Démarrage rapide : Avast Small Office Protection

Pour obtenir une aide supplémentaire ou des informations de résolution des problèmes, consultez notre documentation en ligne :

https://businesshelp.avast.com/

Sommaire

Configuration de votre appareil

Le nouveau produit Small Office Protection d'Avast se distingue d'Avast Business Antivirus sur plusieurs points, à savoir :

- licence limitée à 10 postes, le produit étant destiné à des petites entreprises équipées d'un nombre limité d'appareils
- *ne peut pas* être installé sur des systèmes d'exploitation de type serveur
- peut être installé sur des appareils Android/iOS
- contient de nombreux composants différents
- n'est accessible qu'aux appareils *non gérés*

Pour plus d'informations sur les différents composants disponibles pour Avast Business Antivirus par rapport à ceux de Small Office Protection, consultez Présentation des composants (uniquement en anglais).

Vérifier la configuration système requise

Terminaux Small Office Protection

Windows :

- 7 SP2 ou version supérieure, 8.x à l'exception de RT et Starter Edition, 10 à l'exception de Mobile et IoT Core Edition

Mac :

- MacOS 10.10 (Mavericks ou version ultérieure avec au moins 500 Mo d'espace libre sur le disque dur)

Android :

- Android 4.1 (Jelly Bean) ou version supérieure

iPhone/iPad :

- iOS 12.0 ou version supérieure

Vérifier la configuration requise pour le pare-feu

Pour le fonctionnement global et pour permettre aux clients Small Office Protection de s'authentifier et/ou de se mettre à jour, vous devez autoriser certains ports et adresses URL sur votre pare-feu ou serveur proxy.

Ports

TCP et UDP :

- 53 – Services DNS sécurisés (uniquement si le composant Real Site est utilisé)
- 80 – Vérification des vulnérabilités Internet et mises à jour des fonctionnalités
- 443 – Négociation des clés de chiffrement FFL (uniquement si le composant Real Site est utilisé)

URL

- *.avast.com
- *.avcdn.net
- *.mailshell.net (uniquement si l'Anti-Spam est utilisé)

Installation de Small Office Protection sur les appareils

Postes de travail Windows

Pour un client Small Office Protection non géré, vous pouvez télécharger le programme d'installation ici. Une fois le programme d'installation téléchargé, vous pouvez l'exécuter sur l'appareil Windows sur lequel vous souhaitez installer le programme Antivirus.

Personnalisation de l'installation

1. Copiez le fichier d'installation à un emplacement accessible à l'appareil final.
2. Double-cliquez sur le fichier d'installation pour l'exécuter.
3. Si vous êtes invité à autoriser l'application à apporter des modifications à votre appareil, cliquez sur **Oui**.
4. Dans la section **Personnaliser**, procédez de l'une des façons suivantes :
    - Sélectionnez **Protection recommandée** pour installer tous les composants.
    - Sélectionnez **Protection minimale** pour installer uniquement l'Agent des fichiers, Web ou email.
    - Sélectionnez **Protection personnalisée** pour cocher et décocher les composants que souhaitez installer.

5. Cliquez sur **Installer** et patientez le temps que Small Office Protection s'installe sur votre appareil
6. Lorsque vous y êtes invité, redémarrez l'appareil.

Composants recommandés pour serveurs et postes de travail

Les besoins d'un environnement professionnel n'étant pas les mêmes que celui d'un particulier, il est déconseillé d'utiliser certains composants dans ce type de réseau, même s'ils sont disponibles dans Small Office Protection.

Recommandé pour les environnements professionnels

Les composants suivants doivent être entièrement désinstallés ou désactivés en mettant les curseurs sur la position **Désactivé** :

- Real Site
- Inspecteur Wi-Fi

Si vous ne supprimez pas ces composants, il se peut que le réseau soit instable, que les ordinateurs soient ralentis ou que vous rencontriez des erreurs.

Appareils MacOS X

Pour un client Small Office Protection non géré, vous pouvez télécharger le programme d'installation ici. Une fois le programme d'installation téléchargé, vous pouvez l'exécuter sur l'appareil MacOS X sur lequel vous souhaitez installer le programme Antivirus.

