

Démarrage rapide : Consoles de gestion AVG Business

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

<https://businesshelp.avast.com/>

Sommaire

Démarrage rapide : Consoles de gestion AVG Business	1
Sommaire.....	2
Présentation des consoles de gestion AVG Business	5
Configuration de la console de gestion	6
Vérifier la configuration système requise pour la console	6
Console cloud AVG Business.....	6
Navigateurs (dernières versions recommandées)	6
Console sur site AVG Business	6
Windows :.....	6
Terminaux AVG Business Antivirus.....	6
Gestion des correctifs AVG Business.....	7
Vérifier la configuration requise du pare-feu pour la console	7
Ports.....	7
URL	7
Configuration de la console	8
Console cloud	8
Console sur site	8
Activation de licences dans la console de gestion	8
Activation de licences supplémentaires	8
Affectation de licences à des appareils	9
Ajout d'appareils via le fichier d'installation ou un lien de partage.....	10
Console cloud et console sur site.....	10
Téléchargement du programme d'installation	10
Console sur site uniquement	11
Envoi du lien de téléchargement par e-mail.....	11

Installation sur le client local	12
Ajout d'appareils via le déploiement à distance	12
Prérequis pour le déploiement à distance	12
Configurez ce qui suit sur chaque appareil :	12
Détails du déploiement à distance	14
Déploiement de programmes d'installation à distance	15
Configuration de politique et composants	17
Composants Antivirus par licence de produit	17
Activation et désactivation de composants	18
Installation et désinstallation de composants	18
Configuration d'exclusions	19
Caractères génériques	19
Exclusions	19
Configuration des mises à jour automatiques	20
Configuration des mises à jour	20
Création et configuration d'analyses	20
Types d'analyses	20
Console cloud	21
Création d'analyses planifiées	21
Création d'analyses uniques	21
Console sur site	22
Configuration de l'analyse	22
Configuration des analyses au démarrage	22
Configuration d'analyses personnalisées	23
Configuration des emplacements	24
Onglet Types de fichiers	24
Onglet Sensibilité	24
Onglet Performances	25

Onglet Actions	25
Onglet Conteneurs	25

Présentation des consoles de gestion AVG Business

Grâce aux consoles de gestion AVG Business, il n'a jamais été aussi simple d'ajouter une protection critique à chaque PC et serveur. La gestion flexible permet de protéger les activités de la manière la plus pratique qui soit. Les consoles de gestion offrent les avantages suivants :

- Contrôle complet du comportement de l'antivirus sur les terminaux
- Gestion centralisée des divers appareils, accessible de n'importe où dans le cloud, ou localement à l'aide de la console sur site
- Vue d'ensemble complète de l'état actuel de l'ensemble de l'environnement avec alertes immédiates
- Mises à jour automatiques et transparentes

Les consoles de gestion AVG Business s'intègrent de manière transparente avec AVG Business Antivirus pour :

- Tirer parti de la virtualisation pour protéger les informations confidentielles
- Protéger plusieurs plateformes : PC et serveurs
- Effectuer une mise à jour automatique ou manuelle vers la dernière version
- Ajouter une protection de pare-feu supplémentaire pour les terminaux distants
- Doter vos serveurs d'une protection complète
- Sécuriser votre client de messagerie

Lorsque vous installez AVG Business Antivirus sur des appareils via les consoles de gestion AVG Business, vous pouvez contrôler AVG Business Antivirus à distance sur ces appareils. Vous pouvez modifier et appliquer les paramètres sur chaque appareil séparément sans avoir à accéder à chaque appareil ou à les rappeler sur le terrain.

Configuration de la console de gestion

Vérifier la configuration système requise pour la console

Console cloud AVG Business

Navigateurs (dernières versions recommandées)

- Google Chrome
- Firefox
- Safari
- Microsoft Edge
- Internet Explorer

Console sur site AVG Business

Windows :

- 7 SP1 ou version supérieure, 8.x, 10
- Server 2008 R2 SP1, 2012 et 2012 R2, 2016, 2019 toute édition
- Small Business Server 2008, 2011 (64 bits uniquement)
- Exchange Server 2003 x86 (jusqu'à la version 18.8), 2007, 2010, 2013, 2016, 2019 (64 bits uniquement)
- SharePoint Server 2003, 2007, 2010, 2012, 2016, 2019 (64 bits uniquement)

