

Bitdefender®

GravityZone

GUIDE D'INSTALLATION

Bitdefender GravityZone Guide d'installation

Date de publication 2019.09.02

Copyright© 2019 Bitdefender

Mentions légales

Tous droits réservés. Aucune partie de ce manuel ne peut être reproduite ou transmise, sous aucune forme et d'aucune façon, électronique ou physique, y compris photocopies, enregistrement, ou par quelque moyen de sauvegarde ou de restauration que ce soit, sans une autorisation écrite d'un représentant officiel de Bitdefender. Il est permis d'inclure de courtes citations dans la rédaction de textes sur le produit, à condition d'en mentionner la source. Le contenu ne peut en aucun cas être modifié.

Avertissement. Ce produit et ses textes sont protégés par copyright. Les informations contenues dans ce document sont données « à titre indicatif », sans garantie. Bien que toutes les précautions aient été prises lors de l'élaboration de ce document, ses auteurs ne sauraient être tenus pour responsables envers toute personne ou entité, des pertes ou dommages directs ou indirects consécutifs à l'utilisation des informations qu'il contient.

Ce manuel contient des liens vers des sites Web tiers qui ne sont pas sous le contrôle de Bitdefender, et Bitdefender n'est pas responsable du contenu de ces sites. Si vous accédez à l'un des sites web d'une tierce partie fourni dans ce document, vous le ferez à vos propres risques. Bitdefender indique ces liens uniquement à titre informatif, et l'inclusion d'un lien n'implique pas que Bitdefender assume ou accepte la responsabilité du contenu de ce site Web.

Marques commerciales. Des noms de marques peuvent apparaître dans ce manuel. Toutes les marques, enregistrées ou non, citées dans ce document, sont la propriété exclusive de leurs propriétaires respectifs.

Table des matières

| | |
|---|----|
| Préface | v |
| 1. Conventions utilisées dans ce guide | v |
| 1. À propos de GravityZone | 1 |
| 2. Couches de protection de GravityZone | 2 |
| 2.1. Antimalware | 2 |
| 2.2. Advanced Threat Control | 4 |
| 2.3. Anti-exploit avancé | 4 |
| 2.4. Pare-feu | 4 |
| 2.5. Contrôle de contenu | 4 |
| 2.6. Gestion des correctifs | 5 |
| 2.7. Contrôle des appareils | 5 |
| 2.8. Chiffrement de disque | 5 |
| 2.9. Security for Exchange | 5 |
| 2.10. Endpoint Risk Analytics (ERA) | 6 |
| 2.11. Disponibilité des couches de protection de GravityZone | 6 |
| 3. L'architecture de GravityZone | 7 |
| 3.1. Console Web (GravityZone Control Center) | 7 |
| 3.2. Security Server | 7 |
| 3.3. Agents de sécurité | 7 |
| 3.3.1. Bitdefender Endpoint Security Tools | 8 |
| 3.3.2. Bitdefender Endpoint Security Tools for Windows Legacy | 10 |
| 3.3.3. Endpoint Security for Mac | 11 |
| 4. Prérequis | 12 |
| 4.1. Control Center | 12 |
| 4.2. Protection des postes de travail | 12 |
| 4.2.1. Matériel | 13 |
| 4.2.2. Systèmes d'exploitation pris en charge | 16 |
| 4.2.3. Système de fichiers pris en charge | 22 |
| 4.2.4. Navigateurs pris en charge | 22 |
| 4.2.5. Security Server | 22 |
| 4.2.6. Utilisation du trafic | 24 |
| 4.3. Protection Exchange | 26 |
| 4.3.1. Environnements Microsoft Exchange pris en charge | 26 |
| 4.3.2. Configuration requise | 27 |
| 4.3.3. Autres prérequis logiciels | 27 |
| 4.4. Chiffrement de disque | 27 |
| 4.5. Protection de stockage | 29 |
| 4.6. Ports de communication de GravityZone | 29 |
| 5. Installation de la protection | 31 |
| 5.1. Gestion des licences | 31 |
| 5.1.1. Trouver un revendeur | 31 |
| 5.1.2. Activation de votre licence | 32 |

| | |
|---|----|
| 5.1.3. Vérification des détails de la licence actuelle | 32 |
| 5.2. Installer la protection des postes de travail | 33 |
| 5.2.1. Installation de Security Server | 33 |
| 5.2.2. Installation des agents de sécurité | 36 |
| 5.3. Installer le Chiffrement complet du disque | 60 |
| 5.4. Installer la protection Exchange | 61 |
| 5.4.1. Préparation de l'Installation | 61 |
| 5.4.2. Installation de la protection sur les serveurs Exchange | 62 |
| 5.5. Installer la Protection de stockage | 62 |
| 5.6. Admin. des authentifications | 63 |
| 5.6.1. Ajouter des identifiants dans l'Administrateur des authentifications | 64 |
| 5.6.2. Supprimer les identifiants de l'Administrateur des authentifications | 65 |
| 6. Intégrations | 66 |
| 6.1. Intégration au service Amazon EC2 | 66 |
| 7. Désinstallation de la protection | 67 |
| 7.1. Désinstallation de la Protection Endpoint | 67 |
| 7.1.1. Désinstallation des agents de sécurité | 67 |
| 7.1.2. Désinstallation de Security Server | 69 |
| 7.2. Désinstallation de la Protection Exchange | 70 |
| 8. Obtenir de l'aide | 71 |
| 8.1. Centre de support de Bitdefender | 71 |
| 8.2. Demande d'aide | 73 |
| 8.3. Utiliser l'Outil de Support | 73 |
| 8.3.1. Utiliser l'outil de support sur les systèmes d'exploitation Windows | 73 |
| 8.3.2. Utiliser l'outil de support sur les systèmes d'exploitation Linux | 75 |
| 8.3.3. Utiliser l'outil de support sur les systèmes d'exploitation Mac | 77 |
| 8.4. Contact | 78 |
| 8.4.1. Adresses Web | 78 |
| 8.4.2. Distributeurs Locaux | 78 |
| 8.4.3. Bureaux de Bitdefender | 79 |
| A. Annexes | 82 |
| A.1. Types de fichiers pris en charge | 82 |

Préface

Ce guide s'adresse aux administrateurs informatique en charge du déploiement de la protection GravityZone sur les sites de leur organisation. Les responsables informatiques en quête d'informations sur GravityZone trouveront dans ce guide les conditions préalables à l'installation de GravityZone ainsi que les modules de protection disponibles.

L'objectif du présent document est d'expliquer comment déployer les agents de sécurité Bitdefender sur tous types de endpoints de votre entreprise, et comment configurer la solution GravityZone.

1. Conventions utilisées dans ce guide

Normes Typographiques

Ce guide utilise différents styles de texte pour une meilleure lisibilité. Le tableau ci-dessous vous informe au sujet de leur aspect et de leur signification.

| Apparence | Description |
|--|---|
| échantillon | Le nom et les syntaxes des lignes de commandes, les chemins et les noms de fichiers, la configuration, la sortie de fichier et les textes d'entrée sont affichés en police monospace. |
| http://www.bitdefender.com | Les liens URL pointent vers un emplacement externe comme un serveur http ou ftp. |
| gravityzone-docs@bitdefender.com | Les adresses e-mail sont insérées dans le texte pour plus d'informations sur les contacts. |
| « Préface » (p. v) | Ceci représente un lien interne vers un emplacement à l'intérieur de ce document. |
| option | Toutes les options du produit sont imprimées à l'aide de caractères gras . |
| mot clé | Les options de l'interface, les mots-clés et les raccourcis sont mis en évidence à l'aide de caractères gras . |

Avertissements

Les avertissements sont des notes textes graphiquement marquées, offrant à votre attention des informations additionnelles relatives au paragraphe actuel.



Note

La note consiste simplement en une courte observation. Bien que vous puissiez les ignorer, les notes apportent des informations non négligeables, comme des fonctions spécifiques ou un lien vers un thème proche.



Important

Cette icône requiert votre attention et il n'est pas recommandé de la passer. Elle fournit généralement des informations non essentielles mais importantes.



Avertissement

Marque une information critique que vous devrez lire attentivement. Rien de négatif ne se passera si vous suivez les indications. A lire très attentivement car décrit une opération potentiellement très risquée.

1. À PROPOS DE GRAVITYZONE

GravityZone est une solution de sécurité pour entreprises conçue nativement pour la virtualisation et le cloud afin de fournir des services de sécurité aux endpoints physiques, aux machines virtuelles de clouds privés et publics et aux serveurs de messagerie Exchange.

GravityZone fournit une console d'administration unifiée disponible dans le cloud (hébergée par Bitdefender) ou en tant qu'appliance virtuelle à installer sur le site de l'entreprise. La solution permet de déployer, d'appliquer et de gérer des politiques de sécurité pour un nombre illimité d'endpoints, de tout type, quel que soit l'endroit où ils se trouvent, à partir d'un point unique d'administration.

GravityZone fournit plusieurs niveaux de sécurité aux endpoints y compris aux serveurs de messagerie Microsoft Exchange : antimalware avec analyse comportementale, protection contre les menaces de type « zero day », liste noire des applications et sandboxing, pare-feu, contrôle des appareils et du contenu, antiphishing et antispham.

2. COUCHES DE PROTECTION DE GRAVITYZONE

GravityZone fournit les couches de protection suivantes :

- Antimalware
- Advanced Threat Control
- Anti-exploit avancé
- Pare-feu
- Contrôle de contenu
- Gestion des correctifs
- Contrôle des appareils
- Chiffrement de disque
- Security for Exchange
- Endpoint Risk Analytics (ERA)

2.1. Antimalware

La couche de protection antimalware est basée sur l'analyse des signatures et l'analyse heuristique (B-HAVE, ATC) afin de détecter les virus, vers, chevaux de Troie, spywares, adwares, keyloggers, rootkits et autres types de logiciels malveillants.

La technologie d'analyse antimalware de Bitdefender s'appuie sur les technologies suivantes :

- Une méthode d'analyse traditionnelle est d'abord utilisée, le contenu analysé est comparé à une base de données de signatures. La base de données de signatures contient des morceaux de code spécifiques à certaines menaces et est régulièrement mise à jour par Bitdefender. Cette méthode d'analyse est efficace contre les menaces ayant fait l'objet de recherches et documentées. Cependant, quelle que soit la vitesse à laquelle la base de données de signatures est mise à jour, il existe toujours une fenêtre de vulnérabilité entre le moment où une nouvelle menace est découverte et la publication de son correctif.
- **B-HAVE**, le moteur heuristique de Bitdefender fournit un second niveau de protection contre les nouvelles menaces, inconnues. Des algorithmes heuristiques détectent les malwares en fonction de caractéristiques comportementales. B-HAVE exécute les fichiers suspects dans un environnement virtuel afin de tester leur impact sur le système et de vérifier

qu'ils ne constituent aucune menace. Si une menace est détectée, l'exécution du malware est bloquée.

Moteurs d'analyse

Bitdefender GravityZone est capable de définir automatiquement les moteurs d'analyse en fonction de la configuration de l'endpoint lors de la création des packages d'agent de sécurité.

L'administrateur peut également personnaliser les moteurs d'analyse en choisissant parmi plusieurs technologies d'analyse :

1. **L'analyse locale**, lorsque l'analyse est effectuée sur l'endpoint local. Le mode d'analyse locale est adapté aux machines puissantes, puisque tous les contenus de sécurité sont stockés en local.
2. **Analyse hybride avec Moteurs Légers (Cloud Public)**, avec une empreinte moyenne, utilisant l'analyse dans le cloud et en partie les contenus de sécurité locaux. Ce mode d'analyse présente l'avantage d'une meilleure consommation des ressources, tout en impliquant l'analyse hors site.
3. **Analyse centralisée dans un Cloud public ou privé**, avec une petite empreinte nécessitant Security Server pour l'analyse. Dans ce cas, aucun jeu de contenus de sécurité n'est stocké en local et l'analyse est transférée vers le Security Server.



Note

Il y a un nombre minimum de moteurs stockés localement, nécessaires pour décompresser les fichiers.

4. **Analyse centralisée (Cloud public ou privé avec Security Server), avec une analyse locale de secours* (moteurs complets)**
5. **Analyse centralisée (Cloud public ou privé avec Security Server), avec une analyse hybride de secours* (Cloud public avec des moteurs légers)**

* Lorsqu'on utilise une analyse à double moteur, si le premier moteur n'est pas disponible, le moteur de secours est utilisé. La consommation des ressources et l'utilisation du réseau dépendent des moteurs utilisés.

2.2. Advanced Threat Control

Pour les menaces échappant même au moteur heuristique, un autre niveau de protection est présent sous la forme d'Advanced Threat Control (ATC).

Advanced Threat Control surveille en permanence les processus en cours d'exécution et évalue les comportements suspects tels que les tentatives visant à : dissimuler le type de processus, exécuter du code dans l'espace d'un autre processus (détourner la mémoire d'un processus pour obtenir des privilèges plus élevés), se répliquer, déposer des fichiers, éviter que des processus ne soient listés par des applications énumérant des processus etc. Chaque comportement suspect fait augmenter le score du processus. À partir d'un certain seuil, une alarme est déclenchée.

2.3. Anti-exploit avancé

Basée sur le machine learning, cet anti-exploit avancé est une technologie proactive qui bloque les attaques de type zero-day menée par le biais d'exploits évasifs. L'Anti-exploit avancé détecte les exploits les plus récents en temps réel et atténue les vulnérabilités de corruption de mémoire pouvant échapper aux autres solutions de sécurité. Il protège les applications les plus utilisées, telles que les navigateurs, Microsoft Office ou Adobe Reader, ou toutes les applications auxquelles vous pourriez penser. Il surveille les processus du système et le protège contre les failles de sécurité et le détournement de processus existants.

2.4. Pare-feu

Le pare-feu contrôle l'accès des applications au réseau et à Internet. L'accès est automatiquement autorisé pour une base de données complète d'applications connues, légitimes. Le pare-feu peut également protéger le système contre le balayage de port, limiter le partage de connexion Internet et prévenir lorsque de nouveaux nœuds rejoignent une connexion Wifi.

2.5. Contrôle de contenu

Le module Contrôle de Contenu aide à appliquer les politiques de l'entreprise liées au trafic autorisé, à l'accès à Internet, à la protection des données et au contrôle des applications. Les administrateurs peuvent définir des options d'analyse du trafic et des exclusions, planifier l'accès à Internet tout en bloquant ou autorisant

certaines catégories web ou URL, configurer des règles de protection des données et définir des permissions pour l'utilisation d'applications spécifiques.

2.6. Gestion des correctifs

Complètement intégré à GravityZone, Patch Management veille à ce que les applications logicielles et les systèmes d'exploitation soient à jour et donne une visibilité complète sur l'état des patches sur les endpoints Windows administrés.

Le module GravityZone Patch Management comprend de nombreuses fonctionnalités, telles que l'analyse des patches à la demande/planifiée, le patching automatique/manuel, ou l'édition de rapports sur les patches manquants.

Pour en apprendre plus sur les prestataires et produits pris en charge par GravityZone Patch Management, consultez cet [article de la base de connaissances](#).



Note

Patch Management est une extension disponible avec une clé de licence séparée pour tous les packs GravityZone.

2.7. Contrôle des appareils

Le module Contrôle des appareils permet d'éviter la fuite de données confidentielles et les infections de malwares par des appareils externes connectés aux endpoints. Cela passe par l'application de règles de blocage et d'exceptions, via une politique, à un large éventail de types d'appareils (tels que les clés USB, les appareils Bluetooth, les lecteurs de CD/DVD, les supports de stockage etc.)

2.8. Chiffrement de disque

Cette couche de protection vous permet d'appliquer le chiffrement de disque entier sur les endpoints en gérant BitLocker sur Windows, ou FileVault et diskutil sur macOS. Vous pouvez chiffrer et déchiffrer des volumes d'amorçage et de non-amorçage en quelques clics, tandis que GravityZone gère l'ensemble du processus, avec une intervention minimale des utilisateurs. En prime, GravityZone stocke les clés de récupération nécessaires pour débloquer les volumes, lorsque les utilisateurs oublient leurs mots de passe.

2.9. Security for Exchange

Bitdefender Security for Exchange offre une protection antimalware, antispam, antiphishing et un filtrage des pièces jointes et du contenu parfaitement intégrés

à Microsoft Exchange Server, afin de garantir un environnement de messagerie et de collaboration sûr et d'augmenter la productivité. À l'aide de technologies antimalware et antispam primées, elle protège les utilisateurs Exchange contre les malwares les plus récents et élaborés ainsi que contre les tentatives de vol de données confidentielles et de valeur d'utilisateurs.



Important

Security for Exchange a été conçu pour protéger l'intégralité de l'organisation Exchange à laquelle le serveur Exchange appartient. Cela signifie qu'il protège l'intégralité des messageries actives, y compris les messageries partagées et celles rattachées à un utilisateur/un bureau/un équipement.

En plus de la protection Microsoft Exchange, la licence couvre également les modules de protection endpoint installés sur le serveur.

La capacité de licences d' Security for Exchange est égale à 150% du nombre total de sièges de licence pour Security for Endpoints. Si le nombre de boîtes e-mail actives de votre organisation dépasse le nombre de boîtes protégées par la licence, une notification vous invitera à étendre votre licence.