1. Copiez le fichier d'installation (.dmg) à un emplacement accessible à votre appareil et veillez à ce qu'aucun autre logiciel antivirus ou application n'est en cours d'exécution.
2. Double-cliquez sur le fichier d'installation téléchargé.
3. Double-cliquez sur l'icône Small Office Protection, puis fermez la fenêtre.
4. Cliquez sur **Continuer** dans la fenêtre contextuelle, consultez la Politique de confidentialité, puis cliquez sur **Continuer**.
5. Cliquez sur **Continuer** pour confirmer que vous avez lu le *Contrat de licence de l'utilisateur final*, puis cliquez sur **Accepter** pour confirmer que vous acceptez les conditions.
6. Si vous souhaitez apporter des modifications à votre installation par défaut, cliquez sur **Personnaliser**. Sinon, cliquez sur **Installer**.

7. Si vous y êtes invité, utilisez votre Touch ID ou le mot de passe administrateur pour accorder une autorisation d'installation, puis cliquez sur **Installer le logiciel**.
8. Cliquez sur OK pour autoriser Small Office Protection à accéder à votre dossier de téléchargements.
9. Lorsque la notification *Extension système bloquée* s'affiche, cliquez sur **Ouvrir les préférences de sécurité**, puis procédez comme suit :
    1. Cliquez sur l'icône de cadenas, entrez votre mot de passe administrateur, cliquez sur **Déverrouiller**, puis sur **Autoriser**.
    2. Sélectionnez **Confidentialité**, puis activez *Accès complet au disque* pour Small Office Protection. Lorsque vous y êtes invité, cliquez sur **Quitter**, puis fermez la fenêtre **Sécurité et confidentialité**.
10. Décochez éventuellement la case si vous ne souhaitez pas que Google Chrome soit installé comme navigateur par défaut, puis cliquez sur **Continuer**.
11. Cliquez sur **Fermer** une fois l'installation terminée, puis sur **Déplacer vers la corbeille**.
12. Cliquez sur **OK** pour autoriser le programme d'installation de Small Office Protection à accéder à votre dossier de téléchargements.

Appareils Android

Vous pouvez télécharger Small Office Protection sur votre téléphone Android à partir de Google Play Store.

1. Ouvrez l'application Play Store.
2. Lancez une recherche sur « Avast ».
3. Sélectionnez **Avast Antivirus - Mobile Security & Virus** dans la liste.
4. Cliquez sur **Installer**.
5. Si nécessaire, cliquez sur **Accepter** pour permettre le démarrage du téléchargement.

Appareils iOS

Vous pouvez télécharger Small Office Protection pour votre appareil iOS à partir de l'App Store.

1. Ouvrez l'App Store.
2. Lancez une recherche sur « Avast Mobile Security ».

3. Sélectionnez **Avast Security & Privacy** dans la liste.
4. Appuyez sur l'icône de téléchargement.
5. Une fois l'application téléchargée, appuyez sur **Ouvrir**.
6. Si vous y êtes invité, appuyez sur **Autoriser** pour autoriser Avast Security & Privacy à vous envoyer des notifications.

Activation des licences sur votre appareil

Vous pouvez activer votre abonnement Small Office Protection après avoir installé le programme sur votre ou vos appareils. En achetant Small Office Protection, vous avez dû obtenir un code d'abonnement dont vous pouvez vous servir pour activer vos appareils, qui sont normalement liés à votre compte Avast. Le nombre d'appareils que vous pouvez activer dépend de l'abonnement que vous avez acheté.

Postes de travail Windows

1. Ouvrez l'interface utilisateur de Small Office Protection sur l'appareil.
2. Cliquez sur **Menu**.
3. Cliquez sur **Saisir un code d'activation**.
4. Saisissez votre code d'activation, puis cliquez sur **Entrer**.
5. Si nécessaire, confirmez les détails de votre abonnement et des composants concernés.

