

The background of the cover is a dark, futuristic digital space. It features glowing blue and cyan light trails, circular patterns, and a central bright light source that creates a lens flare effect. The overall aesthetic is high-tech and cybernetic.

Bitdefender®

GravityZone

GUIDE DE L'ADMINISTRATEUR

Bitdefender GravityZone Guide de l'administrateur

Date de publication 2021.04.20

Copyright© 2021 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 ix
 - 1. Conventions utilisées dans ce guide ix
- 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. HyperDetect 4
 - 2.4. Anti-exploit avancé 4
 - 2.5. Pare-feu 5
 - 2.6. Contrôle de contenu 5
 - 2.7. Network Attack Defense 5
 - 2.8. Gestion des correctifs 5
 - 2.9. Contrôle des appareils 6
 - 2.10. Chiffrement des disques 6
 - 2.11. Security for Exchange 6
 - 2.12. Contrôle des applications 7
 - 2.13. Sandbox Analyzer 7
 - 2.14. Hypervisor Memory Introspection (HVI) 7
 - 2.15. Network Traffic Security Analytics (NTSA) 8
 - 2.16. Security for Storage 9
 - 2.17. Security for Mobile 9
 - 2.18. Disponibilité des couches de protection de GravityZone 10
- 3. L'architecture de GravityZone 11
 - 3.1. Appliance virtuelle GravityZone 11
 - 3.1.1. Base de données de GravityZone 12
 - 3.1.2. Serveur de mise à jour GravityZone 12
 - 3.1.3. Serveur de communication GravityZone 12
 - 3.1.4. Console Web (GravityZone Control Center) 12
 - 3.1.5. Base de données Créateur de rapports 12
 - 3.1.6. Processeurs Créateur de rapports 13
 - 3.2. Security Server 13
 - 3.3. Package de complément HVI 13
 - 3.4. Agents de sécurité 13
 - 3.4.1. Bitdefender Endpoint Security Tools 14
 - 3.4.2. Endpoint Security for Mac 16
 - 3.4.3. GravityZone Mobile Client 17
 - 3.4.4. Bitdefender Tools (vShield) 17
 - 3.5. Architecture de Sandbox Analyzer 17
- 4. Pour commencer 20
 - 4.1. Connexion au Control Center 20
 - 4.2. Le Control Center en un coup d'œil 21
 - 4.2.1. Présentation du Control Center 21
 - 4.2.2. Données du tableau 23

4.2.3. Barres d'outils d'actions	24
4.2.4. Menu contextuel	25
4.2.5. Sélecteur d'affichage	25
4.3. Gestion de votre compte	26
4.4. Changer de mot de passe de connexion	29
5. Comptes utilisateur	30
5.1. Rôles Utilisateur	31
5.2. Droits de l'utilisateur	32
5.3. Gestion des comptes utilisateurs	33
5.3.1. Gérer des comptes utilisateurs individuellement	33
5.3.2. Gestion de multiples comptes utilisateurs	37
5.4. Réinitialiser les mots de passe de connexion	41
5.5. Gérer l'authentification à deux facteurs	41
6. Gestion des objets du réseau	43
6.1. Travailler avec les affichages réseau	45
6.1.1. Ordinateur / Machine virtuelle	45
6.1.2. Machines virtuelles	46
6.1.3. Appareils mobiles	47
6.2. Ordinateurs	48
6.2.1. Vérifier l'état des ordinateurs	49
6.2.2. Afficher des informations sur un ordinateur	52
6.2.3. Organiser les ordinateurs dans des groupes	65
6.2.4. Trier, filtrer et rechercher des ordinateurs	67
6.2.5. Lancer des tâches	71
6.2.6. Créer des rapports rapides	104
6.2.7. Affecter des politiques	105
6.2.8.	106
6.2.9. Synchronisation avec Active Directory	107
6.3. Machines virtuelles	108
6.3.1. Vérifier l'état des machines virtuelles	109
6.3.2. Afficher des informations sur les machines virtuelles	113
6.3.3. Organiser les machines virtuelles en groupes	122
6.3.4. Trier, filtrer et rechercher des machines virtuelles	124
6.3.5. Exécuter des tâches sur les machines virtuelles	128
6.3.6. Créer des rapports rapides	165
6.3.7. Affecter des politiques	166
6.3.8. Utiliser Recovery Manager for Encrypted Volumes (système de récupération pour volumes chiffrés)	167
6.3.9. Libérer les sièges de licence	168
6.4. Appareils mobiles	169
6.4.1. Ajouter des utilisateurs personnalisés	170
6.4.2. Ajouter des appareils mobiles aux utilisateurs	171
6.4.3. Organiser les utilisateurs personnalisés dans des groupes	174
6.4.4. Consulter l'état des appareils mobiles	176
6.4.5. Appareils Conformés et Non conformes	177
6.4.6. Consulter des informations détaillées sur les utilisateurs et les appareils mobiles ..	178
6.4.7. Trier, filtrer et rechercher des appareils mobiles	182

6.4.8. Exécuter des tâches sur les appareils mobiles	186
6.4.9. Créer des rapports rapides	191
6.4.10. Affecter des politiques	192
6.4.11. Synchronisation avec Active Directory	193
6.4.12. Supprimer des utilisateurs et des appareils mobiles	193
6.5. Inventaire des applications	195
6.6. Inventaire des patches	201
6.6.1. Consulter les informations des patches	202
6.6.2. Rechercher et filtrer des patches	204
6.6.3. Ignorer des correctifs	205
6.6.4. Installer des patches	205
6.6.5. Désinstallation des patches	207
6.6.6. Création de statistiques sur les patches	209
6.7. Afficher et gérer des tâches	210
6.7.1. Vérifier l'état d'une tâche	210
6.7.2. Afficher les rapports sur les tâches	213
6.7.3. Relancement des tâches	213
6.7.4. Arrêt des Tâches d'analyse Exchange	213
6.7.5. Supprimer des tâches	214
6.8. Supprimer des endpoints de l'inventaire du réseau	214
6.9. Configuration des paramètres du réseau	216
6.9.1. Paramètres de l'inventaire réseau	216
6.9.2. Nettoyage des machines hors ligne	216
6.10. Configuration des paramètres de Security Server	218
6.11. Admin. des authentifications	219
6.11.1. Système d'exploitation	220
6.11.2. Environnement virtuel	221
6.11.3. Supprimer les identifiants de l'Administrateur des authentifications	222
7. Politiques de sécurité	223
7.1. Administration des politiques	224
7.1.1. Création de politiques	225
7.1.2. Affecter des politiques	227
7.1.3. Modification des paramètres de la politique	237
7.1.4. Renommer des politiques	238
7.1.5. Suppression de politiques	238
7.2. Politiques des ordinateurs et machines virtuelles	239
7.2.1. Généraux	240
7.2.2. HVI	254
7.2.3. Antimalware	263
7.2.4. Sandbox Analyzer	304
7.2.5. Pare-feu	312
7.2.6. Protection du réseau	327
7.2.7. Gestion des correctifs	343
7.2.8. Contrôle des applications	346
7.2.9. Contrôle des appareils	352
7.2.10. Relais	358
7.2.11. Protection Exchange	360
7.2.12. Chiffrement de disque	392

7.2.13. NSX	397
7.2.14. Protection de stockage	397
7.3. Politiques des appareils mobiles	401
7.3.1. Généraux	402
7.3.2. Gestion de l'appareil	402
8. Tableau de bord de supervision	424
8.1. Tableau de bord	424
8.1.1. Actualiser les données du portlet	425
8.1.2. Modification des paramètres d'un portlet	425
8.1.3. Ajouter un nouveau portlet	426
8.1.4. Suppression d'un portlet	426
8.1.5. Réorganiser les portlets	426
9. Utilisation des rapports	427
9.1. Types de rapport :	427
9.1.1. Rapports Ordinateur et Machine virtuelle	428
9.1.2. Rapports Serveur Exchange	443
9.1.3. Rapports Appareils Mobiles	446
9.2. Création de rapports	448
9.3. Afficher et gérer des rapports planifiés	451
9.3.1. Afficher les rapports	451
9.3.2. Modifier les rapports planifiés	452
9.3.3. Supprimer les rapports planifiés	454
9.4. Prendre des actions basées sur un rapport	454
9.5. Enregistrer des rapports	455
9.5.1. Exportation de rapports	455
9.5.2. Télécharger des Rapports	455
9.6. Envoyer des rapports par e-mail	456
9.7. Impression des rapports	456
9.8. Créateur de rapports	457
9.8.1. Types de requête	458
9.8.2. Gestion des requêtes	459
9.8.3. Afficher et gérer des rapports	465
10. Mise en quarantaine	468
10.1. Explorer la Quarantaine	468
10.2. Quarantaine Ordinateurs et Machines virtuelles	469
10.2.1. Afficher les informations sur la quarantaine	469
10.2.2. Gérer les fichiers en quarantaine	470
10.3. Quarantaine Serveurs Exchange	475
10.3.1. Afficher les informations sur la quarantaine	475
10.3.2. Objets en quarantaine	477
11. Utiliser Sandbox Analyzer	481
11.1. Filtrage des fiches d'envoi	482
11.2. Afficher les détails d'une analyse	483
11.3. Renvoyer un échantillon	485
11.4. Supprimer les fiches d'envoi	486
11.5. Envoi manuel	487

11.6. Gestion de l'infrastructure Sandbox Analyzer	489
11.6.1. Consulter l'état de Sandbox Analyzer	490
11.6.2. Configurer les détonations simultanées	491
11.6.3. Vérifier l'état des images VM	492
11.6.4. Configurer et gérer les images VM	493
12. Journal d'activité de l'utilisateur	494
13. Utilisation des outils	496
13.1. Injection d'outils personnalisés avec HVI	496
14. Notifications	498
14.1. Types de notifications	498
14.2. Afficher les notifications	506
14.3. Supprimer des notifications	507
14.4. Configurer les paramètres de notification	508
15. État du système	511
15.1. État OK	512
15.2. État Attention	512
15.3. Métriques	513
16. Obtenir de l'aide	516
16.1. Centre de support de Bitdefender	516
16.2. Demande d'aide	518
16.3. Utiliser l'Outil de Support	518
16.3.1. Utiliser l'outil de support sur les systèmes d'exploitation Windows	518
16.3.2. Utiliser l'outil de support sur les systèmes d'exploitation Linux	520
16.3.3. Utiliser l'outil de support sur les systèmes d'exploitation Mac	521
16.4. Contact	522
16.4.1. Adresses Web	523
16.4.2. Distributeurs Locaux	523
16.4.3. Bureaux de Bitdefender	523
A. Annexes	526
A.1. Types de fichiers pris en charge	526
A.2. États et types d'objets du réseau	527
A.2.1. Types d'objets du réseau	527
A.2.2. États des objets du réseau	528
A.3. Types de fichiers d'applications	529
A.4. Types de fichiers du filtrage des pièces jointes	530
A.5. Variables du système	530
A.6. Outils du Contrôle des applications	532
A.7. Objets de Sandbox Analyzer	533
A.7.1. Types et extensions de fichier pris en charge pour l'envoi manuel	533
A.7.2. Types de fichier pris en charge par le préfiltrage de contenu lors de l'envoi automatique	534
A.7.3. Exclusions par défaut de l'envoi automatique	534
A.7.4. Applications recommandées pour les VM de détonation	534
A.8. Processeurs de données	535



Glossaire 538

Préface

Ce guide est destiné aux administrateurs réseau chargés de gérer la protection GravityZone dans les locaux de leur entreprise.

L'objectif de ce document est d'expliquer comment appliquer et afficher les paramètres de sécurité sur les endpoints du réseau sous votre compte à l'aide de GravityZone Control Center. Vous apprendrez à afficher l'inventaire de votre réseau dans Control Center, à créer et appliquer des politiques sur les endpoints gérés, à créer des rapports, à gérer les éléments de la quarantaine et à utiliser le tableau de bord.

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. ix)	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, appareils mobiles, machines virtuelles dans les clouds privés et publics et les 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 », contrôle des applications et sandboxing, pare-feu, contrôle des appareils et du contenu, antiphishing et antispam.

2. COUCHES DE PROTECTION DE GRAVITYZONE

GravityZone fournit les couches de protection suivantes :

- Antimalware
- Advanced Threat Control
- HyperDetect
- Anti-exploit avancé
- Pare-feu
- Contrôle de contenu
- Gestion des correctifs
- Contrôle des appareils
- Chiffrement des disques
- Security for Exchange
- Contrôle des applications
- Sandbox Analyzer
- Hypervisor Memory Introspection (HVI)
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

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. HyperDetect

Bitdefender HyperDetect est une couche supplémentaire de sécurité spécialement conçue pour détecter les attaques sophistiquées et les activités suspectes lors de la phase de pré-exécution. HyperDetect contient des modèles de Machine Learning et une technologie de détection des attaques furtives contre les menaces telles que : attaques zero-day, menaces persistantes avancées (APT), malwares obfusqués, attaques sans fichier, (détournement de PowerShell, Windows Management Instrumentation, etc.), vol d'identifiant, attaques ciblées, malwares personnalisés, attaques par scripts, exploits, outils de hacking, trafic réseau suspect, applications potentiellement indésirables (PUA), ransomwares.



Note

Ce module est un complément disponible avec une clé de licence distincte.

2.4. 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.

2.5. 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.

2.6. 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.

2.7. Network Attack Defense

Le module Network Attack Defense s'appuie sur une technologie de Bitdefender qui se concentre sur la détection des attaques réseau conçues pour accéder aux endpoints via des techniques spécifiques comme la force brute, les exploits réseau, les passwords stealers, les vecteurs d'infection drive-by-download, les bots et les chevaux de Troie.

2.8. 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.

2.9. 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.)

2.10. Chiffrement des disques

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.

**Note**

Full Disk Encryption est une extension disponible avec une clé de licence séparée pour tous les packs GravityZone.

2.11. 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.

2.12. Contrôle des applications

Le module de Contrôle des Applications protège des malwares, des attaques 0-Day et améliore la sécurité sans impacter la productivité. Le module de Contrôle des Applications renforce la flexibilité des politiques de listes blanches d'applications et empêche l'installation et l'exécution d'applications indésirables ou malveillantes.

2.13. Sandbox Analyzer

Offrant une puissante couche de protection contre les menaces avancées, le Sandbox Analyzer for Endpoints de Bitdefender effectue des analyses automatiques détaillées des fichiers suspects, qui n'ont pas encore été signalés par les moteurs antimalware de Bitdefender. Le sandbox utilise un large éventail de technologies Bitdefender afin d'exécuter des charges dans un environnement virtuel confiné hébergé par Bitdefender ou déployé en local, d'analyser leur comportement et de signaler toute modification observée au sein du système, révélatrice d'une intention malveillante.

