une activité virale. En cas de détection d'un virus ou d'un cheval de Troie, VirusScan USB tente de le nettoyer. Si l'opération est impossible, il tente de le renommer. La surveillance en temps réel est activée par défaut.

### Analyse à la demande

L'analyse à la demande vous permet d'analyser votre périphérique USB à tout moment, à la recherche de virus et de chevaux de Troie. Si vous venez par exemple d'ajouter un programme ou un fichier au périphérique USB, vous pouvez l'analyser pour vérifier l'absence d'infection de l'élément. En cas de détection d'un virus ou d'un cheval de Troie, VirusScan USB tente de le nettoyer. Si l'opération est impossible, il tente de le renommer.

---

## CHAPITRE 2

# Installation et mise à jour de VirusScan USB

VirusScan USB s'installe sur votre périphérique USB comme la plupart des autres programmes USB U3, sauf que vous devez vous enregistrer auprès de McAfee. Cette inscription vous permet de recevoir les mises à jour du programme VirusScan USB et des fichiers de définition de virus dès leur publication. Lors de votre première inscription auprès de McAfee, vous devez indiquer votre nom, une adresse e-mail et un mot de passe. Si vous êtes déjà inscrit, connectez-vous à l'aide de l'adresse e-mail et du mot de passe indiqués pendant l'inscription.

Lorsque vous aurez installé et enregistré VirusScan USB, vous pourrez, à tout moment, le mettre à jour à l'aide des derniers fichiers de protection antivirus (DAT). Les mises à jour s'exécutent en arrière-plan. Lors d'une mise à jour, vous pouvez même lancer une analyse ou fermer le programme. Si la surveillance en temps réel est activée, VirusScan USB lance une mise à jour automatique toutes les quatre heures. Pour en savoir plus sur la surveillance en temps réel, consultez la section Réglage des options d'analyse (page 9).

---

**Remarque :** si un programme antivirus est déjà installé sur votre périphérique USB, McAfee vous recommande de le supprimer avant d'installer VirusScan USB.

---

## Contenu de ce chapitre

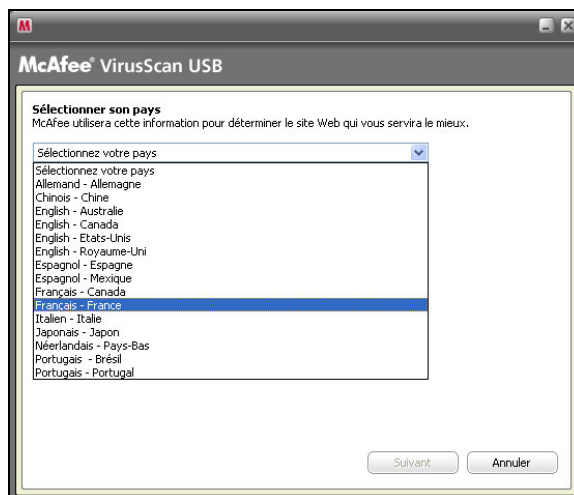
Installation de VirusScan USB.....	6
Mise à jour de VirusScan USB .....	8

## Installation de VirusScan USB

VirusScan USB s'installe sur votre périphérique USB comme la plupart des autres programmes USB U3, sauf que vous devez vous enregistrer auprès de McAfee. Cette inscription vous permet de recevoir les mises à jour du programme VirusScan USB et des fichiers de définition de virus dès leur publication.

### Pour installer VirusScan USB :

- 1 Insérez votre périphérique USB dans votre ordinateur.
- 2 Sur le Launchpad U3, cliquez sur **Ajouter des programmes**, puis sur l'option d'**installation depuis votre ordinateur**.
- 3 Dans la boîte de dialogue Ouvrir, recherchez le dossier contenant le fichier d'installation, sélectionnez-le, puis cliquez sur **Ouvrir**.
- 4 Dans l'assistant d'ajout de programme, cliquez sur **Suivant**.
- 5 Dans la boîte de sélection du pays, cliquez sur la combinaison de pays et de langue qui représente le mieux votre situation, puis cliquez sur **Suivant**.



- 6 Dans la boîte de dialogue de configuration du programme, lisez la politique de confidentialité, puis cliquez sur **Suivant**.
- 7 Dans la boîte de dialogue concernant l'accord de licence pour utilisateur final, sélectionnez un pays, lisez l'accord, puis cliquez sur **Accepter**.
- 8 Effectuez l'une des opérations suivantes :
  - Si vous vous inscrivez pour la première fois, tapez votre prénom, votre nom, votre adresse e-mail, votre mot de passe et sa confirmation dans les cases concernées, puis cliquez sur **Soumettre**.



- Si vous avez déjà enregistré un programme auprès de McAfee, cliquez sur l'option de **connexion**, tapez l'adresse e-mail et le mot de passe associés à votre compte McAfee, puis cliquez sur l'option de **connexion**.



McAfee VirusScan USB

Utilisateur McAfee actuel  
Si vous avez déjà un compte McAfee, connectez-vous.

Créer un compte McAfee

Prénom :

Nom :

Adresse e-mail :

Mot de passe :

Confirmer le mot de passe :

- 9 Dans la boîte de dialogue de configuration du programme terminée, sauvegardez vos informations d'enregistrement, puis cliquez sur **Terminer**.