Appareils Android

Activation avec un code d'activation

1. Appuyez sur l'icône *Avast Mobile Security* sur votre appareil pour ouvrir l'application.
2. Appuyez sur **Menu** ▸ **Supprimer les publicités**.
3. Appuyez sur les **trois points** en haut à droite, puis sur **Déjà acheté**.
4. Sélectionnez **Entrer un code d'activation**.
5. Saisissez ou collez votre code d'activation dans la zone de texte en incluant les tirets.
6. Appuyez sur **Utiliser ce code** pour terminer l'activation.

Activation avec un compte Avast

1. Appuyez sur l'icône *Avast Mobile Security* sur votre appareil pour ouvrir l'application.
2. Appuyez sur **Menu** ▸ **Supprimer les publicités**.
3. Appuyez sur les **trois points** en haut à droite, puis sur **Déjà acheté**.
4. Sélectionnez **Restaurer depuis le compte Avast**.
5. Sélectionnez **Adresse email**.
6. Saisissez les informations d'identification de votre compte Avast.
7. Appuyez sur **Vous connecter à votre compte Avast**.

Appareils iOS

1. Appuyez sur l'icône *Avast Security & Privacy* sur votre appareil pour ouvrir l'application.
2. Appuyez sur Mettre à niveau.
3. Appuyez sur **Déjà acheté**.
4. Sélectionnez **Entrer le code d'abonnement Avast**.
5. Saisissez ou collez votre code d'activation dans la zone de texte en incluant les tirets.
6. Appuyez ensuite sur **OK** pour terminer l'activation.

Configuration des paramètres et composants

Small Office Protection propose de nombreux composants, aussi bien pour les postes de travail que pour les appareils mobiles.

Composants par système d'exploitation

Composant	Postes de travail Windows	MacOS X	Android	iOS
Agent des fichiers	X	X		
Agent Web	X	X	X	
Agent email	X	X		
Agent actions suspectes	X			
Agent anti-ransomwares	X	X		
Agent contre l'accès à distance	X			
Inspecteur Wi-Fi	X	X		
Real Site	X			
Pare-feu	X			
Sandbox	X			
Anti-spam				
Exchange				
Sharepoint				
Agent webcam	X			
Agent de données sensibles	X			
VPN SecureLine				
Broyeur de fichiers	X			
Mots de passe	X			
Agent mots de passe	X			
Mise à jour de logiciels	X			
Nettoyage du navigateur	X			
Mode Ne pas déranger	X			
Disque de secours	X			

Composant	Postes de travail Windows	MacOS X	Android	iOS
Scanner de fichiers			X	
Coffre-fort de photos			X	X
Identity Protection				X
Verrou d'applications			X	
Antivol			X	
Piège photo			X	
Dernier emplacement connu			X	
Sécurité SIM			X	
Blocage d'appels			X	
Mode économie d'énergie			X	
Augmentation de la RAM			X	
Nettoyage des données inutiles			X	
Test de vitesse de connexion Wi-Fi			X	
Sécurité du réseau Wi-Fi			X	X
Statistiques d'applications			X	
Application autonome VPN			X	X

Activation et désactivation de composants

La plupart des agents et des outils disponibles dans Small Office Protection peuvent être activés ou désactivés sur l'appareil. Cela est particulièrement utile lorsque vous tentez d'installer seulement quelques composants sur un serveur ou que vous souhaitez vous limiter au minimum le nombre d'outils. Toutefois, certains outils ne peuvent être installés ou désinstallés qu'en intégralité. Tel est le cas de Sandbox et Disque de secours.

1. Ouvrez l'interface utilisateur du client Small Office Protection.
2. Cliquez sur l'onglet correspondant au composant à activer ou désactiver :

- **Protection :** Agent des fichiers, Agent Web, Agent email, Agent actions suspectes, Sandbox, Inspecteur Wi-Fi, Real Site, Pare-feu.
- **Confidentialité :** Passwords, Anti-spam, Broyeur de fichiers, Agent webcam.
- **Performances :** Mise à jour de logiciels

3. Cliquez sur le bouton correspondant au composant.
4. En regard du composant à modifier, procédez de l'une des façons suivantes :
   - Pour activer le composant, mettez le curseur sur la position **Activé**.
   - Pour désactiver le composant, mettez le curseur sur la position **Désactivé**.
5. Si nécessaire, confirmez votre choix.