Sandbox Analyzer utilise un ensemble de capteurs pour détoner des contenus depuis les endpoints gérés, le flux du trafic endpoints réseau, une quarantaine centralisée ou des serveurs ICAP.

En outre, Sandbox Analyzer permet d'envoyer des échantillons manuellement ou via une API.

2.14. Hypervisor Memory Introspection (HVI)

Il est de notoriété publique que les pirates organisés et guidés par l'appât du gain cherchent les vulnérabilités (vulnérabilités zero day), ou utilisent des exploits temporaires (exploits zero day) et autre outils. Les pirates utilisent également des techniques pour retarder et séquencer les charges d'attaques pour camoufler les activités malveillantes. Les attaques inédites et motivées par le profit sont créées pour être furtives et lutter contre les outils de sécurité traditionnels.

Pour les environnements virtualisés, le problème est désormais résolu, HVI protégeant les centres de données avec une forte densité de machines virtuelles contre les menaces avancées et sophistiquées que les moteurs basés sur des

signatures ne peuvent pas neutraliser. Cela met en place une forte isolation, assurant une détection des attaques en temps réel, les bloquant quand elles se produisent et supprimant immédiatement les menaces.

Que la machine protégée soit Windows ou Linux, un serveur ou un ordinateur de bureau, HVI fournit une compréhension d'un niveau impossible à atteindre à partir de l'intérieur des systèmes d'exploitation. De la même façon que le l'hyperviseur contrôle l'accès au hardware au nom de chaque machine virtuelle invitée, HVI a une connaissance approfondie à la fois du mode utilisateur et du mode noyau dans sa mémoire "invités". Le résultat est que HVI a un aperçu complet de la mémoire invitée, et donc le contexte entier. En même temps, HVI est isolé des invités protégés, tout comme l'hyperviseur lui-même est isolé. En opérant au niveau de l'hyperviseur et à l'aide des fonctionnalités de l'hyperviseur, HVI surmonte les défis techniques de la sécurité traditionnelle pour révéler les activités malveillantes dans les centres de données.

HVI identifie les techniques d'attaque plus que les schémas d'attaque. De cette façon, la technologie peut identifier, rapporter et empêcher les techniques d'exploitation les plus communes. Le noyau est protégé contre les techniques d'hameçonnage par rootkit qui sont utilisées pendant la chaîne d'attaque pour maintenir la furtivité. Les processus en mode utilisateur sont également protégés contre l'injection de code, le détournement de fonction et l'exécution de code dans une pile ou un segment.

2.15. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) est une solution de sécurité du réseau qui analyse les flux IPFIX, en quête de comportements malveillants et de malwares.

Bitdefender NTSA a été conçu pour fonctionner en parallèle à vos mesures de sécurité existantes en tant que sureté supplémentaire capable de couvrir les angles morts des outils traditionnels.

Les outils de protection du réseau traditionnels essaient généralement de prévenir les infections de malwares en inspectant le trafic entrant (via une sandbox, un pare-feu, un antivirus, etc.). Bitdefender NTSA se concentre uniquement sur la surveillance des comportements malveillants du trafic sortant.

2.16. Security for Storage

GravityZone Security for Storage garantit une protection en temps réel de pointe pour les systèmes de partage de fichiers et de stockage en réseau les plus courants. Le système et les algorithmes de détection des menaces sont mis à jour automatiquement. Cela ne vous demande aucun effort et ne perturbe pas le travail des utilisateurs finaux.

Au moins deux Security Server GravityZone multiplateforme jouent le rôle de serveur ICAP qui effectue un service de lutte contre les malwares pour les appareils de stockage en réseau (NAS) et les systèmes de partage de fichiers conformes au Internet Content Adaptation Protocol (ICAP, standardisé par la norme RFC 3507).

Lorsqu'un utilisateur demande à ouvrir, lire, modifier ou fermer un fichier sur un ordinateur portable, un poste de travail, un smartphone ou un autre appareil ; le client ICAP (un NAS ou un système de partage de fichiers) envoie une demande d'analyse au Security Server et reçoit les conclusions de ce dernier au sujet du fichier concerné. En fonction du résultat, Security Server autorise ou interdit l'accès au fichier. Il peut également le supprimer.



Note

Ce module est un complément disponible avec une clé de licence distincte.

2.17. Security for Mobile

Elle unifie la sécurité au sein de l'entreprise avec l'administration et le contrôle de la conformité des appareils iPhone, iPad et Android en assurant une distribution fiable des logiciels et des mises à jour via les marketplaces Apple et Android. Cette solution a été conçue pour permettre l'adoption contrôlée des initiatives de « Bring your own device » (BYOD) par l'application homogène de politiques d'utilisation sur l'ensemble des appareils portables. Les fonctions de sécurité comprennent le verrouillage de l'écran, le contrôle d'authentification, la localisation de l'appareil, la suppression des données à distance, la détection des appareils rootés ou jailbreakés et des profils de sécurité. Sur les appareils Android, le niveau de sécurité est amélioré par l'analyse en temps réel et le cryptage des supports amovibles. Les appareils mobiles sont donc contrôlés et les informations professionnelles sensibles qui s'y trouvent sont protégées.

2.18. 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

L'architecture unique de GravityZone permet à la solution de s'adapter facilement et de protéger un nombre illimité de systèmes. GravityZone peut être configuré pour utiliser plusieurs appliances virtuelles et plusieurs instances de rôles spécifiques (Base de données, Serveur de communication, Serveur de mise à jour et Console web) pour assurer fiabilité et extensibilité.

Chaque instance de rôle peut être installée sur une appliance différente. Les équilibreurs de rôles intégrés permettent au déploiement de GravityZone de protéger même les plus grands réseaux d'entreprise sans provoquer de ralentissements ni de goulets d'étranglement. Si des logiciels ou du matériel d'équilibrage de charge sont présents dans le réseau, ils peuvent être utilisés au lieu des équilibreurs intégrés.

Fournie sous la forme d'une appliance virtuelle, GravityZone peut être importée pour s'exécuter sur toute plate-forme de virtualisation, y compris VMware, Citrix, Microsoft Hyper-V, Nutanix Prism et Microsoft Azure.

L'intégration à VMware vCenter, Citrix XenServer, Microsoft Active Directory, Nutanix Prism Element et Microsoft Azure facilite le déploiement de la protection pour les endpoints physiques et virtuels.

La solution GravityZone comporte les composants suivants :

- [Appliance virtuelle GravityZone](#)
- [Security Server](#)
- [Package de complément HVI](#)
- [Agents de sécurité](#)

3.1. Appliance virtuelle GravityZone

La solution sur site GravityZone est fournie sous la forme d'une appliance virtuelle sécurisée (VA) Linux Ubuntu, se configurant automatiquement et intégrée à une image de machine virtuelle. Elle est facile à installer et à configurer via une interface en ligne de commande (CLI). L'appliance virtuelle est disponible en plusieurs formats, compatibles avec les principales plates-formes de virtualisation (OVA, XVA, VHD, OVF, RAW).

3.1.1. Base de données de GravityZone

La logique centrale de l'architecture de GravityZone. Bitdefender utilise une base de données non relationnelle MongoDB, facilement extensible et répliquable.

3.1.2. Serveur de mise à jour GravityZone

Le serveur de mise à jour a un important rôle de mise à jour de la solution GravityZone et des agents des endpoints par la réplication et la publication des packages ou des fichiers d'installation nécessaires.

3.1.3. Serveur de communication GravityZone

Le serveur de communication est le lien entre les agents de sécurité et la base de données ; il transmet les politiques et les tâches aux endpoints protégés ainsi que les événements signalés par les agents de sécurité.

3.1.4. Console Web (GravityZone Control Center)

Les solutions de sécurité de Bitdefender sont gérées depuis un seul endroit, la console web Control Center. La gestion est ainsi plus simple, et il est possible d'accéder au niveau général de sécurité, aux menaces de sécurité globales et d'utiliser tous les modules de sécurité en charge de la protection des bureaux physiques ou virtuels, des serveurs et des appareils mobiles. Intégrant l'architecture "Gravity", le Control Center est capable de répondre aux besoins de toutes les entreprises, quelle que soit leur taille.

Control Center s'intègre aux systèmes de surveillance et de gestion des infrastructures existantes afin d'appliquer automatiquement la protection aux postes de travail, serveurs ou appareils mobiles non administrés apparaissant dans Microsoft Active Directory, VMware vCenter, Citrix XenServer, Nutanix Prism Element, ou à ceux qui sont simplement détectés dans le réseau.

3.1.5. Base de données Créateur de rapports

Le rôle Base de données Créateur de rapports fournit les données nécessaires pour créer des rapports basés sur des requêtes.

3.1.6. Processeurs Créateur de rapports

Le rôle Processeurs Créateur de rapports est essentiel pour la création, la gestion et le stockage des rapports basés sur des requêtes qui utilisent les informations de la Base de données Créateur de rapports.

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.

Il existe trois versions de Security Server, pour chaque type d'environnement de virtualisation :

- **Security Server pour VMware NSX.** Cette version s'installe automatiquement sur chaque hôte dans le cluster où Bitdefender a été déployé.
- **Security Server pour VMware vShield Endpoint.** Cette version doit être installée sur chaque hôte à protéger.
- **Security Server multiplate-forme.** Cette version est destinés à différents environnements virtualisés et doit être installé sur un ou plusieurs hôtes pour accueillir les machines virtuelles protégées. Si vous utilisez HVI, un Security Server doit être installé sur chaque hôte contenant les machines virtuelles à protéger.

3.3. Package de complément HVI

Le package HVI assure le lien entre l'hyperviseur et le Security Server sur cet hôte. De cette façon, le Security Server peut surveiller la mémoire use sur l'hôte sur lequel il est installé, en se basant sur les politiques de sécurité GravityZone.

3.4. 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](#)
- [Endpoint Security for Mac](#)
- [GravityZone Mobile Client](#)
- [Bitdefender Tools \(vShield\)](#)

3.4.1. 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 Windows.

Couches de protection

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

- Antimalware
- Advanced Threat Control
- HyperDetect
- Pare-feu
- Contrôle de contenu
- Network Attack Defense
- Gestion des correctifs
- Contrôle des appareils
- Chiffrement des disques
- Security for Exchange
- Sandbox Analyzer
- Contrôle des applications

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 n'est disponible que pour les systèmes d'exploitation PC et serveurs Windows pris en charge. Pour en apprendre plus, consultez le Guide d'installation de GravityZone.

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.
- 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 patches

Les endpoints avec rôle de Relais peuvent également faire office de Serveur de mise en cache des patches. Une fois ce rôle activé, les Relais servent à stocker les patches 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 patches 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 patches 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.

3.4.2. 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
- Advanced Threat Control
- Contrôle de contenu
- Contrôle des appareils
- Chiffrement des disques

3.4.3. GravityZone Mobile Client

GravityZone Mobile Client applique facilement les politiques de sécurité à un nombre illimité d'appareils Android et iOS, les protégeant ainsi de l'utilisation non autorisée, des riskwares et de la perte de données confidentielles. Les fonctions de sécurité comprennent le verrouillage de l'écran, le contrôle d'authentification, la localisation de l'appareil, la suppression des données à distance, la détection des appareils rootés ou jailbreakés et des profils de sécurité. Sur les appareils Android, le niveau de sécurité est amélioré par l'analyse en temps réel et le cryptage des supports amovibles.

GravityZone Mobile Client est distribué exclusivement via Apple App Store et Google Play.

3.4.4. Bitdefender Tools (vShield)

Bitdefender Tools est un agent léger pour les environnements virtualisés VMware qui sont intégrés dans vShield Endpoint. L'agent de sécurité s'installe sur des machines virtuelles protégées par Security Server, afin de vous permettre de profiter de la fonctionnalité supplémentaire qu'il fournit :

- Vous permet d'exécuter des tâches d'analyse de la mémoire et des processus sur la machine.
- Informe l'utilisateur des infections détectées et des actions qui leur ont été appliquées.
- Ajoute plus d'options pour les exclusions d'analyse antimalware.

3.5. Architecture de Sandbox Analyzer

Offrant une puissante couche de protection contre les menaces avancées, le Sandbox Analyzer for Endpoints de Bitdefender effectue des analyses automatiques détaillées des fichiers suspects, qui n'ont pas encore été signalés par les moteurs antimalware de Bitdefender.

Sandbox Analyzer est disponible en deux variantes :

- [Sandbox Analyzer Cloud](#), hébergé par Bitdefender.
- [Sandbox Analyzer On-Premises](#), disponible sous forme d'une appliance virtuelle qui peut être déployée en local.

Sandbox Analyzer Cloud

Sandbox Analyzer Cloud contient les composants suivants :

- **Sandbox Analyzer Portal** – un serveur de communication hébergé, utilisé pour traiter les requêtes entre les endpoints et le cluster de sandbox de Bitdefender.
- **Sandbox Analyzer Cluster** – l'infrastructure sandbox hébergée, où l'analyse comportementale type est effectuée. Les fichiers envoyés sont exécutés sur des machines virtuelles sous Windows 7.

GravityZone Control Center est à la fois console d'administration et de reporting, où vous pourrez configurer les politiques de sécurité, consulter les rapports d'analyses et voir les notifications.

Bitdefender Endpoint Security Tools, l'agent de sécurité de installé sur les endpoints, agit en tant que capteur d'alimentation pour le Sandbox Analyzer.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises est une appliance virtuelle Linux Ubuntu embarquée sur une image de machine virtuelle, facile à installer et à configurer via une interface de ligne de commande. Sandbox Analyzer On-Premises est disponible au format OVA, déployable sur VMWare ESXi.

Une instance Sandbox Analyzer On-Premises contient les composants suivants :

- **Sandbox Manager**. Ce composant est le gestionnaire de la sandbox. Sandbox Manager se connecte à l'hyperviseur ESXi via une API et utilise ses ressources matérielles pour créer et exploiter un environnement d'analyse des malwares.
- **Machines virtuelles de détonation**. Ce composant est constitué de machines virtuelles exploitées par Sandbox Analyzer pour exécuter des fichiers et analyser leur comportement. Les machines virtuelles de détonation peuvent tourner sous les systèmes d'exploitation Windows 7 et Windows 10 64 bits.