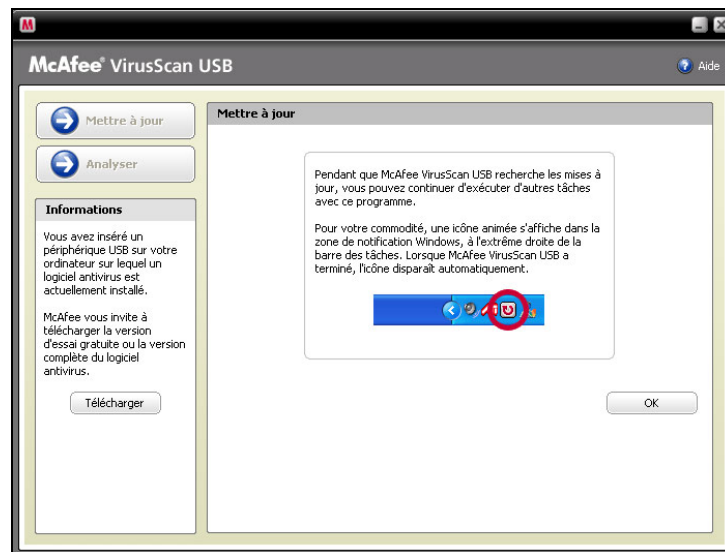
**Remarque :** vous pouvez également exécuter le fichier d'installation de VirusScan USB directement depuis un site Web. Sur le site Web, lancez le téléchargement et cliquez sur **Oui** dans tous les messages d'avertissement de sécurité vous invitant à télécharger le fichier. Exécutez ensuite le fichier d'installation et suivez les instructions fournies dans l'assistant d'installation.

## Mise à jour de VirusScan USB

Lorsque vous avez installé VirusScan USB sur votre périphérique USB, une mise à jour se lance automatiquement chaque fois que vous branchez le périphérique sur votre ordinateur. De plus, vous pouvez à tout moment actualiser manuellement VirusScan USB, en appliquant les dernières mises à jour du programme et des définitions de virus. Les mises à jour s'exécutent en arrière-plan. Lors d'une mise à jour, vous pouvez même lancer une analyse ou fermer le programme.

### Pour mettre à jour VirusScan USB :

- 1 Dans le panneau principal, cliquez sur **Mettre à jour**.



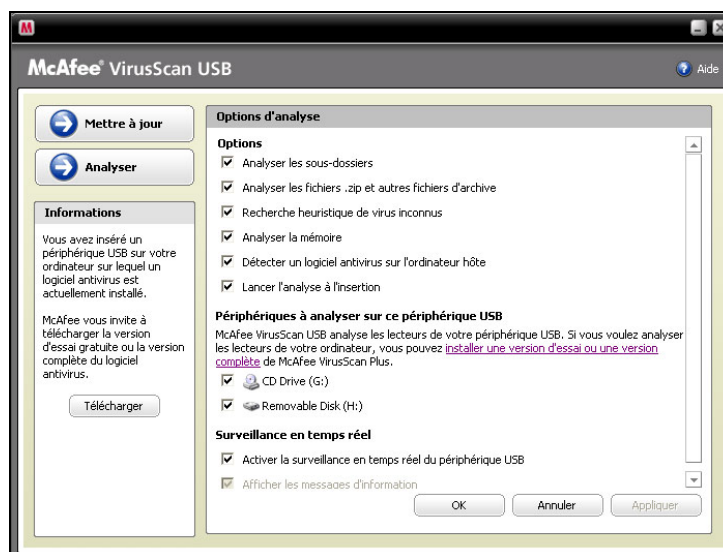
- 2 Cliquez sur **OK**.

**Remarque :** vous devez être connecté à Internet pour pouvoir actualiser VirusScan USB.

## CHAPITRE 3

# Réglage des options d'analyse

Vous pouvez personnaliser le fonctionnement de VirusScan USB en réglant les options d'analyse. Vous pouvez par exemple spécifier les emplacements et les types de fichiers à analyser (archives, sous-dossiers et mémoire de l'ordinateur). Vous pouvez également activer ou désactiver la surveillance en temps réel. Lorsqu'il est activé, VirusScan USB surveille constamment votre périphérique USB, à la recherche de changements de fichiers (par exemple, lorsqu'un nouveau fichier est ajouté au périphérique ou qu'un fichier s'y trouvant est modifié). Si la fonction de surveillance en temps réel détecte un changement de fichier, VirusScan USB analyse le fichier concerné, à la recherche d'une activité virale. En cas de détection d'un virus ou d'un cheval de Troie, VirusScan USB tente de le nettoyer. Si l'opération est impossible, il tente de le renommer. La surveillance en temps réel est activée par défaut et McAfee vous recommande de ne pas la désactiver. Lorsqu'elle est activée, tous les types de fichiers sont surveillés. Lorsque vous exécutez l'analyse à la demande, VirusScan USB analyse les types de fichiers et les emplacements indiqués dans vos options. Pour en savoir plus sur le lancement d'une analyse à la demande, consultez la section Analyse de votre périphérique USB (page 19).



Lorsque vous installez VirusScan USB, il s'ajoute automatiquement à la liste des programmes sur votre Launchpad U3 et se configure pour se lancer en cas d'insertion. Ainsi, l'analyse à la demande de VirusScan USB démarre chaque fois que vous insérez votre périphérique USB dans votre ordinateur. Si vous désactivez l'option de démarrage à l'insertion, l'analyse VirusScan USB à la demande ne démarre qu'à la première insertion de votre périphérique USB dans l'ordinateur. Vous pouvez ensuite configurer VirusScan USB pour qu'il démarre ou non l'analyse en cas d'insertion. Si vous configurez VirusScan USB pour qu'il ne lance pas l'analyse à l'insertion, il démarre seulement lorsque la fonction de surveillance en temps réel détecte une infection ou que vous le lancez manuellement. McAfee vous conseille de ne pas désactiver l'option d'analyse à l'insertion dans VirusScan USB.

