

Démarrage rapide : Business Hub

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

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

Sommaire

Démarrage rapide : Business Hub	1
Sommaire.....	2
Présentation du Business Hub.....	4
Configuration du Hub	5
Vérifier la configuration système requise pour la console	5
Business Hub.....	5
Navigateurs (dernières versions recommandées)	5
Terminaux Avast Business Antivirus	5
Vérifier la configuration requise du pare-feu pour la console	6
Ports.....	6
URL	6
Configuration de la console	6
Inscription.....	6
Configuration de la console	7
Utilisateurs	7
Activation de licences dans le Hub.....	8
Attribution de licences à des appareils	8
Ajout d'appareils via le fichier d'installation ou un lien de partage.....	10
Téléchargement du programme d'installation	10
Installation sur le client local	11
Politiques globales.....	12
Principaux avantages.....	12
Que pouvez-vous en attendre ?.....	12
Création d'une politique globale	13
Configuration de votre politique	13

Vue d'ensemble.....	13
Paramètres généraux.....	13
Paramètres du service	14
Antivirus	14
Gestion des correctifs.....	14
Pare-feu.....	15
Exclusions.....	15
Création d'exclusions spécifiques de site	15
Assignations.....	15

Présentation du Business Hub

Le Business Hub vous permet de gérer plusieurs sites ou clients à partir d'une même console. Cette plateforme basée sur le cloud permet de réduire la charge de maintenance, de configuration et d'optimisation de la sécurité des terminaux. Le Hub s'adresse essentiellement aux acteurs suivants :

- Entreprises de taille moyenne à grande possédant plusieurs bureaux ou sites
- Fournisseurs de services informatiques prenant en charge divers clients
- Utilisateurs existants de la console cloud Avast Business utilisant la fonctionnalité de changement de compte (pour plus d'informations, consultez [Gestion d'entreprises](#) (uniquement en anglais))

Le Business Hub s'intègre de manière transparente avec Avast Business Antivirus pour :

- Tirer parti de la virtualisation pour protéger les informations confidentielles
- Protéger plusieurs plateformes : PC, Macs 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 Avast Business Antivirus sur des appareils via le Business Hub, vous pouvez contrôler Avast 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 du Hub

Vérifier la configuration système requise pour la console

Business Hub

Navigateurs (dernières versions recommandées)

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

Terminaux Avast 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

Mac :

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

Linux :

- CentOS 7 et versions supérieures
- Debian 8 et versions supérieures
- Red Hat Enterprise Linux 7.4 et versions supérieures
- Ubuntu LTS 16.04 et versions supérieures

Vérifier la configuration requise du pare-feu pour la console

Pour le fonctionnement global et pour permettre aux clients Avast Business Antivirus et/ou au Hub 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
- 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
- *.avcdn.net
- *.mailshell.net (uniquement si l'Anti-Spam est utilisé)

Configuration de la console

Inscription

Même si vous êtes actuellement client, vous devez quand même créer un compte pour le Hub en utilisant une adresse e-mail unique.

Partenaires existants :

1. Accédez au [portail des partenaires Avast](#).
2. Accédez à la section Avast Business Management Console, puis cliquez sur **Register** (Inscrire).
3. Suivez les étapes pour créer un Hub

Clients nouveaux ou existants :

1. Accédez à <https://new-business.avast.com/>.
2. Cliquez sur **Créer un compte**.
3. Saisissez l'adresse e-mail de l'administrateur ainsi que le mot de passe de votre choix.
4. Saisissez les informations sur l'entreprise, puis choisissez PME, Grande entreprise, Fournisseur de services gérés (MSP) ou Fournisseur de sécurité (revendeur/DVA/distributeur).
 - o Si vous sélectionnez MSP ou Fournisseur de sécurité, vous êtes invité à utiliser le portail des partenaires si vous êtes enregistré en tant que partenaire Avast.
5. Sélectionnez **Console multi-entreprises**, puis cliquez sur **Terminer et créer la console**.