Installation et désinstallation de composants

La plupart des fonctionnalités de protection active sont installées avec Small Office Protection, mais ces composants peuvent être désinstallés et réinstallés via le menu Dépannage, si nécessaire. Les composants de protection MacOS X ne peuvent être ni installés ni désinstallés, mais ils peuvent être désactivés.

1. Ouvrez l'interface utilisateur du client Small Office Protection.
2. Accédez à **Menu ▸ Paramètres ▸ Général ▸ Dépannage**.
3. Cliquez sur **Ajouter/Modifier des composants**.
4. En regard des composants que vous souhaitez modifier, procédez de l'une des façons suivantes :
   - Si le composant n'est pas encore installé, cochez la case correspondante.
   - Si le composant est déjà installé, décochez la case correspondante.
5. Cliquez sur **Modifier** pour confirmer une fois que vous avez terminé vos modifications.

Pour plus d'informations sur la configuration des différents composants disponibles dans les paramètres de Small Office Protection, consultez Configuration des paramètres dans Small Office Protection (uniquement en anglais).

Configuration d'exclusions

Caractères génériques

La plupart des agents et des autres composants fournis avec Small Office Protection, ainsi que l'antivirus principal lui-même, vous permettent de configurer des exclusions ou de bloquer des chemins d'accès spécifiques. Les caractères génériques sont utiles lorsque vous ne connaissez pas le chemin d'accès exact de fichiers ou le nom des fichiers que vous voulez inclure ou exclure, ou lorsque vous voulez indiquer plusieurs fichiers dans un même chemin d'accès. Certains chemins d'accès n'autorisent pas l'utilisation de caractères génériques.

Caractère	Signification
?	Remplace un seul caractère **Par exemple :** `ab?.html` établit une correspondance avec les fichiers `abc.html`, `abd.html`, `abe.html`, etc., mais **pas** avec le fichier `abc.htm`.
*****	Remplace une absence de caractère ou plusieurs caractères **Par exemple :** `*mtl` établit une correspondance avec les fichiers `abc.html` et `d.html`. `*txt` établit une correspondance avec les fichiers `abc.txt`, `x.txt` et `xyztxt`.

Exclusions

Vous pouvez configurer des exclusions qui se propageront à tous les différents agents et composants de Small Office Protection sous l'onglet *Exceptions* de la page **Paramètres ▸ Général**.

Ajout d'exceptions

1. Ouvrez l'interface utilisateur du client Small Office Protection.
2. Cliquez sur le **Menu** en haut à droite, puis sur **Paramètres**.
3. Dans la section **Général ▸ Exceptions**, cliquez sur **Ajouter une exception**, puis procédez de l'une des façons suivantes :
    - Saisissez ou parcourez le chemin d'accès de fichier que vous souhaitez exclure.

- Saisissez ou parcourez le chemin d'accès de dossier que vous souhaitez exclure.
- Saisissez l'URL que vous souhaitez exclure.

4. Cliquez sur **Ajouter une exception** lorsque vous avez terminé.

Configuration des mises à jour automatiques

Vous pouvez mettre automatiquement à jour les définitions virales et la version du programme Small Office Protection sur votre ou vos appareils lorsque de nouvelles mises à jour sont disponibles. Vous pouvez également configurer une mise à jour manuelle sur le ou les appareils. Pour plus d'informations, consultez Mise à jour de Small Office Protection (uniquement en anglais).

Configuration des mises à jour automatiques

1. Cliquez sur **Menu** dans le coin supérieur droit de l'interface utilisateur.
2. Cliquez sur **Paramètres**.
3. Dans la section *Général*, accédez à l'onglet **Mettre à jour**.
4. En regard des deux boutons **Rechercher des mises à jour**, cliquez sur **Plus d'options**.
5. Sélectionnez **Mise à jour automatique**.

Création et configuration d'analyses

Postes de travail Windows

Vous pouvez configurer les types de fichiers et les programmes qui seront analysés par Small Office Protection dans les paramètres Analyses antivirus. Par conséquent, les principaux détails de l'analyse ne sont pas configurés dans les paramètres d'analyse, tandis que les exclusions sont configurées dans la section Général.