VirusScan USB détecte les virus et les chevaux de Troie sur votre périphérique USB et dans la mémoire de votre ordinateur et détermine si l'antivirus installé est à jour. Si votre protection n'est pas à jour, un message vous demande de télécharger une version d'essai ou une version complète de McAfee VirusScan. Lors du réglage des options d'analyse, vous pouvez désactiver la détection du logiciel antivirus, ce qui évite à VirusScan USB de vérifier la mise à jour de votre logiciel antivirus. De même, si vous avez masqué certaines alertes ou autres boîtes de dialogue informatives, vous pouvez les afficher à nouveau.

## Contenu de ce chapitre

Définition des types de fichiers analysés.....	11
Définition des emplacements à analyser .....	12
Désactivation de la surveillance en temps réel.....	13
Lancement d'une analyse à l'insertion.....	14
Désactivation de la détection de logiciel antivirus ...	15
Affichage des messages d'information .....	15

---

## Définition des types de fichiers analysés

Vous pouvez préciser les types de fichiers qui seront analysés sur votre périphérique USB lors d'une analyse à la demande, à la recherche de virus ou de chevaux de Troie. Vous pouvez par exemple indiquer s'il faut analyser les sous-dossiers et les archives. Vous pouvez aussi décider si VirusScan USB doit analyser la mémoire de votre ordinateur.

### Pour définir les types de fichiers analysés :

- 1 Dans le volet d'accueil de VirusScan USB, sous **Options d'analyse actuelles**, cliquez sur **Configurer**.
- 2 Dans le volet des options d'analyse, sous **Options**, activez ou désactivez les cases à cocher suivantes.
  - **Analyser les sous-dossiers** : les sous-dossiers (dossiers contenus dans d'autres dossiers) sont analysés.
  - **Analyse des fichiers .zip et autres fichiers d'archive** : les fichiers archivés, notamment les fichiers .zip, sont analysés.
  - **Recherche heuristique de virus inconnus** : le programme compare les fichiers aux signatures des virus déjà connus afin de détecter les signes de virus non identifiés. Cette option permet l'analyse la plus complète mais le traitement est généralement plus lent.
  - **Analyser la mémoire** : la mémoire de votre ordinateur est analysée.
- 3 Cliquez sur **OK**.

## Définition des emplacements à analyser

Vous pouvez choisir les emplacements (lecteurs USB) à analyser lors d'une analyse à la demande. VirusScan USB n'analyse que les lecteurs associés à votre périphérique USB. Pour cette raison, les lecteurs de disque non associés n'apparaissent pas dans la liste **Périphériques à analyser sur ce périphérique USB**. Elle répertorie les disques amovibles de votre ordinateur et les lecteurs associés à d'autres périphériques USB.

### Définition des emplacements à analyser :

- 1 Dans le volet d'accueil de VirusScan USB, sous **Options d'analyse actuelles**, cliquez sur **Configurer**.
- 2 Dans le volet des options d'analyse, sous **Périphériques à analyser sur ce périphérique USB**, activez ou désactivez les cases à cocher suivantes.
  - **Système U3** : la partition du CD-ROM sur le périphérique est analysée. Il s'agit de l'emplacement où sont stockés les fichiers du système U3.
  - **Mon lecteur U3** : la partition de données sur le périphérique est analysée. Il s'agit de la lettre affectée au lecteur USB.
- 3 Cliquez sur **OK**.

---

## Désactivation de la surveillance en temps réel

Lorsqu'il est activé, VirusScan USB surveille constamment votre périphérique USB, à la recherche de changements de fichiers (par exemple, lorsqu'un nouveau fichier est ajouté au périphérique ou qu'un fichier s'y trouvant est modifié). Si la fonction de surveillance en temps réel détecte un changement de fichier, VirusScan USB analyse le fichier concerné, à la recherche d'une activité virale. En cas de détection d'un virus ou d'un cheval de Troie, VirusScan USB tente de le nettoyer. Si l'opération est impossible, il tente de le renommer. La surveillance en temps réel s'applique à tous les types de fichiers (indépendamment de vos paramètres d'analyse à la demande). McAfee vous déconseille de désactiver cette fonction.

### **Pour désactiver la surveillance en temps réel :**

- 1 Dans le volet d'accueil de VirusScan USB, sous **Options d'analyse actuelles**, cliquez sur **Configurer**.
- 2 Dans le volet des options d'analyse, sous **Surveillance en temps réel**, désactivez la case à cocher **Activer la surveillance en temps réel du périphérique USB**.
- 3 Cliquez sur **OK**.

---

**Remarque :** si la surveillance en temps réel est activée, elle peut détecter un fichier infecté lors d'une analyse à la demande. Pour garantir que l'infection est signalée au moins une fois, la surveillance en temps réel affiche une alerte normale.