Configuration de la console

1. Cliquez sur **Créer un site** ou sur **+ Site** dans le menu déroulant de gauche.
 - o Le Hub normal permet aux utilisateurs de créer des sites, mais si un partenaire s'enregistre pour le Hub via le portail de partenaires, sa console indique « Clients » et non « Sites ». Ces termes sont plus ou moins utilisés de façon interchangeable dans la documentation.
2. Saisissez le *Nom du site* et le *Pays*.
3. Indiquez si vous souhaitez commencer une période d'essai d'Avast Business Antivirus et de la Gestion des correctifs pour le site.
4. Cliquez sur **Créer le site**.

Le tableau de bord de niveau supérieur est complété avec les informations du ou des sites créés.

Utilisateurs

Vous pouvez ajouter un Administrateur général (pour un accès à tous les clients) ou un Utilisateur site (pour un accès à des sites déterminés).

1. Cliquez sur l'onglet *Utilisateurs*.
2. Cliquez sur **+ Utilisateur** en haut à droite.
3. Saisissez l'adresse e-mail de l'utilisateur.

4. Sélectionnez au choix **Administrateur général** ou **Utilisateur site**.

- o **Il est possible de personnaliser les utilisateurs site en leur attribuant différents niveaux d'accès aux sites, auxquels ils accèdent via la fonctionnalité de changement de compte de la console.**

Lorsqu'il existe plusieurs sites, vous pouvez passer de l'un à l'autre à partir du menu déroulant de gauche.

Activation de licences dans le Hub

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. Sans qu'aucun site ne soit sélectionné dans le menu déroulant de gauche, cliquez sur **Tableau de bord**.
2. En dessous du site que vous allez activer, cliquez sur **Activer un abonnement**.
3. Cliquez sur **Saisir un code d'activation**.
4. Saisissez le code d'activation et vérifiez qu'il est correct.

Attribution de licences à des appareils

Vous ne pouvez effectuer cette action qu'après avoir ajouté un appareil au réseau.

Les partenaires ne disposent pas encore d'une page Appareils leur permettant d'obtenir une vue d'ensemble de tous les clients ou sites. Cependant, vous pouvez sélectionnez un client/site dans le menu déroulant pour afficher les informations sur leurs appareils, telles que le nom, l'état, les alertes, le système d'exploitation des appareils, le groupe et la politique auxquels ils ont été affectés, leur version d'Antivirus, l'abonnement à la Gestion des correctifs, l'abonnement au Contrôle à distance premium ainsi que l'heure à laquelle ils ont été connectés pour la dernière fois à la console cloud.

Vous pouvez modifier l'abonnement associé à un appareil, par exemple si vous achetez des postes pour une version différente d'Antivirus ou un abonnement pour Gestion des correctifs.

1. Dans le Hub, sélectionnez le site que vous souhaitez gérer dans le volet de navigation de gauche.

2. Cliquez sur l'onglet *Appareils*.
3. Procédez de l'une des façons suivantes :
 - Cochez les cases correspondant à plusieurs appareils, puis cliquez sur **Plus** en haut à droite.
 - Cliquez sur les trois points situés dans liste des appareils.
4. Sélectionnez **Modifier** ▶ **Modifier l'abonnement au service**.
5. Dans les listes déroulantes, sélectionnez le ou les abonnements que vous souhaitez utiliser pour l'Antivirus et la Gestion des correctifs.
6. Cliquez sur **Appliquer**.

Cette procédure nécessite le redémarrage du ou des appareils concernés.

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

Vous pouvez ajouter des appareils à un site directement à partir du tableau de bord sans avoir à rechercher le site. Lorsque vous créez des programmes d'installation, les paramètres sélectionnés précédemment sont conservés de façon à ne pas avoir à les sélectionner à nouveau.