2.10. Endpoint Risk Analytics (ERA)

Endpoint Risk Analytics (ERA) identifie, évalue et corrige les faiblesses des endpoints Windows via des analyses de risque de sécurité (à la demande ou planifiées via une politique), en prenant en compte de très nombreux indicateurs de risque. Une fois votre réseau analysé en quête de certains indicateurs de risque, vous obtiendrez une vue d'ensemble de l'état de votre réseau en matière de risque via le tableau de bord **Gestion des risques**, disponible depuis le menu principal. Vous pourrez résoudre automatiquement certains risques de sécurité directement depuis la Control Center GravityZone, et consulter des recommandations pour limiter l'exposition des endpoints.

2.11. Disponibilité des couches de protection de GravityZone

La disponibilité des couches de protection de GravityZone varie en fonction du système d'exploitation de l'endpoint. Pour en apprendre plus, consultez l'article de la base de connaissances [Disponibilité des couches de protection de GravityZone](#).

3. L'ARCHITECTURE DE GRAVITYZONE

La solution GravityZone comporte les composants suivants :

- [Console Web \(Control Center\)](#)
- [Security Server](#)
- [Agents de sécurité](#)

3.1. Console Web (GravityZone Control Center)

Les solutions de sécurité Bitdefender sont gérées dans GravityZone à partir d'un point unique d'administration, la console web Control Center, qui facilite l'administration et la visibilité du niveau de sécurité, des menaces de sécurité globales et le contrôle de l'ensemble des modules de sécurité protégeant les postes de travail et les serveurs virtuels ou physiques. Intégrant l'architecture "Gravity", le Control Center est capable de répondre aux besoins de toutes les entreprises, quelle que soit leur taille.

L'interface web Control Center s'intègre aux systèmes de surveillance et de gestion des systèmes existants afin de permettre d'appliquer facilement la protection de façon aux postes de travail et serveurs non gérés.

3.2. Security Server

Le Security Server est une machine virtuelle dédiée qui déduplique et centralise la plus grande partie de la fonctionnalité antimalware des agents antimalware, en agissant en tant que serveur d'analyse.

Le Security Server doit être installé sur un ou plusieurs hôtes en fonction du nombre de machines virtuelles protégées.

3.3. Agents de sécurité

Pour protéger votre réseau avec Bitdefender, vous devez installer les agents de sécurité de GravityZone adaptés sur les endpoints du réseau.

- [Bitdefender Endpoint Security Tools](#)
- [Bitdefender Endpoint Security Tools for Windows Legacy](#)
- [Endpoint Security for Mac](#)

3.3.1. Bitdefender Endpoint Security Tools

GravityZone assure la protection des machines Windows et Linux physiques et virtuelles avec Bitdefender Endpoint Security Tools, un agent de sécurité intelligent et conscient de son environnement qui s'adapte au type d'endpoint. Bitdefender Endpoint Security Tools peut être déployé sur n'importe quelle machine, physique ou virtuelle, pour fournir un système d'analyse flexible, un choix idéal pour les environnements mixtes (physique, virtuel et cloud).

En plus de la protection du système de fichiers, Bitdefender Endpoint Security Tools comprend également une protection des serveurs de messagerie pour les serveurs Microsoft Exchange.

Bitdefender Endpoint Security Tools utilise un modèle de politique unique pour les machines physiques et virtuelles et un kit d'installation pour tout environnement (physique ou virtuel) sous les éditions actuelles de Windows. Un kit séparé pour les anciennes versions de Windows. Pour en apprendre plus, consultez [BEST for Windows Legacy](#).

Couches de protection

Les couches de protection suivantes sont disponibles avec Bitdefender Endpoint Security Tools :

- [Antimalware](#)
- [Advanced Threat Control](#)
- [Pare-feu](#)
- [Contrôle de contenu](#)
- [Gestion des correctifs](#)
- [Contrôle des appareils](#)
- [Chiffrement de disque](#)
- [Security for Exchange](#)
- [Endpoint Risk Analytics \(ERA\)](#)

Rôles des endpoints

- [Power User](#)
- [Relais](#)
- [Serveur de mise en cache des patches](#)
- [Protection Exchange](#)

Power User

Les administrateurs de Control Center peuvent accorder des droits Power User aux utilisateurs d'endpoints via des paramètres de politique. Le module Power User fournit des droits d'administration au niveau de l'utilisateur, permettant à l'utilisateur de l'endpoint d'accéder et de modifier les paramètres de sécurité via une console locale. Control Center est informé lorsqu'un endpoint est en mode Power User et l'administrateur de Control Center peut toujours écraser les paramètres de sécurité locaux.



Important

Ce module est disponible uniquement pour les systèmes d'exploitation des postes de travail et serveurs Windows pris en charge. Pour plus d'informations, reportez-vous à « [Systèmes d'exploitation pris en charge](#) » (p. 16).

Relais

Les agents des endpoints avec le rôle Bitdefender Endpoint Security Tools Relay servent de serveurs de communication proxy et de serveurs de mise à jour aux autres endpoints du réseau. Les agents d'endpoints avec le rôle relais sont particulièrement nécessaires dans les entreprises ayant des réseaux isolés, dans lesquels tout le trafic passe par un point d'accès unique.

Dans les entreprises ayant de grands réseaux distribués, les agents relais contribuent à diminuer l'utilisation de la bande passante, en empêchant les endpoints protégés et les serveurs de sécurité de se connecter directement à l'appliance GravityZone.

Lorsqu'un agent Bitdefender Endpoint Security Tools Relay est installé dans le réseau, d'autres endpoints peuvent être configurés avec une politique pour communiquer avec Control Center via l'agent relais.

Les agents Bitdefender Endpoint Security Tools Relay remplissent les fonctions suivantes :

- Ils détectent tous les endpoints non protégés dans le réseau.
Cette fonctionnalité est essentielle pour le déploiement de l'agent de sécurité dans un environnement cloud GravityZone.
- Ils déploient l'agent de l'endpoint dans le réseau local.
- Ils mettent à jour les endpoints protégés du réseau.
- Ils assurent la communication entre Control Center et les endpoints connectés.
- Ils agissent en tant que serveurs proxy pour les endpoints protégés.

- Optimiser le trafic réseau pendant les mises à jour, les déploiements, les analyses et autres tâches qui consomment des ressources.

Serveur de mise en cache des patchs

Les endpoints avec rôle de Relais peuvent également faire office de Serveur de mise en cache des patchs. Une fois ce rôle activé, les Relais servent à stocker les patchs téléchargés sur le site Web du fournisseur, et les distribuent aux endpoints cibles de votre réseau. Lorsqu'un des endpoints connectés a un logiciel pour lequel tous les patchs ne sont pas installés, il les récupère sur le serveur et non pas sur le site Web du fournisseur, optimisant ainsi le trafic généré et la bande passante utilisée.



Important

Ce rôle supplémentaire est disponible une fois l'extension Gestion des patchs enregistrée.

Protection Exchange

Bitdefender Endpoint Security Tools avec le rôle Exchange peut être installé sur les serveurs Microsoft Exchange afin de protéger les utilisateurs d'Exchange contre les menaces présentes dans les e-mails.

Bitdefender Endpoint Security Tools avec le rôle Exchange protège à la fois la machine serveur et la solution Microsoft Exchange.

3.3.2. Bitdefender Endpoint Security Tools for Windows Legacy

Compte tenu de l'évolution des technologies de sécurité, certaines fonctionnalités de Bitdefender Endpoint Security Tools ne sont plus prises en charge par les anciennes éditions de Windows. Bitdefender Endpoint Security Tools for Windows Legacy est un kit séparé conçu pour protéger ces versions de Windows sans avoir à faire de compromis de sécurité sur les éditions actuelles.

Bitdefender Endpoint Security Tools for Windows Legacy ne peut pas être déployé à distance depuis la console GravityZone. Les administrateurs doivent installer le package de BEST for Windows Legacy manuellement ou en utilisant l'outil d'une tierce partie, par exemple Microsoft SCCM.

Couches de protection

Les couches de protection suivantes sont disponibles avec Bitdefender Endpoint Security Tools for Windows Legacy :

- Antimalware
- Advanced Threat Control



Important

Advanced Threat Control n'est pas disponible sous Windows Server 2003.

Rôles des endpoints

- Protection Exchange

Les rôles Power User et Relais ne sont pas disponibles sur BEST for Windows Legacy.

3.3.3. Endpoint Security for Mac

Endpoint Security for Mac est un agent de sécurité conçu pour protéger les postes de travail et les ordinateurs portables Macintosh équipés d'un processeur Intel. La technologie d'analyse disponible est l'**Analyse locale**, avec les contenus de sécurité stockés en local.

Couches de protection

Les couches de protection suivantes sont disponibles avec Endpoint Security for Mac :

- Antimalware
- Contrôle de contenu
- Contrôle des appareils
- Chiffrement de disque

4. PRÉREQUIS

Toutes les solutions GravityZone sont installées et gérées via le Control Center.

4.1. Control Center

Pour accéder à la console Web Control Center, la configuration requise est la suivante :

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Résolution d'écran recommandée : 1280 x 800 ou supérieure



Avertissement

Le Control Center ne fonctionnera pas / ne s'affichera pas correctement dans Internet Explorer 9+ avec la fonctionnalité Affichage de compatibilité activée, ce qui revient à utiliser une version de navigateur non supportée.

4.2. Protection des postes de travail

Pour protéger votre réseau avec Bitdefender, vous devez installer les agents de sécurité GravityZone sur les endpoints du réseau. Pour une protection optimisée, vous pouvez également installer des Security Servers. Pour ce faire, vous avez besoin d'un utilisateur Control Center avec des privilèges administrateurs sur les services que vous devez installer et sur les endpoints du réseau que vous gérez.

La configuration requise pour les agents de sécurité varie selon qu'ils ont ou non un rôle complémentaire de serveur (serveur relais, serveur de protection Exchange ou serveur de mise en cache des patches). Pour plus d'informations sur les rôles des agents, reportez-vous à « [Agents de sécurité](#) » (p. 7).

4.2.1. Matériel

Agent de sécurité sans rôle

Util. du proc.

| Systèmes cibles | Type de proc. | Systèmes d'exploitation pris en charge |
|---------------------|--|---|
| Postes de travail | Processeurs compatibles Intel® Pentium, 1 GHz ou plus | Microsoft Windows XP SP3 32 bits et Windows XP SP2 64 bits |
| | Processeurs compatibles Intel® Pentium, 2 GHz ou plus | Systèmes d'exploitation Windows pour postes de travail, sauf Windows XP |
| | Intel® Core 2 Duo, 2 GHz ou plus | macOS |
| Appareils connectés | Processeurs compatibles Intel® Pentium, 800 MHz ou plus | Systèmes d'exploitation intégrés Microsoft Windows |
| Serveurs | Minimum : processeurs compatibles Intel® Pentium 2,4 GHz | Systèmes d'exploitation Microsoft Windows Server et Linux |
| | Recommandé : processeur Intel® Xeon multicœurs, 1,86 GHz ou plus | |

12

Mémoire RAM disponible

À l'installation (Mo)

| OS | MOTEUR UNIQUE | | | | | |
|---------|----------------|--------------------|-----------------|--------------------|---------------------|--------------------|
| | Analyse locale | | Analyse hybride | | Analyse centralisée | |
| | AV seul. | Toutes les options | AV seul. | Toutes les options | AV seul. | Toutes les options |
| Windows | 1024 | 1200 | 512 | 660 | 256 | 400 |
| Linux | 1024 | 1024 | 512 | 512 | 256 | 256 |
| macOS | 1024 | 1024 | n/d | n/d | n/d | n/d |

Pour l'utilisation quotidienne (Mo)*

| OS | Antivirus /n(Moteur unique) | | | Modules de protection | | | | |
|---------|-----------------------------|---------|------------|-------------------------|----------|---------------------|------------|---------------------|
| | Local | Hybride | Centralisé | Analyse comportementale | Pare-feu | Contrôle du contenu | Power User | Mise à jour Serveur |
| Windows | 75 | 55 | 30 | +13 | +17 | +41 | +29 | +80 |
| Linux | 200 | 180 | 90 | - | - | - | - | - |
| macOS | 300 | - | - | - | - | - | - | - |

* Les mesures couvrent l'usage client quotidien d'endpoint, sans prendre en compte les tâches supplémentaires, comme les analyses à la demande ou les mises à jour produit.

Espace disque libre

À l'installation (Mo)

| OS | MOTEUR UNIQUE | | | | | | MOTEUR DOUBLE | | | |
|---------|----------------|--------------------|-----------------|--------------------|---------------------|--------------------|------------------------------|--------------------|-------------------------------|--------------------|
| | Analyse locale | | Analyse hybride | | Analyse centralisée | | Analyse centralisée + locale | | Analyse centralisée + hybride | |
| | AV seul. | Toutes les options | AV seul. | Toutes les options | AV seul. | Toutes les options | AV seul. | Toutes les options | AV seul. | Toutes les options |
| Windows | 1024 | 1200 | 500 | 700 | 350 | 570 | 1024 | 1200 | 500 | 700 |
| Linux | 1300 | 1450 | 800 | 950 | 300 | 450 | 1300 | 1450 | 800 | 950 |
| macOS | 1024 | 1024 | n/d | n/d | n/d | n/d | n/d | n/d | n/d | n/d |

Pour l'utilisation quotidienne (Mo)*

| OS | Antivirus (Moteur unique) | | | Modules de protection | | | | |
|---------|---------------------------|---------|------------|-------------------------|----------|---------------------|------------|---------------------|
| | Local | Hybride | Centralisé | Analyse comportementale | Pare-feu | Contrôle du contenu | Power User | Mise à jour Serveur |
| Windows | 410 | 190 | 140 | +12 | +5 | +60 | +80 | +10 |
| Linux | 500 | 200 | 110 | - | - | - | - | - |
| macOS | 1024 | - | - | - | - | - | - | - |

* Les mesures couvrent l'usage client quotidien d'endpoint, sans prendre en compte les tâches supplémentaires, comme les analyses à la demande ou les mises à jour produit.

Agent de sécurité avec rôle de serveur relais

Le rôle de serveur relais nécessite des ressources supplémentaires, qui s'ajoutent à la configuration de base. Cela permet de prendre en charge le serveur de mise à jour et les packages d'installation hébergés par l'endpoint . :

| Nombre d'endpoint connectés | Processeur prenant en charge le serveur de mise à jour | RAM | Espace disque disponible pour le serveur de mise à jour |
|-----------------------------|---|--------|---|
| 1-300 | Minimum : processeur Intel® Core™ i3 ou équivalent, 2 vCPU par cœur | 1,0 Go | 10 Go |
| 300-1000 | Minimum : processeur Intel® Core™ i5 ou équivalent, 4 vCPU par cœur | 1,0 Go | 10 Go |



Avertissement

Les agents relais ont besoin de disques SSD, pour prendre en charge le grand nombre d'opérations de lecture/écriture.



Important

- Si vous souhaitez sauvegarder les packages d'installation et les mises à jour sur un autre disque que celui sur lequel l'agent est installé, veillez à ce que les deux disques contiennent suffisamment d'espace disponible (10 Go). Sinon l'agent abandonne le processus d'installation. C'est nécessaire uniquement pendant l'installation.

- Sur les endpoints Windows, les liens symboliques local à local doivent être activés.

Agent de sécurité avec rôle de serveur de protection Exchange

La quarantaine des Serveurs Exchange requiert de l'espace disque supplémentaire sur la partition où l'agent de sécurité est installé.

La taille de la quarantaine dépend du nombre d'éléments qu'elle comporte et de leur taille.

Par défaut, l'agent est installé sur la partition système.

Agent de sécurité avec rôle de serveur de mise en cache des patches

L'agent avec rôle de serveur de mise en cache des patches doit cumuler les configurations suivantes :

- La configuration matérielle requise pour l'agent de sécurité simple (sans rôle)
- La configuration matérielle requise pour le rôle de serveur relais
- 100 Go supplémentaires d'espace disponible sur le disque pour le stockage des patches téléchargés



Important

Si vous souhaitez sauvegarder les patches sur un autre disque que celui sur lequel l'agent est installé, veillez à ce que les deux disques contiennent suffisamment d'espace disponible (100 Go). Sinon l'agent abandonne le processus d'installation. C'est nécessaire uniquement pendant l'installation.

4.2.2. Systèmes d'exploitation pris en charge

Systèmes d'exploitation pour postes de travail Windows

Support complet

- Windows 10 May 2019 Update (19H1)
- Mise à jour de Windows 10 du 10 octobre 2018 (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)

- Windows 10 November Update (Threshold 2)
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

Support limité

Sur ces systèmes d'exploitation, l'agent de sécurité dispose seulement de l'Antimalware et de Advanced Threat Control. Les modes Power User et Relay ne sont pas pris en charge.

- Windows Vista avec Service Pack 1
- Windows XP avec Service Pack 2 (64 bits)
- Windows XP avec Service Pack 3 (32 bits)



Avertissement

Bitdefender n'est pas compatible avec les builds du programme Insider de Windows.