---

---

## Lancement d'une analyse à l'insertion

Lorsque vous installez VirusScan USB, il s'ajoute automatiquement à la liste des programmes sur votre Launchpad U3 et se configure pour se lancer en cas d'insertion. Ainsi, l'analyse à la demande de VirusScan USB démarre chaque fois que vous insérez votre périphérique USB dans votre ordinateur. Si vous désactivez l'option de démarrage à l'insertion sur votre Launchpad U3, l'analyse VirusScan USB à la demande démarre la première fois que vous insérez votre périphérique USB dans l'ordinateur. Vous pouvez ensuite configurer VirusScan USB pour qu'il démarre ou non l'analyse en cas d'insertion. Si vous configurez VirusScan USB pour qu'il ne lance pas l'analyse à l'insertion, il démarre seulement lorsque la fonction de surveillance en temps réel détecte une infection ou que vous le lancez manuellement. McAfee vous conseille de ne pas désactiver l'option d'analyse à l'insertion dans VirusScan USB.

### **Pour lancer une analyse à l'insertion :**

- 1 Dans le volet d'accueil de VirusScan USB, sous **Options d'analyse actuelles**, cliquez sur **Configurer**.
- 2 Dans le volet des options d'analyse, sous **Options**, vérifiez que la case à cocher **Lancer l'analyse à l'insertion** est activée.
- 3 Cliquez sur **OK**.

---

**Conseil :** vous pouvez également cocher la case **Lancer l'analyse à l'insertion** dans le panneau Progression de l'analyse lorsqu'une analyse est terminée, interrompue ou annulée.

---



---

## Désactivation de la détection de logiciel antivirus

Par défaut, VirusScan USB détecte si vous disposez d'un logiciel antivirus à jour sur votre ordinateur, mais vous pouvez désactiver cette option.

**Pour désactiver la détection de logiciel antivirus :**

- 1 Dans le volet d'accueil de VirusScan USB, sous **Options d'analyse actuelles**, cliquez sur **Configurer**.
- 2 Dans le volet des options d'analyse, sous **Options**, désactivez la case à cocher **Détecter un logiciel antivirus sur l'ordinateur hôte**.
- 3 Cliquez sur **OK**.

---

## Affichage des messages d'information

Vous pouvez choisir de ne pas afficher certaines alertes et boîtes de dialogue VirusScan USB.

**Pour afficher les messages d'information :**

- 1 Dans le volet d'accueil de VirusScan USB, sous **Options d'analyse actuelles**, cliquez sur **Configurer**.
- 2 Dans le volet des options d'analyse, sous **Options**, activez la case à cocher **Afficher les messages d'information**.
- 3 Cliquez sur **OK**.



---

## CHAPITRE 4

# Utilisation des alertes

McAfee utilise un système d'alertes pour vous aider à gérer la sécurité de votre système. Ces alertes peuvent être classées en trois catégories principales.

- Alerte rouge
- Alerte jaune
- Alerte verte

Vous pouvez alors choisir la méthode de gestion des fichiers détectés, en fonction des recommandations présentes dans les alertes.

## Contenu de ce chapitre

A propos des alertes ..... 17

---

## A propos des alertes

La surveillance en temps réel de VirusScan USB dispose de trois types d'alertes de base : rouge, jaune et vert.

### Alerte rouge

Les alertes rouges signalent qu'un fichier infecté a été détecté mais n'a pu être ni nettoyé ni renommé. Ces alertes vous permettent de supprimer le fichier infecté de votre périphérique USB ou d'ignorer l'infection.

### Alerte jaune

Les alertes jaunes signalent qu'un fichier infecté a été détecté et n'a pas pu être nettoyé, mais qu'il a été renommé avec l'extension .vir. Ces alertes vous permettent de supprimer le fichier infecté de votre périphérique USB ou d'ignorer l'infection.

### Alerte verte

Les alertes vertes signalent qu'un fichier infecté a été détecté et nettoyé. Ces alertes étant principalement informatives, vous pouvez choisir de ne plus les afficher.



## CHAPITRE 5

# Analyse de votre périphérique USB

Lorsque vous installez VirusScan USB, il s'ajoute automatiquement à la liste des programmes sur votre Launchpad U3 et se configure pour se lancer en cas d'insertion. Ainsi, l'analyse à la demande de VirusScan USB démarre chaque fois que vous insérez votre périphérique USB dans votre ordinateur. Si vous désactivez l'option de démarrage à l'insertion, l'analyse VirusScan USB à la demande ne démarre qu'à la première insertion de votre périphérique USB dans l'ordinateur. Vous pouvez ensuite configurer VirusScan USB pour qu'il démarre ou non l'analyse en cas d'insertion. Si vous configurez VirusScan USB pour qu'il ne lance pas l'analyse à l'insertion, il démarre seulement lorsque la fonction de surveillance en temps réel détecte une infection ou que vous lancez une analyse à la demande. Dans ce dernier cas, VirusScan USB analyse les types de fichiers et les emplacements indiqués dans vos options. Pour en savoir plus sur le réglage des options d'analyse à la demande, consultez la section de réglage des options d'analyse (page 9).

