

Addendum à la documentation

Logiciel de sécurité Zone Alarm version 7.1

Ce document décrit les nouvelles fonctionnalités qui n'ont pas été incluses dans les versions localisées du guide de l'utilisateur. Pour plus d'informations, cliquez sur l'option désirée dans la liste ci-dessous.

- **Centre de protection d'identité ZoneAlarm** : vous permet de prévenir et de détecter une usurpation d'identité, et d'y remédier, si nécessaire.
- **Mode Jeu** : supprime temporairement la plupart des analyses, mises à jour de produits et alertes du Logiciel de sécurité ZoneAlarm pour vous permettre de jouer sur votre ordinateur tout en limitant les interruptions.
- **Protections système spéciales OSFirewall** : détermine si les programmes installés sur votre ordinateur peuvent réaliser des opérations spécifiques, telles que la modification de votre page d'accueil dans Internet Explorer ou l'installation de contrôles ActiveX.
- **Options d'analyse de virus**—Permet d'ignorer les fichiers qui dépassent une certaine taille et fournit une base de données de programmes destructeurs conséquente.
- **Analyse de la mémoire système**—Analyse la mémoire RAM de votre ordinateur.
- **Liste d'exceptions**—Permet de gérer une liste d'éléments devant être ignorés par le Logiciel de sécurité ZoneAlarm.
- **Niveau de contrôle des programmes**—Fournit un mode Auto-learn qui réduit le nombre d'alertes pendant que Logiciel de sécurité ZoneAlarm découvre votre ordinateur.
- **Définition des options de sécurité réseau**—Permet de bloquer ou non le trafic Internet qui utilise Internet Protocol version 6 (IPv6).
- **Corrections et mises à jour de la documentation**

Centre de protection d'identité ZoneAlarm

L'avènement du commerce électronique, de l'archivage électronique et du publi-postage financier a entraîné une recrudescence de l'usurpation d'identité au cours des dernières années. Les pirates informatiques peuvent employer des logiciels destructeurs pour intercepter vos données personnelles en ligne, alors que les voleurs peuvent dérober des CD et des ordinateurs portables contenant des informations sur vos clients, ou encore intercepter des courriers électroniques sensibles (tels que des offres de carte de crédit pré-approuvées) incluant des données confidentielles.

Le centre de protection d'identité est un site Web vous permettant de prévenir et de détecter une éventuelle usurpation d'identité, et d'y remédier, si nécessaire. Il contient des astuces de protection d'identité, ainsi que des ressources vous permettant de contrôler l'utilisation de vos données personnelles et de remédier à une usurpation d'identité.

Vous pouvez accéder au centre de protection d'identité dans ZoneAlarm Pro et ZoneAlarm Security Suite.

Pour visiter le centre de protection d'identité :

1. Accédez à **Protection d'identité | Général**.
2. Dans la zone Centre de protection d'identité, cliquez sur **Accéder au centre de protection d'identité ZoneAlarm**.

Mode Jeu

Le mode Jeu supprime temporairement la plupart des analyses, mises à jour de produits et alertes du Logiciel de sécurité ZoneAlarm pour vous permettre de jouer sur votre ordinateur tout en limitant les interruptions. Dans ce mode, vous pouvez autoriser ou refuser temporairement toutes les demandes d'autorisation des programmes afin que le Logiciel de sécurité ZoneAlarm puisse y répondre automatiquement sans afficher d'alertes. Les analyses et les mises à jour logicielles automatiques sont ajournées jusqu'à la désactivation du mode Jeu. Le mode Jeu demeure activé jusqu'à sa désactivation, ou jusqu'à l'arrêt du Logiciel de sécurité ZoneAlarm ou de l'ordinateur.