Systèmes d'exploitation pour tablettes Windows et systèmes embarqués

Support complet

- Windows 10 IoT Enterprise
- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7

Support limité

Sur ces systèmes d'exploitation, l'agent de sécurité prend seulement en charge l'Antimalware et l'Advanced Threat Control. Les modes Power User et Relay ne sont pas pris en charge.

- Windows Embedded POSReady 2009

- Windows Embedded Standard 2009
- Windows XP Embedded avec Service Pack 2⁽¹⁾
- Windows XP Tablet PC Edition⁽¹⁾



Avertissement

(1) Ces composants spécifiques du système d'exploitation embarqués doivent être installés :

- Réseaux TCP/IP avec Client pour réseaux Microsoft
- Binaires support de base
- Gestionnaire de filtres
- Support cache DNS
- Programme d'installation Windows
- WMI Windows Installer Provider
- Service poste de travail
- WinHTTP
- Windows XP Service Pack 2 Resource DLL
- Windows Logon (Standard)
- Explorer shell
- Format NTFS

Windows Server

Support complet

- Windows Server 2019
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

Support limité

Sur ces systèmes d'exploitation, l'agent de sécurité prend seulement en charge l'Antimalware et l'Advanced Threat Control. Les modes Power User et Relay ne sont pas pris en charge. Windows Server 2008 et Windows Small Business Server (SBS) 2008 prennent également en charge la protection Exchange.

- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003
- Windows Small Business Server (SBS) 2008
- Windows Small Business Server (SBS) 2003
- Windows Home Server

**Important**

Bitdefender Endpoint Security Tools supporte la technologie Windows Server Failover Cluster (WSFC).

Linux

**Important**

Les endpoints Linux utilisent des sièges issus du pool de licences pour les systèmes d'exploitation serveur.

- Ubuntu 14.04 LTS ou supérieur
- Red Hat Enterprise Linux / CentOS 6.0 ou supérieur
- SUSE Linux Enterprise Server 11 SP4 ou supérieur
- OpenSUSE Leap 42.x
- Fedora 25 ou supérieur⁽¹⁾
- Debian 8.0 ou supérieur
- Oracle Linux 6.3 ou supérieur
- Amazon Linux AMI 2016.09 ou supérieure

**Avertissement**

(1) Sur Fedora 28, Bitdefender Endpoint Security Tools nécessite une installation manuelle du package `libnsl`, en exécutant la commande suivante :

```
sudo dnf install libnsl -y
```

Prérequis d'Active Directory

Lors de l'intégration d'endpoints Linux avec un domaine Active Directory via le System Security Services Daemon (SSSD), vérifiez que l'outil **ldbsearch** est bien installé.


Prise en charge de l'analyse à l'accès

L'analyse à l'accès est disponible pour tous les systèmes d'exploitation supportés. Sur les systèmes Linux, le support de l'analyse à l'accès est assuré dans les situations suivantes :

| Versions du noyau | Distributions Linux | Prérequis à l'accès |
|------------------------|---|--|
| 2.6.38 ou supérieur* | Red Hat Enterprise Linux / CentOS 6.0 ou supérieur Ubuntu 14.04 ou supérieur SUSE Linux Enterprise Server 11 SP4 ou supérieur OpenSUSE Leap 42.x Fedora 25 ou supérieur Debian 9.0 ou supérieur Oracle Linux 6.3 ou supérieur Amazon Linux AMI 2016.09 ou supérieure | Fanotify (option du noyau) doit être activé. |
| 2.6.38 ou supérieur | Debian 8 | Fanotify doit être activé et en mode « enforce », puis le noyau doit être recompilé. Pour plus d'informations, consultez cet article de la base de connaissances : |
| 2.6.32 - 2.6.37 | CentOS 6.x Red Hat Enterprise Linux 6.x | Bitdefender assure la prise en charge des modules préinstallés avec le noyau via DazukoFS . |
| Tous les autres noyaux | Tous les autres systèmes pris en charge | Le module DazukoFS doit être compilé manuellement. Pour plus d'informations, reportez-vous à « Compiler manuellement le module DazukoFS » (p. 55). |

* Avec certaines limitations décrites ci-dessous.

Limitations de l'analyse à l'accès

| Versions du noyau | Distributions Linux | Détails |
|---------------------|----------------------------------|--|
| 2.6.38 ou supérieur | Tous les systèmes pris en charge | <p>L'analyse à l'accès ne surveille les partages réseau montés que dans les conditions suivantes :</p> <ul style="list-style-type: none"> ● Fanotify est activé sur les systèmes à distance et locaux. ● Le partage est basé sur les systèmes de fichier CIFS et NFS. <p> Note L'analyse à l'accès n'analyse pas les partages réseau montés par SSH ou FTP.</p> |
| Tous les noyaux | Tous les systèmes pris en charge | <p>Pour les systèmes sur lesquels DazukoFS est installé, l'analyse à l'accès n'est pas prise en charge pour les partages réseau montés à des emplacements déjà protégés par le module à l'accès.</p> |



Note

Fanotify et DazukoFS permettent à des applications tierces de contrôler l'accès au fichier sur les systèmes Linux. Pour plus d'informations, reportez-vous à :

- Pages du manuel Fanotify : <http://www.xypron.de/projects/fanotify-manpages/man7/fanotify.7.html>.
- Site web du projet Dazuko : <http://dazuko.dnsalias.org/wiki/index.php/About>.

macOS

- macOS Mojave (10.14.x)
- macOS High Sierra (10.13.x)
- macOS Sierra (10.12.x)
- OS X El Capitan (10.11.x)
- OS X Yosemite (10.10.5)

- OS X Mavericks (10.9.5)

**Note**

OS X Mountain Lion (10.8.5) n'est plus pris en charge, mais les installations existantes continueront de recevoir les mises à jour du contenu de sécurité.

4.2.3. Système de fichiers pris en charge

Bitdefender installe et protège les systèmes de fichier suivants :

AFS, BTRFS, ext2, ext3, ext4, FAT, FAT16, FAT32, VFAT, exFAT, NTFS, UFS, ISO 9660 / UDF, NFS, CIFS/SMB, VXFS, XFS.

**Note**

La prise en charge de l'analyse à l'accès n'est pas fournie pour NFS et CIFS/SMB.

4.2.4. Navigateurs pris en charge

La sécurité du navigateur du poste de travail fonctionne avec les navigateurs suivants :

- Internet Explorer 8+
- Mozilla Firefox 30+
- Google Chrome 34+
- Safari 4+
- Microsoft Edge 20+
- Opera 21+

4.2.5. Security Server

Security Server est une machine virtuelle préconfigurée s'exécutant sur une distribution Ubuntu Server 12.04 LTS (Kernel 3.2)

Plateformes de virtualisation

Bitdefender Security Server peut être installé sur les plates-formes de virtualisation suivantes :

- VMware vSphere 6.7 update 2a, 6.7 update 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0 avec VMware vCenter Server 6.7 update 2a, 6.7 update 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0

- VMware Horizon/View 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- Lecteur VMware 7.x, 6.x, 5.x
- Citrix XenServer 7.x, 6.5, 6.2, 6.0, 5.6 or 5.5 (dont Xen Hypervisor)
- Citrix Virtual Apps et Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp et XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2 ou Windows Server 2008 R2, 2012, 2012 R2 (avec l'hyperviseur Hyper-V)
- Red Hat Enterprise Virtualization 3.0 (avec KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism avec AOS 5.5, 5.6 (Enterprise Edition)
- Nutanix Prism version 2018.01.31 (Community Edition)

**Note**

Le support d'autres plateformes de virtualisation peut être fourni sur demande.

Mémoire et processeur

L'allocation de ressources mémoire et processeur au Security Server dépend du nombre et du type de VM en cours d'exécution sur l'hôte. Le tableau suivant dresse la liste des ressources recommandées à allouer :

| Nombre de VM protégées | RAM | Processeurs |
|------------------------|------|---------------|
| 1-50 VM | 2 Go | 2 processeurs |
| 51-100 VM | 2 Go | 4 processeurs |
| 101-200 VM | 4 Go | 6 processeurs |

Espace disque

Vous devez disposer de 8Go d'espace disque sur chaque hôte de Security Server.

Distribution de Security Server sur les hôtes

Bien que ce ne soit pas obligatoire, Bitdefender recommande d'installer le Security Server sur chaque hôte physique pour de meilleures performances.

Latence du réseau

La latence de communication entre Security Server et les endpoints protégés doit être inférieure à 50 ms.

Charge de Storage Protection

L'impact de la Protection de stockage sur Security Server pour l'analyse de 20 Go est le suivant :

| État de Storage Protection | Ressources du Security Server | Charge du Security Server | Durée du transfert (mm:ss) |
|---------------------------------|-------------------------------|---------------------------|----------------------------|
| Désactivé (valeur de référence) | N/A | N/A | 10:10 |
| Activé | 4 vCPU 4 Go de RAM | Normal | 10:30 |
| Activé | 2 vCPU 2 Go de RAM | Lourde | 11:23 |



Note

Ces résultats sont obtenus avec une variété de fichiers (.exe, .txt, .doc, .eml, .pdf, .zip, etc.) dont la taille est comprise entre 10 Ko et 200 Mo. La durée indiquée est celle du transfert de 20 Go de données contenues dans 46 500 fichiers.

4.2.6. Utilisation du trafic

• Trafic des mises à jour produit entre les endpoints clients et le serveur de mise à jour

Chaque mise à jour produit Bitdefender Endpoint Security Tools périodique génère le trafic téléchargement suivant sur chaque endpoint client :

- Sous Windows : ~20 Mo
- Sous Linux : ~26 Mo

- Sur macOS : ~25 Mo
- **Trafic des mises à jour du contenu de sécurité téléchargé entre les endpoints clients et le serveur de mise à jour (Mo/j)**

| Type de serveur de mise à jour | Type de moteur d'analyse | | |
|---|--------------------------|---------|----------|
| | Local | Hybride | Central. |
| Relais | 65 | 58 | 55 |
| Serveur public de mise à jour Bitdefender | 3 | 3.5 | 3 |

- **Le trafic Analyse centrale entre client endpoint et Security Server**

| Objets analysés | Type de trafic | Téléchargement (Mo) | Upload (Mo) |
|-----------------|------------------|---------------------|-------------|
| Fichiers* | Première analyse | 27 | 841 |
| | Analyse en cache | 13 | 382 |
| Sites Web** | Première analyse | Trafic Web | 621 |
| | | Security Server | 54 |
| | Analyse en cache | Trafic Web | 654 |
| | | Security Server | 0.2 |

* Les données proposées ont été mesurées pour 3.49 GB des fichiers (6,658 fichiers), dont 1.16 GB sont des fichiers Portable Executable (PE).

** Les données proposées ont été mesurées pour les 500 sites web les mieux notés.

- **Le trafic Analyse hybride entre le client endpoint et les services Cloud Bitdefender**

| Objets analysés | Type de trafic | Téléchargement (Mo) | Upload (Mo) |
|-----------------|----------------------------|---------------------|-------------|
| Fichiers* | Première analyse | 1.7 | 0.6 |
| | Analyse en cache | 0.6 | 0.3 |
| Trafic Web** | Trafic Web | 650 | N/A |
| | Services Cloud Bitdefender | 2.6 | 2.7 |

* Les données proposées ont été mesurées pour 3.49 GB des fichiers (6,658 fichiers), dont 1.16 GB sont des fichiers Portable Executable (PE).

** Les données proposées ont été mesurées pour les 500 sites web les mieux notés.

**Note**

La latence du réseau entre le client de l'endpoint et Bitdefender Cloud Server doit être de moins d'1 seconde.

- **Le trafic entre les clients Bitdefender Endpoint Security Tools Relay et le serveur de mise à jour pour le téléchargement du contenu de sécurité**

Les clients avec un rôle Bitdefender Endpoint Security Tools Relay téléchargent ~16 MB / jour* à partir du serveur mise à jour.

* Disponible avec les clients Bitdefender Endpoint Security Tools à partir de la version 6.2.3.569.

- **Le trafic entre les clients endpoint et la web console Control Center**

Un trafic moyen de 618 KB / jour est généré entre les clients endpoint et la web console Control Center.

4.3. Protection Exchange

Security for Exchange est délivré via Bitdefender Endpoint Security Tools, qui peut protéger à la fois le système de fichiers et le serveur de messagerie Microsoft Exchange.

4.3.1. Environnements Microsoft Exchange pris en charge

Security for Exchange est compatible avec les versions et rôles Microsoft Exchange suivants :

- Exchange Server 2019 avec le rôle de Transport Edge ou le rôle Boîte aux lettres
- Exchange Server 2016 avec le rôle de Transport Edge ou le rôle Boîte aux lettres
- Exchange Server 2013 avec le rôle de Transport Edge ou le rôle Boîte aux lettres
- Exchange Server 2010 avec le rôle de Transport Edge, de Transport Hub ou Boîte aux lettres
- Exchange Server 2007 avec le rôle de Transport Edge, de Transport Hub ou Boîte aux lettres

Depuis le 30 janvier 2017, Security for Exchange ne permet plus d'installer Microsoft Exchange 2007 sur Windows Server 2003, 2003 R2 et Small Business Server 2003. Si vous avez toujours besoin d'utiliser Microsoft Exchange 2007, envisagez de migrer votre installation vers Windows Server 2008.

Security for Exchange est compatible avec les Groupes de disponibilité de la base de données Microsoft Exchange (DAG).

4.3.2. Configuration requise

Security for Exchange est compatible avec tout serveur 64 bits physique ou virtuel (Intel ou AMD) ayant une version et un rôle de Serveur Exchange de Microsoft pris en charge. Pour des informations concernant la configuration système requise de Bitdefender Endpoint Security Tools, reportez-vous à « [Agent de sécurité sans rôle](#) » (p. 13).

Ressources serveur disponibles recommandées :

- Mémoire RAM disponible : 1 Go
- Espace disponible sur le disque dur : 1 Go

4.3.3. Autres prérequis logiciels

- Pour Microsoft Exchange Server 2013 avec Service Pack 1 : [KB2938053](#) de Microsoft.
- Pour Microsoft Exchange Server 2007 : .NET Framework 3.5 Service Pack 1 ou version supérieure

4.4. Chiffrement de disque

Le module de chiffrement complet du disque de GravityZone vous permet d'utiliser BitLocker sur les endpoints Windows, ainsi que FileVault et l'utilitaire de ligne de commande diskutil sur les endpoints macOS via Control Center.

Pour une protection garantie de vos données ce module assure le chiffrement complet, pour les volumes de démarrage et les autres, sur des disques durs fixes ; et conserve les clés de récupération au cas où les utilisateurs oublient leurs mots de passe.

Le module de Chiffrement utilise les ressources matérielles de votre environnement GravityZone.

En ce qui concerne le logiciel, la configuration requise est presque la même que pour BitLocker, FileVault et l'utilitaire de ligne de commande diskutil, et la plupart des restrictions sont liées à ces outils.

Sous Windows

Le module de chiffrement de GravityZone est compatible avec BitLocker à partir de la version 1.2, sur les machines équipées ou non d'une puce (Trusted Platform Module).

GravityZone prend en charge BitLocker sur des postes fonctionnant avec les systèmes d'exploitation suivants :

- Windows 10 Education
- Windows 10 Enterprise
- Windows 10 Pro
- Windows 8.1 Enterprise
- Windows 8.1 Pro
- Windows 8 Enterprise
- Windows 8 Pro
- Windows 7 Ultimate (avec TPM)
- Windows 7 Enterprise (avec TPM)
- Windows Server 2019*
- Windows Server 2016*
- Windows Server 2012 R2*
- Windows Server 2012*
- Windows Server 2008 R2* (avec TPM)

*BitLocker n'est pas intégré à ces systèmes d'exploitation et doit être installé séparément. Pour plus d'informations sur le déploiement de BitLocker sur Windows Server, consultez ces articles sur la Base de connaissances Microsoft :

- <https://technet.microsoft.com/en-us/itpro/bitlocker-how-to-deploy-on-windows-server>
- [https://technet.microsoft.com/en-us/library/cc732725\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732725(v=ws.10).aspx)

**Important**

GravityZone ne prend pas en charge le chiffrement sur Windows 7 et Windows 2008 R2 sans TPM.

Pour plus de détails sur la configuration requise pour BitLocker, consultez cet article sur la Base de connaissances Microsoft : [https://technet.microsoft.com/en-us/library/cc766200\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx)

Sous Mac

GravityZone prend en charge FileVault et diskutil sur des postes macOS fonctionnant avec les systèmes d'exploitation suivants :

- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)
- OS X Yosemite (10.10)
- OS X Mavericks (10.9)

**Note**

Sous Mac OS X Mountain Lion (10.8), vous pouvez installer l'agent Bitdefender, mais le module de Chiffrement ne sera pas disponible.