---

**Remarque :** McAfee vous déconseille de désactiver l'option d'analyse à l'insertion dans VirusScan USB.

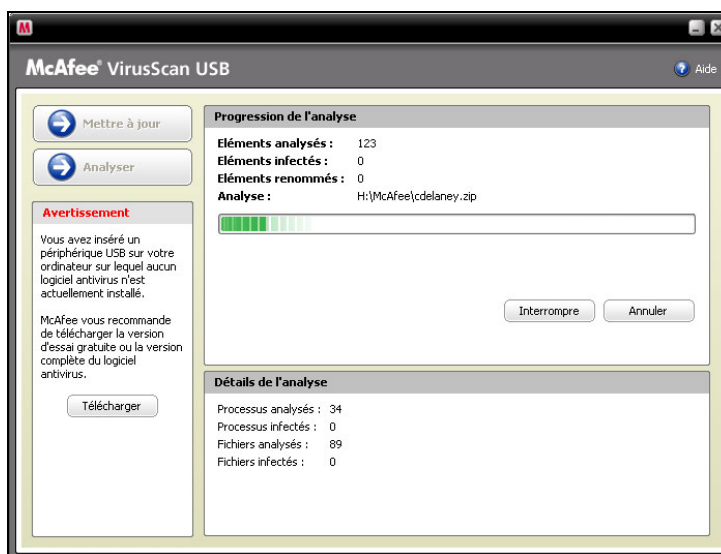
---

Lorsque VirusScan USB détecte un virus ou un cheval de Troie dans l'un des fichiers de votre périphérique USB, il accomplit l'une des opérations suivantes.

- Nettoyer : le virus ou le cheval de Troie est supprimé du fichier.
- Renommer : le fichier est renommé avec une extension .vir (en cas d'échec de l'opération de nettoyage).

S'il est impossible de nettoyer et de renommer le fichier infecté, vous pouvez le supprimer. Pour plus d'informations, consultez la section Suppression d'un fichier infecté (page 25).

Si vous le souhaitez, vous pouvez interrompre l'analyse du périphérique USB et la relancer à un moment plus opportun ; elle reprendra alors au point où elle s'est arrêtée. Par exemple, si vous réalisez une tâche gourmande en ressources alors que VirusScan USB procède à l'analyse, vous pouvez interrompre cette dernière, puis la reprendre une fois l'autre tâche terminée. Vous pouvez également annuler une analyse à tout moment.



## Contenu de ce chapitre

Analyse de votre périphérique USB .....	20
Interruption d'une analyse.....	21
Reprise de l'analyse.....	21
Annulation d'une analyse.....	21

## Analyse de votre périphérique USB

Vous pouvez analyser votre périphérique USB à tout moment. Par exemple, si vous venez d'installer VirusScan USB, vous pouvez effectuer une analyse pour vous assurer que votre périphérique n'est pas infecté par un virus ou exposé à d'autres menaces.

### **Pour analyser manuellement votre périphérique USB :**

- Dans le volet gauche de VirusScan USB, cliquez sur **Analyser**.

---

## Interruption d'une analyse

Vous pouvez interrompre une analyse en cours. Cette opération arrête l'analyse à un point spécifique et vous permet de la reprendre à partir de ce point lorsque vous le souhaitez.

**Pour interrompre l'analyse :**

- Dans le volet Progression de l'analyse, sous **Progression de l'analyse**, cliquez sur **Interrompre**.

---

**Conseil :** pour reprendre l'analyse au point où vous l'avez interrompue, cliquez sur le bouton **Reprendre**.

---

---

## Reprise de l'analyse

Lorsque vous interrompez une analyse, elle est temporairement suspendue. Vous pouvez la reprendre au point où elle s'est arrêtée. Pour plus d'informations sur l'interruption d'une analyse, reportez-vous à la section Interruption d'une analyse (page 21).

**Pour reprendre l'analyse :**

- Dans le volet Progression de l'analyse, sous **Progression de l'analyse**, cliquez sur **Reprendre**.

---

## Annulation d'une analyse

Vous pouvez annuler une analyse à tout moment, c'est-à-dire y mettre fin. A la différence de l'interruption, vous ne pourrez pas la reprendre.

**Pour arrêter l'analyse :**

- Dans le volet Progression de l'analyse, sous **Progression de l'analyse**, cliquez sur **Annuler**, puis sur **Terminer**.



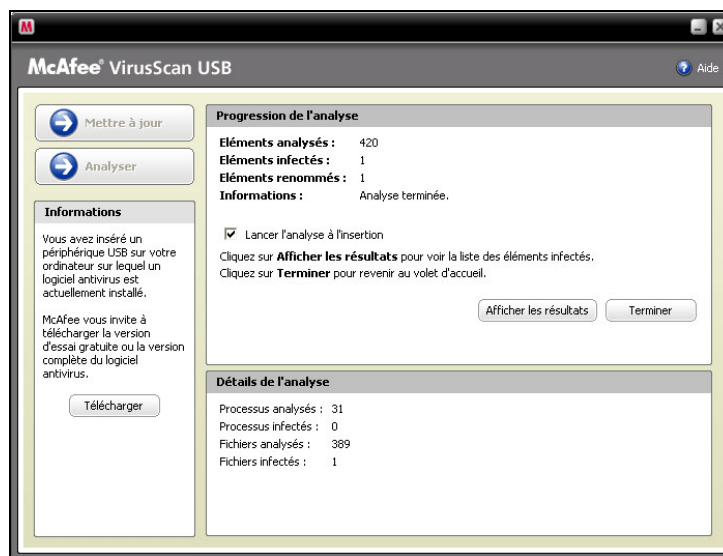


## CHAPITRE 6

# Exploitation des résultats d'analyse

Lorsqu'une analyse est en cours, VirusScan USB affiche le nombre d'éléments analysés, infectés et renommés au-dessus de la barre de progression de l'analyse. Lorsqu'une infection est détectée et que l'analyse se termine, vous pouvez consulter un résumé des résultats comprenant le chemin et le nom de chaque fichier infecté et l'opération réalisée sur ce fichier (nettoyage ou changement de nom, par exemple). Vous pouvez également consulter des informations détaillées sur chaque fichier infecté, notamment le type d'objet, le nom, l'état et le nom du fichier.