Le mode Jeu supprime l'ensemble des alertes informatives et des alertes dans lesquelles vous êtes invité à prendre une décision. Parmi ces dernières, on distingue les alertes causées par les paramètres Demander de la liste des programmes, telles que les alertes d'autorisation déclenchées par des programmes essayant d'envoyer des courriers électroniques ou d'agir en tant que serveurs. Elles incluent également les alertes OSFirewall qui vous invitent à autoriser ou refuser un comportement jugé inhabituel ou suspect. Les paramètres du mode Jeu ne remplacent pas les paramètres Bloquer ou Autoriser de la liste des programmes. Si vous avez configuré le Logiciel de sécurité ZoneAlarm afin qu'il bloque toujours

un programme donné, il maintient le blocage du programme, même si vous avez activé le mode Jeu via le paramètre Autoriser.

L'utilisation du mode Jeu peut diminuer la sécurité du système. Si vous autorisez toutes les demandes de droits d'accès, les risques qu'un programme malveillant nuise à votre ordinateur ou accède à vos données sont plus élevés. Par ailleurs, le refus de toutes les demandes peut provoquer l'interruption des fonctions d'un programme légitime. Par conséquent, il est recommandé de n'activer ce mode que pendant la durée du jeu.


Pour activer le mode Jeu :

1. Cliquez sur l'icône de la barre d'état à l'aide du bouton droit de la souris, puis choisissez **Mode Jeu...**
2. Dans la boîte de dialogue Activer le mode Jeu qui apparaît à l'écran, cliquez sur l'une des options suivantes :

Répondre à toutes les alertes par «Autoriser» : les demandes de droits d'accès sont accordées.

Répondre à toutes les alertes par «Refuser» : les demandes de droits d'accès sont refusées.

3. Laissez la boîte de dialogue Activer le mode Jeu ouverte ou réduisez-la, mais ne la fermez pas (la fermeture de cette dernière provoque en effet la désactivation du mode Jeu).

Lorsque le mode Jeu est activé le Logiciel de sécurité ZoneAlarm affiche une icône spéciale, , dans la barre d'état.

Pour désactiver le mode Jeu :

☞ Effectuez l'une des opérations suivantes :

- Pour fermer la boîte de dialogue Activer le mode Jeu, cliquez sur **Annuler** ou sur l'icône de fermeture (x) dans le coin supérieur droit de la fenêtre.
- Cliquez sur **Quitter le mode Jeu** dans la boîte de dialogue Activer le mode Jeu.
- Cliquez sur l'icône de la barre d'état à l'aide du bouton droit de la souris, puis choisissez **Quitter le mode Jeu**.

Notez que le mode Jeu est automatiquement désactivé à l'arrêt complet de l'ordinateur ou lors de la fermeture du Logiciel de sécurité ZoneAlarm.

Protections système spéciales OSFirewall

Activée par défaut, la fonction de protection OSFirewall identifie les programmes essayant d'effectuer des opérations douteuses sur votre ordinateur par le biais du

système d'exploitation. Vous pouvez également configurer diverses protections système spéciales OSFirewall, qui déterminent si les programmes installés sur votre ordinateur peuvent réaliser des opérations spécifiques, telles que la modification de votre page d'accueil dans Internet Explorer ou l'installation de contrôles ActiveX.

Les protections système spéciales OSFirewall peuvent prévenir quelques-uns des comportements suspects de niveau moyen décrits dans l'annexe "Comportement des programmes".

Pour configurer les paramètres d'OSFirewall :

1. Sélectionnez **Contrôle des programmes | Général**.
2. Dans la zone Contrôle des programmes, cliquez sur **Personnaliser**.
3. Dans la boîte de dialogue Paramètres de contrôle personnalisé des programmes qui apparaît à l'écran, sélectionnez l'onglet **OSFirewall**.
4. Cochez ou désactivez la case **Activer OSFirewall**, selon les besoins (notez que, pour pouvoir configurer les protections système spéciales OSFirewall dans l'étape suivante, il vous faut préalablement cocher cette case).
5. Configurez, si vous le souhaitez, les protections système spéciales OSFirewall. Pour l'une des actions figurant dans la liste, cliquez sur le champ Etat, puis sélectionnez **Autoriser**, **Refuser**, **Demander** ou **Utiliser le paramètre Programme**. Si vous choisissez Utiliser le paramètre Programme, le Logiciel de sécurité Zone Labs vous renvoie aux paramètres de SmartDefense Advisor ou à vos paramètres manuels.
6. Cliquez sur **Appliquer** pour enregistrer vos paramètres et laisser la boîte de dialogue activée ou sur **OK** pour enregistrer les paramètres et fermer la boîte de dialogue.