4.5. Protection de stockage

Solutions de stockage et de partage de fichiers prises en charge :

- Serveurs de stockage en réseau (NAS) et sous-réseaux de stockage compatibles avec le protocole iSCSI, fournis par Dell®, EMC®, IBM®, Hitachi®, HPE® et Oracle®, entre autres.
- Nutanix® Files (anciennement Acropolis File Services ou AFS)
- Citrix® ShareFile

4.6. Ports de communication de GravityZone

GravityZone est une solution distribuée, ce qui signifie que ses composants communiquent entre eux via le réseau local ou Internet. Chaque composant utilise

un ensemble de ports pour communiquer avec les autres. Vous devez veiller à ce que les ports nécessaires à GravityZone soient ouverts.

Pour des informations détaillées au sujet des ports de GravityZone, veuillez vous référer à [cet article KB](#).

5. INSTALLATION DE LA PROTECTION

Pour protéger votre réseau avec Bitdefender, vous devez installer les agents de sécurité de GravityZone sur les endpoints. Pour cela, vous avez besoin d'un utilisateur de la Control Center GravityZone avec des privilèges administrateur sur les endpoints que vous administrez.

5.1. Gestion des licences

GravityZone n'a besoin que d'une clé de licence pour tous ses services de sécurité, sauf le Chiffrement complet du disque, pour lequel il faut une clé de licence annuelle distincte.

Vous pouvez essayer GravityZone gratuitement pendant une période de 30 jours. Pendant la période d'évaluation, toutes les fonctionnalités sont disponibles et vous pouvez utiliser le service sur un nombre illimité d'ordinateurs. Avant la fin de la période d'évaluation, vous devez, si vous souhaitez continuer à utiliser les services, opter pour un plan d'abonnement payant et effectuer l'achat.

Pour acheter une licence, contactez un revendeur Bitdefender ou contactez-nous par e-mail à info@bitdefender.fr.

Votre abonnement est géré par Bitdefender ou par le partenaire Bitdefender qui vous vend le service. Certains partenaires Bitdefender sont des fournisseurs de services de sécurité. Selon les modalités de votre abonnement, le fonctionnement quotidien de GravityZone peut être géré en interne par votre société ou en externe par le fournisseur de services de sécurité.

5.1.1. Trouver un revendeur

Nos revendeurs vous fourniront toutes les informations dont vous avez besoin et vous aideront à choisir la meilleure option de licence pour vous.

Pour trouver un revendeur Bitdefender dans votre pays :

1. Rendez-vous sur la page [Trouver un partenaire](#) du site web de Bitdefender.
2. Sélectionnez le pays dans lequel vous habitez afin de voir les coordonnées des partenaires Bitdefender disponibles.
3. Si vous ne trouvez pas de revendeur Bitdefender dans votre pays, n'hésitez pas à nous contacter par e-mail à l'adresse channel-sales@bitdefender.fr.

5.1.2. Activation de votre licence

Lorsque vous achetez un abonnement payant pour la première fois, une clé de licence est générée pour vous. L'abonnement à GravityZone est activé avec cette clé de licence.



Avertissement

Activer une licence N'AJOUTE PAS ses fonctionnalités à la licence active. La nouvelle licence remplace l'ancienne. Par exemple, activer une licence de 10 postes de travail sur une licence de 100 postes de travail ne se traduira PAS par un abonnement pour 110 postes. Au contraire, cela réduira le nombre de postes protégés en le faisant passer de 100 à 10.

La clé de licence vous est envoyée par e-mail lorsque vous l'achetez. En fonction de l'accord de service, lorsque la clé de licence est émise, votre fournisseur de service peut l'activer pour vous. Vous pouvez également activer votre licence manuellement, en procédant comme suit :

1. Connectez-vous à Control Center avec votre compte.
2. Cliquez sur votre nom d'utilisateur dans l'angle supérieur droit de la console et sélectionnez **Mon Entreprise**.
3. Consultez des informations sur la licence actuelle dans la section **Licence**.
4. Sélectionnez le type de **Licence** dans la section **Licence**.
5. Saisissez votre clé de licence dans le champ **Clé de licence**,
6. Cliquez sur le bouton **Vérifier** et attendez que le Control Center récupère des informations sur la clé de licence saisie.
7. Dans le champ **Clé d'extension**, entrez la clé d'une extension spécifique, par exemple le Chiffrement.
8. Cliquez sur **Ajouter**. Les détails de l'extension s'affichent dans un tableau : type, clé de licence et option de retrait de la clé.
9. Cliquez sur **Enregistrer**.
10. Pour pouvoir utiliser l'extension, vous devez vous déconnecter de Control Center puis vous reconnecter. L'extension sera alors visible dans GravityZone.

5.1.3. Vérification des détails de la licence actuelle

Pour afficher des informations sur votre licence :

1. Connectez-vous au Control Center avec votre e-mail et le mot de passe que vous avez reçu par e-mail.
2. Cliquez sur votre nom d'utilisateur dans l'angle supérieur droit de la console et sélectionnez **Mon Entreprise**.
3. Consultez des informations sur la licence actuelle dans la section **Licence**. Vous pouvez également cliquer sur le bouton **Vérifier** et attendre que le Control Center récupère les dernières informations sur la clé de licence actuelle.

5.2. Installer la protection des postes de travail

Selon la configuration de la machine et l'environnement de réseau, vous pouvez choisir d'installer uniquement les agents de sécurité ou d'utiliser également un [Security Server](#). Dans ce dernier cas, vous devez d'abord installer Security Server, puis les agents de sécurité.

Il est recommandé d'utiliser Security Server si les machines ont peu de ressources matérielles.



Important

Seul Bitdefender Endpoint Security Tools supportent une connexion à Security Server. Pour plus d'informations, reportez-vous à « [L'architecture de GravityZone](#) » (p. 7).

5.2.1. Installation de Security Server

Security Server est une machine virtuelle dédiée qui déduplique et centralise une grande partie de la fonctionnalité antimalware des clients antimalwares, en agissant en tant que serveur d'analyse.

Vous devez installer Security Server sur un ou plusieurs hôtes en fonction du nombre de machines virtuelles à protéger.

Vous devez prendre en compte le nombre de machines virtuelles protégées, les ressources disponibles pour Security Server sur les hôtes, ainsi que la connectivité réseau entre le Security Server et les machines virtuelles protégées.

L'agent de sécurité installé sur les machines virtuelles se connecte au Security Server via TCP/IP, à l'aide des informations configurées lors de l'installation ou via une politique.

Le package du Security Server peut être téléchargé à partir du Control Center dans différents formats compatibles avec les principales plateformes de virtualisation.

Téléchargement des packages d'installation du Security Server :

Pour télécharger des packages d'installation du Security Server :

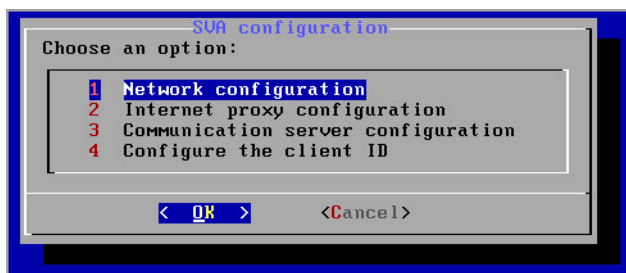
1. Accédez à la page **Réseau > Packages**.
2. Sélectionnez le package du Security Server par défaut.
3. Cliquez sur le bouton **+ Télécharger** en haut du tableau et sélectionnez le type de package dans le menu.
4. Enregistrez le package sélectionné à l'emplacement de votre choix.

Déploiement des packages d'installation du Security Server :

Lorsque vous avez le package d'installation, déployez-le sur l'hôte à l'aide de l'outil de déploiement de machines virtuelles de votre choix.

Après le déploiement, configurez le Security Server de la façon suivante :

1. Accédez à la console de l'appliance à partir de votre outil de gestion de la virtualisation (par exemple, vSphere Client). Vous pouvez également vous connecter à l'appliance via SSH.
2. Connectez-vous avec les identifiants par défaut.
 - Nom d'utilisateur : `root`
 - Mot de passe : `sve`
3. Exécutez la commande `sva-setup`. Vous accédez à l'interface de configuration de l'appliance.



Interface de configuration de Security Server (menu principal)

Pour naviguer entre les menus et les options, utilisez l'Onglet et les flèches.
Pour sélectionner une option spécifique, appuyez sur **Entrée**.

4. Configurez les paramètres du réseau.

Security Server utilise le protocole TCP/IP pour communiquer avec les autres composants de GravityZone. Vous pouvez configurer l'appliance afin qu'elle obtienne automatiquement les paramètres du réseau à partir du serveur DHCP ou configurer manuellement les paramètres du réseau, comme indiqué ci-après :

- a. Dans le menu principal, sélectionnez **Configuration du réseau**.
- b. Sélectionnez l'interface réseau.
- c. Sélectionnez le mode de configuration de l'IP :
 - **DHCP**, si vous souhaitez que le Security Server obtienne automatiquement les paramètres réseau du serveur DHCP.
 - **Statique**, si un serveur DHCP est absent ou si une réservation de l'IP d'une appliance a été effectuée sur le serveur DHCP. Dans ce cas, vous devez configurer manuellement les paramètres du réseau.
 - i. Indiquez le nom d'hôte, l'adresse IP, le masque de réseau, la passerelle et les serveurs DNS dans les champs correspondants.
 - ii. Sélectionnez **OK** pour enregistrer les modifications.



Note

Si vous êtes connecté à l'appliance via un client SSH, modifier les paramètres réseau fermera immédiatement votre session.

5. Configurez les paramètres du proxy.

Si un serveur proxy est utilisé dans le réseau, vous devez indiquer ses informations afin que le Security Server puisse communiquer avec GravityZone Control Center.



Note

Seuls les proxy avec l'authentification de base sont pris en charge.

- a. Dans le menu principal, sélectionnez **Configuration du proxy Internet**.

- b. Indiquez le nom d'hôte, le nom d'utilisateur, le mot de passe et le domaine dans les champs correspondants.
 - c. Sélectionnez **OK** pour enregistrer les modifications.
6. Configurez l'adresse du serveur de communication.
- a. Dans le menu principal, sélectionnez **Configuration du serveur de communication**.
 - b. Indiquez l'une des adresses suivantes pour le Serveur de Communication :
 - `https://cloud-ecs.gravityzone.bitdefender.com:443`
 - `https://cloudgz-ecs.gravityzone.bitdefender.com:443`



Important

Cette adresse doit être la même que celle qui apparaît dans les paramètres de politique Control Center. Vous vérifiez le lien, allez sur la page **Politiques**, ajoutez ou ouvrez une politique personnalisée, allez dans la section **Général > Communication > Affectation des serveurs de communication aux postes de travail** et saisissez le nom de serveur Communication dans le champs de la colonne. Le bon serveur apparaîtra dans les résultats de recherche.

- c. Sélectionnez **OK** pour enregistrer les modifications.
7. Configurez l'ID du client.
- a. Dans le menu principal, sélectionnez **Configurer l'ID du client**.
 - b. Indiquez l'ID de la société.

L'ID est constitué de 32 caractères, et figure sur la page des détails de l'entreprise dans Control Center.
 - c. Sélectionnez **OK** pour enregistrer les modifications.

5.2.2. Installation des agents de sécurité

Pour protéger vos endpoints physiques et virtuels, vous devez installer un agent de sécurité sur chacun d'entre eux. Outre la gestion de la protection sur l'endpoint local, l'agent de sécurité communique également avec Control Center pour recevoir les commandes de l'administrateur et envoyer les résultats de ses actions.

Pour en savoir plus à propos des agents de sécurité, veuillez vous référer à « [Agents de sécurité](#) » (p. 7).

Sur les machines Windows et Linux, l'agent de sécurité peut avoir deux rôles, et vous pouvez l'installer comme suit :

1. En tant que simple agent de sécurité pour vos endpoints.
2. En tant que **Relais**, servant d'agent de sécurité et de serveur de communication, proxy et de mise à jour aux autres endpoints du réseau.



Avertissement

- Le premier endpoint sur lequel vous installez la protection doit avoir le rôle Relais, car vous ne pourriez alors plus installer à distance l'agent de sécurité sur d'autres endpoints du même réseau.
- L'endpoint Relais doit être allumé et en ligne pour que les agents connectés communiquent avec Control Center.

Vous pouvez installer les agents de sécurité sur des endpoints physiques et virtuels **en exécutant des packages d'installation localement** ou **en exécutant des tâches d'installation à distance** depuis Control Center.

Merci de lire attentivement et de respecter les instructions avant de préparer l'installation.

En mode normal, les agents de sécurité ont une interface utilisateur minimale. Il permet uniquement aux utilisateurs de consulter l'état de la protection et d'exécuter des tâches de sécurité de base (mises à jour et analyses) sans fournir d'accès aux paramètres.

Si l'administrateur réseau l'a permis via le package d'installation et la politique de sécurité, l'agent de sécurité peut également s'exécuter en **mode Power User** sur les endpoints Windows, ce qui autorise l'utilisateur de l'endpoint à afficher et modifier les paramètres de politique. Cependant, l'administrateur de Control Center peut toujours contrôler quels paramètres de politique s'appliquent, en écrasant le mode Power User.

Par défaut, la langue d'affichage de l'interface utilisateur sur les endpoints Windows protégés est définie au moment de l'installation en fonction de la langue de votre compte GravityZone.

Sur Mac, la langue d'affichage de l'interface utilisateur est définie au moment de l'installation en fonction de la langue du système d'exploitation de l'endpoint. Sur Linux, l'agent de sécurité ne possède pas d'interface utilisateur localisée.

Pour installer l'interface utilisateur dans une autre langue sur certains endpoints Windows, vous pouvez créer un package d'installation et définir la langue de votre

choix dans ses options de configuration. Cette option n'est pas disponible pour les endpoints Mac et Linux. Pour plus d'informations sur la création de packages d'installation, reportez-vous à « [Créer des packages d'installation](#) » (p. 40).

Préparation de l'Installation

Avant l'installation, suivez ces étapes préparatoires pour vous assurer de son bon déroulement :

1. Vérifiez que les endpoints cibles disposent de la [configuration système minimale requise](#). Pour certains endpoints, vous pouvez avoir besoin d'installer le dernier service pack du système d'exploitation disponible ou de libérer de l'espace disque. Établissez une liste d'endpoints ne correspondant pas aux critères nécessaires afin de pouvoir les exclure de l'administration.
2. Désinstallez (ne vous contentez pas de désactiver) tout logiciel antimalware ou de sécurité Internet sur les endpoints cibles. Faire fonctionner simultanément l'agent de sécurité avec d'autres logiciels de sécurité installés sur un endpoint peut affecter leur fonctionnement et causer d'importants problèmes avec le système.

Un grand nombre de programmes de sécurité incompatibles sont automatiquement détectés et supprimés au moment de l'installation.

Pour plus d'informations et pour vérifier la liste du logiciel de sécurité détecté par Bitdefender Endpoint Security Tools pour les systèmes d'exploitation Windows actuels, reportez-vous à [cet article de la base de connaissances](#).

Pour vérifier la liste du logiciel de sécurité détecté par Bitdefender Endpoint Security Tools pour les anciens systèmes d'exploitation Windows, reportez-vous à [cet article de la base de connaissances](#).



Important

Si vous voulez déployer l'agent de sécurité sur un ordinateur sur lequel Bitdefender Antivirus for Mac 5.X est déjà installé, vous devez d'abord désinstaller celui-ci manuellement. Pour les instructions, veuillez vous référer à [l'article de support](#).

3. L'installation requiert des privilèges d'administration et un accès à Internet. Si les endpoints cibles sont dans un domaine Active Directory, vous devriez utiliser des identifiants d'administrateur de domaine pour une installation à distance. Autrement, assurez-vous de disposer des identifiants nécessaires pour tous les endpoints.
4. Les endpoints doivent disposer d'une connectivité à Control Center.

5. Il est recommandé d'utiliser une adresse IP statique pour le serveur relais. Si vous ne configurez pas d'adresse IP statique, utilisez le nom d'hôte de la machine.
6. Lors du déploiement de l'agent via un relais Linux, les conditions additionnelles suivantes doivent être respectées :
 - L'endpoint relais doit avoir installé le package Samba (`smbclient`) version 4.1.0 ou supérieure et la procédure binaire/commande `net` pour déployer des agents Windows.

**Note**

La procédure binaire/commande `net` est habituellement contenue dans les packages `samba-client` et/ou `samba-common`. Sur certaines distributions Linux (telles que CentOS 7.4), la commande `net` est uniquement installée lors de l'installation de la suite Samba complète (Common + Client + Server). Assurez-vous que la commande `net` est disponible sur votre endpoint relais.

- Le Partage administratif et le Partage réseau des endpoints cibles sous Windows doivent être activés.
 - SSH doit être activé pour les endpoints Linux et Mac cibles.
7. À partir de macOS High Sierra (10.13), après avoir installé Endpoint Security for Mac manuellement ou à distance, les utilisateurs sont invités à approuver les extensions de noyau Bitdefender sur leurs ordinateurs. Tant que les utilisateurs n'auront pas approuvé les extensions de noyau Bitdefender, certaines fonctionnalités de Endpoint Security for Mac ne fonctionneront pas. Afin d'éviter l'intervention des utilisateurs, vous pouvez pré-approuver les extensions de noyau Bitdefender en les inscrivant sur une liste blanche à l'aide d'un outil de gestion des appareils mobiles.