GravityZone Control Center est à la fois console d'administration et de reporting, où vous pourrez configurer les politiques de sécurité, consulter les rapports d'analyses et voir les notifications.

Sandbox Analyzer On-Premises utilise les capteurs d'alimentation suivants :

- **Capteur de l'endpoint**. Bitdefender Endpoint Security Tools pour Windows fait office de capteur d'alimentation installé sur les endpoints. L'agent Bitdefender utilise des algorithmes avancés de Machine Learning et de réseau neuronal

pour détecter les contenus suspects et les envoyer à Sandbox Analyzer, y compris parmi les objets de la quarantaine centralisée.

- **Capteur réseau.** Network Security Virtual Appliance (NSVA) est une appliance virtuelle déployable sur le même environnement virtualisé ESXi que l'instance Sandbox Analyzer. Le capteur réseau extrait le contenu des flux réseau et l'envoie à Sandbox Analyzer.
- **Capteur ICAP** Déployé sur un serveur de stockage en réseau utilisant le protocole ICAP, Bitdefender Security Server prend en charge l'envoi de contenu à Sandbox Analyzer.

En plus de ces capteurs, Sandbox Analyzer On-Premises permet d'envoyer des échantillons manuellement ou via une API. Pour plus de détails, consultez le chapitre **Utilisation de Sandbox Analyzer** du Guide de l'administrateur de GravityZone.

4. POUR COMMENCER

Les solutions GravityZone peuvent être configurées et administrées via une plateforme d'administration centralisée nommée Control Center. Le Control Center est une interface Web à laquelle vous pouvez accéder avec un nom d'utilisateur et un mot de passe.

4.1. Connexion au Control Center

L'accès au Control Center se fait via les comptes utilisateurs. Vous recevrez vos informations de connexion par e-mail une fois que votre compte aura été créé.

Prérequis :

- 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.

Pour se connecter au Control Center :

1. Dans la barre d'adresses de votre navigateur Web, saisissez l'adresse IP ou le nom d'hôte DNS de l'appliance Control Center (en utilisant le préfixe `https://`).
2. Saisissez votre nom d'utilisateur et votre mot de passe.
3. Saisissez le code à six chiffres de Google Authenticator, Microsoft Authenticator, ou tout autre système d'authentification TOTP (Time-Based One-Time Password Algorithm) - compatible avec le [standard RFC6238](#). Pour plus d'informations, reportez-vous à « [Gestion de votre compte](#) » (p. 26).
4. Cliquez sur **Connexion**.

Après votre première connexion, vous devez accepter le Contrat de service de Bitdefender. Cliquez sur **Continuer** pour commencer à utiliser GravityZone.

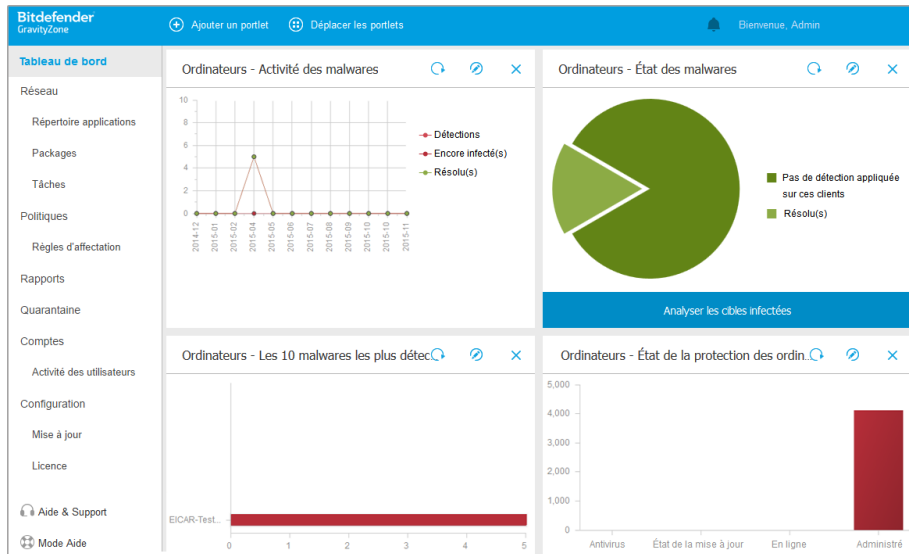


Note

Si vous avez oublié votre mot de passe, utilisez le lien de récupération du mot de passe pour recevoir un nouveau mot de passe. Vous devez indiquer l'adresse e-mail de votre compte.

4.2. Le Control Center en un coup d'œil


Le Control Center est organisé afin de permettre un accès simplifié à toutes les fonctionnalités. Utilisez la barre de menu à droite pour vous déplacer dans la console. Les fonctionnalités disponibles dépendent du type d'utilisateur accédant à la console.



Le tableau de bord

4.2.1. Présentation du Control Center

Les utilisateurs avec le rôle Administrateur de la société disposent de l'ensemble des privilèges de configuration du Control Center et des paramètres de sécurité du réseau alors que les utilisateurs avec le rôle Administrateur ont accès aux fonctionnalités de sécurité du réseau, y compris à l'administration des utilisateurs.

Utilisez le bouton  **Menu affichage** situé dans le coin supérieur gauche pour réduire en passant en vue icône, masquer ou afficher les options de menu. Cliquez sur le bouton pour parcourir les options ou double-cliquez dessus pour passer cette étape.

En fonction de votre rôle, vous pouvez accéder aux options de menu suivantes :

Tableau de bord

Voir des graphiques faciles à lire fournissant des informations de sécurité clés au sujet de votre réseau.

Réseau

Installer une protection, appliquer des politiques pour gérer les paramètres de sécurité, exécuter les tâches à distance et créer des rapports rapides.

Politiques

Créer et gérer les politiques de sécurité.

Rapports

Obtenir des rapports de sécurité sur les clients administrés.

Mise en quarantaine

Administrer à distance les fichiers en quarantaine.

Comptes

Gérer l'accès au Control Center pour d'autres employés de l'entreprise.

Vous trouverez également sous ce menu la page **Activité de l'utilisateur** qui permet d'accéder au journal d'activité de l'utilisateur.



Note

Ce menu est disponible uniquement aux utilisateurs disposant du droit **Gérer les utilisateurs**.

Configuration

Configurez les paramètres de Control Center, comme le serveur de messagerie, l'intégration à Active Directory ou aux environnements de virtualisation, les certificats de sécurité et les paramètres de l'inventaire réseau, notamment les règles planifiées de nettoyage automatique des machines virtuelles inutilisées.





Note

Ce menu est disponible uniquement pour les utilisateurs disposant du droit **Gérer la solution**.

En cliquant sur votre nom d'utilisateur dans l'angle supérieur droit de la console, les options suivantes sont disponibles :





- **Mon Compte.** Cliquez sur cette option pour gérer les détails et les préférences de votre compte utilisateur.
- **Admin. des authentifications.** Cliquez sur cette option pour ajouter et gérer les informations d'authentification requises pour les tâches d'installation à distance.
- **Aide et support technique.** Cliquez sur cette option pour obtenir des informations sur l'aide et le support.
- **Votre avis.** Cliquez sur cette option pour faire apparaître un formulaire vous permettant de modifier et d'envoyer vos messages concernant votre avis au sujet de l'utilisation de GravityZone.
- **Déconnexion.** Cliquez sur cette option pour vous déconnecter de votre compte.

En prime, en haut à droite de la console, vous pourrez trouver :

- L'icône  **Mode Aide**, qui active les cases info-bulle déroulantes positionnées sur éléments de Control Center. Vous trouverez facilement des informations utiles au sujet des fonctionnalités du Control Center.
- L'icône  **Notifications**, qui permet d'accéder facilement aux messages de notification et à la page **Notifications**.

4.2.2. Données du tableau

Les tableaux sont souvent utilisés dans la console pour organiser les données dans un format facile à utiliser.

   				
<input type="checkbox"/>	Nom du rapport	Type	Périodicité	Afficher le rapport
<input type="checkbox"/>	<input type="text" value="Rapport sur l'état des malwares"/>	État des malwares	Tous les jours	23 Jun 2015 - 00:00

Première page — Page de 1 — Dernière page 1 éléments

La page Rapports

Naviguer entre les pages

Les tableaux de plus de 20 entrées comportent plusieurs pages. Par défaut, seules 20 entrées sont affichées par page. Pour parcourir les pages, utilisez les boutons de navigation en bas du tableau. Vous pouvez modifier le nombre d'entrées affichées par page en sélectionnant une option différente dans le menu à côté des boutons de déplacement.

Rechercher des entrées spécifiques

Pour trouver facilement certaines entrées, utilisez les zones de recherche en-dessous des en-têtes de colonne.

Indiquez le terme recherché dans le champ correspondant. Les éléments correspondants apparaissent dans le tableau au moment de leur saisie. Pour rétablir le contenu du tableau, effacez les champs de recherche.

Trier les données

Pour trier les données en fonction d'une colonne spécifique, cliquez sur l'en-tête de la colonne. Cliquez de nouveau sur l'en-tête de colonne pour rétablir l'ordre de tri.




Actualiser les données du tableau

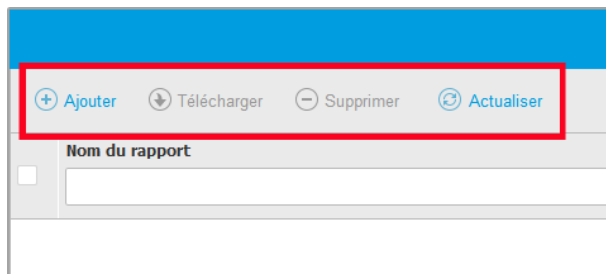
Pour que la console affiche des informations à jour, cliquez sur le bouton **Actualiser** en haut du tableau.

Cela peut être nécessaire lorsque vous passez du temps sur la page.

4.2.3. Barres d'outils d'actions

Dans le Control Center, les barres d'outils d'actions vous permettent d'effectuer certaines opérations spécifiques appartenant à la section dans laquelle vous vous trouvez. Chaque barre d'outils consiste en un ensemble d'icônes se trouvant généralement en haut du tableau. Par exemple, la barre d'outils d'actions de la section **Rapports** vous permet d'effectuer les actions suivantes :

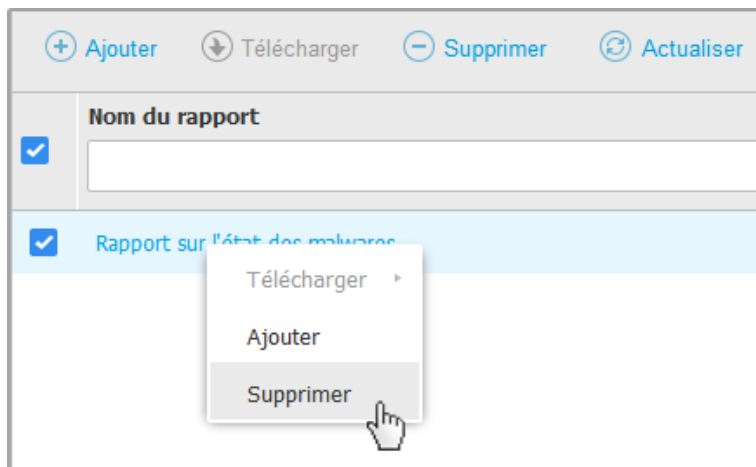
-  Créer un nouveau rapport.
-  Téléchargez un rapport planifié.
-  Supprimer un rapport planifié.



La page Rapports - Barre d'outil d'actions

4.2.4. Menu contextuel

Les commandes de la barre d'outils d'actions sont également accessibles à partir du menu contextuel. Faites un clic droit sur la section de Control Center que vous utilisez en ce moment et sélectionnez la commande dont vous avez besoin dans la liste disponible.



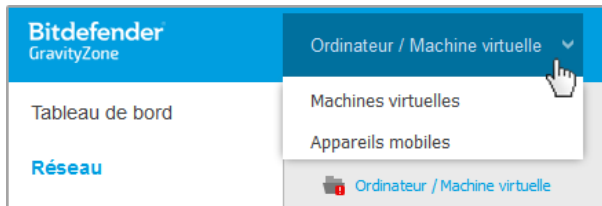
La page Rapports - Menu contextuel

4.2.5. Sélecteur d'affichage

Si vous travaillez avec différents types d'endpoints, vous pouvez les trouver regroupés sur la page **Réseau** par type sous différents affichages du réseau :

- **Ordinateurs & et Machines virtuelles** : affiche les ordinateurs et les groupes Active Directory ainsi que les postes de travail physiques et virtuels hors d'Active Directory qui sont découverts dans le réseau.
- **Machines virtuelles** : affiche l'infrastructure de l'environnement virtuel intégré à Control Center et toutes les machines virtuelles.
- **Appareils mobiles** : affiche les utilisateurs et les appareils mobiles qui leur sont affectés.

Pour sélectionner l'affichage du réseau de votre choix, cliquez sur le menu d'affichages dans l'angle supérieur droit de la page.



Le sélecteur d'affichage

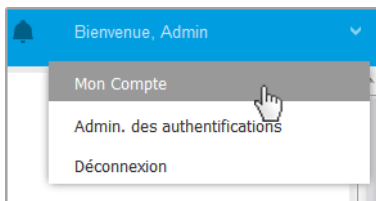
Note

Vous verrez uniquement les endpoints que vous êtes autorisé à voir, ces permissions vous étant accordées par l'administrateur qui a ajouté votre utilisateur à Control Center.

4.3. Gestion de votre compte

Pour consulter ou modifier les détails et les paramètres de votre compte :

1. Cliquez sur votre nom d'utilisateur dans l'angle supérieur droit de la console et sélectionnez **Mon Compte**.



Le menu Compte Utilisateur

2. Sous **Détails du compte**, corrigez ou actualisez les détails de votre compte. Si vous utilisez un compte utilisateur Active Directory, vous ne pouvez pas changer les détails du compte.
 - **Utilisateur.** Le nom d'utilisateur est l'identifiant unique d'un compte utilisateur et il ne peut pas être changé.
 - **Prénom & Nom .** Indiquez votre nom complet.
 - **E-mail.** Ceci est votre Login et votre e-mail de contact. Des rapports et d'importantes notifications de sécurité sont envoyés à cette adresse. Des notifications par e-mail sont envoyées automatiquement lorsque des situations présentant un risque important sont détectées dans le réseau.
 - Un lien **Changer de mot de passe** vous permet de changer de mot de passe de connexion.
3. Sous **Paramètres**, configurez les paramètres du compte en fonction de vos préférences.
 - **Fuseau horaire.** Sélectionnez dans le menu le fuseau horaire de votre compte. La console affichera les informations horaires en fonction du fuseau horaire sélectionné.
 - **Langue.** Choisissez dans le menu la langue d'affichage de la console.
 - **Temps imparti à la session.** Sélectionnez la période d'inactivité avant que votre session utilisateur n'expire.
4. Dans **Sécurité de la connexion**, configurez l'authentification à deux facteurs et contrôlez l'état des politiques disponibles pour sécuriser votre compte GravityZone. Les politiques configurées pour l'ensemble de l'entreprise sont en lecture seule.