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)
 - MacOS X .dmg
2. 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 Avast pour télécharger les autres services.**
3. Sélectionnez les abonnements pour Avast Business Antivirus, Gestion des correctifs et indiquez si le Contrôle à distance doit ou non être activé.
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.
6. Vérifiez le cas échéant que vous avez défini le bon serveur proxy dans la politique que vous appliquez à l'appareil.
7. Cliquez sur **Télécharger le programme d'installation** 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.

Installation sur le client local

Après vous être procuré un fichier d'installation ou un lien de téléchargement à partir du Business Hub, vous devez installer Avast 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'Avast 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.

Politiques globales

À partir du 16 décembre 2020, les clients qui utilisent le Hub en version Bêta pourront créer et gérer des politiques à l'échelle de leur réseau et à l'intention de sites ou de clients déterminés.

Principaux avantages

- Les politiques sont configurées dans une même page.
- Les politiques sont appliquées à tous les appareils, quel que soit le système d'exploitation.
- Les exclusions sont créées et gérées à un même emplacement.
- Les exclusions propres à un site ou à un client sont créées en ouvrant une politique globale à partir de l'onglet Politiques du site.
- Les paramètres prédéfinis sont utilisés pour les postes de travail et les serveurs.

Que pouvez-vous en attendre ?

- Pour permettre cette évolution, les politiques existantes subiront les modifications suivantes :
 - Les politiques présentant des paramètres pour plusieurs systèmes d'exploitation seront scindées en plusieurs politiques en fonction du système d'exploitation.
 - **Exemple : si votre politique présente des paramètres différents pour les postes de travail Windows, les serveurs Windows et les appareils MacOS X, vous obtenez trois politiques différentes. Le type de système d'exploitation est indiqué à titre d'information à la fin de ces politiques.**
 - Le nom des politiques est inchangé.
 - Les politiques sont automatiquement affectées aux appareils en fonction du système d'exploitation.
 - **Exemple : les postes de travail Windows qui utilisaient une stratégie avec des paramètres pour les postes de travail, les serveurs et les appareils MacOS X se voient affecter la politique prévue pour les postes de travail.**

Création d'une politique globale

1. Ouvrez le Hub.
2. Cliquez sur l'onglet **Politiques**.
3. Cliquez sur **+ Politique**.
4. Saisissez le nom que vous souhaitez attribuer à la politique.
5. Saisissez éventuellement une description pour la politique.
6. Déterminez si la nouvelle politique doit être basée sur une politique Avast prédefinie ou sur une politique existante, puis effectuez une sélection dans le menu déroulant.
7. Cliquez sur **Créer**.

Configuration de votre politique

Une fois que vous avez créé une politique, vous pouvez en modifier les paramètres en cliquant sur son nom dans le tableau. Un tiroir s'ouvre avec cinq onglets et quelques boutons dans la partie supérieure. Vous pouvez utiliser ces boutons pour rétablir les paramètres d'origine de la politique ou pour dupliquer cette dernière. Si vous voulez supprimer la politique, cliquez sur les **trois points** et sélectionnez **Supprimer la politique**.

Vue d'ensemble

Cet onglet fournit quelques détails brefs sur la politique. Vous pouvez modifier la description en cliquant sur l'icône crayon. Vous pouvez également voir à quel moment la politique a été créée et mise à jour pour la dernière fois.

Paramètres généraux

Paramètres généraux : à l'aide des boutons bascule, activez ou désactivez l'Agent mots de passe, le mode silencieux, les services d'analyse de réputation, l'enregistrement du débogage, l'icône de la barre d'état Avast et l'analyse des lecteurs externes. Vous pouvez également choisir la version d'Avast Business Antivirus que doivent utiliser les appareils affectés en saisissant un numéro de version, « plus récent » ou « stable » dans la section Changer de version.

Mises à jour : optez pour des mises à jour automatiques ou manuelles pour la base de données virale et le programme (consultez [Configuration des mises à jour de la base de données virale et d'Antivirus](#) (uniquement en anglais)). Si nécessaire, vous pouvez

configurer les paramètres du proxy à utiliser pendant les mises à jour (consultez [Configuration de paramètres proxy pour des appareils](#) (uniquement en anglais)).