Terminaux AVG Business Antivirus

Windows :

- 7 SP1 ou version supérieure, 8.x à l'exception de RT et Starter Edition, 10 à l'exception de Mobile et IoT Core Edition
- Server 2008 R2, 2012 R2, 2016, 2019, toute édition dotée du dernier Service Pack à l'exclusion de Server Core
- Microsoft Exchange Server 2010 SP2, 2013, 2016, 2019

- Microsoft SharePoint Services 3.0 et SharePoint Server 2010 et versions supérieures

Gestion des correctifs AVG Business

Windows uniquement :

- 7 SP1 ou version supérieure, 8.x, 10
- Server 2008 R2 avec le dernier Service Pack à l'exclusion de Server Core, 2012, 2016, 2019
- Exchange Server 2010 SP2, 2013, 2016

Vérifier la configuration requise du pare-feu pour la console

Pour le fonctionnement global et pour permettre aux clients AVG Business Antivirus et/ou aux consoles de gestion 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 :

- 80 – Vérification des vulnérabilités Internet et mises à jour des fonctionnalités
- 443 – Négociation des clés de chiffrement FFL
- 8080, 8090 – Communication entre la console et les clients au sein du réseau local (uniquement pour la console sur site)
- 4158 – Miroir, pour les mises à jour locales au sein du réseau local
- 7074 – Déploiement à distance au sein du réseau local

URL

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

Configuration de la console

Console cloud

1. Accédez à <https://console.avg.com/>.
2. Cliquez sur **Enregistrer** et complétez toutes les informations nécessaires pour configurer l'accès.

Console sur site

1. Accédez à <https://www.avg.com/en-us/installation-files-business>.
2. Sous l'onglet Business, cliquez sur **Télécharger** en regard d'AVG On-Premise Management Console.

Pour la console sur site, suivez le processus d'installation correspondant à votre système d'exploitation tel que détaillé dans [Gestion de la console sur site](#) (uniquement en anglais).

Activation de licences dans la console de gestion

Vous avez besoin d'un code d'activation pour confirmer votre achat. Il contient des informations sur l'édition que vous avez achetée. Votre code correspond à la licence permettant d'activer votre logiciel.

1. Lorsque vous exécutez la console pour la première fois, l'écran vous invite à saisir votre code de licence.
2. Saisissez votre code de licence.
3. Cliquez sur **Activer le code de licence**.

Activation de licences supplémentaires

1. Accédez à la page *Abonnements*.
2. Procédez de l'une des façons suivantes :
 - Si vous avez un code de licence, cliquez sur **Avez-vous un code d'activation ?**, saisissez le code, puis cliquez sur **Activer**
 - En regard de l'abonnement que vous souhaitez acheter, cliquez sur **Acheter**, puis finalisez la transaction.

Affectation de licences à des appareils

Vous ne pouvez effectuer cette action qu'à partir du moment où vous avez ajouté un appareil à votre réseau.

Cette procédure nécessite le redémarrage de l'appareil.

1. Dans la page *Appareils*, procédez de l'une des façons suivantes :
 - Pour inclure tous les appareils d'un groupe, cliquez sur le bouton **Plus** en regard du nom du groupe. Cliquez ensuite sur **Modifier le groupe**.
 - Pour inclure plusieurs appareils, cochez les cases correspondant à ces appareils. Cliquez ensuite sur **Actions** ▶ **Changer d'abonnement**.
 - Pour un seul appareil, cliquez sur le bouton **Plus** en regard d'un appareil, puis sur **Changer d'abonnement**.
2. Sélectionnez la licence que vous souhaitez utiliser dans le ou les menus déroulants.
3. Cliquez sur **Appliquer** pour la licence choisie ou sur **Enregistrer le groupe** si vous changez d'abonnement pour tout un groupe d'appareils.