Pour activer l'authentification à deux facteurs :

- a. **Authentification à deux facteurs.** L'authentification à deux facteurs ajoute une couche de sécurité supplémentaire à votre compte GravityZone, en demandant un code d'identification en plus de vos identifiants Control Center. Lors de votre première connexion à votre compte GravityZone, il vous sera demandé de télécharger et d'installer Google Authenticator, Microsoft Authenticator, ou tout autre système d'authentification TOTP (Time-Based One-Time Password Algorithm) - compatible avec le [standard RFC6238](#) sur un appareil mobile, de le lier à votre compte GravityZone, puis de l'utiliser lors de chaque connexion à Control Center. Google Authenticator génère un nouveau code à six chiffres toutes les 30 secondes. Pour vous connecter à Control Center, vous devrez saisir le code à six chiffres de Google Authenticator après avoir saisi votre mot de passe.

 **Note**

Vous pouvez passer trois fois cette procédure, après cela vous ne serez plus en mesure de vous identifier sans l'authentification à deux facteurs.

Pour activer l'authentification à deux facteurs :

- i. Cliquez sur le bouton **Activer** situé sous le message **Authentification à deux facteurs**.
- ii. Sur la boîte de dialogue, cliquez sur le lien approprié pour télécharger et installer Google Authenticator sur votre appareil mobile.
- iii. Sur votre appareil mobile, ouvrez Google Authenticator.
- iv. Sur l'écran **Ajouter un compte**, scannez le code QR pour lier l'application à votre compte GravityZone.

Vous pouvez également saisir à la main la clé secrète.

Cette action n'est à réaliser qu'une fois pour activer la fonctionnalité dans GravityZone.

 **Important**

Veillez à faire une copie de la clé secrète et de la conserver dans un endroit sûr. Cliquez sur **Print a backup** pour créer un fichier PDF contenant le code QR et la clé secrète. Si l'appareil mobile utilisé pour activer l'authentification à deux facteurs est perdu ou remplacé, vous devrez installer Google Authenticator sur un nouvel appareil et saisir de nouveau cette clé secrète pour le lier à votre compte GravityZone.

- v. Saisissez le code à six chiffres dans le champs **Google Authenticator**
- vi. Cliquez sur **Activer** pour finaliser l'activation de la fonctionnalité.

 **Note**

L'administrateur de votre entreprise peut rendre l'authentification à deux facteurs obligatoire pour tous les comptes GravityZone. Dans ce cas, il vous sera demandé de configurer votre authentification à deux facteurs lors de la connexion. De même, vous ne pourrez pas désactiver l'authentification à deux facteurs de votre compte tant que cette fonctionnalité sera rendue obligatoire par l'administrateur de votre entreprise.

Attention, si l'authentification à deux facteurs actuellement configurée est désactivée pour votre compte, la clé secrète ne sera plus valide.

- b. **Politique d'expiration du mot de passe.** Les modifications régulières de votre mot de passe fournissent une couche de protection supplémentaire contre l'utilisation non autorisée de vos mots de passe, ou limitent la durée de ces utilisations frauduleuses. Lorsqu'elle est activée, GravityZone vous demande de modifier votre mot de passe au plus tard après les 90 jours.
 - c. **Politique de verrouillage de compte.** Cette politique empêche l'accès à votre compte après cinq tentatives de connexion ratées consécutives. Cette mesure permet de vous protéger contre les attaques par force brute.
Pour déverrouiller votre compte, vous devez réinitialiser votre mot de passe depuis la page de connexion ou contacter un autre administrateur de GravityZone.
5. Cliquez sur **Enregistrer** pour appliquer les modifications.

**Note**

Vous ne pouvez pas supprimer votre propre compte.

4.4. Changer de mot de passe de connexion

Une fois votre compte créé, vous recevrez un e-mail avec les identifiants de connexion.

À moins que vous n'utilisiez les identifiants d'Active Directory pour accéder à Control Center, nous vous recommandons de réaliser les actions suivantes :

- Changez le mot de passe de connexion par défaut lorsque vous vous connectez au Control Center pour la première fois.
- Changez régulièrement de mot de passe de connexion.

Pour changer le mot de passe de connexion :

1. Cliquez sur votre nom d'utilisateur dans l'angle supérieur droit de la console et sélectionnez **Mon Compte**.
2. Sous **Détails du compte**, cliquez sur **Changer de mot de passe**.
3. Saisissez votre mot de passe actuel et le nouveau mot de passe dans les champs correspondants.
4. Cliquez sur **Enregistrer** pour appliquer les modifications.

5. COMPTES UTILISATEUR

Vous pouvez créer le premier compte utilisateur de GravityZone lors de la configuration initiale du Control Center, après avoir déployé l'appliance GravityZone. Le compte utilisateur initial du Control Center a le rôle administrateur de la société avec l'ensemble des droits de configuration du Control Center et d'administration du réseau. Vous pouvez créer à partir de ce compte tous les autres comptes utilisateur requis pour l'administration du réseau de votre entreprise.

Voici ce que vous avez besoin de savoir sur les comptes utilisateur de GravityZone :

- Pour autoriser à d'autres employés d'accéder à Control Center, vous pouvez créer des comptes utilisateurs individuellement ou activer l'accès dynamique pour de multiples comptes via les intégrations d'Active Directory ou des règles d'accès. Vous pouvez affecter différents rôles aux comptes utilisateur, en fonction de leur niveau d'accès dans la société.
- Pour chaque compte utilisateur, vous pouvez personnaliser l'accès aux fonctionnalités de GravityZone ou à certaines parties du réseau auquel il appartient.
- Vous pouvez uniquement administrer des comptes ayant les mêmes privilèges, ou moins, que votre compte.

	Nom d'utilisateur	E-mail	Rôle	Services
<input type="checkbox"/>	reporter	office@comp.com	Rapporteur	Ordinateurs, Machines virtuelles

La page Comptes

Les comptes existants s'affichent dans le tableau. Pour chaque compte utilisateur, vous pouvez afficher :

- Le nom d'utilisateur du compte (utilisé pour se connecter au Control Center).

- L'adresse e-mail du compte (utilisée comme adresse de contact). Des rapports et d'importantes notifications de sécurité sont envoyés à cette adresse. Des notifications par e-mail sont envoyées automatiquement lorsque des situations présentant un risque important sont détectées dans le réseau.
- Rôle utilisateur (administrateur de la société / administrateur réseau / analyste de sécurité / personnalisé).
- Les services de sécurité de GravityZone que l'utilisateur est autorisé à gérer (Ordinateurs, Machines virtuelles, Appareils mobiles).
- Le statut de l'authentification à deux facteurs, qui permet de contrôler rapidement si l'utilisateur a activé celle-ci.
- État de la règle d'accès, indique un compte utilisateur créé au moyen d'une règle de permission d'accès. Les comptes utilisateurs créés manuellement afficheront N/A.

5.1. Rôles Utilisateur

Un rôle utilisateur consiste en une combinaison spécifique de droits de l'utilisateur. Lorsque vous créez un compte utilisateur, vous pouvez sélectionner l'un des rôles prédéfinis ou créer un rôle personnalisé, en sélectionnant uniquement certains droits de l'utilisateur.

Note

Vous pouvez accorder aux comptes utilisateur les mêmes privilèges que votre compte, ou moins.

Les rôles utilisateur suivants sont disponibles :

1. **Administrateur de la société** - Généralement, un compte utilisateur unique avec le rôle Administrateur de la société est créé pour chaque société, avec un accès complet à toutes les fonctionnalités d'administration des solutions GravityZone. Un administrateur de la société configure les paramètres de Control Center, gère les clés de licence des services de sécurité et les comptes utilisateur tout en ayant des privilèges d'administration sur les paramètres de sécurité du réseau de l'entreprise. Les administrateurs de la société peuvent partager ou déléguer leurs responsabilités opérationnelles à des comptes utilisateurs administrateurs et analystes de sécurité secondaires.
2. **Administrateur réseau** - Plusieurs comptes avec un rôle Administrateur réseau peuvent être créés pour une société, avec des privilèges d'administration sur

le déploiement de l'ensemble des agents de sécurité de la société ou sur un groupe spécifique d'endpoints, y compris l'administration des utilisateurs. Les administrateurs Réseau sont responsables de la gestion active des paramètres de sécurité du réseau.

3. **Analyste de sécurité** - Les comptes analystes de sécurité sont des comptes en lecture seule. Ils permettent d'accéder uniquement aux données, rapports et journaux relatifs à la sécurité. Ces comptes peuvent être alloués aux membres du personnel ayant des responsabilités de surveillance ou à d'autres employés devant se maintenir informés de l'état de sécurité.
4. **Personnalisé** - Les rôles utilisateur prédéfinis comprennent une certaine combinaison de droits des utilisateurs. Si un rôle prédéfini ne correspond pas à vos besoins, vous pouvez créer un compte personnalisé en sélectionnant uniquement les droits qui vous intéressent.

Le tableau suivant résume les relations entre différents rôles de comptes et leurs droits. Pour plus d'informations, reportez-vous à « [Droits de l'utilisateur](#) » (p. 32).

Rôle du Compte	Comptes Enfants Autorisés	Droits de l'utilisateur
Administrateur de la société	Administrateurs de la société, Administrateurs Réseau, Analystes sécurité	Gérer la solution Gérer l'entreprise Gérer les utilisateurs Gérer les réseaux Afficher et analyser les données
Administrateur Réseau	Administrateurs réseau, Analystes de sécurité	Gérer les utilisateurs Gérer les réseaux Afficher et analyser les données
Analyste sécurité	-	Afficher et analyser les données

5.2. Droits de l'utilisateur

Vous pouvez affecter les droits utilisateurs suivants aux comptes utilisateurs de GravityZone :

- **Gérer la solution.** Vous permet de configurer les paramètres du Control Center (paramètres du serveur de messagerie et proxy, intégration à Active Directory et plateformes de virtualisation, certificats de sécurité et mises à jour de

GravityZone). Ce privilège est spécifique aux comptes administrateur de la société.

- **Gérer les utilisateurs.** Créer, modifier ou supprimer des comptes utilisateurs
- **Gérer l'entreprise.** Les utilisateurs peuvent gérer leur propre clé de licence GravityZone et modifier les paramètres du profil de leur entreprise. Ce privilège est spécifique aux comptes administrateur de la société.
- **Gérer les réseaux.** Fournit des privilèges d'administration sur les paramètres de sécurité du réseau (inventaire du réseau, politiques, tâches, packages d'installation, quarantaine). Ce privilège est spécifique aux comptes administrateur réseau.
- **Afficher et analyser les données.** Visualiser les événements et les journaux relatifs à la sécurité, gérer les rapports et le tableau de bord.

5.3. Gestion des comptes utilisateurs

Pour créer, modifier, supprimer ou configurer des comptes utilisateurs, utilisez les méthodes suivantes :

- **Gérer des comptes utilisateurs individuellement.** Utilisez cette méthode pour ajouter des comptes utilisateurs locaux ou des comptes Active Directory. !pour configurer une intégration d'AD, veuillez vous référer au Guide d'installation de GravityZone.

Avant de créer un compte utilisateur, vérifiez que vous disposez de l'adresse e-mail requise. L'utilisateur reçoit les informations de connexion à GravityZone à l'adresse e-mail indiquée.

- **Gestion de multiples comptes utilisateurs.** Utilisez cette méthode pour activer l'accès dynamique via les règles de permission d'accès. Cette méthode nécessite une intégration de domaine Active Directory. Pour plus d'informations l'intégration d'Active Directory, veuillez vous référer au Guide d'installation de GravityZone.

5.3.1. Gérer des comptes utilisateurs individuellement

Depuis Control Center, vous pouvez créer, modifier et supprimer des comptes utilisateurs individuellement.

Dépendances

- Les comptes créés en local peuvent supprimer les comptes créés via une intégration Active Directory, quel que soit leur rôle.
- Les comptes créés en local ne peuvent pas supprimer de comptes similaires, quel que soit leur rôle.

Créer des comptes utilisateurs individuellement

Pour ajouter un nouveau compte utilisateur dans Control Center :

1. Allez sur la page **Comptes**.
2. Cliquez sur le bouton **+Ajouter** en haut du tableau. Une fenêtre de configuration s'affichera.
3. Dans la section **Détails**, saisissez les paramètres suivants :

- Pour les comptes utilisateurs Active Directory saisissez les paramètres suivants :

Nom d'utilisateur des comptes utilisateurs Active Directory (AD). Choisissez un compte utilisateur dans le menu déroulant et passez à l'étape 4.

Vous pouvez uniquement ajouter des comptes utilisateurs AD si l'intégration est configurée. Lors de l'ajout d'un compte utilisateur AD, les informations sur l'utilisateur sont importées depuis le domaine qui lui est associé. L'utilisateur se connecte à Control Center en utilisant le nom d'utilisateur et le mot de passe AD.