Installation locale

Il est possible d'installer l'agent de sécurité sur un endpoint en exécutant un package d'installation en local.

Vous pouvez créer et gérer des packages d'installation sur la page **Réseau > Packages**.

| Bitdefender GravityZone | | | | | | |
|--|---|---------------------------|--------------------|--|----------------------------|------------------------------|
| <div> <div>Tableau de bord</div> <div> <div>Ajouter</div> <div>Télécharger</div> <div>Envoyer le lien de téléchargement</div> <div>Supprimer</div> <div>Actualiser</div> </div> </div> | | | | | | |
| Réseau | | | | | | |
| Packages | <input type="checkbox"/> <div> <div>Nom</div> <div>Type</div> <div>Langue</div> <div>Description</div> <div>État</div> <div>Entreprise</div> </div> | | | | | |
| Tâches | <input type="checkbox"/> <div>Appliance virtuelle du serve...</div> | <div>Serveur de ...</div> | <div>English</div> | <div>Security for Virtualized Environments Security Server</div> | <div>Prêt à téléc...</div> | <div>GravityZone Cloud</div> |
| Politiques | <input type="checkbox"/> <div>eps</div> | <div>BEST</div> | <div>English</div> | <div>en</div> | <div>Prêt à téléc...</div> | <div>COMP</div> |

La page Packages



Avertissement

- La première machine sur laquelle vous installez la protection doit avoir le rôle Relais pour que vous puissiez déployer l'agent de sécurité sur les autres endpoints du réseau.
- La machine avec le rôle Relais doit être allumée et en ligne pour que les clients communiquent avec Control Center.

Une fois le premier client installé, il sera utilisé pour détecter d'autres endpoints du même réseau, à partir de la fonction Network Discovery. Pour plus d'informations sur la fonction Network Discovery, merci de vous référer à « [Fonctionnement de Network Discovery](#) » (p. 57).

Pour installer l'agent de sécurité en local sur un endpoint, procédez comme suit :

1. [Créez un package d'installation](#) en fonction de vos besoins.



Note

Cette étape n'est pas obligatoire si un package d'installation a déjà été créé pour le réseau sous votre compte.

2. [Téléchargez le package d'installation](#) sur l'endpoint cible.

Vous pouvez également [envoyer les liens de téléchargement du package d'installation par e-mail](#) à plusieurs utilisateurs de votre réseau.

3. [Exécutez le package d'installation](#) sur l'endpoint cible.

Créer des packages d'installation

Pour créer un package d'installation :

1. Connectez-vous et identifiez-vous sur le Control Center.
2. Accédez à la page **Réseau > Packages**.

3. Cliquez sur le bouton **+ Ajouter** en haut du tableau. Une fenêtre de configuration s'affichera.

Nouveau Package Endpoint

Général

Nom: * relay

Description:

Langue: Français

Entreprise: PABD

Modules:

- ☒ Antimalware
- ☒ Advanced Threat Control
- ☒ Pare-feu
- ☒ Contrôle de contenu
- ☒ Contrôle des appareils
- ☐ Power User

Rôles:

- ☒ Relais
- ☐ Protection Exchange

Mode d'analyse

Créer des packages - Options

4. Indiquez un nom et une description explicites pour le package d'installation que vous souhaitez créer.
5. Dans le champ **Langue**, sélectionnez la langue souhaitée pour l'interface du client.



Note

Cette option n'est disponible que pour les systèmes d'exploitation Windows.

6. Sélectionnez les modules de protection que vous voulez installer.



Note

Seuls les modules pris en charge pour chaque système d'exploitation seront installés. Pour plus d'informations, reportez-vous à « [Agents de sécurité](#) » (p. 7).

7. Sélectionnez le rôle de l'endpoint cible :

- **Relais**, pour créer le package d'un endpoint avec le rôle Relais. Pour plus d'informations, reportez-vous à « [Relais](#) » (p. 9)



Avertissement

Le rôle Relay n'est pas pris en charge sur les anciens systèmes d'exploitation. Pour plus d'informations, reportez-vous à « [Systèmes d'exploitation pris en charge](#) » (p. 16).

- **Serveur cache du module Gestion des patchs**, pour faire du Relais un serveur interne pour la distribution des patchs logiciels. Ce rôle est affiché lorsque le rôle de relais est sélectionné. Pour plus d'informations, reportez-vous à « [Serveur de mise en cache des patchs](#) » (p. 10)
 - **Protection Exchange**, pour installer les modules de protection pour les Serveurs Microsoft Exchange Servers, y compris l'antimalware, l'antispam, le filtrage de contenu et des pièces jointes pour le trafic de messagerie Exchange et l'analyse antimalware à la demande des bases de données Exchange. Pour plus d'informations, reportez-vous à « [Installer la protection Exchange](#) » (p. 61).
8. **Mode d'analyse.** Choisissez la technologie d'analyse qui correspond le mieux à votre environnement réseau et aux ressources de vos endpoints. Vous pouvez définir le mode d'analyse en sélectionnant l'un des types suivants :
- **Automatique.** Dans ce cas, l'agent de sécurité détectera automatiquement la configuration de l'endpoint et adaptera la technologie d'analyse en conséquence :
 - Analyse centralisée dans le cloud public ou privé (avec Security Server), avec une analyse hybride de secours (Moteurs légers) pour les ordinateurs physiques peu performants et pour les machines virtuelles. Ce cas nécessite le déploiement d'au moins un Security Server dans le réseau.
 - Analyse locale (avec des moteurs complets) pour les ordinateurs physiques très performants.



Note

On considère comme ordinateurs à faibles performances ceux ayant une fréquence de processeur inférieure à 1,5 GHz, ou moins de 1 Go de mémoire vive.

- **Paramètres.** Vous pouvez dans ce cas configurer le mode d'analyse en choisissant entre plusieurs technologies d'analyse pour les machines physiques et virtuelles :
 - Analyse centralisée dans le cloud public ou privé (avec Security Server), avec en solution de secours* une analyse locale (avec des moteurs complets) ou une analyse hybride (avec des moteurs légers).
 - Analyse hybride (avec des moteurs légers)
 - Analyse locale (avec des moteurs complets)

Le mode d'analyse par défaut des instances EC2 est l'analyse locale (le contenu de sécurité est stockées dans l'agent de sécurité installé et l'analyse est exécutée localement sur la machine). Pour analyser vos instances EC2 à l'aide d'un Security Server, vous devez configurer le package d'installation de l'agent de sécurité et la politique appliquée en conséquence.

Le mode d'analyse par défaut des machines virtuelles Microsoft Azure est l'analyse locale (le contenu de sécurité est stocké dans l'agent de sécurité installé et l'analyse est exécutée localement sur la machine). Pour analyser vos machines virtuelles Microsoft Azure à l'aide d'un Security Server, vous devez configurer le package d'installation de l'agent de sécurité et la politique appliquée en conséquence.

* Lorsqu'on utilise une analyse à double moteur, si le premier moteur n'est pas disponible, le moteur de secours est utilisé. La consommation des ressources et l'utilisation du réseau dépendront des moteurs utilisés.

Pour plus d'informations sur les technologies d'analyse disponibles référez-vous à « [Moteurs d'analyse](#) » (p. 3)





Avertissement


Endpoint Security (agent héritage) ne supporte qu'une analyse locale.

9. Lorsque vous personnalisez les moteurs d'analyse à l'aide de l'analyse Cloud Public ou Privé (Security Server), l'on vous demande de sélectionner les Security Server installés en local que vous souhaitez utiliser et de configurer leur priorité dans la section **Affectation du Security Server** :
 - a. Cliquez sur la liste de Security Server dans l'en-tête du tableau. La liste des Security Server détectés s'affiche.
 - b. Sélectionnez une entité.

- c. Cliquez sur le bouton  **Ajouter** de l'en-tête de la colonne **Actions**.

Le Security Server est ajouté à la liste.

- d. Procédez de la même façon pour ajouter plusieurs serveurs de sécurité, si possible. Vous pouvez dans ce cas configurer leur priorité à l'aide des flèches  vers le haut et  vers le bas se trouvant à droite de chaque élément. Lorsque le premier Security Server n'est pas disponible, le suivant est utilisé et ainsi de suite.

- e. Pour retirer un élément de la liste, cliquez sur le bouton  **Supprimer** correspondant en haut du tableau.

Vous pouvez choisir de crypter la connexion à Security Server en sélectionnant l'option **Utiliser SSL**.

10. Sélectionnez **Analyser avant l'installation** si vous souhaitez vous assurer que les machines sont saines avant d'y installer le client. Une analyse rapide dans le cloud sera réalisée sur les machines cibles avant de commencer l'installation.
11. Sur les endpoints Windows, Bitdefender Endpoint Security Tools est installé dans le répertoire d'installation par défaut. Sélectionnez **Utiliser le chemin d'installation personnalisé** si vous souhaitez installer Bitdefender Endpoint Security Tools à un emplacement différent. Dans ce cas, saisissez le chemin souhaité dans le champ correspondant. Utilisez les conventions Windows lorsque vous saisissez le chemin (par exemple, D:\folder). Si le dossier spécifié n'existe pas, il sera créé lors de l'installation.
12. Vous pouvez, si vous le souhaitez, définir un mot de passe pour empêcher les utilisateurs de supprimer la protection. Sélectionnez **Mot de passe de désinstallation** et indiquez le mot de passe souhaité dans les champs correspondants.
13. Si les endpoints cibles sont dans le Répertoire réseau sous **Groupes personnalisés**, vous pouvez choisir de les déplacer dans un dossier spécifié immédiatement après que le déploiement de l'agent de sécurité soit terminé.
Sélectionnez **Utiliser dossier personnalisé** et choisissez un dossier dans le tableau correspondant.
14. Sous la section **Système de déploiement**, sélectionnez l'entité à laquelle les endpoints cibles se connecteront pour installer et mettre à jour le client :
 - **Cloud Bitdefender**, si vous souhaitez mettre à jour les clients directement à partir d'Internet.

Dans ce cas, vous pouvez également définir les paramètres du proxy, si les endpoints cibles se connectent à Internet via un proxy. Dans ce cas, sélectionnez **Utiliser le proxy pour la communication** et saisissez les paramètres du proxy requis dans les champs ci-dessous.

- **Relais Endpoint Security**, si vous souhaitez connecter les endpoints à un client relais installé dans votre réseau. Toutes les machines avec le rôle relais détectés dans votre réseau apparaîtront dans le tableau ci-dessous. Choisissez la machine relais de votre choix. Les endpoints connectés communiqueront avec Control Center uniquement via le relais spécifié.



Important

Le port 7074 doit être ouvert pour que le déploiement via Bitdefender Endpoint Security Tools Relay fonctionne.

15. Cliquez sur **Enregistrer**.

Le nouveau package créé sera ajouté à la liste de packages.



Note

Les paramètres configurés dans un package d'installation s'appliqueront aux endpoints immédiatement après l'installation. Dès qu'une politique sera appliquée au client, les paramètres configurés dans la politique s'appliqueront et remplaceront certains paramètres du package d'installation (comme les serveurs de communication ou les paramètres du proxy).

Téléchargement de packages d'installation

Téléchargez les packages d'installation des agents de sécurité :

1. Identifiez-vous auprès de Control Center à partir de l'endpoint sur lequel vous souhaitez installer la protection.
2. Accédez à la page **Réseau > Packages**.
3. Sélectionnez le package d'installation que vous souhaitez télécharger.
4. Cliquez sur le bouton  **Télécharger** en haut du tableau et sélectionnez le type de programme d'installation que vous souhaitez utiliser. Deux types de fichiers d'installation sont disponibles :
 - **Programme de téléchargement** . Le downloader commence par télécharger le kit d'installation complet sur les serveurs cloud de Bitdefender avant de lancer l'installation. Il est peu volumineux et peut être exécuté à la fois sur

les systèmes 32 et 64 bits (ce qui facilite sa distribution). Il requiert par contre une connexion active à Internet.

- **Kit complet.** Les kits d'installation complets sont plus volumineux et doivent être exécutés sur le type de système d'exploitation spécifique.

Le kit complet est à utiliser pour installer la protection sur les endpoints avec une connexion Internet lente ou sans connexion. Téléchargez ce fichier sur un endpoint connecté à Internet puis transmettez-le à d'autres endpoints à l'aide de supports de stockage externes ou d'un partage réseau.



Note

Versions du kit complet disponibles :

- **OS Windows** : systèmes 32 et 64 bits
- **Anciennes versions du système d'exploitation Windows** : systèmes 32 bits et 64 bits
- **OS Linux** : systèmes 32 et 64 bits
- **macOS** : seulement les systèmes 64-bits

Veillez à utiliser la version adaptée au système sur lequel vous l'installez.

5. Enregistrez le fichier sur l'endpoint.



Avertissement


- L'exécutable du downloader ne doit pas être renommé car il ne pourra sinon plus télécharger les fichiers d'installation à partir du serveur de Bitdefender.

6. En outre, si vous avez choisi le programme de téléchargement, vous pouvez créer un package MSI pour les endpoints Windows. Pour plus d'informations, veuillez consulter cet [article KB](#).

Envoyer les liens de téléchargement des packages d'installation par e-mail

Vous pouvez avoir besoin d'informer rapidement d'autres utilisateurs qu'un package d'installation peut être téléchargé. Dans ce cas, suivez les étapes décrites ci-après :

1. Accédez à la page **Réseau > Packages**.
2. Sélectionnez le package d'installation que vous souhaitez.

3. Cliquez sur le bouton  **Envoyer le lien de téléchargement** en haut du tableau. Une fenêtre de configuration s'affichera.
4. Indiquez l'adresse e-mail de chaque utilisateur à qui vous souhaitez envoyer le lien de téléchargement du package d'installation. Appuyez sur **Entrée** après chaque e-mail.
Veuillez vérifier que chaque adresse e-mail indiquée est valide.
5. Si vous souhaitez afficher les liens de téléchargement avant de les envoyer par e-mail, cliquez sur le bouton **Liens d'installation**.
6. Cliquez sur **Envoyer**. Un e-mail contenant le lien d'installation est envoyé à chaque adresse e-mail spécifiée.

Exécution de packages d'installation

Pour que l'installation fonctionne, le package d'installation doit être lancé à l'aide des privilèges administrateur.

Le package s'installe différemment sur chaque système d'exploitation, comme suit :

- Sur les systèmes d'exploitation Windows et macOS :
 1. Sur l'endpoint cible, téléchargez le dossier d'installation à partir de la Control Center ou copiez-le à partir d'un réseau de partage.
 2. Si vous avez téléchargé le kit complet, extraire les fichiers à partir des archives.
 3. Exécutez le Fichier Exécutable.
 4. Suivez les instructions à l'écran.



Note

Sur macOS, après avoir installé Endpoint Security for Mac, les utilisateurs sont invités à approuver les extensions de noyau Bitdefender sur leurs ordinateurs. Tant que les utilisateurs n'auront pas approuvé les extensions de noyau Bitdefender, certaines fonctionnalités de l'agent de sécurité ne fonctionneront pas. Pour plus d'informations, consultez [cet article de la base de connaissances](#) :

- Sur les systèmes d'exploitation Linux :
 1. Connectez-vous et identifiez-vous sur le Control Center.

2. Téléchargez ou copiez le package d'installation sur l'endpoint cible.
3. Si vous avez téléchargé le kit complet, extraire les fichiers à partir des archives.
4. Obtenez des privilèges root, en exécutant la commande `sudo su`.
5. Changez les permissions du dossier d'installation afin de pouvoir l'exécuter :

```
# chmod +x installer
```

6. Exécutez le fichier d'installation :

```
# ./installer
```

7. Pour vérifier que l'agent a bien été installé sur l'endpoint, exécutez cette commande :

```
$ service bd status
```

Une fois l'agent de sécurité installé, l'endpoint apparaît comme étant administré dans Control Center (page **Réseau**) après quelques minutes.



Important

Si vous utilisez le système VMware Horizon View Persona Management, nous vous conseillons de configurer la politique de groupe Active Directory de manière à exclure les processus suivants de Bitdefender (sans indiquer le chemin complet) :

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationsservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Ces exclusions doivent s'appliquer tant que l'agent de sécurité s'exécute sur le endpoint. Pour plus d'informations, consultez cette [page de la documentation VMware Horizon](#).

Installation à distance

Control Center vous permet d'installer à distance l'agent de sécurité sur les endpoints détectés dans le réseau à l'aide des tâches d'installation.

Une fois que vous avez installé en local le premier client avec le rôle relais, quelques minutes peuvent être nécessaires pour que les autres endpoints du réseau deviennent visibles dans Control Center. Vous pouvez alors installer à distance l'agent de sécurité sur les endpoints que vous administrez à l'aide de tâches d'installation à partir de Control Center.

Bitdefender Endpoint Security Tools comprend un mécanisme de découverte du réseau automatique qui permet de détecter d'autres endpoints du même réseau. Les endpoints détectés apparaissent comme étant **non administrés** sur la page **Réseau**.

Pour activer la découverte du réseau, Bitdefender Endpoint Security Tools doit être déjà installé sur au moins un endpoint du réseau. Cet endpoint sera utilisé pour analyser le réseau et installer Bitdefender Endpoint Security Tools sur les endpoints non protégés.