Lorsque VirusScan USB détecte un virus ou un cheval de Troie dans l'un des fichiers de votre périphérique USB, il tente de nettoyer le fichier infecté. Si l'opération échoue, il tente de le renommer. S'il est impossible de nettoyer et de renommer le fichier infecté, vous pouvez le supprimer de votre périphérique USB.



VirusScan USB affiche également un résumé de la dernière analyse sur le volet d'accueil de sorte que vous puissiez revoir les processus analysés, les processus infectés, les fichiers analysés, les fichiers infectés et la date de la dernière analyse.

## Contenu de ce chapitre

Visualisation des résultats d'une analyse .....	24
Suppression d'un fichier infecté .....	25
Visualisation du résumé de la dernière analyse.....	26
Visualisation du résumé du programme	
VirusScan USB .....	26

---

## Visualisation des résultats d'une analyse

Au terme d'une analyse, vous pouvez consulter les résultats pour obtenir une liste des éléments infectés.

### **Pour visualiser les résultats d'une analyse :**

- 1 Dans le volet Progression de l'analyse, sous **Progression de l'analyse**, cliquez sur **Afficher les résultats**.
- 2 Dans le volet Progression de l'analyse, cliquez sur un nom de fichier infecté.
- 3 Sous **Détails**, affichez des informations plus spécifiques sur le fichier infecté.
- 4 Cliquez sur **Terminer**.

---

**Remarque :** le bouton **Afficher les résultats** s'affiche seulement lorsque les fichiers infectés ont été détectés.

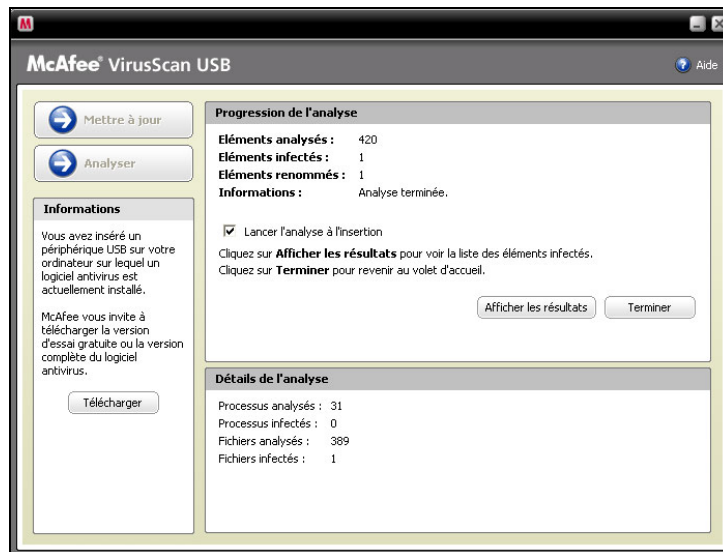
---

## Suppression d'un fichier infecté

Lorsque VirusScan USB détecte un virus ou un cheval de Troie dans l'un des fichiers de votre périphérique USB, il tente de nettoyer le fichier infecté. Si l'opération échoue, il tente de le renommer. S'il est impossible de nettoyer et de renommer le fichier infecté, vous pouvez le supprimer de votre périphérique USB.

### Pour supprimer un fichier infecté :

- 1 Dans le volet Progression de l'analyse, sous **Progression de l'analyse**, cliquez sur **Afficher les résultats**.
- 2 Dans le volet Progression de l'analyse, cliquez sur un nom de fichier infecté.



- 3 Sous **Je souhaite**, cliquez sur **Supprimer**.
- 4 Cliquez sur **Terminer**.

---

## Visualisation du résumé de la dernière analyse

VirusScan USB affiche un résumé de la dernière analyse sur le volet d'accueil, que vous pouvez consulter.

**Pour visualiser le résumé de la dernière analyse :**

- Dans le volet d'accueil de VirusScan USB, consultez les détails sous **Résumé de la dernière analyse**.

---

## Visualisation du résumé du programme VirusScan USB

VirusScan USB affiche, sur le volet d'accueil, la date de la dernière vérification de mise à jour et la version actuelle de vos fichiers de définition de virus (DAT).

**Pour visualiser le résumé du programme VirusScan USB :**

- Dans le volet d'accueil de VirusScan USB, visualisez les détails sous **Résumé du programme**.

---

## CHAPITRE 7

# Protection de votre ordinateur

VirusScan USB ne surveille pas et n'analyse pas les fichiers stockés sur votre ordinateur. Cette protection est apportée par McAfee VirusScan. Vous pouvez en télécharger une version d'essai ou une version complète sur le site de téléchargement de McAfee.

## Contenu de ce chapitre

Téléchargement d'un logiciel antivirus pour votre ordinateur .....27

---

## Téléchargement d'un logiciel antivirus pour votre ordinateur

Si VirusScan USB est configuré pour détecter si un logiciel antivirus à jour est installé sur votre ordinateur et s'il détecte qu'il n'en existe pas, un message vous demande de télécharger une version d'essai ou une version complète de McAfee VirusScan.

### **Pour télécharger un logiciel antivirus sur votre ordinateur :**

- 1 Sous **Avertissement** ou **Information**, dans le volet de gauche, cliquez sur **Télécharger**.
- 2 Suivez les instructions à l'écran pour télécharger McAfee VirusScan.