Note

- Pour que les dernières modifications d'Active Directory soient importées dans le Control Center, cliquez sur le bouton **Synchroniser**
 - Les utilisateurs avec le droit **Gérer la solution** peuvent configurer l'intervalle de synchronisation d'Active Directory à l'aide des options disponibles sur l'onglet **Configuration > Active Directory**. Pour plus d'informations, référez-vous aux chapitres **Installer la protection > Installation et Configuration de GravityZone > Configurer les paramètres de Control Center Center** du Guide d'installation de GravityZone.
- Pour les comptes utilisateurs locaux, saisissez les paramètres suivants :

- **Nom d'utilisateur** pour le compte local. Désactivez **Importer depuis Active Directory** et saisissez un nom d'utilisateur.
 - **E-mail**. Indiquez l'adresse e-mail de l'utilisateur.
L'adresse e-mail doit être unique. Vous ne pouvez pas créer d'autre compte utilisateur avec la même adresse e-mail.
GravityZone utilise cette adresse e-mail pour envoyer des notifications.
 - **Prénom et Nom**. Saisissez le nom complet de l'utilisateur.
 - **Mot de passe**. Saisissez le mot de passe que l'utilisateur utilisera pour se connecter.
Le mot de passe doit contenir au moins une majuscule, une minuscule et un chiffre ou un caractère spécial.
 - **Confirmer**. Confirmer le mot de passe pour valider.
4. Sous la section **Paramètres et Privilèges**, configurez les paramètres suivants :
- **Fuseau horaire**. Choisissez dans le menu le fuseau horaire du compte. La console affichera les informations horaires en fonction du fuseau horaire sélectionné.
 - **Langue**. Choisissez dans le menu la langue d'affichage de la console.
 - **Rôle**. Sélectionnez le rôle de l'utilisateur. Pour des informations concernant les rôles utilisateur, reportez-vous à « [Rôles Utilisateur](#) » (p. 31).
 - **Droits**. Chaque rôle utilisateur prédéfini dispose d'une certaine configuration de droits. Vous pouvez cependant sélectionner uniquement les droits dont vous avez besoin. Le rôle utilisateur devient alors **Personnalisé**. Pour des informations concernant les droits des utilisateurs, reportez-vous à « [Droits de l'utilisateur](#) » (p. 32).
 - **Sélectionner les cibles**. Sélectionnez les groupes du réseau auxquels l'utilisateur aura accès pour chaque service de sécurité disponible. Vous pouvez restreindre l'accès de l'utilisateur à un service de sécurité GravityZone spécifique ou à certaines zones du réseau.

**Note**

Les options de la sélection cible ne s'afficheront pas pour les utilisateurs ayant le droit Gérer la solution qui, par défaut, ont des privilèges sur l'ensemble du réseau et les services de sécurité.



Important

Lorsque vous effectuez des modifications à la structure de votre réseau ou lorsque vous configurez une nouvelle intégration à un autre système vCenter Server ou XenServer, pensez à vérifier et mettre à jour les privilèges d'accès des utilisateurs existants.

5. Cliquez sur **Enregistrer** pour ajouter l'utilisateur. Le nouveau compte apparaîtra dans la liste des comptes utilisateurs.

Le Control Center envoie automatiquement à l'utilisateur un e-mail avec les détails de connexion, à condition que les paramètres du serveur de messagerie aient été configurés correctement. Pour plus d'informations sur la configuration du serveur e-mail, référez-vous au chapitre **Installer la protection > Installation et Configuration de GravityZone > Configurer les paramètres de Control Center Center** du Guide d'installation de GravityZone.

Modifier des comptes utilisateurs individuellement

Pour ajouter un compte utilisateur dans Control Center

1. Connectez-vous à la Control Center.
2. Allez sur la page **Comptes**.
3. Cliquez sur le nom de l'utilisateur.
4. Modifier les détails et les paramètres du compte utilisateur selon vos besoins.
5. Cliquez sur **Enregistrer** pour appliquer les modifications.




Note

Tous les comptes ayant un rôle **Administrateur** peuvent créer, éditer et supprimer d'autres comptes utilisateur. Vous pouvez uniquement administrer des comptes ayant les mêmes privilèges, ou moins, que votre propre compte.

Supprimer des comptes utilisateurs individuellement

Pour supprimer un compte utilisateur dans Control Center

1. Connectez-vous à la Control Center.
2. Allez sur la page **Comptes**.
3. Sélectionnez le compte utilisateur dans la liste.
4. Cliquez sur le bouton  **Supprimer** en haut du tableau.

Cliquez sur **Oui** pour confirmer.

5.3.2. Gestion de multiples comptes utilisateurs

Créer des règles d'accès pour donner à GravityZone Control Center l'accès aux utilisateurs Active Directory, en fonction des groupes de sécurité.

Configuration nécessaire

Pour gérer de multiples comptes utilisateurs, un domaine Active Directory doit être intégré à GravityZone. Pour intégrer et synchroniser un domaine Active Directory, consultez le chapitre **Active Directory** du Guide d'installation de GravityZone.

Dépendances

Les règles de permission d'accès sont liées aux groupes de sécurité Active Directory (AD) et aux comptes utilisateurs associés. Tous les changements appliqués aux domaines Active Directory peuvent avoir un impact sur les règles de permission d'accès associées. Voici ce que vous devez savoir sur la relation entre règles, utilisateurs et domaines Active Directory :

- Une règle de permission accès ajoute un compte utilisateur uniquement si l'adresse e-mail n'est pas déjà associée à un compte existant.
- Pour les adresses e-mail au sein d'un groupe de sécurité, la règle de permission d'accès crée un compte utilisateur GravityZone uniquement pour le premier compte utilisateur Active Directory qui se connecte à Control Center.

Par exemple, un groupe de sécurité contient une adresse e-mail dupliquée pour différents utilisateurs et ils essaient tous de se connecter à Control Center en utilisant leurs identifiants Active Directory. Si une règle de permission d'accès est associée à ce domaine Active Directory spécifique, elle créera un compte utilisateur uniquement pour le premier utilisateur à se connecter à Control Center en utilisant l'adresse e-mail dupliquée.

- Les comptes utilisateurs créés via des règles de permission d'accès deviennent inactifs s'ils sont supprimés du groupe de sécurité AD auquel ils sont associés. Les mêmes utilisateurs peuvent devenir inactifs s'ils sont associés à une nouvelle règle d'accès.
- Les règles d'accès passent en lecture seule lorsqu'un domaine Active Directory associé n'est plus intégré à GravityZone. Les utilisateurs associés à cette règle deviennent inactifs.

- Les comptes utilisateur créés via des règles d'accès ne peuvent pas supprimer des utilisateurs créés en local.
- Les comptes utilisateur créés via des règles d'accès ne peuvent pas supprimer de comptes similaires ayant le rôle d'Administrateur de la société.

Créer de multiples comptes utilisateurs

Pour ajouter de multiples comptes utilisateurs, vous devez créer des règles de permission d'accès. Les règles de permission d'accès sont associées aux groupes de sécurité Active Directory.

Pour ajouter une règle de permission d'accès :

1. Allez sur **Configuration > Active Directory > Permissions d'accès**.
2. Si vous avez de multiples intégrations, sélectionnez un domaine dans le coin supérieur gauche du tableau.
3. Cliquez sur **+ Ajouter** à gauche du tableau.
4. Configurez les paramètres de la permission d'accès suivante :
 - **Priorité.** Les règles sont traitées par ordre de priorité. Plus le numéro de la règle est petit, plus la priorité est élevée.
 - **Nom.** Le nom de la règle d'accès.
 - **Domaine.** Le domaine depuis lequel ajouter des groupes de sécurité.
 - **Groupes de sécurité.** Les groupes de sécurité qui contiennent vos futurs utilisateurs GravityZone. Vous pouvez utiliser le champ à complétion automatique. Les groupes de sécurité ajoutés à cette liste ne sont pas sujets à changement, ajout ou suppression une fois la règle d'accès enregistrée.
 - **Fuseau horaire.** Le fuseau horaire de l'utilisateur.
 - **Langue.** La langue d'affichage de la console.
 - **Rôle.** Rôles utilisateurs prédéfinis. Pour plus de détails, consultez le chapitre **Comptes utilisateurs** du Guide de l'administrateur de GravityZone.



Note

Vous pouvez octroyer des privilèges à d'autres utilisateurs (et révoquer ces privilèges), pour peu que ces derniers disposent des mêmes privilèges ou de moins de privilèges que ceux de votre compte.

- **Droits.** Chaque rôle utilisateur prédéfini dispose d'une certaine configuration de droits. Pour plus de détails, consultez le chapitre **Droits de l'utilisateur** du Guide de l'administrateur de GravityZone.
- **Sélectionner les cibles** Sélectionnez les groupes du réseau auxquels l'utilisateur aura accès pour chaque service de sécurité disponible. Vous pouvez restreindre l'accès de l'utilisateur à un service de sécurité GravityZone spécifique ou à certaines zones du réseau.

**Note**

Les options de la sélection cible ne s'afficheront pas pour les utilisateurs ayant le droit Gérer la solution qui, par défaut, ont des privilèges sur l'ensemble du réseau et les services de sécurité.

5. Cliquez sur Enregistrer.

La règle d'accès est enregistrée s'il n'y a aucun impact utilisateur. Il vous est autrement demandé de définir des exclusions d'utilisateur. Par exemple, lorsque vous ajoutez une règle avec une priorité plus élevée, les utilisateurs impactés associés à d'autres règles sont liés à l'ancienne règle.

6. Si besoin, sélectionnez l'utilisateur que vous voulez exclure. Pour en apprendre plus, consultez [Exclusions des comptes utilisateurs](#).
7. Cliquez sur **Confirmer**. La règle est affichée sur la page **Permissions d'accès**.

Les utilisateurs appartenant aux groupes de sécurité spécifiés par les règles d'accès peuvent désormais accéder à la Control Center GravityZone à l'aide de leurs identifiants de domaine. La Control Center crée automatiquement de nouveaux comptes utilisateurs lorsqu'ils se connectent pour la première fois, en utilisant leur adresse e-mail et leur mot de passe Active Directory.

Les comptes utilisateurs créés au moyen d'une règle d'accès ont le nom de la règle d'accès affichée sur la page **Comptes**, dans la colonne **Règle d'accès**.

Modifier de multiples comptes utilisateurs

Pour modifier une règle de permission d'accès :

1. Allez sur **Configuration > Active Directory > Permissions d'accès**.
2. Sélectionnez le nom de votre règle d'accès pour ouvrir la fenêtre de configuration.
3. Modifier les paramètres d'une permission d'accès. Pour plus d'informations, reportez-vous à [Ajouter des permissions d'accès](#).

4. Cliquez sur **Enregistrer**. La règle est enregistrée s'il n'y a aucun impact utilisateur. Il vous est autrement demandé de définir des exclusions des comptes utilisateurs. Par exemple, si vous modifiez la priorité d'une règle, les utilisateurs impactés peuvent basculer sur une autre règle.
5. Si besoin, sélectionnez l'utilisateur que vous voulez exclure. Pour en apprendre plus, consultez [Exclusions des comptes utilisateurs](#).
6. Cliquez sur **Confirmer**.

**Note**

Vous pouvez dissocier des comptes utilisateurs créés au moyen d'une règle d'accès en modifiant leurs droits dans la Control Center. Le compte utilisateur ne peut être associé de nouveau à la règle d'accès.

Supprimer de multiples comptes utilisateurs

Pour supprimer une règle d'accès :

1. Allez sur **Configuration > Active Directory > Permissions d'accès**.
2. Sélectionnez la règle d'accès que vous souhaitez supprimer et cliquez sur **Supprimer**. Une fenêtre vous invite à confirmer votre action. En cas d'impact sur l'utilisateur, il vous sera demandé de définir des exclusions de comptes utilisateurs. Par exemple, vous pouvez souhaiter définir des exclusions d'utilisateur pour les utilisateurs impacté par la suppression d'une règle.
3. Si besoin, sélectionnez l'utilisateur que vous voulez exclure. Pour en apprendre plus, consultez [Exclusions des utilisateurs](#).
4. Cliquez sur **Confirmer**.

Supprimer une règle révoquera l'accès aux comptes utilisateurs associés. Tous les utilisateurs créés par ce biais seront retirés, sauf si d'autres règles leur donnent des accès.

Exclusions des comptes utilisateurs

Lorsque vous ajoutez, modifiez ou supprimez des règles de permission d'accès qui ont un impact sur l'utilisateur, vous pouvez souhaiter définir des exclusions de comptes utilisateurs. Vous pouvez également pouvoir voir les effets sur les utilisateurs impactés.

Définissez des exclusions d'utilisateurs comme suit :

1. Sélectionnez l'utilisateur que vous voulez exclure. Ou cochez la case située en haut du tableau pour ajouter tous les utilisateurs à la liste.
2. Cliquez sur le **X** dans la case d'un utilisateur pour le retirer de la liste.

5.4. Réinitialiser les mots de passe de connexion

Les propriétaires de comptes qui oublient leur mot de passe peuvent le réinitialiser à l'aide du lien de récupération du mot de passe de la page de connexion. Vous pouvez également réinitialiser un mot de passe de connexion oublié en modifiant le compte correspondant à partir de la console.

Pour réinitialiser le mot de passe de connexion d'un utilisateur :

1. Connectez-vous à la Control Center.
2. Allez sur la page **Comptes**.
3. Cliquez sur le nom de l'utilisateur.
4. Indiquez un nouveau mot de passe dans les champs correspondants (sous **Détails**).
5. Cliquez sur **Enregistrer** pour appliquer les modifications. Le propriétaire du compte recevra un e-mail avec le nouveau mot de passe.

5.5. Gérer l'authentification à deux facteurs

En cliquant sur un compte utilisateur, vous pourrez voir le statut de son authentification à deux facteurs (activée ou désactivée) dans la section **Authentification à deux facteurs**. Vous pouvez prendre les mesures suivantes :

- **Réinitialiser ou désactiver l'authentification à deux facteurs de l'utilisateur.** Si un utilisateur avec l'authentification à deux facteurs a changé d'appareil mobile ou l'a réinitialisé, et a perdu sa clé secrète :
 1. Saisissez votre mot de passe GravityZone dans le champ correspondant.
 2. Cliquez sur **Réinitialiser** (si l'authentification à deux facteurs est obligatoire) ou **Désactiver** (si elle ne l'est pas).
 3. Un message de confirmation vous informera que l'authentification à deux facteurs a été réinitialisée / désactivée pour l'utilisateur sélectionné.

Une fois l'authentification à deux facteurs réinitialisée, si cette fonctionnalité a été rendue obligatoire, une fenêtre de configuration demandera à l'utilisateur de la configurer de nouveau avec une nouvelle clé secrète.

- Si l'authentification à deux facteurs de l'utilisateur est désactivée et que vous voulez l'activer, vous devrez demander à l'utilisateur de le faire depuis les paramètres de son compte.



Note

Si vous avez un compte administrateur pour votre entreprise, vous pouvez rendre l'authentification à deux facteurs obligatoire pour tous les comptes GravityZone. Pour en apprendre plus, rendez-vous dans le chapitre **Installation de la protection > Installation et configuration de GravityZone > Configuration des paramètres du Control Center**.



Important

L'application d'authentification choisie (Google Authenticator, Microsoft Authenticator, ou toute autre application d'authentification TOTP (Time-Based One-Time Password Algorithm) - compatible avec le [standard RFC6238](#)) combine la clé secrète avec l'horodatage actuel de l'appareil mobile pour générer un code à six chiffres. Attention, la date et l'heure de l'appareil mobile et de l'appliance GravityZone doivent être identiques pour que le code à six chiffres soit valide. Pour éviter tout problème de synchronisation des dates et heures, nous recommandons d'activer leur configuration automatique sur l'appareil mobile.