Options d'analyse de virus

Vous pouvez configurer votre analyse anti-virus de manière à ce que tous les fichiers dépassant une certaine taille soient ignorés (la valeur par défaut est 8 Mo). Cette option réduit la durée d'analyse sans accroître les risques puisque la taille des fichiers virus est en règle générale inférieure à 8 Mo. Les fichiers de taille importante pouvant contenir des virus, votre ordinateur est toujours protégé si vous avez activé l'analyse lors de l'accès.

Vous pouvez également activer la base de données étendue. Cette base de données inclut, outre la liste des virus standard, une liste complète des programmes destructeurs. Toutefois, certains programmes destructeurs mentionnés dans la base de données étendue peuvent également être listés dans la base de données standard de logiciels espions ; il est possible que des programmes destructeurs suspects soient analysés deux fois. De plus, la liste de programmes destructeurs de la base de données étendue peut également comprendre des programmes que vous considérez comme bénins.

Pour spécifier les options d'analyse de virus :

1. Sélectionnez **Anti-virus/anti-espion | Général**, puis cliquez sur **Options avancées**.

La boîte de dialogue Options avancées s'affiche.

2. Dans la zone **Gestion des virus**, sélectionnez **Options d'analyse**.

3. Cochez ou désactivez la case **Ignorer si l'objet est supérieur à**.

Si vous avez coché cette case, saisissez une taille maximale pour l'objet dans le champ **Mo**.

4. Cochez ou désactivez la case **Activer une base de données étendue**, puis cliquez sur **OK**.

Analyse de la mémoire système

Pour analyser la mémoire système, procédez comme suit.

Pour analyser la mémoire système

1. Sélectionnez **Anti-virus/anti-espion | Général**.

2. Cliquez sur **Options avancées**.

La boîte de dialogue Options avancées s'affiche.

3. Sous **Gestion des virus**, sélectionnez **Cibles de l'analyse**.

4. Sélectionnez les disques, dossiers et fichiers à analyser.

5. Cochez ou désactivez la case **Analyser les secteurs de démarrage de tous les disques locaux**.

6. Cochez ou désactivez la case **Analyser la mémoire système**, puis cliquez sur **OK**.

Liste d'exceptions

Bien que certains logiciels considérés comme suspects par la base de données étendue puissent nuire à votre ordinateur, endommager ou rendre vos données vulnérables aux pirates informatiques, de nombreuses applications potentiellement bénignes seront identifiées comme des virus lors d'une analyse. Si vous utilisez l'une de ces applications, vous pouvez les exclure des analyses anti-virus en les ajoutant à la liste d'exceptions. Vous pouvez ajouter des programmes à la liste des exceptions en cliquant sur l'élément désiré avec le bouton droit de la souris dans la liste Résultats de l'analyse, puis en choisissant **Toujours ignorer** dans le menu.

Une fois que les logiciels figurent dans la liste des exceptions, ils ne seront plus identifiés au cours des analyses anti-virus. Si un virus a été ajouté par inadvertance à la liste d'exceptions, vous pouvez l'en supprimer manuellement.

Pour supprimer un virus de la liste des exceptions, procédez comme suit :

1. Sélectionnez **Anti-virus/anti-espion | Général**, puis cliquez sur **Options avancées**.
2. Sous Gestion des virus, sélectionnez **Exceptions**.
3. Dans la zone Exceptions de traitement des virus, sélectionnez le virus que vous désirez supprimer, puis cliquez sur **Supprimer de la liste**.
4. Cliquez sur **OK**.