---

**Conseil :** vous pouvez également télécharger le logiciel en cliquant sur le lien figurant sous **Périphériques à analyser sur ce périphérique USB** dans le volet des options d'analyse.

---



---

## CHAPITRE 8

# Renouvellement de votre abonnement à VirusScan USB

À l'expiration de votre abonnement à VirusScan USB, le logiciel ne fonctionne plus et vous ne recevez plus les mises à jour du programme ou des fichiers de définitions de virus (DAT). Toutefois, vous pouvez toujours accéder au volet d'accueil principal de VirusScan USB, qui vous demande de renouveler votre abonnement.

**Conseil :** si vous renouvelez un abonnement avant son expiration, le temps restant est reporté dans la nouvelle période d'abonnement.

## Contenu de ce chapitre

Renouvellement de votre abonnement  
à VirusScan USB .....29

---

# Renouvellement de votre abonnement à VirusScan USB

Lorsque votre abonnement à VirusScan USB se termine, il vous est demandé de le renouveler chaque fois que le périphérique USB est connecté ou que vous essayez d'exécuter le programme. Même si VirusScan USB n'analyse plus votre périphérique USB et ne reçoit plus les mises à jour après l'expiration de votre abonnement, il vous permet toutefois de renouveler votre abonnement.

### **Pour renouveler votre abonnement à VirusScan USB :**

- Dans le volet d'accueil de VirusScan USB, sous **Résumé du programme**, cliquez sur **Renouveler**.





---

## CHAPITRE 9

# Questions fréquentes

Cette section regroupe les réponses aux questions les plus fréquemment posées.

## Contenu de ce chapitre

Une menace a été détectée. Que faire ? .....	31
Dois-je être connecté à Internet pour lancer une analyse ? .....	31
VirusScan USB analyse-t-il les fichiers compressés (.zip) ? .....	32
Comment faire pour obtenir une aide supplémentaire de McAfee ? .....	32

---

## Une menace a été détectée. Que faire ?

McAfee utilise un système d'alertes pour vous aider à gérer la sécurité de votre système. Ces alertes peuvent être classées en trois catégories principales.

- Alerte rouge
- Alerte jaune
- Alerte verte

Vous pouvez alors choisir la méthode de gestion des fichiers détectés, en fonction des recommandations présentes dans les alertes.

---

## Dois-je être connecté à Internet pour lancer une analyse ?

Vous n'avez pas besoin d'être connecté à Internet pour lancer une analyse, mais vous devez vous connecter au moins une fois par semaine pour recevoir les mises à jour McAfee.

---

## VirusScan USB analyse-t-il les fichiers compressés (.zip) ?

VirusScan USB analyse les fichiers compressés (.zip) et autres fichiers d'archive.

---

## Comment faire pour obtenir une aide supplémentaire de McAfee ?

Pour obtenir une aide supplémentaire et des réponses aux questions fréquentes, visitez la page d'accueil de l'assistance technique et du service clientèle de McAfee à l'adresse <http://www.mcafeeaide.com> (<http://www.mcafeehelp.com>).

## CHAPITRE 10

# Glossaire

Ce glossaire répertorie et définit les termes de sécurité les plus utilisés dans les produits McAfee.

---

# Glossaire

## A

### Analyse à la demande

Analyse lancée à la demande (c'est-à-dire lorsque vous cliquez sur le bouton **Analyser**). A la différence de l'analyse ou de la surveillance en temps réel, les analyses à la demande ne se lancent pas automatiquement.

## C

### Cheval de Troie

Programmes qui prétendent être des applications inoffensives. Les chevaux de Troie ne sont pas des virus, car ils ne se répliquent pas, mais ils sont tout aussi ravageurs.

## Clé

Reportez-vous à la section Périphérique USB.

## F

### Fichiers DAT

Fichiers de définition de virus. Ces fichiers contiennent les définitions de virus utilisées pour la détection des virus et des chevaux de Troie sur votre ordinateur ou votre périphérique USB.

## L

### Launchpad

Composant de l'interface U3 qui agit comme point de départ pour lancer et gérer les programmes USB U3.

## P

### Périphérique USB

Petit lecteur mémoire qui se branche sur un port USB de l'ordinateur. Un périphérique USB agit comme un petit lecteur de disque et facilite le transfert de fichiers entre deux ordinateurs.

## S

### Surveillance en temps réel

Le programme recherche constamment des modifications dans les fichiers et les dossiers (fichier ajouté à un dossier, fichier modifié...). Si la fonction de surveillance en temps réel détecte un changement de fichier, VirusScan USB analyse le fichier concerné à la recherche d'une activité virale. S'il détecte un virus ou un cheval de Troie, il nettoie le fichier. Si l'opération est impossible, il le renomme.

## U

### U3

(Plus simple, plus intelligent et mobile.) Plate-forme permettant d'exécuter Windows 2000 ou XP directement depuis un périphérique USB. L'initiative U3 a été lancée en 2004 par M-Systems et SanDisk. Elle permet aux utilisateurs d'exécuter des programmes U3 sur un ordinateur Windows, sans installer ni stocker de données ou de paramètres sur l'ordinateur.

### USB

(Universal Serial Bus.) Interface informatique standardisée permettant de connecter des périphériques.

## V

### Virus

Programmes qui se propagent et peuvent endommager vos fichiers et données. En général, leur expéditeur semble digne de foi ou leur contenu apparaît comme fiable.