Ajout d'appareils via le fichier d'installation ou un lien de partage

Console cloud et console sur site

Téléchargement du programme d'installation

1. Sélectionnez le type de programme d'installation dont vous avez besoin :
 - Windows .exe (pour les postes de travail et les serveurs)
 - Windows .msi (pour un déploiement utilisant un objet de stratégie de groupe, ou GPO)
2. Sélectionnez les produits de l'abonnement.
3. Cliquez sur **Paramètres avancés** pour afficher les options suivantes.
4. Choisissez le groupe et la politique que doit utiliser l'appareil.
 - o **Si vous le souhaitez, vous pouvez activer vos appareils et sélectionner l'abonnement à utiliser après l'installation en cochant la case correspondante.**
5. Indiquez si vous souhaitez que les produits antivirus concurrents soient supprimés automatiquement de l'appareil.
 - o **L'option de suppression des produits antivirus concurrents est cochée par défaut. Nous vous recommandons de laisser cette option cochée lors de l'installation du service Antivirus.**
6. Sélectionnez la taille de l'installation (légère ou complète).
 - o **Si vous optez pour une installation légère, les autres services sont téléchargés au moment de l'installation de l'agent Antivirus. Si vous prévoyez d'installer Antivirus sur plusieurs appareils à la fois, cette option est déconseillée dans la mesure où chaque machine va contacter individuellement les serveurs AVG pour télécharger les autres services.**
7. Vérifiez le cas échéant que vous avez défini le bon serveur proxy dans la politique que vous appliquez à l'appareil.

8. Cliquez sur **Télécharger maintenant** et indiquez à quel emplacement enregistrer le package d'installation (par exemple, sur une clé USB ou un lecteur réseau).

Vous pouvez également envoyer un lien de téléchargement de cette page en cliquant sur **Partager le lien de téléchargement** en dessous du bouton *Télécharger maintenant*. Vous pouvez ensuite copier et envoyer l'URL de téléchargement privée aux destinataires de votre choix.

Console sur site uniquement

Envoi du lien de téléchargement par e-mail

Avant de pouvoir envoyer des liens de téléchargement à partir de la console sur site, vous devez définir votre serveur SMTP.

1. Saisissez les adresses e-mail des utilisateurs cibles dans la zone *Envoyer à* en les séparant par des virgules.
2. Si vous le souhaitez, modifiez la ligne *Objet* de l'e-mail à envoyer.
3. Pour configurer le message à envoyer dans l'e-mail, cochez *Ajoutez votre message personnalisé*, puis saisissez un message dans l'espace prévu à cet effet.
4. Sélectionnez les produits de l'abonnement.
5. Cliquez sur **Paramètres avancés** pour afficher les options suivantes.
6. Choisissez le groupe et la politique que doit utiliser l'appareil.
 - o **Si vous le souhaitez, vous pouvez activer vos appareils et sélectionner l'abonnement à utiliser après l'installation en cochant la case correspondante.**
7. Indiquez si vous souhaitez que les produits antivirus concurrents soient supprimés automatiquement de l'appareil.
 - o **L'option de suppression des produits antivirus concurrents est cochée par défaut. Nous vous recommandons de laisser cette option cochée lors de l'installation du service Antivirus.**
8. Sélectionnez la taille de l'installation (légère ou complète).
 - o **Si vous optez pour une installation légère, les autres services sont téléchargés au moment de l'installation de l'agent Antivirus. Si vous prévoyez d'installer Antivirus sur plusieurs appareils à la fois,**

cette option est déconseillée dans la mesure où chaque machine va contacter individuellement les serveurs AVG pour télécharger les autres services.

9. Vérifiez le cas échéant que vous avez défini le bon serveur proxy dans le modèle de paramètres que vous appliquez à l'appareil.
10. Cliquez sur **Envoyer**.

Installation sur le client local

Après vous être procuré un fichier d'installation ou un lien de téléchargement d'AVG Business Management Console, vous devez installer AVG Business Antivirus sur le ou les appareils finaux.

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. Patientez le temps qu'AVG Business Antivirus s'installe sur l'appareil.
5. Lorsque vous y êtes invité, redémarrez l'appareil.
6. L'appareil doit maintenant être visible dans la console.

Ajout d'appareils via le déploiement à distance

Prérequis pour le déploiement à distance

- Informations d'identification administrateur pour l'ordinateur ou le domaine Windows. Si vous utilisez des informations d'identification de domaine, incluez le nom de domaine : (par ex., VOTRE_DOMAINE\nomutilisateur).
- Informations réseau concernant les appareils sur lesquels vous effectuez le déploiement. Ces informations sont nécessaires pour localiser les appareils sur votre réseau.
- Préparez les ordinateurs à l'installation du client. Désinstallez les éventuels logiciels antivirus tiers si vous installez Avast Business Antivirus.