Niveau de contrôle des programmes

Le Logiciel de sécurité ZoneAlarm met à votre disposition plusieurs méthode de contrôle de programmes. Le contrôle de base des programmes vous permet de déterminer les droits d'accès et les droits relatifs au serveur pour les programmes individuels. Le contrôle avancé des programmes empêche les programmes destructeurs de se servir de programmes sécurisés. Le contrôle d'interaction entre les applications vous alerte si un processus tente d'en utiliser un autre ou si un programme essaie de démarrer un autre programme. La fonction de protection OSFirewall identifie les programmes essayant d'effectuer des opérations douteuses sur votre ordinateur par le biais du système d'exploitation.

Pour limiter le nombre d'alertes affichées, procédez comme suit :

- Si vous utilisez le Logiciel de sécurité ZoneAlarm avec Anti-virus, utilisez le niveau de contrôle des programmes en mode Auto-learn. Le mode Auto-learn permet un niveau de protection modéré pendant les 7 à 21 premiers jours d'utilisation du Logiciel de sécurité ZoneAlarm. Une fois que le Logiciel de sécurité ZoneAlarm «connaît» votre ordinateur, le niveau de contrôle des programmes est remis sur le maximum.
- Afin de bénéficier des paramètres de configuration de programme recommandés par Zone Alarm, utilisez SmartDefense Advisor avec le contrôle des programmes.

Pour définir le niveau de contrôle des programmes :

1. Sélectionnez **Contrôle des programmes | Général**.

2. Dans la zone Contrôle des programmes, cliquez sur le curseur et déplacez-le jusqu'au paramètre souhaité.

Max (pour les versions avec Anti-virus) Elevé (pour les versions sans Anti-virus)	<p>Lorsque c'est le cas, de nombreuses alertes peuvent s'afficher.</p> <ul style="list-style-type: none"> ◆ Les programmes doivent demander des droits d'accès à Internet et au serveur. ◆ OSFirewall surveille les comportements suspects. ◆ Le contrôle des programmes Avancé et le Contrôle d'interaction entre les applications sont activés. ◆ Le contrôle des composants est désactivé par défaut.*
Auto (pour les versions avec Anti-virus)	<p>Ce mode réduit le nombre d'alertes.</p> <ul style="list-style-type: none"> ◆ Ce niveau de contrôle est moins sûr pendant les 7 à 21 premiers jours. ◆ Le réseau et OSFirewall vont analyser certains programmes.
Moyen (pour les versions sans Anti-virus)	<p>Il s'agit du paramètre par défaut.</p> <ul style="list-style-type: none"> ◆ Les programmes doivent demander des droits d'accès à Internet et au serveur. ◆ OSFirewall surveille les comportements suspects. ◆ Le contrôle des composants est désactivé par défaut.*
Min (pour les versions avec Anti-virus)	<ul style="list-style-type: none"> ◆ OSFirewall est désactivé. ◆ Le contrôle des composants est désactivé par défaut.* ◆ Les modes Furtif et Contrôle du serveur sont disponibles.
Bas (pour les versions sans Anti-virus)	<ul style="list-style-type: none"> ◆ OSFirewall est désactivé. ◆ Le contrôle des composants est désactivé par défaut.* ◆ Les modes Furtif et Contrôle du serveur ne sont pas disponibles.
Désactivé	<p>Le Contrôle des programmes est désactivé.</p> <ul style="list-style-type: none"> ◆ Aucun programme ni aucun composant n'est authentifié ni identifié. ◆ Aucune autorisation de programme n'est appliquée. ◆ Des droits d'accès et de serveur sont accordés à tous les programmes. ◆ Tous les programmes sont autorisés à effectuer des actions suspectes. ◆ Aucune alerte de programme n'est affichée.