Une autre manière de contrôler les changements relatifs à l'authentification à deux facteurs des comptes utilisateurs consiste à se rendre sur la page [Comptes > Activité des utilisateurs](#) et de filtrer les journaux d'activités avec les filtres suivants :

- Zone > Comptes / Entreprise
- Action > Modifiée

Pour en apprendre plus sur l'activation de l'authentification à deux facteurs, consultez « [Gestion de votre compte](#) » (p. 26)

6. GESTION DES OBJETS DU RÉSEAU

La page **Réseau** fournit plusieurs fonctionnalités pour explorer et gérer chaque type d'objet du réseau disponible dans Control Center (ordinateurs, machines virtuelles et appareils mobiles). La section **Réseau** consiste en une interface à deux panneaux affichant l'état en temps réel des objets du réseau :

Nom	OS	IP	Dernière connexion	Étiquette
WIN-Q2HJJBVA15	Windows	10.10.113.3	N/D	N/D
WIN_2K3_SP2_R2_	Windows 2003	10.10.125.24	N/D	N/D
WIN-3AUH2117FQJ	Windows 2008 R2	10.10.18.228	N/D	N/D
WIN-3FLSCA80PRS	Windows	10.10.15.48	N/D	N/D
WIN-3FTVUCH2MEU	Windows 2012	10.10.124.238	N/D	N/D

La Page Réseau

1. Le panneau de gauche affiche l'arborescence du réseau disponible. Selon l'affichage réseau sélectionné, ce panneau affiche l'infrastructure réseau intégrée à Control Center telle qu'Active Directory, vCenter Server ou Xen Server.

En même temps, tous les ordinateurs et les machines virtuelles détectés dans votre réseau n'appartenant à aucune infrastructure intégrée apparaissent sous **Groupes personnalisés**.

Tous les endpoints supprimés sont conservés dans le dossier **Supprimé**. Pour en savoir plus, reportez-vous à « [Supprimer des endpoints de l'inventaire du réseau](#) » (p. 214).



Note

Vous pouvez afficher et gérer uniquement les groupes pour lesquels vous avez des droits d'administrateur.

2. Le panneau de droite affiche le contenu du groupe que vous avez sélectionné dans le panneau de gauche. Ce panneau consiste en une grille dans laquelle les lignes contiennent des objets du réseau et les colonnes affichent des informations spécifiques pour chaque type d'objet.

Ce panneau vous permet d'effectuer les actions suivantes :

- Afficher des informations détaillées sur chaque élément du réseau sous votre compte. Vous pouvez connaître l'état de chaque objet en consultant l'icône qui se trouve à côté de son nom. Placez le curseur de la souris sur l'icône pour afficher des info-bulles. Cliquez sur le nom de l'objet pour faire apparaître une fenêtre contenant plus de précisions.

Chaque type d'objet tel qu'un ordinateur, une machine virtuelle ou un dossier est représenté par une icône spécifique. En même temps, chaque objet du réseau peut avoir un certain état, concernant l'état d'administration, les problèmes de sécurité, la connectivité, etc. Pour des informations concernant la description de chaque icône d'objet du réseau et les états existants, consultez « États et types d'objets du réseau » (p. 527).

- Utilisez la [barre d'outils d'actions](#) en haut du tableau pour effectuer certaines opérations pour chaque objet du réseau (telles qu'exécuter des tâches, créer des rapports, affecter des politiques et supprimer) et [actualisez](#) les données du tableau.
3. le [sélecteur d'affichage](#) en haut des panneaux du réseau permet d'alterner entre différents contenus d'inventaire du réseau, en fonction du type d'endpoint avec lequel vous souhaitez travailler.
 4. Le menu **Filtres** disponible en haut des panneaux réseau vous aide à afficher facilement seulement des objets de réseau spécifiques, fournissant plusieurs critères de filtrage. Les options de menu **Filtres** sont liés à l'affichage réseau actuellement sélectionné.

La section **Réseau** vous permet également de gérer les packages d'installation et les tâches pour chaque type d'objet du réseau.

Note

Pour plus d'informations sur les packages d'installation, consultez le Guide d'installation de GravityZone.

Pour plus d'informations sur les objets réseau, merci de vous référer à :

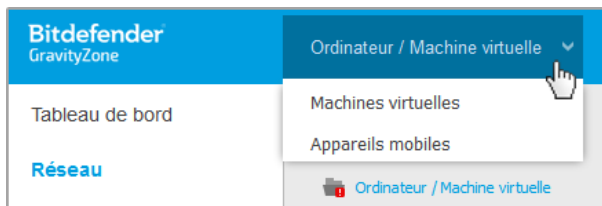
- « [Travailler avec les affichages réseau](#) » (p. 45)
- « [Ordinateurs](#) » (p. 48)
- « [Machines virtuelles](#) » (p. 108)
- « [Appareils mobiles](#) » (p. 169)
- « [Inventaire des patchs](#) » (p. 201)
- « [Afficher et gérer des tâches](#) » (p. 210)
- « [Supprimer des endpoints de l'inventaire du réseau](#) » (p. 214)
- « [Configuration des paramètres du réseau](#) » (p. 216)

- « Configuration des paramètres de Security Server » (p. 218)
- « Admin. des authentifications » (p. 219)

6.1. Travailler avec les affichages réseau

Les différents types d'endpoints disponibles dans Control Center sont regroupés sur la page **Réseau** par différents affichages réseau. Chaque affichage réseau affiche un type d'infrastructure réseau spécifique en fonction du type d'endpoint que vous souhaitez gérer.

Pour changer l'affichage du réseau, rendez-vous dans l'angle supérieur gauche de la page **Réseau** et cliquez sur le sélecteur d'affichage :




Le sélecteur d'affichage

Les affichages réseau suivants sont disponibles :

- [Ordinateur / Machine virtuelle](#)
- [Machines virtuelles](#)
- [Appareils mobiles](#)

6.1.1. Ordinateur / Machine virtuelle

Cet affichage est conçu pour les ordinateurs et les machines virtuelles intégrés à Active Directory, fournissant des [actions](#) et des [options de filtrage](#) spécifiques pour gérer les ordinateurs de votre réseau. Si une intégration à Active Directory est disponible, l'arborescence Active Directory est chargée, avec les endpoints correspondants.

Lorsque vous travaillez dans l'affichage **Ordinateurs et Machines virtuelles**, vous pouvez synchroniser à tout moment le contenu de Control Center avec votre Active Directory à l'aide du bouton  **Synchronisation avec Active Directory** de la barre d'outils des actions.

En même temps, tous les ordinateurs et les machines virtuelles qui ne sont pas intégrés à Active Directory sont regroupés sous Groupes personnalisés. Ce dossier peut contenir les types d'endpoints suivants :

- Ordinateurs et machines virtuelles disponibles dans votre réseau hors d'Active Directory.
- Machines virtuelles d'une infrastructure virtualisée disponibles dans votre réseau.
- Les serveurs de sécurité déjà installés et configurés sur un hôte de votre réseau.



Note

Lorsqu'une infrastructure virtualisée est disponible, vous pouvez déployer et gérer des Serveurs de Sécurité à partir de l'affichage **Machines virtuelles**. Les Serveurs de Sécurité peuvent sinon uniquement être installés et configurés en local sur l'hôte.



Important

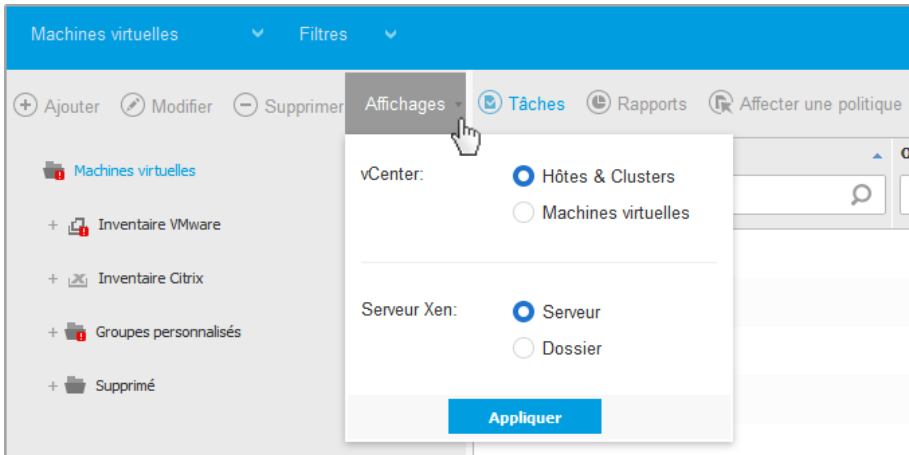
L'affectation de politiques aux machines virtuelles à partir de l'affichage **Ordinateurs et Machines virtuelles** peut être limitée par le gestionnaire de la solution GravityZone lors de la configuration du Serveur vCenter ou du Serveur Xen sur la page **Configuration > Responsable virtualisation Virtualisation**. Pour plus d'informations, référez-vous au chapitre **Installer la protection > Installation et Configuration de GravityZone** du Guide d'Installation de GravityZone.

6.1.2. Machines virtuelles

Cet affichage est spécialement conçu pour afficher vos intégrations à l'infrastructure virtualisée. Les [options de filtrage](#) disponibles dans cet affichage vous permettent de sélectionner des critères spéciaux pour afficher les entités de l'environnement virtuel.

Vous pouvez afficher vos inventaires virtuels Nutanix, VMware ou Citrix dans le panneau de gauche.

Vous trouverez également en haut du panneau de gauche le menu **Affichages**, vous permettant de choisir le mode d'affichage des inventaires virtuels.



La page Réseau - Affichages Machines virtuelles

Toutes les machines virtuelles de votre réseau qui ne sont pas intégrées dans une infrastructure virtuelle apparaissent sous **Groupes personnalisés**.

Pour accéder à l'infrastructure virtualisée intégrée à Control Center, vous devez indiquer vos identifiants utilisateur pour chaque système vCenter Server disponible. Le Control Center utilise vos identifiants pour se connecter à l'infrastructure virtualisée, en affichant uniquement les ressources auxquelles vous avez accès (en fonction de ce qui est défini dans vCenter Server). Si vous n'avez pas précisé vos informations d'authentification, on vous demandera de les saisir lorsque vous tenterez de parcourir l'inventaire de tout vCenter Server. Les authentifiants que vous avez indiqués sont enregistrés dans votre Administrateur des authentifications afin que vous n'ayez pas besoin de les saisir la prochaine fois.

6.1.3. Appareils mobiles

Cet affichage est conçu exclusivement pour afficher et gérer les appareils mobiles disponibles dans votre réseau, en fournissant des **actions** et des **options de filtrage** spécifiques.

Cet affichage spécifique vous permet d'afficher les entités du réseau par utilisateur ou par appareil.

Le panneau du réseau affiche la structure arborescente de votre Active Directory, le cas échéant. Dans ce cas, tous les utilisateurs d'Active Directory apparaîtront

dans l'inventaire de votre réseau ainsi que les appareils mobiles qui leur sont affectés.



Note

Les détails de l'utilisateur Active Directory sont chargés automatiquement et ne peuvent pas être modifiés.

Groupes personnalisés contient tous les utilisateurs d'appareils mobiles que vous avez ajoutés manuellement à Control Center.

6.2. Ordinateurs

Pour afficher les ordinateurs sous votre compte, allez sur la page **Réseau** et sélectionnez **Ordinateurs et Machines virtuelles** dans le [sélecteur d'affichage](#).

Vous pouvez voir la structure du réseau disponible dans le panneau de gauche et des informations sur chaque endpoint dans le panneau de droite.


Au début, tous les ordinateurs et les machines virtuelles détectés dans votre réseau apparaissent sous [non administré](#) de sorte que vous pouvez installer leur protection à distance.

Pour personnaliser les informations sur un ordinateur présentées dans le tableau :

1. Cliquez sur le bouton **III Colonnes** à droite de la [barre d'action](#).
2. Sélectionnez les colonnes que vous souhaitez afficher.
3. Cliquez sur le bouton **Réinitialiser** pour rétablir l'affichage des colonnes par défaut.

La page **Réseau** vous permet de gérer les ordinateurs comme suit :

- [Vérifier l'état de l'ordinateur](#)
- [Afficher des informations sur un ordinateur](#)
- [Organiser les ordinateurs dans des groupes](#)
- [Trier, filtrer et rechercher](#)
- [Gérer les patchs](#)
- [Exécuter des tâches](#)
- [Créer des rapports rapides](#)
- [Affecter des politiques](#)
- [Synchronisation avec Active Directory](#)

Pour afficher les informations les plus récentes dans le tableau, cliquez sur le bouton  **Actualiser** dans l'angle inférieur gauche du tableau. Cela peut être nécessaire lorsque vous passez du temps sur la page.

6.2.1. Vérifier l'état des ordinateurs

Chaque ordinateur est représenté sur la page du réseau par une icône spécifique à son type et à son état.





Consultez « [États et types d'objets du réseau](#) » (p. 527) pour une liste des types d'icônes et des états existants.

Pour de plus amples informations sur l'état, reportez-vous à :

- [État d'administration](#)
- [État de la connectivité](#)
- [État de sécurité](#)



État d'administration

Les ordinateurs peuvent avoir les états d'administration suivants :

-  **Administré** - ordinateurs sur lesquels l'agent de sécurité est installé.
-  **Redémarrage en attente** - endpoints nécessitant un redémarrage système après l'installation ou la mise à jour de la protection Bitdefender.
-  **Non administré** - ordinateurs détectés sur lesquels l'agent de sécurité n'a pas encore été installé.
-  **Supprimés** - les ordinateurs que vous avez supprimés de Control Center. Pour plus d'informations, reportez-vous à « [Supprimer des endpoints de l'inventaire du réseau](#) » (p. 214).

État de la connectivité

L'état de la connectivité concerne uniquement les ordinateurs administrés. De ce point de vue, les ordinateurs administrés peuvent être :

-  **En ligne**. Une icône bleue indique que l'ordinateur est en ligne.
-  **Hors connexion**. Une icône grise indique que l'ordinateur est hors connexion.

Un ordinateur est hors connexion si l'agent de sécurité est inactif pendant plus de 5 minutes. Les raisons pour lesquelles vos ordinateurs apparaissent hors-ligne :

- L'ordinateur est arrêté, en veille ou en veille prolongée.