Pour plus d'informations sur la fonction Network Discovery, merci de vous référer à « [Fonctionnement de Network Discovery](#) » (p. 57).

Configuration requise pour l'installation à distance

Pour que l'installation à distance fonctionne :

- Bitdefender Endpoint Security Tools Relay doit être installé dans votre réseau.
- Sous Windows:
 - Le partage administratif `admin$` doit être activé. Configurez chaque poste de travail cible afin qu'il n'utilise pas le partage de fichiers avancé.
 - Configurer le Contrôle de compte d'utilisateur (UAC) en fonction du système d'exploitation présent sur les endpoints cibles. Si les endpoints sont dans un domaine Active Directory, vous pouvez utiliser une politique de groupe pour configurer le Contrôle de compte d'utilisateur. Pour plus d'informations, consultez [cet article de la base de connaissances](#) :

- Désactivez le pare-feu Windows ou configurez-le pour autoriser le trafic au moyen du protocole de Partage de fichiers et d'imprimantes.

**Note**

Le déploiement à distance ne fonctionne que sur les systèmes d'exploitation modernes, à partir de Windows 7 / Windows Server 2008 R2, pour lesquels Bitdefender propose une assistance complète. Pour plus d'informations, reportez-vous à « [Systèmes d'exploitation pris en charge](#) » (p. 16).

- Sur Linux : SSH doit être activé.
- Sur macOS : la connexion à distance et le partage de fichiers doivent être activés.

Exécution de tâches d'installation à distance

Pour exécuter une tâche d'installation à distance :

1. Connectez-vous et identifiez-vous sur le Control Center.
2. Allez sur la page **Réseau**.
3. Sélectionnez le groupe souhaité dans le panneau de gauche. Les entités contenues dans le groupe sélectionné apparaissent dans le tableau du panneau de droite.

**Note**

Vous pouvez aussi appliquer des filtres pour afficher uniquement les endpoints non administrés. Cliquez sur le menu **Filtres** et sélectionnez les options suivantes : **Non administré** dans l'onglet **Sécurité** et **Tous les éléments de manière récurrente** dans l'onglet **Profondeur**.

4. Sélectionnez les entités (endpoints ou groupes d'endpoints) sur lesquelles vous souhaitez installer la protection.
5. Cliquez sur le bouton **Tâches** en haut du tableau et sélectionnez **Installer**
L'assistant **Installer le client** apparaît.

Installer le client

Options

☒ Maintenant

☐ Planifié

☐ Redémarrage automatique

Admin. des authentifications

| Utilisateur | Mot de passe | Description | Action |
|--------------------------------|--------------|-------------|---|
| <input type="checkbox"/> admin | ***** | | <input checked="" type="button" value="X"/> |

Première page ← Page 1 de 1 → Dernière page 20 1 éléments

Installer Bitdefender Endpoint Security Tools à partir du menu des Tâches

6. Configurez l'heure d'installation dans la section **Options** :

- **Maintenant**, afin de lancer immédiatement le déploiement.
- **Planifié**, afin de planifier un déploiement à intervalle régulier. Dans ce cas, sélectionnez le temps d'intervalle désiré (par heure, par jour ou par semaine) et configurez le selon vos besoin.



Note

Par exemple, lorsque certaines opérations sont nécessaires sur une machine cible avant l'installation du client (comme désinstaller d'autres logiciels et redémarrer l'OS), vous pouvez planifier les tâches de déploiement afin qu'elle s'exécute toutes les deux heures. La tâche va commencer sur chacune des cibles toutes les deux heures jusqu'à ce que déploiement soit un succès.

7. Si vous souhaitez que les endpoints cibles redémarrent automatiquement pour terminer l'installation, sélectionnez **Redémarrer automatiquement (si nécessaire)**.
8. Dans la section **Admin. des authentifications**, indiquez les identifiants d'administration requis pour l'authentification à distance sur les endpoints sélectionnés. Vous pouvez ajouter les identifiants en saisissant l'utilisateur et le mot de passe de tous les systèmes d'exploitation cibles.



Important

Pour les postes de travail Windows 8.1, vous devez indiquer les identifiants du compte administrateur intégré ou d'un compte administrateur de domaine. Pour en savoir plus, reportez-vous à [cet article KB](#).

Pour ajouter les identifiants du système d'exploitation requis :


- a. Saisissez le nom d'utilisateur et le mot de passe d'un compte administrateur dans les champs correspondants à partir de l'en-tête.

Si les ordinateurs sont dans un domaine, il suffit d'indiquer les identifiants de l'administrateur du domaine.

Utilisez les conventions Windows lorsque vous saisissez le nom (d'un compte utilisateur).

- pour les machines Active Directory, utilisez ces syntaxes : `username@domain.com` and `domain\username`. Pour vous assurer que les identifiants saisis fonctionneront, ajoutez-les dans les deux formes (`username@domain.com` et `domain\username`).
- Pour les machines Workgroup, il suffit de saisir le nom d'utilisateur, sans le nom du groupe de travail.

Vous pouvez également ajouter une description qui vous aidera à identifier chaque compte plus facilement.

- b. Cliquez sur le bouton  **Ajouter**. Le compte est ajouté à la liste des identifiants.



Note

Les identifiants spécifiés sont enregistrés automatiquement dans votre [Administrateur des authentifications](#) afin que vous n'ayez pas à les saisir la prochaine fois. Pour accéder à l'Administrateur des authentifications, pointez simplement sur votre nom d'utilisateur dans l'angle supérieur droit de la console.



Important

Si les identifiants indiqués ne sont pas valides, le déploiement du client échouera sur les endpoints correspondants. Veillez à mettre à jour les identifiants du système d'exploitation saisis dans l'Administrateur des authentifications lorsque ceux-ci sont modifiés sur les endpoints cibles.

9. Cochez les cases correspondant aux comptes que vous souhaitez utiliser.

**Note**

Un message d'avertissement s'affiche tant que vous n'avez sélectionné aucun identifiant. Cette étape est obligatoire pour installer à distance l'agent de sécurité sur les endpoints.

10. Sous la section **Système de déploiement**, configurez le relais auquel les endpoints cibles se connecteront pour installer et mettre à jour le client :

- Toutes les machines avec le rôle relais détectées dans votre réseau apparaîtront dans le tableau disponible sous la section **Système de déploiement**. Chaque nouveau client doit être connecté à au moins un client relais du même réseau, qui servira de serveur de communication et de mise à jour. Sélectionnez le relais que vous souhaitez associer aux endpoints cibles. Les endpoints connectés communiqueront avec Control Center uniquement via le relais spécifié.

**Important**

Le port 7074 doit être ouvert pour que le déploiement via l'agent relais fonctionne.

Système de déploiement

Système de déploiement: Relais Endpoint Security

| Nom | IP | Nom/IP du serveur personn... | Étiquette |
|-----------|---------------|------------------------------|-----------|
| MASTER-PC | 10.10.127.162 | | N/D |

Première page ← Page 1 de 1 → Dernière page 20 1 éléments

- Si les endpoints cibles communiquent avec l'agent relais via proxy, vous avez également besoin de définir les paramètres du proxy. Dans ce cas, sélectionnez **Utiliser le proxy pour la communication** et saisissez les paramètres du proxy requis dans les champs ci-dessous.
11. Vous devez sélectionner un package d'installation pour le déploiement actuel. Cliquez sur la liste **Utiliser le package** et sélectionnez le package d'installation de votre choix. Vous y trouverez tous les packages d'installation créés pour

vosre compte ainsi que le package d'installation disponible par défaut avec Control Center.

12. Si besoin, vous pouvez modifier certains paramètres du package d'installation sélectionné en cliquant sur le bouton **Personnalisé** à côté du champ **Utiliser le package**.

Les paramètres du package d'installation apparaîtront ci-dessous et vous pouvez effectuer toutes les modifications dont vous avez besoin. Pour plus d'informations sur la modification des packages d'installation référez-vous à « [Créer des packages d'installation](#) » (p. 40).

Si vous souhaitez enregistrer les modifications en tant que nouveau package, sélectionnez l'option **Enregistrer en tant que package** en bas de la liste des paramètres du package et indiquez un nom pour le nouveau package d'installation.

13. Cliquez sur **Enregistrer**. Une message de confirmation s'affichera.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**.



Important

Si vous utilisez le système VMware Horizon View Persona Management, nous vous conseillons de configurer la politique de groupe Active Directory de manière à exclure les processus suivants de Bitdefender (sans indiquer le chemin complet) :

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationsservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Ces exclusions doivent s'appliquer tant que l'agent de sécurité s'exécute sur le endpoint. Pour plus d'informations, consultez cette [page de la documentation VMware Horizon](#).

Préparation des systèmes Linux pour l'analyse à l'accès

Bitdefender Endpoint Security Tools pour Linux intègre des fonctionnalités d'analyse à l'accès qui fonctionnent avec des distributions et des versions de noyaux spécifiques. Pour en apprendre plus, consultez la [configuration recommandée](#).

Vous apprendrez ensuite comment compiler manuellement le module DazukoFS.

Compiler manuellement le module DazukoFS

Veillez suivre les étapes suivantes pour compiler DazukoFS pour la version Kernel du système puis chargez le module :

1. Téléchargez les headers du kernel correspondant.

- Sur les systèmes **Ubuntu**, lancez cette commande :

```
$ sudo apt-get install linux-headers-`uname -r`
```

- Sur les systèmes **RHEL/CentOS**, lancez cette commande :

```
$ sudo yum install kernel-devel kernel-headers-`uname -r`
```

2. Sur les systèmes **Ubuntu**, vous avez besoin de `build-essential` :

```
$ sudo apt-get install build-essential
```

3. Copiez et décompressez le code source DazukoFS dans un répertoire favori :

```
# mkdir temp
# cd temp
# cp /opt/BitDefender/share/modules/dazukofs/dazukofs-source.tar.gz
# tar -xzf dazukofs-source.tar.gz
# cd dazukofs-3.1.4
```

4. Compilez le module :

```
# make
```

5. Installez et chargez le module :

```
# make dazukofs_install
```

Conditions requises à l'utilisation de l'analyse à l'accès avec DazukoFS

Pour que DazukoFS et l'analyse à l'accès fonctionnent ensemble, différentes conditions doivent être remplies. Veuillez vérifier que l'une des affirmations ci-dessous s'applique à votre système Linux et suivez les recommandations pour éviter les problèmes.

- La politique SELinux doit être désactivée ou réglée sur **permissive**. Pour consulter et ajuster la configuration de la politique SELinux, éditez le fichier `/etc/selinux/config`.
- Bitdefender Endpoint Security Tools est compatible exclusivement avec la version de DazukoFS incluse dans le package d'installation. Si DazukoFS est déjà installé sur le système, supprimez-le avant d'installer Bitdefender Endpoint Security Tools.
- DazukoFS supporte certaines versions de noyau. Si le package DazukoFS fourni avec Bitdefender Endpoint Security Tools n'est pas compatible avec la version du noyau du système, le module ne pourra pas se charger. Vous pouvez dans ce cas mettre à jour le noyau vers la version supportée ou recompiler le module DazukoFS pour votre version de noyau. Le package DazukoFS se trouve dans le répertoire d'installation de Bitdefender Endpoint Security Tools :

`/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz`

- Lors du partage de fichiers à l'aide de serveurs dédiés tels que NFS, UNFSv3 ou Samba, vous devez lancer les services dans l'ordre suivant :

1. Activez l'analyse à l'accès par politique à partir de Control Center.

Pour plus d'informations, veuillez vous référer au Guide Administrateur de GravityZone.

2. Lancez le service de partage réseau.

Pour NFS :

```
# service nfs start
```

Pour UNFSv3 :

```
# service unfs3 start
```

Pour Samba :

```
# service smb start
```

**Important**

Pour le service NFS, DazukoFS est compatible uniquement avec le serveur NFS User Server.

Fonctionnement de Network Discovery

Outre l'intégration à Active Directory, GravityZone inclut également un mécanisme de découverte du réseau automatique conçu pour détecter les ordinateurs du groupe de travail.

GravityZone s'appuie sur le service **Explorateur d'ordinateurs de Microsoft** et sur l'outil **NBTscan** pour réaliser la découverte du réseau.

Le service Explorateur d'ordinateurs est une technologie de réseau utilisée par les ordinateurs Windows pour maintenir des listes actualisées de domaines, groupes de travail et les ordinateurs qui s'y trouvent et pour fournir ces listes aux ordinateurs clients sur demande. Les ordinateurs détectés dans le réseau par le service Explorateur d'ordinateurs peuvent être consultés en exécutant la commande **net view** dans une fenêtre d'invite de commandes.

```
Z:\>net view
Server Name      Remark
-----
\\SCIREFDL
\\SCIREFJM
\\SCIREFL
\\SCIREFMB
\\SCIREFMN
\\SCIREFMP
\\SCIREFYS
```

La commande Net view

L'outil NBTscan analyse les réseaux en utilisant NetBIOS. Il envoie des requêtes à chaque endpoint du réseau et récupère des informations telles que l'adresse IP, le nom NetBIOS et l'adresse MAC.

Pour activer la découverte automatique du réseau, Bitdefender Endpoint Security Tools Relay doit être déjà installé sur au moins un ordinateur du réseau. Cet ordinateur sera utilisé pour analyser le réseau.



Important

Le Control Center n'utilise pas d'informations du réseau d'Active Directory ou de la fonctionnalité Mappage réseau disponible dans Windows Vista et versions ultérieures. Le mappage réseau exploite une technologie de découverte du réseau différente : le protocole LLTD (Link Layer Topology Discovery).

Control Center n'est pas impliqué activement dans le fonctionnement du service Explorateur d'ordinateurs. Bitdefender Endpoint Security Tools demande uniquement au service Explorateur d'ordinateurs la liste des postes de travail et serveurs visibles dans le réseau (nommée liste de parcours) puis l'envoi à Control Center. Le Control Center gère la liste de parcours, en ajoutant les ordinateurs détectés récemment à sa liste de **Ordinateurs non administrés**. Les ordinateurs détectés auparavant ne sont pas supprimés après une nouvelle requête de découverte du réseau, vous devez donc exclure & supprimer manuellement les ordinateurs qui ne sont plus dans le réseau.

La requête initiale de la liste de parcours est effectuée par le premier Bitdefender Endpoint Security Tools installé dans le réseau.

- Si le relais est installé sur l'ordinateur d'un groupe de travail, seuls les ordinateurs de ce groupe de travail seront visibles dans Control Center.
- Si le relais est installé sur l'ordinateur d'un domaine, seuls les ordinateurs de ce domaine seront visibles dans Control Center. Les ordinateurs d'autres domaines peuvent être détectés s'il y a une relation d'approbation avec le domaine dans lequel le relais est installé.

Les requêtes de découverte du réseau suivantes sont réalisées régulièrement à chaque heure. Pour chaque nouvelle requête, Control Center divise l'espace des ordinateurs administrés en des zones de visibilité puis désigne un relais dans chaque zone pour effectuer la tâche. Une zone de visibilité est un groupe d'ordinateurs qui se détectent les uns les autres. Une zone de visibilité est généralement définie par un groupe de travail ou domaine, mais cela dépend de la topologie et de la configuration du réseau. Dans certains cas, une zone de visibilité peut consister en de multiples domaines et groupes de travail.

Si le relais sélectionné ne parvient pas à effectuer la requête, Control Center attend la requête suivante planifiée, sans choisir d'autre relais pour réessayer.

Pour une visibilité complète du réseau, le relais doit être installé sur au moins un ordinateur de chaque groupe de travail ou domaine de votre réseau. Idéalement,

Bitdefender Endpoint Security Tools devrait être installé sur au moins un ordinateur de chaque sous-réseau.

Plus d'informations sur le service Explorateur d'ordinateurs de Microsoft

Présentation rapide du service Explorateur d'ordinateurs :

- Fonctionne indépendamment d'Active Directory.
- Fonctionne exclusivement sur les réseaux IPv4 et opère de manière indépendante, dans les limites d'un groupe LAN (groupe de travail ou domaine). Une liste de parcours est établie et gérée pour chaque groupe LAN.
- Utilise généralement des diffusions de serveurs sans connexion pour communiquer entre les nœuds.
- Utilise NetBIOS sur TCP/IP (NetBT).
- Nécessite une résolution de noms NetBIOS. Il est recommandé d'avoir une infrastructure WINS (Windows Internet Name Service) opérationnelle dans le réseau.
- N'est pas activé par défaut dans Windows Server 2008 et 2008 R2.

Pour des informations détaillées sur le service Explorateur d'ordinateurs, consultez le sujet technique [Computer Browser Service](#) sur Microsoft Technet.