* Le contrôle des composants est désactivé par défaut. Si vous avez activé le contrôle des composants, son état reste inchangé aussi longtemps que le niveau de contrôle des programmes est défini sur Elevé, Moyen ou Bas.

Définition des options de sécurité réseau

La détection automatique de réseau simplifie la configuration de la zone sûre et évite l'interruption des activités habituelles du réseau local, telles que le partage de fichiers et d'imprimantes. Le Logiciel de sécurité ZoneAlarm ne détecte que les réseaux auxquels vous êtes connecté physiquement. Les connexions à des réseaux routés ou virtuels ne sont pas détectées.

Vous pouvez configurer le Logiciel de sécurité ZoneAlarm de manière à inclure chaque réseau détecté dans la zone sûre sans que vous en soyez averti, ou pour qu'il vous demande à chaque fois si un nouveau réseau détecté doit être ajouté.

Pour spécifier les paramètres réseau :

1. Sélectionnez **Pare-feu | Général**.
2. Cliquez sur **Avancé**.
3. Dans la zone Paramètres réseau, choisissez vos paramètres de sécurité.

Inclure les réseaux dans la zone sûre lors de leur détection	Place automatiquement les nouveaux réseaux dans la zone sûre. Ce paramètre offre le niveau de sécurité le plus bas.
Exclure les réseaux de la zone sûre lors de leur détection	Bloque automatiquement l'ajout des nouveaux réseaux à la zone sûre et les place dans la zone Internet. Ce paramètre offre le niveau de sécurité le plus élevé.
Demander la zone dans laquelle placer les nouveaux réseaux lors de la détection	Le Logiciel de sécurité ZoneAlarm affiche une alerte Nouveau réseau ou l'Assistant de configuration réseau, qui permet de spécifier la zone.
Ajouter automatiquement les nouveaux réseaux sans fil non protégés (WEP ou WPA) dans la zone Internet	Place automatiquement des réseaux sans fil non sécurisés dans la zone Internet, empêchant ainsi l'accès non autorisé à vos données par d'autres utilisateurs accédant au réseau.
Activer la mise en réseau IPv6	Permet d'activer le trafic réseau IPv6 pour accéder à votre ordinateur.

Corrections et mises à jour de la documentation

Les sections suivantes abordent les corrections et les mises à jour qui n'ont pas été incluses dans le corps principal des versions localisées de l'aide en ligne ou du guide de l'utilisateur :

- “Analyses de logiciels espions,” page 9
- “Exclusion de logiciels espions des analyses,” page 9
- “Résultats de l'analyse des logiciels espions et des virus,” page 9
- “Contrôle des composants,” page 9
- “Nouveau comportement de l'option Conserver ce paramètre,” page 10

- “Modification de nom dans le volet Pare-feu,” page 10
- “Nouvelles icônes de la barre d’état,” page 10

Analyses de logiciels espions

Dans les versions précédentes du Logiciel de sécurité ZoneAlarm, la documentation indiquait la possibilité d'initier une analyse des logiciels espions en ouvrant un fichier ou en choisissant une option d'analyse après avoir cliqué sur un fichier avec le bouton droit de la souris. Cette information est incorrecte.

Vous pouvez initier une analyse de logiciels espions de deux manières différentes :

- Vous pouvez cliquer sur **Rechercher les logiciels espions** dans la zone Anti-espion de l'onglet Général du volet **Anti-virus/anti-espion**.
- Vous pouvez programmer une analyse système pour une exécution unique ou régulière. (Pour plus de détails sur la configuration de cette option, consultez l'aide en ligne correspondante.)