Types d'analyses

- **Analyse antivirus complète** : exécute une analyse en profondeur de votre système, vérifiant tous les disques durs, rootkits et programmes à démarrage automatique.
- **Analyse ciblée** : analyse uniquement les dossiers sélectionnés au lancement de l'analyse.

- **Scan lancé depuis Explorer** : effectue une analyse des dossiers ou des lecteurs que vous spécifiez, mais n'est accessible qu'à partir du menu contextuel Windows qui s'affiche lorsque vous effectuez un clic droit sur un fichier, un dossier ou un lecteur.
- **Scan au démarrage (MS Windows uniquement)** : exécute une analyse au démarrage de l'appareil.

Vous pouvez accéder aux paramètres des différents types d'analyses en cliquant sur Menu ▸ Paramètres, puis en accédant à Protection ▸ Analyses antivirus.

Personnalisation des analyses antivirus complètes

Sensibilité

Vous pouvez déterminer la sensibilité de l'analyse en ajustant ses paramètres. Plus la sensibilité est élevée, plus le niveau de protection augmente, et avec lui le potentiel de détection d'un malware faux positif. En réduisant la sensibilité, vous diminuez le risque de détection de faux positifs, mais aussi l'efficacité de l'analyse. La sensibilité de l'analyse (moyenne, élevée ou faible) peut être ajustée en faisant glisser le curseur.

Rechercher des PPI : permet à Avast de rechercher des programmes téléchargés discrètement avec d'autres programmes pouvant effectuer des activités indésirables.

Suivre les liens durant l'analyse : permet à Avast d'analyser les autres fichiers utilisés par les fichiers en cours d'analyse pour détecter tout contenu potentiellement dangereux.

Tester les fichiers en entier (très lent pour les fichiers de grande taille) : permet à Avast d'analyser les fichiers en entier et pas seulement les parties généralement affectées par du code malveillant.

Priorité de l'analyse : détermine le nombre de ressources que peut utiliser Avast pendant l'analyse. Plus la priorité est élevée, plus l'analyse est rapide, mais cela peut ralentir les autres processus en cours d'exécution sur l'appareil.

Zones d'analyse

Sélectionnez ou cochez les cases situées en regard des zones répertoriées pour les inclure dans votre analyse. Les principales zones proposées sont les suivantes :

- **Tous les disques durs** : permet à Avast d'analyser tous les disques durs de votre PC.

- **Lecteur système** : les options de cette section s'appliquent aux données stockées sur les supports physiques que sont notamment les disques durs et les clés USB.

Les options d'analyse suivantes s'appliquent alors à la zone spécifiée ci-dessus.

Tous les médias amovibles : permet à Avast d'analyser les applications qui se lancent automatiquement lorsque vous insérez une clé USB ou tout autre dispositif amovible dans votre PC.

Rootkits : permet à Avast de rechercher les menaces cachées dans le système.

UEFI BIOS : permet à Avast d'analyser les principales interfaces de microprogramme pendant le démarrage.

Lecteurs CD-ROM et DVD : permet à Avast de rechercher du contenu malveillant sur les lecteurs de CD et de DVD.

Modules chargés en mémoire vive : permet à Avast d'analyser les applications et processus qui se lancent après le démarrage du système ou qui s'exécutent en arrière-plan.

Conteneurs et archives

Dans la section Conteneurs et archives, vous pouvez indiquer les types de fichiers compressés qu'Avast doit décompresser pendant l'analyse.

- **Analyser uniquement les programmes d'installation courants** : analyse le contenu des fichiers exécutables utilisés pendant l'installation d'applications.
- **Analyser toutes les archives** : analyse le contenu de tous les fichiers d'archive, ce qui peut considérablement ralentir l'analyse.
- **Ne pas analyser les archives** : désactive l'analyse des fichiers d'archive réalisée par Avast.

Types de fichiers

Indiquez les types de fichiers prioritaires lors de la recherche de malwares sur votre PC :

- **Types basés sur le contenu (lent)** : analyse les fichiers qui sont généralement plus vulnérables aux attaques de malwares.
- **Types basés sur les extensions (rapide)** : analyse seulement les fichiers dont l'extension présente des risques comme .exe, .com, .bat.