**Note**

Les ordinateurs apparaissent en ligne, même quand ils sont verrouillés ou que l'utilisateur est déconnecté.

- L'agent de sécurité n'a pas de connectivité avec le Serveur de communication de GravityZone :
 - L'ordinateur peut être déconnecté du réseau.
 - Un routeur ou un pare-feu du réseau peut bloquer la communication entre l'agent de sécurité et le Serveur de communication de GravityZone.
 - L'ordinateur se trouve derrière un serveur proxy et les paramètres du proxy n'ont pas été configurés correctement dans la politique qui est appliquée.

**Avertissement**

Pour les ordinateurs derrière un serveur proxy, les paramètres du proxy doivent être correctement configurés dans le package d'installation de l'agent de sécurité, sans quoi l'ordinateur ne communiquera pas avec la console GravityZone et apparaîtra toujours comme étant hors connexion, même si une [politique avec les paramètres du proxy adaptés](#) est appliquée après l'installation.

- L'agent de sécurité pourrait ne pas fonctionner correctement.

Pour connaître la durée d'inactivité des ordinateurs :

1. Affichez uniquement les ordinateurs administrés. Cliquez sur le menu **Filtres** situé au-dessus du tableau, sélectionnez toutes les options « Administré » dont vous avez besoin dans l'onglet **Sécurité**, sélectionnez **Tous les éléments de manière récurrente** dans l'onglet **Profondeur** et cliquez sur **Enregistrer**.
2. Cliquez sur l'en-tête de la colonne **Dernière connexion** pour trier les ordinateurs par période d'inactivité.

Vous pouvez ignorer les périodes d'inactivité les plus courtes (minutes, heures), car elles sont probablement le résultat d'une condition temporaire. Par exemple, l'ordinateur est actuellement arrêté.



De longues périodes d'inactivité (jours, semaines) indiquent en général un problème avec l'ordinateur.

**Note**

Nous vous recommandons d'[actualiser](#) le tableau du réseau de temps en temps, afin que les informations sur les endpoints tiennent compte des dernières modifications.

État de sécurité


L'état de sécurité concerne uniquement les ordinateurs administrés. Vous pouvez identifier les ordinateurs ayant des problèmes de sécurité en vérifiant les icônes d'état présentant un symbole d'avertissement :

-  Ordinateur administré, avec des problèmes, en ligne.
-  Ordinateur administré, avec des problèmes, hors connexion.

Un ordinateur a des problèmes de sécurité si au moins l'une des situations suivantes est remplie :

- La protection antimalware est désactivée.
- La licence est arrivée à expiration.
- Le produit de l'agent de sécurité n'est pas à jour.
- Le contenu de sécurité est périmé.
- Des malwares ont été détectés.
- La connexion avec les Services Cloud Bitdefender n'a pas pu être établie. Il se peut que cela soit dû à l'une des raisons suivantes :
 - L'ordinateur a des problèmes de connectivité Internet.
 - Un pare-feu du réseau bloque la connexion avec les Services Cloud Bitdefender.
 - Le port 443, requis pour la communication avec les Services Cloud Bitdefender, est fermé.

Dans ce cas, la protection antimalware repose uniquement sur des moteurs locaux, alors que l'analyse dans le cloud est désactivée, ce qui signifie que l'agent de sécurité ne peut pas fournir une protection en temps réel complète.

Si vous remarquez un ordinateur avec des problèmes de sécurité, cliquez sur son nom pour afficher la fenêtre **Informations**. Vous pouvez identifier les problèmes de sécurité par l'icône . Pensez à rechercher les informations de sécurité dans tous les [onglets de la page des informations](#). Affichez l'info-bulle de l'icône pour plus d'informations. D'autres enquêtes locales peuvent être nécessaires.



Note

Nous vous recommandons d'[actualiser](#) le tableau du réseau de temps en temps, afin que les informations sur les endpoints tiennent compte des dernières modifications.

6.2.2. Afficher des informations sur un ordinateur

Vous pouvez obtenir des informations détaillées sur chaque ordinateur à partir de la page **Réseau** comme suit :

- [Consulter la page Réseau](#)
- [Consulter la fenêtre Information](#)

Consulter la page Réseau

Pour en apprendre plus sur un ordinateur, consultez les informations disponibles dans le tableau situé à droite de la page **Réseau**.

Vous pouvez supprimer ou ajouter des colonnes d'informations sur l'endpoint en cliquant sur le bouton **III Colonnes** situé en haut à droite du panneau.

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
3. Sélectionnez le groupe souhaité dans le panneau de gauche.
Tous les endpoints disponibles dans le groupe sélectionné apparaissent dans le tableau du panneau de droite.
4. Vous pouvez identifier facilement l'état de l'ordinateur en consultant l'icône correspondante. Pour plus d'informations, reportez-vous à « [Vérifier l'état des ordinateurs](#) » (p. 49).
5. Consultez les informations affichées sur les colonnes pour chaque ordinateur. Utilisez la ligne d'en-tête pour retrouver au fil de votre saisie le nom des endpoints, en fonction des critères disponibles :
 - **Nom** : nom de l'endpoint.
 - **FQDN** : nom de domaine complet comprenant le nom d'hôte et le nom de domaine.
 - **OS** : système d'exploitation installé sur l'endpoint.
 - **IP** : adresse IP de l'endpoint.
 - **Dernière connexion** : date et heure auxquelles l'endpoint a été vu en ligne pour la dernière fois.

 **Note**

Il est important de surveiller le champ **Dernière connexion** car de longues périodes d'inactivité peuvent signifier qu'il existe un problème de communication ou qu'un ordinateur est déconnecté.

- **Étiquette** : une chaîne personnalisée contenant des informations supplémentaires relatives au endpoint. Vous pouvez ajouter une étiquette dans la fenêtre **Information** de l'endpoint pour l'utiliser pour vos recherches.
- **Politique** : la politique appliquée au endpoint, avec un lien pour consulter ou modifier les réglages de la politique.

Consulter la fenêtre Information

Dans la partie droite de la page **Réseau**, cliquez sur le nom de l'endpoint que vous voulez voir dans la fenêtre **Information**. La fenêtre n'affiche que les données disponibles pour l'endpoint sélectionné, regroupées en plusieurs onglets.

Vous trouverez ci-après une liste exhaustive des informations que vous pouvez trouver dans la fenêtre **Information**, en fonction du type d'endpoint et de ses informations de sécurité.

Onglet Général

- Informations générales sur l'ordinateur telles que les nom, nom de domaine complet, adresse IP, système d'exploitation, infrastructure, groupe parent et état actuel de la connexion.

Dans cette section, vous pouvez affecter une étiquette à un endpoint. Vous pourrez retrouver facilement les endpoints avec la même étiquette et réaliser des actions sur eux, quel que soit leur emplacement sur le réseau. Pour plus d'informations sur le filtrage des endpoints, consultez « [Trier, filtrer et rechercher des ordinateurs](#) » (p. 67).

- Informations relatives aux couches de sécurité, avec notamment la liste des technologies de sécurité dont vous avez fait l'acquisition pour votre solution GravityZone et le statut de leur licence, qui peut être :
 - **Disponible / Active** – la clé de licence de cette couche de protection est active sur l'endpoint.
 - **Expiré** – la clé de licence de cette couche de protection est expirée.
 - **En attente** – la clé de licence n'est pas confirmée pour le moment.



Note

Des informations supplémentaires concernant les couches de protection sont disponibles dans l'onglet **Protection**.

- **Connexion du relais:** Le nom, l'IP et l'étiquette du relais auquel l'endpoint est connecté, le cas échéant.

Informations			
Général Protection Politique Journaux			
Ordinateur	Couches de protection		
Nom:	CC-WIN7X32	Endpoint:	Actif
FQDN:	cc-win7x32.newdomain.loc iz		
IP:	10.10.192.149		
OS:	Windows 8.1 Pro		
Étiquette:	<input type="text"/>		
Infrastructure:	Groupes personnalisés		
Groupe:	Custom Groups		
État:	En ligne		
Dernier changement d'état:	En ligne		
Enregistrer		Fermer	


Fenêtre Informations - Onglet Général


Onglet Protection

Cet onglet contient des détails sur la protection appliquée à l'endpoint, et traite des éléments suivants :

- Informations relatives à l'agent de sécurité telles que le nom et la version du produit, l'état de mise à jour et l'emplacement des mises à jour. Pour la protection Exchange, un moteur antispam est également disponible.
- Statut de sécurité pour chaque couche de protection. Ce statut apparaît à droite du nom de la couche de protection :
 - **Sécurisé**, quand il n'est fait état d'aucun problème de sécurité sur l'endpoint bénéficiant de la couche de protection.
 - **Vulnérable**, quand il est fait état de problèmes de sécurité sur l'endpoint bénéficiant de la couche de protection. Pour plus d'informations, reportez-vous à « [État de sécurité](#) » (p. 51).

- Security Server associé. Chaque Security Server affecté est affiché en cas de déploiements sans agent ou lorsque les moteurs d'analyse des agents de sécurité sont paramétrés pour utiliser l'analyse à distance. Les informations relatives au Security Server vous aident à identifier l'appliance virtuelle et à obtenir son état de mise à jour.
- L'état des modules de protection. Vous pouvez afficher facilement les modules de protection ayant été installés sur l'endpoint ainsi que l'état des modules disponibles (**Activés/Désactivés**) configurés via la politique appliquée.
- Un aperçu rapide concernant l'activité des modules et les rapports sur les malwares dans la journée en cours.

Cliquez sur le lien  **Affichage** pour accéder aux options de rapport puis générer le rapport. Pour plus d'informations, reportez-vous à « [Création de rapports](#) » (p. 448)

- Informations relatives à la couche de protection Sandbox Analyzer :
 - État d'utilisation de Sandbox Analyzer sur l'endpoint, affiché à droite de la fenêtre :
 - **Actif** : Sandbox Analyzer dispose d'une licence et est activé via une politique sur l'endpoint.
 - **Inactif** : Sandbox Analyzer dispose d'une licence, mais n'est pas activé via une politique sur l'endpoint.
 - Nom de l'agent agissant en tant que capteur d'alimentation.
 - État du module sur le endpoint :
 - **Éteint** - Sandbox Analyzer n'est pas activé sur l'endpoint via une politique.
 - **Éteint** - Sandbox Analyzer n'est pas activé sur l'endpoint via une politique.
 - Détection des menaces survenues la semaine précédente, en cliquant sur le lien  **Afficher** afin d'accéder au rapport.
- Informations supplémentaires concernant le module de chiffrement :
 - Volumes détectés (y compris le disque de démarrage).
 - L'état de chiffrement de chaque volume (qui peut être **Chiffré**, **Chiffrement en cours**, **Déchiffrement en cours**, **Non chiffré**, **Bloqué** ou **En pause**).

Cliquez sur le lien **Récupération** afin d'obtenir la clé de récupération correspondant au volume chiffré associé. Pour de plus amples informations relatives aux clés de récupérations, veuillez vous référer à « » (p. 106).

- L'état de la télémétrie de la sécurité, qui vous informe si la connexion entre l'endpoint et le serveur SIEM est établie et fonctionnelle, est désactivée, ou rencontre des problèmes.

Informations

Général Protection Politique Journaux

Protection des postes de travail Vulnérable !

B Agent

Type: BEST

Version du produit: 6.2.4.649

Dernière mise à jour du produit: 21 octobre 2015 09:33:15

Version des signatures: 7.63005 !

Dernière mise à jour des signatures: 21 octobre 2015 09:33:15

Moteur d'analyse principal: Analyse locale

Moteur d'analyse de secours: Aucun(e)

C Présentation

↳ Modules

Antimalware: Activé

Power user: Désactivé

Advanced Threat Control: Activé

↳ Rapport(aujourd'hui)

État des malwares: -> Aucune détection Afficher

Activité des malwares: -> Aucune activité Afficher

Enregistrer Fermer

Fenêtre Informations - Onglet Protection

Onglet Politique

Un endpoint peut disposer d'une ou de plusieurs politiques, mais seule une politique peut être active à la fois. L'onglet **Politique** affiche des informations sur toutes les politiques qui s'appliquent au endpoint.

- Le nom de la politique active. Cliquez sur le nom de la politique pour ouvrir le modèle de la politique et afficher ses paramètres.
- Le type de politique active, qui peut être :
 - **Appareil** : lorsque la politique est manuellement affectée au endpoint par l'administrateur réseau.

- **Emplacement** : une politique à base de règle assignée au endpoint si les réglages réseau de l'endpoint respectent les conditions d'une **règle d'affectation** existante.
 Par exemple, un ordinateur a assigné deux politiques liées à l'emplacement : l'une appelée *Bureau*, qui est active lorsqu'elle est connectée au LAN de l'entreprise, et *Itinérance*, qui s'active lorsque l'utilisateur travaille à distance et se connecte à d'autres réseaux.
- **Utilisateur** : une politique à base de règle assignée au endpoint s'il respecte l'objectif Active Directory d'une règle d'affectation existante.
- **Externe (NSX)** : lorsque la politique est définie dans l'environnement VMware NSX.
- Le type d'affectation de politique active, qui peut être :
 - **Directe** : lorsque la politique est directement appliquée au endpoint.
 - **Héritée** : lorsque l'endpoint hérite la politique d'un groupe parent.
- **Politiques applicables** : affiche la liste des politiques liées aux règles d'affectation existantes. Ces politiques peuvent s'appliquer au endpoint lorsqu'il remplit les conditions des règles d'affectation liées.

Informations ✕

Général Protection **Politique** Journaux

Résumé

Politique active: [Politique par défaut](#)

Type: Appareil

Attribution: Hérité de Machines virtuelles

Politiques applicables

Nom de la politique	État	Type	Règles d'affectation
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	
PolicyComplianceReport_1j6	Appliqué	Emplacement	RuleForPolicyComplianceReport_...
Default policy	Appliqué	Appareil	N/D

Première page ← Page de 1 → Dernière page

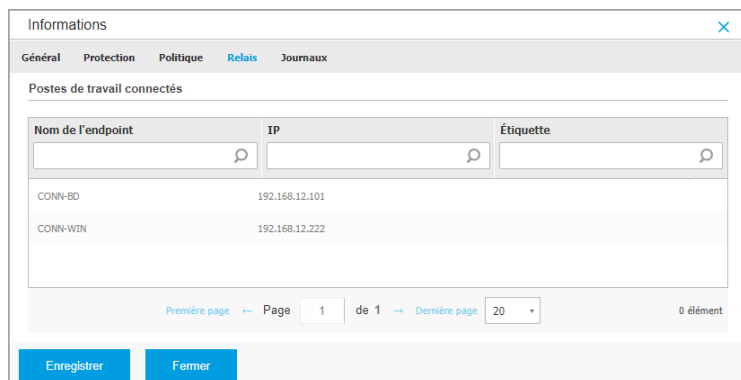
2 éléments

Fenêtre Informations - Onglet Politique

Pour plus d'informations sur les politiques, reportez-vous à « [Modification des paramètres de la politique](#) » (p. 237)

Onglet Endpoints connectés

L'onglet **Endpoints connectés** est disponible uniquement pour les endpoints avec le rôle Relais. Cet onglet affiche des informations sur les endpoints connectés au réseau actuel, comme le nom, l'IP et l'étiquette.