Configurez ce qui suit sur chaque appareil :

Windows Vista/7/8.x/10

Présentation des 12
consoles de
gestion AVG
Business

Activer le trafic WMI

- Exécutez la commande NETSH : netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes

Activer le partage ADMIN

- Ouvrez l'Éditeur du Registre.
- Accédez à : HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Créez un DWORD « LocalAccountTokenFilterPolicy » et attribuez-lui la valeur 1.

Activer le partage d'imprimantes et de fichiers

- Dans le Panneau de configuration ▶ Réseau et Internet ▶ Centre Réseau et partage
- Cliquez sur Modifier les paramètres de partage avancés, puis sur Activer le partage de fichiers et d'imprimantes.

Pare-feu

1. Ouvrez les paramètres du Pare-feu.
2. Accédez à Paramètres ▶ Profils ▶ Directement connecté à Internet ▶ Applications ▶ Generic Host Process - et Generic Host Process 2
3. Autoriser :
 - Données de serveur DCOM
 - Serveur Microsoft DCOM
 - Données de client DCOM (doit être autorisé par défaut)
 - Client Microsoft DCOM (doit être autorisé par défaut)

Activer DCOM

1. Exécutez dcomcnfg.
2. Accédez à Services de composants ▶ Ordinateurs.
3. Cliquez avec le bouton droit sur Poste de travail ▶ Propriétés.
4. Cliquez sur l'onglet Propriétés par défaut.
5. Cliquez sur la case à cocher *Activer Distributed COM sur cet ordinateur.*

Activer RPC

1. Exécutez services.msc.

2. Accédez à « Appel de procédure distante (RPC) » et activez-le.

Détails du déploiement à distance

L'option Déploiement à distance n'est disponible qu'après l'ajout d'au moins un appareil au réseau avec une autre méthode d'installation. Sachant que vous devez également désigner un Master Agent, le premier appareil que vous ajoutez au réseau doit être de préférence celui que vous prévoyez d'utiliser comme Master Agent. Vous trouverez ci-dessous un récapitulatif du processus de déploiement :

Détection d'appareils

Le processus de détection d'appareils utilise le protocole ARP (Address Resolution Protocol) pour envoyer une requête ping à toutes les adresses IP du sous-réseau afin d'obtenir leur adresse MAC. Ce processus peut prendre jusqu'à 15 minutes, voire plus, en fonction du réseau.

Si une réponse est reçue avec une adresse MAC, une recherche DNS inversée se produit pour obtenir le nom d'hôte pour l'IP. En cas de réception d'un nom d'hôte, un enregistrement d'appareil est créé et stocké dans une liste, qui est transmise au service web une fois la détection terminée.

Une fois l'authentification initiale terminée, le processus recherche régulièrement des appareils hôtes et compare le résultat à la liste déjà stockée. À partir de là, le processus ne fait qu'ajouter de nouveaux appareils hôtes et n'en supprime aucun.

Authentification

Pendant le déploiement à distance, une liste d'informations d'identification administrateur (par ex., VOTRE_DOMAINE\nom_utilisateur et mot de passe) est transmise au processus de déploiement à distance jusqu'à ce que l'une d'entre elles donne accès à l'ordinateur cible. Si aucune ne fonctionne, le processus s'arrête et renvoie un message d'erreur.

Le client attend que des modifications soient apportées aux appareils/tables de connexions pour voir si quelque chose est marqué pour le déploiement, en fonction de l'adresse MAC de l'ordinateur hôte.

Prérequis

Pour déployer automatiquement l'antivirus sur plusieurs appareils à distance, voici ce dont vous devez disposer :

- Console cloud ou Console sur site version 6.0 ou supérieure
- Antivirus version 18.6 ou supérieure

- Au moins un appareil installé et activé
- Un Master Agent opérationnel
- L'option Partage de fichiers et d'imprimantes pour réseaux Microsoft activée
- Un système d'exploitation Microsoft Windows pris en charge par Active Directory
- Des informations d'identification valides pour Active Directory avec des droits d'administrateur
- Tous les ports nécessaires ouverts (7074)

Déploiement de programmes d'installation à distance

Analyse du réseau

1. Cliquez sur **Commencer le processus de déploiement.**
 - Si vous ne disposez d'aucun Master Agent, cliquez sur **Ajouter le nouveau Master Agent**, puis suivez le processus pour définir un Master Agent.
 - Si vous disposez d'un ou plusieurs Master Agents, sélectionnez celui que vous souhaitez utiliser.
2. Dans la section Informations d'identification Active Directory, saisissez les informations suivantes :
 - Domaine
 - Nom de l'utilisateur
 - Mot de passe
3. Cliquez sur **Analyser votre réseau** et attendez que le processus de détection d'appareils aboutisse.