## A propos de McAfee

McAfee, Inc., leader mondial en gestion des risques de sécurité et prévention des intrusions et dont le siège social est basé à Santa Clara, Californie, propose des solutions et services proactifs et éprouvés de sécurisation des systèmes et réseaux dans le monde entier. Avec son expérience de la sécurité et son engagement à l'innovation sans égal, McAfee donne aux particuliers, aux entreprises, au secteur public et aux prestataires de service la capacité de bloquer les attaques, de prévenir les perturbations et d'assurer et d'améliorer régulièrement leur sécurité.

## Copyright

Copyright © 2006 McAfee, Inc. Tous droits réservés. Cette publication ne peut faire l'objet, même partiellement, d'aucune reproduction, transmission, transcription, d'aucun stockage dans un système d'extraction ou d'aucune traduction dans aucune langue, sous aucune forme et d'aucune manière que ce soit sans autorisation écrite préalable de McAfee, Inc. McAfee et les autres marques mentionnées dans le présent document sont des marques de McAfee, Inc. et/ou de ses associés aux Etats-Unis et/ou dans certains autres pays. La couleur rouge utilisée pour identifier des fonctionnalités liées à la sécurité est propre aux produits de marque McAfee. Toutes les autres marques, déposées ou non, ainsi que les éléments soumis à un copyright mentionnés dans ce document sont la propriété exclusive de leurs détenteurs respectifs.

### ATTRIBUTION DES MARQUES COMMERCIALES

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (EN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE ET DESIGN, CLEAN-UP, DESIGN (E STYLISE), DESIGN (N STYLISE), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (EN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (EN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M ET DESIGN, MCAFEE, MCAFEE (EN KATAKANA), MCAFEE ET DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (EN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SITEADVISOR, SITEADVISOR, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (EN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (EN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER ET YOUR NETWORK. OUR BUSINESS.



A TOUS LES UTILISATEURS : LISEZ ATTENTIVEMENT L'ACCORD JURIDIQUE CORRESPONDANT A LA LICENCE QUE VOUS AVEZ ACHETEE. IL DEFINIT LES CONDITIONS GENERALES D'UTILISATION DU LOGICIEL SOUS LICENCE. SI VOUS IGNOREZ LE TYPE DE LICENCE QUE VOUS AVEZ ACQUIS, REPORTEZ-VOUS AUX DOCUMENTS COMMERCIAUX ET AUTRES DOCUMENTS D'OCTROI DE LICENCE, OU AU BON DE COMMANDE, QUI ACCOMPAGNENT VOTRE PROGIciel OU QUI VOUS ONT ÉTÉ TRANSMIS SÉPARÉMENT DANS LE CADRE DE VOTRE ACHAT (SOUS LA FORME D'UN LIVRET, D'UN FICHER INCLUS DANS LE CD DU PRODUIT OU D'UN FICHER DISPONIBLE SUR LE SITE WEB A PARTIR DUQUEL VOUS AVEZ TÉLÉCHARGÉ LE PROGIciel). SI VOUS N'ETES PAS D'ACCORD AVEC CERTAINS TERMES DE CET ACCORD, N'INSTALLEZ PAS LE LOGICIEL. LE CAS ECHEANT, VOUS POUVEZ RENVOYER LE PRODUIT A MCAFEE, INC. OU A L'ENDROIT OU VOUS L'AVEZ ACHETE AFIN D'EN OBTENIR LE REMBOURSEMENT INTEGRAL.

# Index

## A

A propos de McAfee.....	37
A propos des alertes.....	17
Affichage des messages d'information ..	15
Analyse à la demande.....	34
Analyse de votre périphérique USB ..	9, 19, 20
Annulation d'une analyse .....	21

## C

Caractéristiques.....	4
Cheval de Troie.....	34
Clé.....	34
Comment faire pour obtenir une aide supplémentaire de McAfee ? .....	32
Copyright .....	38

## D

Définition des emplacements à analyser .....	12
Définition des types de fichiers analysés .....	11
Désactivation de la détection de logiciel antivirus .....	15
Désactivation de la surveillance en temps réel.....	13
Dois-je être connecté à Internet pour lancer une analyse ? .....	31

## E

Exploitation des résultats d'analyse .....	23
--	----

## F

Fichiers DAT .....	34
--------------------	----

## G

Glossaire.....	33
----------------	----

## I

Installation de VirusScan USB .....	6
Installation et mise à jour de VirusScan USB.....	5
Interruption d'une analyse .....	21

## L

Lancement d'une analyse à l'insertion ..	14
--	----

Launchpad.....	34
----------------	----

## M

McAfee VirusScan USB .....	3
Mise à jour de VirusScan USB .....	8

## P

Périphérique USB.....	34
Protection de votre ordinateur.....	27

## Q

Questions fréquentes .....	31
----------------------------	----

## R

Réglage des options d'analyse.....	5, 9, 19
Renouvellement de votre abonnement à VirusScan USB.....	29
Reprise de l'analyse.....	21

## S

Suppression d'un fichier infecté .....	19, 25
Surveillance en temps réel.....	34

## T

Téléchargement d'un logiciel antivirus pour votre ordinateur .....	27
---	----

## U

U3 .....	35
Une menace a été détectée. Que faire ? .	31
USB.....	35
Utilisation des alertes.....	17

## V

Virus .....	35
VirusScan USB analyse-t-il les fichiers compressés (.zip) ?.....	32
Visualisation des résultats d'une analyse .....	24
Visualisation du résumé de la dernière analyse .....	26
Visualisation du résumé du programme VirusScan USB.....	26