- **Analyser tous les fichiers (très lent)** : analyse tous les fichiers de votre PC à la recherche de malwares.

Exécuter des actions automatiques durant cette analyse : activez cette option et définissez l'action automatique effectuée lorsqu'un fichier infecté est trouvé :

- **Corriger automatiquement** : permet à Avast de réparer le fichier infecté. Si la réparation n'est pas possible, le fichier est déplacé vers la Zone de quarantaine, et si cette opération échoue, le fichier est supprimé.
- **Déplacer le fichier vers la zone de quarantaine** : le fichier infecté n'est pas réparé automatiquement, mais déplacé vers la zone de quarantaine.
- **Supprimer le fichier :** Avast ne tente pas de réparer le fichier infecté ou de le déplacer vers la Zone de quarantaine ; le fichier est supprimé automatiquement.

Éteindre l'ordinateur une fois l'analyse terminée : permet à Avast d'éteindre votre ordinateur une fois que l'analyse est terminée.

Générer le fichier de rapport : permet à Avast de créer et stocker automatiquement un fichier de rapport. L'emplacement du fichier de rapport est indiqué en dessous de cette option.

Exceptions

Bien qu'il soit déconseillé d'exclure des fichiers ou des dossiers d'une analyse, vous pouvez définir des exceptions pour exclure provisoirement certains fichiers ou dossiers d'une analyse à des fins de résolution de problèmes. Au bas de la page des paramètres de l'analyse, cliquez sur **Voir les exceptions**. À ce stade, vous pouvez suivre les étapes décrites dans **Configuration d'exclusions**.

Personnalisation des analyses ciblées

Sensibilité

Vous pouvez déterminer la sensibilité de l'analyse en ajustant ses paramètres. Plus la sensibilité est élevée, plus le niveau de protection augmente, et avec lui le potentiel de détection d'un malware faux positif. En réduisant la sensibilité, vous diminuez le risque de détection de faux positifs, mais aussi l'efficacité de l'analyse. La sensibilité de l'analyse (moyenne, élevée ou faible) peut être ajustée en faisant glisser le curseur.

Rechercher des PPI : permet à Avast de rechercher des programmes téléchargés discrètement avec d'autres programmes pouvant effectuer des activités indésirables.

Suivre les liens durant l'analyse : permet à Avast d'analyser les autres fichiers utilisés par les fichiers en cours d'analyse pour détecter tout contenu potentiellement dangereux.

Tester les fichiers en entier (très lent pour les fichiers de grande taille) : permet à Avast d'analyser les fichiers en entier et pas seulement les parties généralement affectées par du code malveillant.

Priorité de l'analyse : détermine le nombre de ressources que peut utiliser Avast pendant l'analyse. Plus la priorité est élevée, plus l'analyse est rapide, mais cela peut ralentir les autres processus en cours d'exécution sur l'appareil.

Fichiers compressés et archives

Dans la section Conteneurs et archives, vous pouvez indiquer les types de fichiers compressés qu'Avast doit décompresser pendant l'analyse.

- **Analyser uniquement les programmes d'installation courants** : analyse le contenu des fichiers exécutables utilisés pendant l'installation d'applications.
- **Analyser toutes les archives** : analyse le contenu de tous les fichiers d'archive, ce qui peut considérablement ralentir l'analyse.
- **Ne pas analyser les archives** : désactive l'analyse des fichiers d'archive réalisée par Avast.

Types de fichiers

Indiquez les types de fichiers prioritaires lors de la recherche de malwares sur votre PC :

- **Types basés sur le contenu (lent)** : analyse les fichiers qui sont généralement plus vulnérables aux attaques de malwares.
- **Types basés sur les extensions (rapide)** : analyse seulement les fichiers dont l'extension présente des risques comme .exe, .com, .bat.
- **Analyser tous les fichiers (très lent)** : analyse tous les fichiers de votre PC à la recherche de malwares.

Exécuter des actions automatiques durant cette analyse : activez cette option et définissez l'action automatique effectuée lorsqu'un fichier infecté est trouvé :

- **Corriger automatiquement** : permet à Avast de réparer le fichier infecté. Si la réparation n'est pas possible, le fichier est déplacé vers la Zone de quarantaine, et si cette opération échoue, le fichier est supprimé.