Déploiement réseau

1. Dans la section *Groupes Active Directory*, accédez à un réseau contenant des appareils non protégés, puis cochez les cases correspondant aux appareils sur lesquels vous souhaitez effectuer le déploiement.
2. Cliquez sur **Définir des paramètres d'installation.**
3. Dans la section *Sélectionner une licence*, choisissez un de vos abonnements Antivirus disponibles.
4. Dans la section *Déployer dans un groupe dans la console AVG Business*, procédez de l'une des façons suivantes :
 - Sélectionnez un groupe.

- Sélectionnez **Copier la structure du groupe Active Directory dans le groupe sélectionné** pour utiliser la structure du groupe existant d'Active Directory.
 - Sélectionnez une politique.
5. Indiquez si vous souhaitez que les programmes antivirus en conflit sur l'appareil soient supprimés automatiquement.
 6. Cliquez sur **Commencer le déploiement vers des appareils.**
 - o **Patiencez le temps que l'antivirus soit déployé sur les appareils. Vous pouvez accéder à d'autres pages pendant le processus et utiliser le bouton Déploiement à distance dans le menu de navigation pour revenir en arrière et suivre la progression de votre déploiement à distance.**
 7. Cliquez sur **Annuler le déploiement à distance.**

Configuration de politique et composants

Les politiques représentent le principal moyen de gérer vos appareils. Il s'agit de groupes de règles de sécurité pour plusieurs systèmes d'exploitation (Poste de travail Windows, Windows Server et MacOS X) qui déterminent le mode de fonctionnement d'AVG Business Antivirus sur les terminaux. Les modifications apportées à une politique sont appliquées aux appareils et groupes qui lui sont affectés.

Les consoles de gestion AVG Business intègrent un modèle par défaut qui est déjà défini avec la configuration suggérée. Vous pouvez appliquer ce modèle, créer le vôtre en dupliquant le modèle par défaut et en le personnalisant ou encore créer un modèle entièrement nouveau. Le modèle par défaut ne peut pas être supprimé tant qu'une autre politique n'a pas été créée.

Une même politique contient des paramètres pour les postes de travail Windows et les serveurs Windows. Vous n'avez donc pas besoin de créer de politiques distinctes pour chaque système d'exploitation. Vous pouvez ainsi configurer les paramètres d'un groupe d'appareils qui contient plusieurs types de systèmes d'exploitation à la fois. Vous pouvez créer des messages en cliquant sur **Ajouter une politique** dans la page *Politiques*. Vous pourrez ainsi nommer la politique avant de configurer les paramètres des divers composants.

Composants Antivirus par licence de produit

Composant	AVG File Server Business	AVG Email Server Business	Antivirus AVG Business	AVG Internet Security Business
Agent des fichiers	X	X	X	X
Agent Web			X	X
Agent email			X	X
Agent actions suspectes			X	X
Anti-spam			X	X
Pare-feu amélioré			X	X
Broyeur de fichiers			X	X
Exchange		X		X
Sharepoint	X	X	X	X

Activation et désactivation de composants

La quasi-totalité des agents et des outils disponibles dans AVG Business Antivirus peuvent être activés ou désactivés dans la politique. 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.

1. Dans la politique que vous configurez, sélectionnez l'onglet *Protection active*.
2. Sélectionnez l'onglet du système d'exploitation approprié (Poste de travail Windows, Windows Server)
3. En regard des composants 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**.

Installation et désinstallation de composants

La plupart des fonctionnalités de la protection active sont installées avec AVG Business Antivirus, mais ces composants peuvent être désinstallés et réinstallés via la politique, si nécessaire.

1. Dans la politique que vous configurez, sélectionnez l'onglet *Protection active*.
2. Sélectionnez l'onglet du système d'exploitation approprié (Poste de travail Windows, Windows Server).
3. En regard des composants à modifier, procédez de l'une des façons suivantes :
 - Si le composant n'est pas encore installé, cliquez sur **Installer le composant**. Cliquez ensuite sur **J'ai compris, installer le composant**.
 - Si le composant est déjà installé, cliquez sur le bouton **Plus** en regard du composant, puis cliquez sur **Désinstaller le composant**. Cliquez ensuite sur **J'ai compris, désinstaller le composant**.