Configuration requise pour la découverte du réseau

Afin de découvrir tous les ordinateurs (serveurs et postes de travail) qui seront administrés depuis le Control Center, les conditions suivantes doivent être remplies :

- Les ordinateurs doivent faire partie d'un groupe de travail ou d'un domaine et être connectés via un réseau local IPv4. Le service Explorateur d'ordinateurs ne fonctionne pas sur les réseaux IPv6.
- Plusieurs ordinateurs dans chaque groupe LAN (groupe de travail ou domaine) doivent exécuter le service Explorateur d'ordinateurs. Les contrôleurs principaux de domaine doivent également exécuter le service.
- NetBIOS sur TCP/IP (NetBT) doit être activé sur les ordinateurs. Le pare-feu local doit autoriser le trafic NetBT.
- En cas d'utilisation d'un relais Linux pour découvrir d'autres endpoints Linux et Mac, vous devez soit installer Samba sur les endpoints cibles, ou les joindre

dans Active Directory et utiliser le DHCP. De cette manière, leur NetBIOS sera automatiquement configuré.

- Le partage de fichiers doit être activé sur les ordinateurs. Le pare-feu local doit autoriser le partage de fichiers.
- Une infrastructure WINS (Windows Internet Name Service) doit être installée et opérationnelle.
- Pour Windows Vista et les versions ultérieures, la découverte du réseau doit être activée (**Panneau de configuration > Centre Réseau et partage > Modifier les paramètres de partage avancés**).

Pour pouvoir activer cette fonctionnalité, les services suivants doivent d'abord être lancés :

- DNS Client
 - Function Discovery Resource Publication
 - SSDP Discovery
 - UPnP Device Host
- Dans les environnements avec plusieurs domaines, il est recommandé d'établir des relations d'approbation entre les domaines afin que les ordinateurs puissent accéder aux listes de parcours d'autres domaines.

Les ordinateurs à partir desquels Bitdefender Endpoint Security Tools demande le service Explorateur d'ordinateurs doivent être capables de résoudre les noms NetBIOS.



Note

Le mécanisme de découverte du réseau fonctionne pour tous les systèmes d'exploitation supportés, y compris les versions Windows Embedded, à condition de disposer de la configuration requise.

5.3. Installer le Chiffrement complet du disque

Le Chiffrement complet du disque dur doit être activé au moyen d'une clé de licence.

Pour plus d'informations sur les clés de licence, consultez « [Gestion des licences](#) » (p. 31).

Les agents de sécurité de Bitdefender prennent en charge le Chiffrement complet du disque dur à partir des versions 6.2.22.916 sur Windows et 4.0.0173876 sur Mac. Pour vérifier que les agents sont pleinement compatibles avec ce module, vous avez deux options :

- Installez les agents de sécurité avec le module de Chiffrement inclus.
- Utilisez la fonction **Reconfigurer**.

Pour plus d'informations sur l'utilisation du Chiffrement complet du disque dur sur votre réseau, consultez le chapitre **Politiques de sécurité > Chiffrement** du Guide de l'administrateur de GravityZone.

5.4. Installer la protection Exchange

Security for Exchange s'intègre automatiquement aux Serveurs Exchange, en fonction du rôle du serveur. Pour chaque rôle, seules les fonctionnalités compatibles sont installées, comme indiqué ici :

| Caractéristiques | Microsoft Exchange 2016/2013 | | Microsoft Exchange 2010/2007 | | |
|----------------------------------|--------------------------------|---------------------|--------------------------------|-----|---------------------|
| | Rôle serveur de transport Edge | Boîte de messagerie | Rôle serveur de transport Edge | Hub | Boîte de messagerie |
| Niveau du transport | | | | | |
| Filtrage | x | x | x | x | |
| Antimalware | x | x | x | x | |
| Filtrage antispam | x | x | x | x | |
| Filtrage du contenu | x | x | x | x | |
| Pièces jointes | | | | | |
| Base Exchange | | | | | |
| Analyse antimalware à la demande | | x | | | x |

5.4.1. Préparation de l'Installation

Avant d'installer Security for Exchange, veillez à respecter l'ensemble de la [configuration requise](#) ; Bitdefender Endpoint Security Tools pourrait sinon être installé sans le module de Protection Exchange.

Pour que le module Protection Exchange fonctionne correctement et pour éviter les conflits et les résultats indésirables, désinstallez tout agent antimalware ou de filtrage de messagerie.

Bitdefender Endpoint Security Tools détecte et désinstalle automatiquement la plupart des produits antimalware et désactive l'agent antimalware intégré à Exchange Server depuis la version 2013. Pour plus d'informations sur la liste des logiciels de sécurité détectés, référez-vous à [cet article KB](#).

Vous pouvez réactiver manuellement l'agent antimalware intégré à Exchange à tout moment, bien que cela ne soit pas recommandé.

5.4.2. Installation de la protection sur les serveurs Exchange

Pour protéger vos serveurs Exchange, vous devez installer Bitdefender Endpoint Security Tools avec le rôle Protection Exchange sur chacun d'entre eux.

Vous pouvez déployer Bitdefender Endpoint Security Tools sur les serveurs Exchange de différentes façons :

- Par une installation locale, en téléchargeant et en exécutant le package d'installation sur le serveur.
- Par une installation à distance, en exécutant une tâche **Installation**.
- À distance, en exécutant la tâche **Reconfigurer le client** si Bitdefender Endpoint Security Tools fournit déjà une protection du système de fichiers sur le serveur.

Pour les étapes d'installation détaillées, référez-vous à « [Installation des agents de sécurité](#) » (p. 36).

5.5. Installer la Protection de stockage

Security for Storage est un service de Bitdefender conçu pour protéger les serveurs de stockage en réseau (NAS) et les systèmes de partage de fichiers conformes à l'ICAP (Internet Content Adaptation Protocol). Pour consulter la liste des systèmes de partage de fichiers, voir « [Protection de stockage](#) » (p. 29).

Pour utiliser Security for Storage avec votre solution GravityZone

1. Installez et configurez au moins deux Security Server dans votre environnement pour faire office de serveurs CAP. Les Security Server de Bitdefender analysent les fichiers, envoient des verdicts aux systèmes de stockage et prennent les mesures appropriées si nécessaire. En cas de surcharge, le premier Security Server renvoie le surplus de données au second.

**Note**

En terme de bonnes pratiques, installez des Security Server dédiés à la protection de stockage de manière séparée des Security Server utilisés pour d'autres rôles, tels que l'analyse antimalware.

Pour en apprendre plus sur la procédure d'installation de Security Server, consultez la section **Installer Security Server** du présent guide.

2. Configurez le module **Protection de stockage** depuis les paramètres de politique GravityZone.

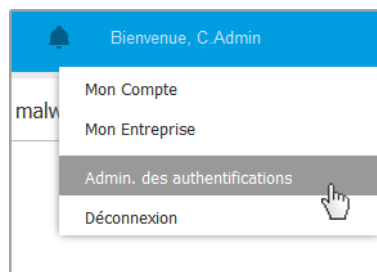
Pour en apprendre plus, consultez le Guide de l'administrateur GravityZone, chapitre **Politiques de sécurité > Ordinateurs et Machines virtuelles > Protection de stockage**.

Pour en apprendre plus sur la configuration et la gestion des serveurs ICAP sur un NAS ou système de partage de fichier particulier, consultez la documentation de la plateforme concernée.

5.6. Admin. des authentifications

L'Administrateur des authentifications vous aide à définir les identifiants requis pour l'authentification à distance sur les différents systèmes d'exploitation de votre réseau.

Pour ouvrir l'Administrateur des authentifications, cliquez sur votre nom d'utilisateur dans l'angle supérieur droit de la page et sélectionnez **Admin. des authentifications**.

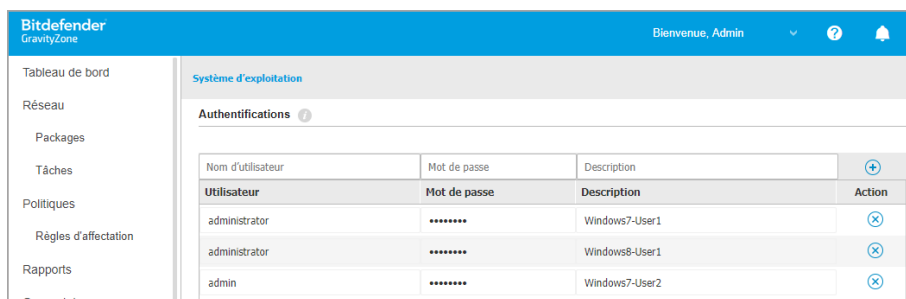


Le menu Admin. des authentifications

5.6.1. Ajouter des identifiants dans l'Administrateur des authentifications

L'Administrateur des authentifications vous permet de gérer les identifiants de l'administrateur requis pour l'authentification à distance lors des tâches d'installation envoyées aux ordinateurs et aux machines virtuelles de votre réseau.

Pour ajouter un ensemble d'identifiants :



| Nom d'utilisateur | Mot de passe | Description | |
|-------------------|--------------|----------------|--------|
| Utilisateur | Mot de passe | Description | Action |
| administrator | ***** | Windows7-User1 | ⊗ |
| administrator | ***** | Windows8-User1 | ⊗ |
| admin | ***** | Windows7-User2 | ⊗ |

Admin. des authentifications

1. Saisissez le nom d'utilisateur et le mot de passe d'un compte administrateur de tous les systèmes d'exploitation cibles dans les champs correspondants en haut du titre du tableau. Vous pouvez également ajouter une description qui vous aidera à identifier chaque compte plus facilement. Si les ordinateurs sont dans un domaine, il suffit d'indiquer les identifiants de l'administrateur du domaine.

Utilisez les conventions Windows lorsque vous saisissez le nom (d'un compte utilisateur).


- pour les machines Active Directory, utilisez ces syntaxes : `username@domain.com` and `domain\username`. Pour vous assurer que les identifiants saisis fonctionneront, ajoutez-les dans les deux formes (`username@domain.com` et `domain\username`).
 - Pour les machines Workgroup, il suffit de saisir le nom d'utilisateur, sans le nom du groupe de travail.
2. Cliquez sur le bouton **+ Ajouter** à droite du tableau. Le nouveau jeu d'authentifiants est ajouté au tableau.

**Note**

Si vous n'avez pas spécifié les informations d'authentification, vous serez invité à les saisir lorsque vous lancerez des tâches d'installation. Les identifiants spécifiés sont enregistrés automatiquement dans votre Administrateur des authentifications afin que vous n'ayez pas à les saisir la prochaine fois.

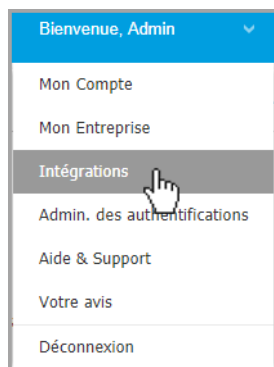
5.6.2. Supprimer les identifiants de l'Administrateur des authentifications

Pour supprimer des identifiants obsolètes de l'Administrateur des authentifications :

1. Pointez sur la ligne du tableau contenant les identifiants que vous souhaitez supprimer.
2. Cliquez sur le bouton  **Supprimer** à droite de la ligne du tableau correspondante. Le compte sélectionné sera supprimé.

6. INTÉGRATIONS

GravityZone offre la possibilité d'intégrer la Control Center à des solutions tierces. Vous pouvez configurer l'intégration de vos solutions tierces sur la page **Intégrations**, à laquelle vous pouvez accéder en pointant sur votre nom d'utilisateur dans l'angle supérieur droit de la console et en sélectionnant **Intégrations**.



À partir de cette page, vous pouvez ajouter, modifier ou supprimer les intégrations en fonction de vos besoins.

6.1. Intégration au service Amazon EC2

Si votre entreprise possède une licence de service Bitdefender Security for AWS, ou que vous disposez d'un abonnement Bitdefender Security for AWS d'essai, vous pouvez configurer l'intégration avec ce service à partir de la Control Center GravityZone et déployer, gérer et contrôler de manière centralisée la sécurité de Bitdefender sur leur inventaire d'instances. Les serveurs d'analyse propriétaires sont hébergés par Bitdefender dans le Cloud AWS pour assurer une empreinte optimale sur les instances protégées et supprimer la surcharge d'analyse ayant lieu avec des logiciels de sécurité traditionnels.

Pour des informations complètes concernant l'architecture Bitdefender Security for AWS, les prérequis, le mode d'abonnement, la création et la gestion de l'intégration au service Amazon EC2, veuillez vous référer au [Guide d'intégration Amazon EC2](#).

7. DÉINSTALLATION DE LA PROTECTION

Vous pouvez désinstaller et réinstaller les composants GravityZone dans certains cas, comme lorsque vous avez besoin d'utiliser une clé de licence sur une autre machine, de corriger des erreurs ou lors d'une mise à niveau.

Pour désinstaller correctement la protection des endpoints de Bitdefender de votre réseau, suivez les instructions décrites dans ce chapitre.

- [Désinstallation de la Protection Endpoint](#)
- [Désinstallation de la Protection Exchange](#)

7.1. Désinstallation de la Protection Endpoint

Pour désinstaller en toute sécurité la protection de Bitdefender, vous devez d'abord désinstaller les agents de sécurité, puis le Security Server, si besoin. Si vous souhaitez désinstaller seulement le Security Server, vérifiez que ses agents sont bien connectés à un autre Security Server.

- [Désinstallation des agents de sécurité](#)
- [Désinstallation de Security Server](#)

7.1.1. Désinstallation des agents de sécurité

Vous avez deux options pour désinstaller les agents de sécurité :

- [À distance](#) depuis la Control Center
- [Manuellement](#) sur la machine cible



Avertissement

Les agents de sécurité et les Serveurs de Sécurité sont essentiels pour protéger vos endpoints. C'est pourquoi les désinstaller peut mettre votre réseau en danger.

Désinstallation à distance

Pour désinstaller la protection de Bitdefender depuis n'importe quel endpoint administré à distance :

1. Allez sur la page **Réseau**.

2. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Tous les ordinateurs du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
3. Sélectionnez les endpoints dont vous souhaitez désinstaller l'agent de sécurité de Bitdefender.
4. Cliquez sur le bouton **Tâches** en haut du tableau et sélectionnez **Désinstaller le client**. Une fenêtre de configuration s'affiche.
5. Dans la fenêtre de tâche de **désinstallation de l'agent** vous pouvez choisir de conserver les fichiers mis en quarantaine sur le endpoint ou de les supprimer.
6. Cliquez sur **Enregistrer** pour créer la tâche. Une message de confirmation s'affiche.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**.

Si vous souhaitez réinstaller les agents de sécurité, veuillez vous référer à « [Installer la protection des postes de travail](#) » (p. 33).

Désinstallation locale

Pour désinstaller manuellement l'agent de sécurité Bitdefender sur une machine Windows :

1. Selon votre système d'exploitation :
 - Sous Windows 7, allez dans **Démarrer > Panneau de configuration > Désinstaller un programme** dans le menu **Programmes**.
 - Sous Windows 8, allez dans **Paramètres > Panneau de configuration > Désinstaller un programme** dans le menu **Programmes**.
 - Sous Windows 8.1, faites un clic droit sur le bouton **Démarrer** puis choisissez **Panneau de configuration > Programmes et fonctionnalités**.
 - Sous Windows 10, allez dans **Démarrer > Paramètres > Système > Applications & fonctionnalités**.
2. Sélectionnez l'agent Bitdefender dans la liste des programmes.
3. Cliquez sur **Désinstaller**.
4. Saisissez le mot de passe de Bitdefender, si l'option est activée dans les politiques de sécurité. Durant la désinstallation, vous pouvez voir la progression de la tâche.

Pour désinstaller manuellement l'agent de sécurité de Bitdefender sur une machine Linux :

1. Ouvrez le terminal.
2. Obtenez l'accès root en utilisant les commandes `su` ou `sudo su`.
3. Naviguez en utilisant la commande `cd` vers le chemin suivant :
`/opt/BitDefender/bin`
4. Exécutez le script :

```
# ./remove-sve-client
```

5. Saisissez le mot de passe de Bitdefender pour continuer, si l'option est activée dans les politiques de sécurité.


Pour désinstaller manuellement l'agent de Bitdefender sur un Mac :


1. Allez dans le **Finder > Applications**.
2. Ouvrez le dossier de Bitdefender.
3. Double-cliquez sur **Bitdefender Mac Uninstall**.
4. Dans la fenêtre de confirmation, cliquez à la fois sur **Vérifier** et **Désinstaller** pour continuer.

Si vous souhaitez réinstaller les agents de sécurité, veuillez vous référer à « [Installer la protection des postes de travail](#) » (p. 33).

7.1.2. Désinstallation de Security Server

Pour supprimer Security Server :

1. Éteignez et supprimez la machine virtuelle Security Server de votre environnement de virtualisation.
2. Connectez-vous à Control Center GravityZone.
3. Rendez-vous dans **Réseau** et recherchez Security Server dans l'inventaire. Peu de temps après la suppression de la machine virtuelle, Security Server apparaîtra comme étant hors ligne.
4. Sélectionnez la case à cocher correspondant à Security Server.
5. Cliquez sur le bouton  **Supprimer** de la barre d'action.

Security Server sera déplacé vers le dossier **Supprimé**, depuis lequel vous pourrez complètement le supprimer en cliquant sur le bouton  **Supprimer** de la barre d'action.

7.2. Désinstallation de la Protection Exchange

Vous pouvez désinstaller la protection Exchange de n'importe quel serveur Microsoft Exchange sur lequel Bitdefender Endpoint Security Tools est installé avec ce rôle. Vous pouvez réaliser la désinstallation depuis la Control Center.