Exclusion de logiciels espions des analyses

Dans les versions précédentes de la documentation, les instructions d'exclusion de programmes particuliers des analyses ont omis certains détails. Voici le texte corrigé :

Bien que certains logiciels espions soient capables de nuire à votre ordinateur, d'endommager ou de rendre vos données vulnérables aux pirates informatiques, il existe de nombreuses applications bénignes qui seront toujours identifiées comme des logiciels espions lors d'une analyse. Si vous utilisez l'une de ces applications (logiciel de reconnaissance vocale, par exemple), vous pouvez les exclure des analyses de logiciels espions en les ajoutant à la liste d'exceptions. Vous pouvez ajouter des logiciels espions à la liste des exceptions en cliquant sur l'élément désiré avec le bouton droit de la souris dans la liste Résultats de l'analyse, puis en choisissant Toujours ignorer dans le menu contextuel.

Résultats de l'analyse des logiciels espions et des virus

La boîte de dialogue Résultats de l'analyse contenant les résultats des analyses de virus et de logiciels espions inclut à présent une zone intitulée Détails. Dans le cas d'analyses de logiciels espions, cette zone répertorie les chemins complets de toutes les traces de logiciels espions (telles que les clés de registre, les cookies, etc.). Ces informations peuvent s'avérer d'une grande utilité pour les utilisateurs expérimentés désireux d'effectuer un suivi des logiciels espions non traités automatiquement par le Logiciel de sécurité ZoneAlarm. Dans le cas d'analyses de virus, la zone Détails reste vide.

Contrôle des composants

La documentation inclut désormais des détails décrivant l'interaction entre le contrôle des programmes et celui des composants. Voici le texte mis à jour :

Quels que soient vos paramètres de contrôle des programmes, le contrôle des composants est désactivé par défaut. La modification du niveau de contrôle des

programmes n'entraîne pas systématiquement l'activation du contrôle des composants. Toutefois, si vous activez le contrôle des composants, son état reste inchangé aussi longtemps que le niveau de contrôle des programmes est défini sur Elevé, Moyen ou Bas.

Nouveau comportement de l'option Conserver ce paramètre

La version 6.5 introduit un nouveau comportement pour la case **Conserver ce paramètre** dans les alertes de programme. Voici la nouvelle description :




Tant que SmartDefense Advisor est défini sur Auto, le Logiciel de sécurité Zone Labs n'émet des alertes de programme que si aucun paramètre automatique n'est disponible. Si vous choisissez **Conserver ce paramètre** dans une alerte de programme lors de l'autorisation ou du refus d'un accès au programme, Logiciel de sécurité Zone Labs conserve ce paramètre, excepté si un paramètre différent est défini dans SmartDefense Advisor ou si vous le modifiez manuellement dans l'onglet Programmes. Si vous ne choisissez pas **Conserver ce paramètre**, le Logiciel de sécurité Zone Labs émet une autre alerte de programme la prochaine fois que le programme tente de recommencer la même opération.

Modification de nom dans le volet Pare-feu

Le nom de l'un des paramètres Niveau de sécurité de la zone Internet et Niveau de sécurité de la zone sûre, situés dans l'onglet Général du volet Pare-feu, a changé. Le paramètre Bas devient Désactivé.

Nouvelles icônes de la barre d'état

Les nouvelles icônes de barre d'état suivantes ont été intégrées à la version 6.5 :

Icône	Description
	Le Logiciel de sécurité ZoneAlarm effectue une analyse des logiciels espions et/ou des virus. Pour plus de détails sur les analyses de logiciels espions ou de virus, consultez l'aide en ligne correspondante, ainsi que les sections relatives aux logiciels espions contenues dans le chapitre "Corrections et mises à jour de la documentation," page 8 du présent document. Si cette icône est visible, vous pouvez cliquer dessus à l'aide du bouton droit de la souris et sélectionner Afficher l'analyse pour accéder à la boîte de dialogue Etat de l'analyse.
	Le mode Jeu est activé, entraînant la suppression des mises à jour, des analyses et de la plupart des alertes par le Logiciel de sécurité ZoneAlarm. Pour plus de détails sur le mode Jeu, reportez-vous à la section "Mode Jeu," page 2.
	Le Logiciel de sécurité ZoneAlarm reçoit une mise à jour, telle qu'une mise à jour des nouvelles définitions de logiciels espions ou de virus.