Pour plus d'informations sur la configuration des différents composants disponibles dans les politiques des consoles de gestion AVG Business, consultez [Configuration des paramètres et des politiques dans les consoles de gestion AVG Business \(uniquement en anglais\)](#).

Configuration d'exclusions

Caractères génériques

La plupart des agents et des autres composants fournis avec AVG Business Antivirus, 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 : <code>ab?.html</code> établit une correspondance avec les fichiers <code>abc.html</code> , <code>abd.html</code> , <code>abe.html</code> , etc., mais pas avec le fichier <code>abc.htm</code> .
*	Remplace une absence de caractère ou plusieurs caractères Par exemple : <code>*mtl</code> établit une correspondance avec les fichiers <code>abc.html</code> et <code>d.html</code> . <code>*txt</code> établit une correspondance avec les fichiers <code>abc.txt</code> , <code>x.txt</code> et <code>xyztxt</code> .

Exclusions

Vous pouvez configurer des exclusions qui se propageront à tous les différents agents et composants d'AVG Business Antivirus sous l'onglet *Paramètres d'antivirus* de vos politiques.

Les modifications apportées aux exclusions au sein des politiques se propagent sur le réseau toutes les 5-10 minutes. Les politiques de la console se substituent aux paramètres locaux.

1. Accédez à l'onglet *Paramètres d'antivirus* du système d'exploitation correspondant.
2. Dans la section *Exclusions*, procédez de l'une des façons suivantes :
 - Cliquez sur **Accès au fichier**, saisissez le chemin d'accès de fichier à exclure, puis cliquez sur **Ajouter**.

- Cliquez sur **Adresses URL**, saisissez l'URL que vous souhaitez exclure, puis cliquez sur **Ajouter**.

3. Cliquez sur **Appliquer les modifications** lorsque vous avez terminé.

Si vous avez plusieurs types de systèmes d'exploitation et qu'ils utilisent la même politique, veillez à ajouter les exclusions à cette section sous les onglets Poste de travail Windows et/ou Windows Server.

Configuration des mises à jour automatiques

Vous pouvez définir vos appareils de sorte qu'ils mettent automatiquement à jour le programme AVG Business Antivirus et la base de données virale.

Configuration des mises à jour

Les mises à jour sont envoyées directement via les serveurs AVG ou les éventuels Master Agents/Local Update Servers configurés sur votre réseau. Si vous avez opté pour des mises à jour manuelles, vous devez procéder à des mises à jour manuelles via la page *Appareils* pour que tous les appareils de votre réseau restent à jour avec les dernières protections en date.

Création et configuration d'analyses

Vous pouvez configurer les types de fichiers et les programmes qui seront analysés par AVG Business Antivirus lorsque vous configurez la tâche d'analyse, dans la mesure où vous avez sélectionné un type d'analyse avancée (personnalisée, au démarrage). Par conséquent, les principaux détails de l'analyse ne sont pas configurés dans les politiques, à la différence des exclusions.

Types d'analyses

- **Analyse rapide** : recherche les menaces courantes.
- **Analyse système complète** : exécute une analyse détaillée de chaque fichier de l'appareil.
- **Analyse des médias amovibles** : analyse les clés USB et les médias portables connectés à l'appareil.
- **Analyse personnalisée** : exécute une analyse en fonction de vos choix : types de fichiers, sensibilité de l'analyse, performances, actions et inclusion ou non des fichiers compressés.

- **Analyse au démarrage (MS Windows uniquement)** : exécute une analyse au démarrage de l'appareil.

Console cloud

Création d'analyses planifiées

Vous pouvez créer uniquement des analyses planifiées rapides ou complètes du système.

1. Accédez à la page *Politiques*.
2. Cliquez sur la politique à laquelle vous souhaitez ajouter des analyses planifiées.
3. Cliquez sur l'onglet **Paramètres du service**.
4. Développez la section **Analyses antivirus**.
5. Configurez les paramètres d'**Analyse rapide** et d'**Analyse système complète** suivants :
 - **Fréquence** : choisissez entre Quotidienne, Hebdomadaire ou Mensuelle.
 - **Jour de la semaine/du mois** : choisissez le jour d'exécution souhaité de l'analyse.
 - **Heure de début** : choisissez l'heure du jour à laquelle vous souhaitez que l'analyse s'exécute.
6. Lorsque vous avez terminé, cliquez sur **Appliquer**.