- **Déplacer le fichier vers la zone de quarantaine** : le fichier infecté n'est pas réparé automatiquement, mais déplacé vers la zone de quarantaine.
- **Supprimer le fichier :** Avast ne tente pas de réparer le fichier infecté ou de le déplacer vers la Zone de quarantaine ; le fichier est supprimé automatiquement.

Éteindre l'ordinateur une fois l'analyse terminée : permet à Avast d'éteindre votre ordinateur une fois que l'analyse est terminée.

Générer le fichier de rapport : permet à Avast de créer et stocker automatiquement un fichier de rapport. L'emplacement du fichier de rapport est indiqué en dessous de cette option.

Personnalisation des analyses de l'explorateur

Sensibilité

Vous pouvez déterminer la sensibilité de l'analyse en ajustant ses paramètres. Plus la sensibilité est élevée, plus le niveau de protection augmente, et avec lui le potentiel de détection d'un malware faux positif. En réduisant la sensibilité, vous diminuez le risque de détection de faux positifs, mais aussi l'efficacité de l'analyse. La sensibilité de l'analyse (moyenne, élevée ou faible) peut être ajustée en faisant glisser le curseur.

Rechercher des PPI : permet à Avast de rechercher des programmes téléchargés discrètement avec d'autres programmes pouvant effectuer des activités indésirables.

Suivre les liens durant l'analyse : permet à Avast d'analyser les autres fichiers utilisés par les fichiers en cours d'analyse pour détecter tout contenu potentiellement dangereux.

Tester les fichiers en entier (très lent pour les fichiers de grande taille) : permet à Avast d'analyser les fichiers en entier et pas seulement les parties généralement affectées par du code malveillant.

Priorité de l'analyse : détermine le nombre de ressources que peut utiliser Avast pendant l'analyse. Plus la priorité est élevée, plus l'analyse est rapide, mais cela peut ralentir les autres processus en cours d'exécution sur l'appareil.

Conteneurs et archives

Dans la section Conteneurs et archives, vous pouvez indiquer les types de fichiers compressés qu'Avast doit décompresser pendant l'analyse.

- **Analyser uniquement les programmes d'installation courants** : analyse le contenu des fichiers exécutables utilisés pendant l'installation d'applications.

- **Analyser toutes les archives** : analyse le contenu de tous les fichiers d'archive, ce qui peut considérablement ralentir l'analyse.
- **Ne pas analyser les archives** : désactive l'analyse des fichiers d'archive réalisée par Avast.

Types de fichiers

Indiquez les types de fichiers prioritaires lors de la recherche de malwares sur votre PC :

- **Types basés sur le contenu (lent)** : analyse les fichiers qui sont généralement plus vulnérables aux attaques de malwares.
- **Types basés sur les extensions (rapide)** : analyse seulement les fichiers dont l'extension présente des risques comme .exe, .com, .bat.
- **Analyser tous les fichiers (très lent)** : analyse tous les fichiers de votre PC à la recherche de malwares.

Exécuter des actions automatiques durant cette analyse : activez cette option et définissez l'action automatique effectuée lorsqu'un fichier infecté est trouvé :

- **Corriger automatiquement** : permet à Avast de réparer le fichier infecté. Si la réparation n'est pas possible, le fichier est déplacé vers la Zone de quarantaine, et si cette opération échoue, le fichier est supprimé.
- **Déplacer le fichier vers la zone de quarantaine** : le fichier infecté n'est pas réparé automatiquement, mais déplacé vers la zone de quarantaine.
- **Supprimer le fichier :** Avast ne tente pas de réparer le fichier infecté ou de le déplacer vers la Zone de quarantaine ; le fichier est supprimé automatiquement.

Éteindre l'ordinateur une fois l'analyse terminée : permet à Avast d'éteindre votre ordinateur une fois que l'analyse est terminée.

Générer le fichier de rapport : permet à Avast de créer et stocker automatiquement un fichier de rapport. L'emplacement du fichier de rapport est indiqué en dessous de cette option.