Dépannage : à l'aide des boutons bascule, activez ou désactivez le moniteur anti-rootkit, le module d'auto-défense d'Avast, l'accès limité au programme pour les comptes Invité et l'assistance matérielle à la virtualisation. Vous pouvez également saisir les détails de vos ports de messagerie.

Options de redémarrage : indiquez quand redémarrer les terminaux : seulement lorsque le programme Antivirus ou le service Gestion des correctifs l'exige, automatiquement, lorsque l'utilisateur se déconnecte ou pas du tout. Pour plus d'informations sur ces options, consultez [Configuration des redémarrages et de l'effacement du cache](#) (uniquement en anglais).

Paramètres du service

Antivirus

Paramètres généraux : activez ou désactivez CyberCapture et le mode renforcé.

Analyses antivirus : définissez la fréquence et le planning de l'analyse rapide et de l'analyse antivirus système complète. Pour plus d'informations, consultez [Tâches d'analyse des appareils](#) (uniquement en anglais).

Protection antivirus : activez, désactivez et configurez des paramètres pour les principaux composants de protection.

Protection des données : activez, désactivez et configurez des paramètres pour cette catégorie de composants.

Protection de l'identité : activez, désactivez et configurez des paramètres pour cette catégorie de composants.

Pour plus d'informations sur ces composants, consultez [Vue d'ensemble des composants](#) (uniquement en anglais). Vous pouvez accéder aux paramètres des composants configurables en cliquant sur la flèche déroulante en regard de leur nom.

Gestion des correctifs

Analyse et déploiement des correctifs : définissez la fréquence de recherche de correctifs manquants et indiquez si ceux-ci doivent être déployés immédiatement, selon un planning précis, ou manuellement.

Autres paramètres : indiquez quand effacer les fichiers correctifs locaux sur l'appareil final.

Pour plus d'informations les différents paramètres du service Gestion des correctifs, consultez [Gestion des correctifs](#) (uniquement en anglais).

Pare-feu

Paramètres du pare-feu ▶ Réseaux : sélectionnez les profils de pare-feu pour les connexions réseau non définies, puis définissez les réseaux.

Règles du pare-feu : définissez les diverses règles système, règles pour applications et règles avancées pour les paquets.

Pour plus d'informations, consultez les articles de la section *Firewall* (Pare-feu) de la page consacrée à la [configuration des paramètres et des politiques](#) (uniquement en anglais).

Exclusions

Exclusions antivirus : saisissez les chemins à exclure de toutes les analyses et agents ou d'agents spécifiques. Pour plus d'informations, consultez [Configuration d'exclusions antivirus standard](#) (uniquement en anglais) et [Configuration d'exclusions spécifiques de composants](#) (uniquement en anglais).

Gestion des correctifs : saisissez des exclusions pour certains éditeurs de correctifs et certains niveaux de gravité. Pour plus d'informations, consultez [Exclusions de correctifs](#) (uniquement en anglais).

Création d'exclusions spécifiques de site

1. Sélectionnez le client dans le menu déroulant situé en haut à gauche.
2. Cliquez sur l'onglet **Politiques**.
3. Sélectionnez le nom de la politique globale dans la liste.
 - o **Vérifiez que le site peut accéder à la politique globale en l'assignant (voir ci-dessous).**
4. Accédez à **Exclusions ▶ Exclusions antivirus**
5. Saisissez la ou les exclusions spécifiques de site sous l'onglet souhaité.
6. Cliquez sur **Enregistrer**.

Assignations

Cliquez sur **+ Assigner aux sites** pour permettre à des sites spécifiques d'utiliser la politique globale. Vous pouvez également supprimer des sites de la liste des

assignations en utilisant les cases à cocher et en cliquant sur **Annuler l'assignation de la politique**.

Après avoir apporté les modifications à la politique, cliquez sur Enregistrer dans la partie inférieure droite du tiroir.