Création d'analyses uniques

1. Accédez à la page *Appareils*, puis procédez de l'une des façons suivantes :
 - Pour un seul appareil, cliquez sur le bouton **Plus** à droite du nom de l'appareil.
 - Pour plusieurs appareils, cochez les cases de tous les appareils à inclure, puis cliquez sur **Actions**.
2. Placez le curseur sur **Analyses antivirus**.
3. Cliquez sur le type de tâche à créer :
 - Analyse antivirus rapide
 - Analyse antivirus système complète
 - Analyse antivirus avancée

4. Complétez les détails et les paramètres de la tâche, puis cliquez sur **Créer**.

Console sur site

1. Cliquez sur **Analyser l'appareil**.
2. Sélectionnez un type d'analyse :
 - **Analyse rapide** : recherche les menaces courantes.
 - **Analyse système complète** : exécute une analyse détaillée de chaque fichier de l'appareil.
 - **Analyse des médias amovibles** : analyse les clés USB et les médias portables connectés à l'appareil.
 - **Analyse personnalisée** : exécute une analyse en fonction de vos choix : types de fichiers, sensibilité de l'analyse, performances, actions et inclusion ou non des fichiers compressés.
 - **Analyse au démarrage (MS Windows uniquement)** : exécute une analyse au démarrage de l'appareil.
- o **Si vous optez pour une analyse personnalisée ou une analyse au démarrage, sélectionnez les options de configuration supplémentaires pour votre analyse.**
3. Si vous souhaitez en faire une tâche récurrente, sélectionnez *Planifier l'analyse*, définissez la fréquence (une fois, quotidienne, hebdomadaire ou mensuelle), puis planifiez la date et l'heure de début.
4. Saisissez un nom personnalisé pour l'analyse.
5. Cliquez sur **Lancer l'analyse**.

Les menaces détectées pendant l'analyse sont généralement envoyées vers la Zone de quarantaine de l'appareil. Vous pouvez examiner et gérer ces détections dans Détails de l'appareil.

Configuration de l'analyse

Configuration des analyses au démarrage

Seuls les appareils Microsoft Windows ont accès aux analyses au démarrage, qui se produisent lorsque l'appareil se met à démarrer.

Emplacements Windows à analyser : vous pouvez sélectionner des emplacements prédéfinis à analyser dans le menu déroulant, qui sont ensuite ajoutés à la liste. Si vous le souhaitez, vous pouvez également saisir le chemin d'accès à un emplacement spécifique à inclure dans l'analyse. Les emplacements que vous ne souhaitez pas inclure dans l'analyse peuvent être supprimés de la liste en cliquant sur le bouton Supprimer.

Redémarrer l'appareil maintenant : redémarre immédiatement l'appareil pour effectuer une analyse au démarrage. Si vous ne cochez pas cette option, l'analyse au démarrage s'exécute au prochain redémarrage de l'appareil.

Avertir les utilisateurs avec un message avant le redémarrage : saisissez le message à afficher à l'attention de l'utilisateur final pour l'avertir que l'appareil va redémarrer sous peu.

Spécifier quand le message ci-dessus sera affiché : sélectionnez à quel moment le message doit s'afficher : 1 minute, 10 minutes, 30 minutes ou 1 heure avant le redémarrage.

Heuristique : la composante heuristique permet à l'antivirus de détecter les malwares (logiciels malveillants) inconnus en recherchant dans le code des commandes susceptibles d'indiquer une intention malveillante. La valeur par défaut est Normal. Une plus grande sensibilité augmente la probabilité de détection de malwares, mais entraîne également davantage de détections de faux positifs qui identifient de manière incorrecte des fichiers comme étant des malwares.

LPI et fichiers suspects : indiquez si l'analyse doit inclure les programmes potentiellement indésirables (LPI).

Décompresser les fichiers archive : indiquez si les types de fichiers archive doivent être décompressés pendant l'analyse, qui est alors plus lente, mais plus poussée.

Lorsqu'une menace est détectée : choisissez l'action que doit effectuer AVG lorsqu'une menace est détectée : Nettoyer automatiquement, Déplacer vers la Zone de quarantaine, Réparer, Supprimer ou Ne rien faire.