Personnalisation des analyses au démarrage

Sensibilité

Vous pouvez déterminer la sensibilité de l'analyse en ajustant ses paramètres. Plus la sensibilité est élevée, plus le niveau de protection augmente, et avec lui le potentiel de

détection d'un malware faux positif. En réduisant la sensibilité, vous diminuez le risque de détection de faux positifs, mais aussi l'efficacité de l'analyse. La sensibilité de l'analyse (moyenne, élevée ou faible) peut être ajustée en faisant glisser le curseur.

Rechercher des PPI : permet à Avast de rechercher des programmes téléchargés discrètement avec d'autres programmes pouvant effectuer des activités indésirables.

Décompresser les fichiers archive : permet à Avast d'extraire (« décompresser ») les fichiers et les dossiers des archives à des fins d'analyse.

Zones d'analyse

Sélectionnez ou cochez les cases situées en regard des zones répertoriées pour les inclure dans votre analyse. Les principales zones proposées sont les suivantes :

- **Tous les disques durs** : permet à Avast d'analyser tous les disques durs de votre PC.
- **Lecteur système** : les options de cette section s'appliquent aux données stockées sur les supports physiques que sont notamment les disques durs et les clés USB.

Les options d'analyse suivantes s'appliquent alors à la zone spécifiée ci-dessus.

Programmes démarrant automatiquement : permet à Avast de vérifier tous les programmes à démarrage automatique.

Exécuter des actions automatiques durant cette analyse : activez cette option et définissez l'action automatique effectuée lorsqu'un fichier infecté est trouvé :

- **Corriger automatiquement** : permet à Avast de réparer le fichier infecté. Si la réparation n'est pas possible, le fichier est déplacé vers la Zone de quarantaine, et si cette opération échoue, le fichier est supprimé.
- **Déplacer le fichier vers la zone de quarantaine** : le fichier infecté n'est pas réparé automatiquement, mais déplacé vers la zone de quarantaine.
- **Supprimer le fichier :** Avast ne tente pas de réparer le fichier infecté ou de le déplacer vers la Zone de quarantaine ; le fichier est supprimé automatiquement.

Appareils Android

L'option Analyser vous permet d'analyser toutes les applications installées sur votre appareil et vous informe des risques de sécurité que représentent les modifications apportées aux paramètres Android par défaut. Les définitions de virus utilisées par l'analyse sont automatiquement mises à jour.

1. Appuyez sur l'icône *Avast Mobile Security* sur votre appareil pour ouvrir l'application.
2. Appuyez sur **Analyser** sur l'écran principal.

Une fois l'analyse terminée, l'application indique que tout est normal ou liste les problèmes rencontrés et propose des solutions pour les résoudre. Vous pouvez appuyer sur **Résoudre** ou sur **Activer** si ces actions sont disponibles.

Analyse de la mémoire interne

Par défaut, l'analyse de la mémoire interne est désactivée. Si vous voulez que le stockage interne de votre appareil soit inclus dans les analyses, vous pouvez activer cette option dans les paramètres.

1. Appuyez sur l'icône *Avast Mobile Security* sur votre appareil pour ouvrir l'application.
2. Appuyez sur **Menu** ▸ **Paramètres**.
3. Appuyez sur **Protection**.
4. Cliquez sur le curseur pour activer l'*analyse du stockage interne*.

Appareils iOS

L'option Analyser vous permet d'analyser toutes les applications installées sur votre appareil et vous informe des risques de sécurité que représentent les modifications apportées aux paramètres iOS par défaut. Les définitions de virus utilisées par l'analyse sont automatiquement mises à jour.

1. Appuyez sur l'icône *Avast Security & Privacy* sur votre appareil pour ouvrir l'application.
2. Appuyez sur **Analyser** sur l'écran principal.

Une fois l'analyse terminée, l'application indique que tout est normal ou liste les problèmes rencontrés et propose des solutions pour les résoudre. Vous pouvez appuyer sur **Résoudre** ou sur **Activer** si ces actions sont disponibles.

Small Office Protection propose bien plus de fonctionnalités et d'options. Pour plus d'informations, consultez notre base de connaissances à l'adresse https://businesshelp.avast.com/.