1. Allez sur la page **Réseau**.
2. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Les entités seront affichées dans le volet de droite du tableau.
3. Sélectionnez l'endpoint dont vous souhaitez désinstaller la protection Exchange.
4. Cliquez sur **Reconfigurer le client** dans le menu **Tâches**, dans le volet de droite du tableau. Une fenêtre de configuration s'affiche.
5. Dans la section **Général**, décochez la case **Protection Exchange**.



Avertissement

Dans la fenêtre de configuration, vérifiez que tous les autres rôles sélectionnés sont actifs sur l'endpoint. Sinon, ils seront aussi désinstallés.

6. Cliquez sur **Enregistrer** pour créer la tâche.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**.

Si vous souhaitez réinstaller la protection Exchange, veuillez vous référer à « [Installer la protection Exchange](#) » (p. 61).

8. OBTENIR DE L'AIDE

Bitdefender fait le maximum pour apporter à ses clients une aide fiable, rapide et efficace. Si vous rencontrez le moindre problème ou si avez une question à poser concernant votre produit Bitdefender, consultez notre [Centre d'assistance en ligne](#). Il propose de la documentation que vous pouvez utiliser pour trouver rapidement une solution ou obtenir une réponse. Si vous le désirez, vous pouvez également contacter l'équipe du Service Clients de Bitdefender. Nos membres du support technique répondront à vos questions aussi rapidement que possible et vous fourniront l'assistance dont vous avez besoin.



Note

Vous trouverez des informations sur les services d'aide et de support que nous fournissons ainsi que des détails sur notre politique d'assistance.

8.1. Centre de support de Bitdefender

Le [Centre de support de Bitdefender](#) fournit toute l'assistance dont vous avez besoin concernant votre produit Bitdefender.

Vous pouvez utiliser différentes ressources pour trouver rapidement une solution ou une réponse :

- Articles de connaissances de base
- Forum du Support Bitdefender
- Documentations produits

Vous pouvez également utiliser votre moteur de recherche favori pour obtenir plus d'informations sur la sécurité informatique, les produits et l'entreprise Bitdefender.

Articles de connaissances de base

La base de connaissances de Bitdefender est un ensemble d'informations en ligne concernant les produits Bitdefender. Il contient, dans un format facilement accessible, les rapports d'incidents survenus, ainsi que les bugs constatés, par le support technique de Bitdefender. Vous y découvrirez également des articles généraux sur la prévention des antivirus, sur la gestion, en détail, des solutions Bitdefender et beaucoup d'autres articles.

La base de connaissances de Bitdefender est accessible au public et peut être consultée gratuitement. Cet ensemble d'informations est une autre manière de

fournir aux clients de Bitdefender les informations techniques dont ils ont besoin. Toutes les requêtes valides d'informations ou de rapports de bugs provenant de clients Bitdefender trouvent une réponse dans la base de connaissances de Bitdefender, comme les rapports de corrections de bugs, les solutions de rechange ou les articles d'informations venant compléter les fichiers d'aide des produits.

La base de connaissances des produits pour Entreprises de Bitdefender est accessible à tout moment à l'adresse <http://www.bitdefender.fr/support/business.html>.

Forum du Support Bitdefender

Le Forum du Support Bitdefender fournit aux utilisateurs de Bitdefender une manière simple d'obtenir de l'aide et d'aider les autres. Vous pouvez poster tout problème ou toute question concernant votre produit Bitdefender.

Les techniciens du support Bitdefender surveillent le forum à la recherche de nouvelles publications afin de vous aider. Vous pouvez également obtenir une réponse ou une solution d'un utilisateur Bitdefender plus expérimenté.

Avant de publier un problème ou une question, recherchez s'il existe une rubrique similaire ou connexe dans le forum.

Le forum de support de Bitdefender est disponible à <https://forum.bitdefender.com/index.php?showforum=59>, dans 5 langues différentes : français, anglais, allemand, espagnol et roumain. Cliquez sur le lien **Protection des entreprises** pour accéder à la section dédiée aux produits pour entreprises.

Documentations produits

La documentation de votre produit est la source d'informations la plus riche.

La manière la plus simple de consulter la documentation est de se rendre sur la page **Aide & Support** de la Control Center. Cliquez sur votre nom d'utilisateur en haut à droite de la console, sélectionnez **Aide & Support** puis le guide qui vous intéresse. Le guide s'ouvrira dans un nouvel onglet de votre navigateur.

Vous pouvez également consulter et télécharger la documentation sur le [Centre de support](#), dans la section **Documentation** disponible sur la page de support de chaque produit.

8.2. Demande d'aide

Vous pouvez demander de l'aide par le biais de notre Centre de support en ligne. Remplissez le [formulaire de contact](#) et envoyez-le.

8.3. Utiliser l'Outil de Support

L'Outil de Support GravityZone est conçu pour aider les utilisateurs et les techniciens du support à obtenir facilement les informations dont ils ont besoin pour la résolution des problèmes. Exécutez l'Outil de Support sur les ordinateurs affectés et envoyez l'archive créée avec les informations de résolution de problèmes au représentant du support Bitdefender.

8.3.1. Utiliser l'outil de support sur les systèmes d'exploitation Windows

Exécution de l'application Outil support

Pour générer le journal sur l'ordinateur affecté, suivez l'une de ces méthodes :

- [Ligne de commande](#)
- [Assistant graphique](#)

Si BEST n'est pas installé sur l'ordinateur, utilisez le fichier exécutable de l'Outil Support BEST.

Méthode en ligne de commande

1. Ouvrez une Invite de commande avec les privilèges administrateur.
2. Rendez-vous dans le dossier d'installation du produit. Le chemin par défaut est le suivant :

```
C:\Program Files\Bitdefender\Endpoint Security
```

3. Récupérez et sauvegardez les journaux en exécutant la commande suivante :

```
Product.Support.Tool.exe collect
```

Par défaut, les journaux sont enregistrés dans C:\Windows\Temp.

Si vous le voulez, vous pouvez enregistrer le journal de l'Outil Support dans le dossier de votre choix, en utilisant le chemin optionnel :

```
Product.Support.Tool.exe collect [path="<path-to-file>"]
```

Exemple :

```
Product.Support.Tool.exe collect path="D:\Test"
```

Une fois la commande exécutée, une barre de progression apparaît à l'écran. Lorsque la procédure est terminée, le nom de l'archive contenant les fichiers journaux et son emplacement apparaissent à l'écran.

Méthode par l'interface graphique

1. Téléchargez l'Outil Support BEST en suivant l'un des liens suivants :

- Pour le système d'exploitation Windows 32 bits, cliquez [ici](#).
- Pour le système d'exploitation Windows 64 bits, cliquez [ici](#).

2. Suivez les instructions à l'écran pour exécuter l'Outil support.

Le fichier de sortie est une archive située sur le Bureau, et dénommée comme suit : BDST_[nomdelamachine]_[dateactuelle].

Soumettre le fichier journal

Pour soumettre le journal de l'Outil Support, suivez les instructions suivantes, en fonction de la méthode utilisée :

Si vous avez utilisé des lignes de commande :

1. Rendez-vous dans C:\Windows\Temp pour trouver l'archive dénommée ST_[nomdel'ordinateur]_[dateactuelle].
2. Dans cette archive, ouvrez le fichier problem.txt.
3. Remplissez le fichier avec les données nécessaires.
4. Joignez l'archive à votre ticket de support pour que la procédure de dépannage puisse se poursuivre.

Si vous avez utilisé l'interface graphique :

1. Rendez-vous sur votre Bureau pour trouver l'archive dénommée BDST_[nomdel'ordinateur]_[dateactuelle].

2. Joignez l'archive à votre ticket de support pour que la procédure de dépannage puisse se poursuivre.

8.3.2. Utiliser l'outil de support sur les systèmes d'exploitation Linux

Pour les systèmes d'exploitation Linux, l'Outil de Support est intégré à l'agent de sécurité de Bitdefender.

Pour recueillir des informations sur le système Linux à l'aide de l'Outil de Support, exécutez la commande suivante :

```
# /opt/BitDefender/bin/bdconfigure
```

en utilisant les options disponibles suivantes :

- `--help` pour dresser la liste de toutes les commandes de l'Outil de Support
- `enablelogs` pour activer les journaux du module de communication et du produit (tous les services seront redémarrés automatiquement)
- `disablelogs` pour désactiver les journaux du module de communication et du produit (tous les services seront redémarrés automatiquement)
- `deliverall` pour créer :
 - Une archive contenant les journaux du module de communication et du produit, dans le dossier `/tmp` au format suivant : `bitdefender_machineName_timeStamp.tar.gz`.

Une fois l'archive créée :

1. L'on vous demandera si vous souhaitez désactiver les journaux. Si nécessaire, les services sont redémarrés automatiquement.
 2. L'on vous demandera si vous souhaitez supprimer les journaux.
- `deliverall -default` fournit les mêmes informations que l'option précédente, mais les actions par défaut s'appliqueront aux journaux, sans que l'utilisateur ne soit consulté (les journaux sont désactivés et supprimés).

Vous pouvez également exécuter la commande `/bdconfigure` directement depuis le package BEST (complet ou downloader) sans que le produit soit installé.

Pour signaler un problème GravityZone affectant vos systèmes Linux, procédez comme indiqué ci-dessous, en utilisant les options décrites précédemment :

1. Activez les journaux du module de communication et du produit.
2. Essayez de reproduire le problème.
3. Désactivez les journaux.
4. Créez l'archive des journaux.
5. Ouvrez un ticket de support par e-mail à l'aide du formulaire disponible sur la page **Aide & Support** de Control Center, avec une description du problème et en joignant l'archive des journaux.

L'Outil de Support pour Linux fournit les informations suivantes :

- Les dossiers `etc`, `var/log`, `/var/crash` (si disponible) et `var/epag` de `/opt/BitDefender`, contenant les journaux et les paramètres de Bitdefender
- Le fichier `/var/log/BitDefender/bdinstall.log`, contenant des informations sur l'installation
- Le fichier `network.txt`, contenant des informations sur la connectivité de la machine / les paramètres du réseau
- Le fichier `product.txt`, y compris le contenu de tous les fichiers `update.txt` dans `/opt/BitDefender/var/lib/scan` et une liste récursive complète de tous les fichiers dans `/opt/BitDefender`
- Le fichier `system.txt`, contenant des informations générales sur le système (versions de la distribution et du noyau, mémoire RAM disponible et espace libre sur le disque dur).
- Le fichier `users.txt`, contenant des informations sur les utilisateurs
- Autres informations concernant le produit liées au système, telles que les connexions externes de processus et l'utilisation du processeur.
- Journaux système

8.3.3. Utiliser l'outil de support sur les systèmes d'exploitation Mac

Lorsque vous envoyez une requête à l'équipe de support locale Bitdefender, vous devez fournir :

- Décrivez de façon détaillée le problème que vous rencontrez.
- Une capture d'écran (si possible) du message d'erreur exact.
- Le Journal Outil support.

Pour rassembler des informations sur le système Mac à l'aide de l'Outil support :

1. Téléchargez [l'archive ZIP](#) qui contient l'Outil support.
2. Extrayez le fichier **BDProfiler.tool** de l'archive.
3. Ouvrir une fenêtre de terminal.
4. Naviguez vers l'emplacement du fichier **BDProfiler.tool**.

Par exemple :

```
cd /Users/Bitdefender/Desktop;
```

5. Ajouter des permissions d'exécution au fichier :

```
chmod +x BDProfiler.tool;
```

6. Exécutez l'outil.

Par exemple :

```
/Users/Bitdefender/Desktop/BDProfiler.tool;
```

7. Appuyez sur **Y** et saisissez le mot de passe lorsqu'on vous demande de saisir le mot de passe administrateur.

Attendez quelques minutes que l'outil finisse de générer le journal. Vous trouverez le fichier d'archive qui en résulte (**Bitdefenderprofile_output.zip**) sur votre Bureau.

8.4. Contact

Une communication efficace est la clé d'une relation réussie. Au cours des 15 dernières années, Bitdefender s'est bâti une réputation incontestable dans sa recherche constante d'amélioration de la communication pour dépasser les attentes de ses clients et de ses partenaires. N'hésitez pas à nous contacter pour toute question.

8.4.1. Adresses Web

Ventes : channel-sales@bitdefender.fr

Centre de support en ligne : <http://www.bitdefender.fr/support/business.html>

Documentation : gravityzone-docs@bitdefender.com

D i s t r i b u t e u r s L o c a u x :

<https://www.bitdefender.fr/partenaires/trouver-un-partenaire.html>

Programme Partenaires : channel-sales@bitdefender.fr

Relations Presse : communication@bitdefender.fr

Virus Submissions: virus_submission@bitdefender.com

Spam Submissions: spam_submission@bitdefender.com

Report Abuse: abuse@bitdefender.com

Site Internet : <http://www.bitdefender.com>

8.4.2. Distributeurs Locaux

Les distributeurs locaux Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux.

Pour trouver un distributeur Bitdefender dans votre pays :

1. Allez à <https://www.bitdefender.fr/partenaires/trouver-un-partenaire.html>.
2. Allez dans **Trouver un partenaire**.
3. Les informations de contact des distributeurs locaux de Bitdefender devraient s'afficher automatiquement. Si ce n'est pas le cas, sélectionnez votre pays de résidence pour afficher les informations.
4. Si vous ne trouvez pas de distributeur Bitdefender dans votre pays, n'hésitez pas à nous contacter par e-mail à l'adresse channel-sales@bitdefender.fr.

8.4.3. Bureaux de Bitdefender

Les bureaux de Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux. Leur adresse respective et contacts sont listés ci-dessous.

Etats-Unis

Bitdefender, LLC

PO Box 667588

Pompano Beach, FL 33066

United States

Téléphone (Service commercial et support technique) : 1-954-776-6262

Ventes : sales@bitdefender.comSite Web : <http://www.bitdefender.com>Centre de support en ligne : <http://www.bitdefender.com/support/business.html>

France

Bitdefender

49, Rue de la Vanne

92120 Montrouge

Fax : +33 (0)1 47 35 07 09

Téléphone : +33 (0)1 47 35 72 73

E-mail : b2b@bitdefender.frSite Web : <http://www.bitdefender.fr>Centre de support en ligne : <http://www.bitdefender.fr/support/business.html>

Espagne

Bitdefender España, S.L.U.

Avda. Diagonal, 357, 1º 1ª

08037 Barcelona

España

Fax : (+34) 93 217 91 28

Téléphone (services administratif et commercial) : (+34) 93 218 96 15

Téléphone (support technique) : (+34) 93 502 69 10

Ventes : comercial@bitdefender.esSite Web : <http://www.bitdefender.es>Centre de support en ligne : <http://www.bitdefender.es/support/business.html>

Allemagne

Bitdefender GmbH

Technologiezentrum Schwerte

Lohbachstrasse 12

D-58239 Schwerte

Deutschland

Téléphone (services administratif et commercial) : +49 (0) 2304 94 51 60

Téléphone (support technique) : +49 (0) 231 98 92 80 16

Ventes : firmenkunden@Bitdefender.de

Site Web : <http://www.bitdefender.de>

Centre de support en ligne : <http://www.bitdefender.de/support/business.html>

Royaume-Uni et Irlande

Genesis Centre Innovation Way

Stoke-on-Trent, Staffordshire

ST6 4BF

UK

Téléphone (Service commercial et support technique) : (+44) 203 695 3415

E-mail : info@bitdefender.co.uk

Ventes : sales@bitdefender.co.uk

Site Web : <http://www.bitdefender.co.uk>

Centre de support en ligne : <http://www.bitdefender.co.uk/support/business.html>

Roumanie

BITDEFENDER SRL

rsOrhideea Towe

15A Orhideelor Street

060071 Bucharest, Sector 6

Fax : +40 21 2641799

Téléphone (Service commercial et support technique) : +40 21 2063470

Ventes : sales@bitdefender.ro

Site Web : <http://www.bitdefender.ro>

Centre de support en ligne : <http://www.bitdefender.ro/support/business.html>

Émirats arabes unis

Bitdefender FZ-LLC

Dubai Internet City, Building 17

Office # 160

Dubai, UAE

Téléphone (Service commercial et support technique) : 00971-4-4588935 /
00971-4-4589186

Fax : 00971-4-44565047

Ventes : sales@bitdefender.com

Site Web : <http://www.bitdefender.com>

Centre de support en ligne : <http://www.bitdefender.com/support/business.html>

A. Annexes

A.1. Types de fichiers pris en charge

Les moteurs d'analyse anti-malware compris dans les solutions de sécurité de Bitdefender peuvent analyser tous types de fichiers pouvant contenir des menaces. La liste ci-dessous comprend les types de fichiers les plus communément analysés.

```
{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde;
accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain;
air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax;
bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm;
cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh;
dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with
HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4;
dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget;
gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt;
iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif;
jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf;
mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml;
mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg;
msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx;
odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak;
pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot;
potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz;
prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz;
py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm;
rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr;
script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm;
snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2;
td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa;
url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm;
wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws;
ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;
```




xls; xlsb; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf;
xsn; xtp; xz; z; zip; zl?; zoo