Annuler l'analyse sur le poste de travail : indiquez si l'analyse s'exécutant sur le poste de travail doit être annulée.

Configuration d'analyses personnalisées

Les analyses personnalisées permettent de mieux contrôler les types de fichiers, dossiers, programmes et processus à inclure dans l'analyse AVG Business Antivirus. Vous pouvez sélectionner différentes options d'analyse pour les postes de travail

Windows, les serveurs Windows et les appareils MacOS X dans la même tâche d'analyse.

Configuration des emplacements

Vous pouvez sélectionner des emplacements prédéfinis à analyser dans le menu déroulant, qui sont ensuite ajoutés à la liste. Si vous le souhaitez, vous pouvez également saisir le chemin d'accès à un emplacement spécifique à inclure dans l'analyse. Les emplacements que vous ne souhaitez pas inclure dans l'analyse peuvent être supprimés de la liste en cliquant sur le bouton Supprimer.

Onglet Types de fichiers

Vous pouvez choisir d'analyser tous les fichiers (ou seulement les zones les plus couramment visées par les menaces). De plus, vous pouvez configurer l'analyse pour qu'elle reconnaisse les types de fichiers par leur contenu, ce qui demande une analyse du fichier entier, ou par leur extension. Dans ce cas, l'analyse porte uniquement sur les fichiers dont vous avez saisi l'extension dans la zone de texte qui s'affiche lorsque cette option est sélectionnée.

Onglet Sensibilité

Sensibilité heuristique : la méthode heuristique permet à l'antivirus de détecter les malwares inconnus en recherchant dans le code des commandes susceptibles d'indiquer une intention malveillante. La valeur par défaut est Normal. Une plus grande sensibilité augmente la probabilité de détection de malwares, mais entraîne également davantage de détections de faux positifs qui identifient de manière incorrecte des fichiers comme étant des malwares. Des émulations de code décompressent et testent un malware suspecté dans un environnement émulé où le fichier ne pourra pas endommager des appareils. L'option *Utiliser l'émulation de code* est activée par défaut.

Sensibilité : choisissez de tester les fichiers complets. Dans ce cas, l'analyse est plus lente, mais plus poussée.

LPI et fichiers suspects : indiquez si l'analyse doit inclure les programmes potentiellement indésirables (LPI).

Sensibilité : indiquez si les liens contenus dans les fichiers doivent être suivis pendant l'analyse. Dans ce cas, l'analyse est plus lente, mais plus poussée.

Onglet Performances

Priorité : choisissez la priorité de l'analyse sur le ou les appareils finaux. Une priorité élevée donne une analyse plus rapide, mais utilise plus de ressources.

Antémémorisation avancée : indiquez si vous souhaitez accélérer l'analyse en utilisant l'antémémorisation avancée et/ou si vous souhaitez stocker les données sur les fichiers analysés dans l'antémémoire permanente, ce qui ralentit l'analyse.

Accès aux fichiers : indiquez si vous souhaitez accélérer l'analyse en lisant les fichiers dans l'ordre où ils sont stockés sur le disque, ce qui s'applique uniquement aux volumes NTFS.

Onglet Actions

Appliquer une action : indiquez si des mesures doivent être automatiquement prises pendant l'analyse lorsqu'un virus, un programme potentiellement indésirable (LPI) ou un fichier suspect est détecté. Les options sont Nettoyer automatiquement, Déplacer vers la Zone de quarantaine, Réparer, Supprimer ou Ne rien faire.

Si, pour une raison quelconque, AVG ne peut pas mener à bien l'action principale, l'action sélectionnée sous *Si l'action échoue, utiliser* est exécutée.

Options : indiquez si l'action sélectionnée doit être exécutée au redémarrage.

Traitement des archives infectées : indiquez si vous souhaitez supprimer uniquement le fichier compressé de l'archive (et ne rien faire en cas d'échec), supprimer le fichier compressé de l'archive (et supprimer l'archive entière en cas d'échec) ou supprimer l'archive entière.

Onglet Conteneurs

Indiquez si vous souhaitez extraire tous les fichiers d'archive pour l'analyse.

Les consoles de gestion AVG Business proposent bien plus de fonctionnalités et d'options. Pour plus d'informations, consultez notre base de connaissances à l'adresse <https://businesshelp.avast.com/>.