The screenshot shows a window titled 'Informations' with a close button (X) in the top right corner. Below the title bar is a navigation menu with tabs: 'Général', 'Protection', 'Politique', 'Relais' (selected), and 'Journaux'. The main content area is titled 'Postes de travail connectés' and contains a table with three columns: 'Nom de l'endpoint', 'IP', and 'Étiquette'. Each column has a search icon. The table lists two entries: 'CONN-BD' with IP '192.168.12.101' and 'CONN-WIN' with IP '192.168.12.222'. Below the table is a pagination control showing 'Première page', 'Page 1 de 1', 'Dernière page', and '20' items. At the bottom of the window are two buttons: 'Enregistrer' and 'Fermer'.

Nom de l'endpoint	IP	Étiquette
CONN-BD	192.168.12.101	
CONN-WIN	192.168.12.222	

Fenêtre Informations - Onglet Endpoints connectés

Onglet Détails du référentiel

L'onglet **Détails du référentiel** est disponible uniquement pour les endpoints avec le rôle Relais. Il contient des informations les mises à jour de l'agent de sécurité et le contenu de sécurité.

Il donne notamment des informations sur le produit et les versions des signatures stockées sur le relais, ainsi que sur celles disponibles dans le référentiel officiel et les boucles de mise à jour. Il indique également le jour et l'heure de la dernière mise à jour et de la dernière recherche de nouvelles versions.



← Back | AST-TB-W7X86-2

General Protection Policy Connected Endpoints **Repository details** Scan Logs Troubleshooting

Bitdefender Endpoint Security Tools

BEST (Windows)

Product version (stored locally)

Slow ring:	6.6.18.265
Fast ring:	6.6.19.273

Product version (Bitdefender repository)

Slow ring:	N/A
Fast ring:	N/A
Last update time:	26 June 2020 18:4...
Last check time:	N/A

Security Content

FULL ENGINES (Local Scan)		LIGHT ENGINES (Hybrid Scan)	
Signatures stored locally		Signatures stored locally	
x86:	7.84969	x86:	N/A
x64:	N/A	x64:	7.84969
Signatures in Bitdefender repository		Signatures in Bitdefender repository	
x86:	7.84969	x86:	N/A
x64:	N/A	x64:	7.84969
Last update time:	29 June 2020 14:5...	Last update time:	29 June 2020 14:5...
Last check time:	29 June 2020 16:0...	Last check time:	29 June 2020 16:0...
Status:	● Up to date	Status:	● Up to date

Fenêtre Informations - Onglet Détails du référentiel

Onglet Journaux

L'onglet **Journaux d'analyse** présente des informations détaillées sur toutes les tâches d'analyse effectuées sur l'endpoint.

Les journaux sont regroupés par couche de protection et vous pouvez choisir dans le menu déroulant la couche pour laquelle vous souhaitez afficher les journaux.

Cliquez sur la tâche d'analyse qui vous intéresse et le journal s'ouvrira dans une nouvelle page du navigateur.

Lorsque de nombreux journaux d'analyse sont disponibles, ils peuvent occuper plusieurs pages. Pour parcourir les pages, utilisez les options de navigation en bas du tableau. S'il y a trop d'entrées, vous pouvez utiliser les options de filtrage disponibles en haut du tableau .

Informations
✕

Général
Protection
Politique
Journaux

Journaux d'analyse disponibles

Afficher les journaux d'analyse pour : Endpoint Protection ▾

Type	Créé
Analyse rapide	26 octobre 2017, 14:13:51
Analyse complète	05 septembre 2017, 16:16:02

Première page ← Page 1 de 1 → 20 Dernière page 4 éléments

Enregistrer
Fermer

Fenêtre Informations - Onglet Journaux d'analyse

Onglet Résolution des problèmes

Cette section est dédiée aux activités de résolution des problèmes de l'agent. Vous pouvez collecter des journaux généraux ou spécifiques pour contrôler l'endpoint ou prendre des mesures relatives à l'événement en cours de résolution, et voir les activités précédentes.



Important

La résolution des problèmes est disponible pour les machines Windows, Linux, macOS et tous les types de Serveur de sécurité.

← Précédent
DESKTOP-30507PT

Général
Protection
Politique
Journaux
Résolution de problèmes
Actualiser

Collecter les journaux

Gather logs and general information necessary for troubleshooting.

Collecter les journaux

Séssion de débogage

Activate advanced logging to gather specific Bitdefender logs while reproducing the issue.

Démarrer la session

Dernière activité

Nom de l'activité	Démarrée le	Terminée le	État	Actions par défaut
Session de débogage	26 mars 2020, 10:55:31	26 mars 2020, 17:02:29	Terminé	Redémarrer
Collecter les journaux	23 mars 2020, 11:17:47	23 mars 2020, 11:18:02	Arrêtée	Redémarrer

Fenêtre Informations - Onglet Résolution des problèmes

● Collecter les journaux

Cette option vous aide à collecter un ensemble de journaux et d'informations générales nécessaires pour la résolution des problèmes, comme les réglages de l'endpoint, les modules actifs ou la politique appliquée à la machine cible. Toutes les données générées sont sauvegardées dans une archive.

Il est recommandé d'utiliser cette option quand la cause du problème est incertaine.

Pour débuter le processus de résolution des problèmes :

1. Cliquez sur le bouton **Collecter les journaux**. Une fenêtre de configuration s'affiche.
2. Dans la section **Stockage des journaux**, choisissez un emplacement de stockage :
 - **Machine cible** : l'archive des journaux est enregistrée dans le dossier local indiqué. Le chemin n'est pas configurable pour les Serveurs de sécurité.
 - **Partage réseau** : l'archive des journaux est enregistrée dans le dossier partagé indiqué.

Vous pouvez utiliser l'option **Enregistrer les journaux sur la machine cible** pour enregistrer une copie de sauvegarde des journaux sur la machine affectée.

3. Remplissez les informations nécessaires (chemin local, identifiants pour le partage réseau, chemin vers l'emplacement partagé) en fonction de l'emplacement sélectionné.
 4. Cliquez sur le bouton **Collecter les journaux**.
- **Session de débogage**

Avec une session de débogage, vous pouvez activer la création avancée de journaux sur la machine cible afin de collecter des journaux spécifiques au moment de la reproduction du problème.

Vous devriez utiliser cette option lorsque vous avez découvert quel module provoque des erreurs ou selon les recommandations du support pour entreprises de Bitdefender. Toutes les données générées sont sauvegardées dans une archive.

Pour débuter le processus de résolution des problèmes :

1. Cliquez sur le bouton **Débuter la session**. Une fenêtre de configuration s'affiche.



2. Dans la section **Type de problème**, sélectionnez le problème qui affecte selon vous la machine :

Types de problème pour les machines Windows et macOS :


Type de problème	Cas d'utilisation
Antimalware (analyse à l'accès et à la demande)	<ul style="list-style-type: none"> - Ralentissement général de l'endpoint - Un programme ou une ressource du système prend trop de temps à répondre - Un processus d'analyse prend plus de temps que d'habitude - Erreur, pas de connexion au service de sécurité de l'hôte
Erreurs de mise à jour	<ul style="list-style-type: none"> - Messages d'erreur reçus pendant une mise à jour du produit ou du contenu de sécurité
Contrôle des contenus (analyse du trafic et contrôle de l'utilisateur)	<ul style="list-style-type: none"> - Le site web ne charge pas - Des éléments de la page web n'apparaissent pas correctement
Connectivité aux services Cloud	<ul style="list-style-type: none"> - L'endpoint ne peut pas se connecter aux services dans le cloud de Bitdefender
Problèmes généraux du produit (verbosité élevée des journaux)	<ul style="list-style-type: none"> - Reproduire un problème générique identifié avec des journaux détaillés

Types de problème pour les machines Linux :

Type de problème	Cas d'utilisation
Antimalware et Mise à jour	<ul style="list-style-type: none"> - L'analyse prend plus de temps que d'habitude et consomme plus de ressources - Messages d'erreur reçus pendant une mise à jour du produit ou du contenu de sécurité - L'endpoint ne parvient pas à se connecter à la console GravityZone

Type de problème	Cas d'utilisation
Problèmes généraux du produit (verbosité élevée des journaux)	– Reproduire un problème générique identifié avec des journaux détaillés

Types de problème pour les Serveurs de sécurité :

Type de problème	Cas d'utilisation
Antimalware (analyse à l'accès et à la demande)	<p>Tout comportement inattendu du Serveur de sécurité, notamment :</p> <ul style="list-style-type: none"> – Les machines virtuelles ne sont pas correctement protégées – Les tâches d'analyse antimalware ne s'exécutent pas ou prennent plus de temps qu'à la normale – Les mises à jour du produit n'ont pas été installées correctement. – Dysfonctionnement générique du Serveur de sécurité (des daemons bd ne s'exécutent pas)
Communication avec GravityZone Control Center	<p>Tout comportement inattendu observé depuis la console GravityZone :</p> <ul style="list-style-type: none"> – Les machines virtuelles n'apparaissent pas correctement dans la console GravityZone – Problèmes de politique (la politique n'est pas appliquée) – Le Serveur de sécurité ne peut pas établir une connexion avec la console GravityZone <p>Note  Utilisez cette méthode si le support pour entreprises de Bitdefender la recommande.</p>

3. Dans **Durée de la session de débogage**, choisissez le délai après lequel la session de débogage s'arrêtera automatiquement.

 **Note**

Il est recommandé d'arrêter manuellement la session en utilisant l'option **Terminer la session** juste après avoir reproduit le problème.

4. Dans la section **Stockage des journaux**, choisissez un emplacement de stockage :
 - **Machine cible** : l'archive des journaux est enregistrée dans le dossier local indiqué. Le chemin n'est pas configurable pour les Serveurs de sécurité.
 - **Partage réseau** : l'archive des journaux est enregistrée dans le dossier partagé indiqué.

Vous pouvez utiliser l'option **Enregistrer les journaux sur la machine cible** pour enregistrer une copie de sauvegarde des journaux sur la machine affectée.

5. Remplissez les informations nécessaires (chemin local, identifiants pour le partage réseau, chemin vers l'emplacement partagé) en fonction de l'emplacement sélectionné.
6. Cliquez sur le bouton **Débuter la session**.

 **Important**

Vous ne pouvez exécuter qu'un processus de résolution des problèmes à la fois (**Collecter les journaux / Session de débogage**) sur la machine affectée.

● Historique des résolutions de problèmes

La section **Dernière activité** présente les activités de résolution des problèmes sur l'ordinateur affecté. La grille ne contient que les 10 derniers événements de résolution des problèmes en ordre chronologique inverse et supprime automatiquement les activités de plus de 30 jours.

La grille affiche les détails relatifs à chaque processus de résolution des problèmes.

Le processus a des statuts principaux et intermédiaires. En fonction des paramètres personnalisés, vous pouvez voir les statuts suivants, qui vous invitent à prendre des mesures :

- **En cours (Prêt à reproduire le problème)** – accédez à la machine affectée manuellement ou à distance et reproduisez le problème.

Vous disposez de plusieurs manières de stopper un processus de résolution des problèmes :

- **Terminer la session**: met un terme à la session de débogage et au processus de collecte d'informations sur la machine ciblée tout en enregistrant toutes les données collectées à l'emplacement de stockage choisi.

Il est recommandé d'utiliser cette option juste après avoir reproduit le problème.

- **Annuler**: cette option annule le processus et aucun journal n'est collecté. Utilisez cette méthode si vous ne voulez pas collecter de journaux de la machine cible.

- **Forcer l'arrêt**: force l'arrêt du processus de résolution des problèmes.


Utilisez cette option lorsque l'annulation de la session prend trop de temps ou que la machine ciblée ne répond pas et vous serez en mesure d'ouvrir une nouvelle session après quelques minutes d'attente.

Pour redémarrer un processus de résolution des problèmes :

- **Redémarrer** : ce bouton, associé à chaque événement et situé sous **Actions**, redémarre l'activité de résolution des problèmes sélectionnée tout en conservant ses paramètres.



Important

- Pour être certain que la console affiche les dernières informations, utilisez le bouton  **Actualiser** situé en haut à droite de la page **Résolution des problèmes**.
- Pour en apprendre plus sur un événement spécifique, cliquez sur le nom de l'événement dans la grille.

6.2.3. Organiser les ordinateurs dans des groupes

Vous pouvez gérer les groupes d'ordinateurs dans le panneau de gauche de la page **Réseau**.

L'un des principaux avantages de cette fonctionnalité est que vous pouvez utiliser des politiques de groupes pour répondre à différents besoins en sécurité.

Les ordinateurs importés d'Active Directory sont regroupés sous le dossier **Active Directory**. Vous ne pouvez pas modifier les groupes Active Directory. Vous pouvez uniquement afficher et gérer les ordinateurs correspondants.

Tous les ordinateurs non Active Directory découverts dans votre réseau sont placés sous **Groupes personnalisés**, où vous pouvez les organiser dans des groupes selon vos besoins. **Groupes personnalisés** vous permet de [créer](#), [supprimer](#), [renommer](#) et [déplacer](#) des groupes d'ordinateurs dans une structure arborescente personnalisée.

Note

- Un groupe peut contenir à la fois des ordinateurs et d'autres groupes.
- Lors de la sélection d'un groupe dans le panneau de gauche, vous pouvez afficher tous les ordinateurs à l'exception de ceux placés dans ses sous-groupes. Pour afficher tous les ordinateurs contenus dans le groupe et ses sous-groupes, cliquez sur le menu **Filtres** situé en-haut du tableau et sélectionnez **Tous les éléments de manière récurrente** dans la section **Profondeur**.

Création de groupes

Avant de commencer à créer des groupes, pensez aux raisons pour lesquelles vous en avez besoin et ayez en tête un modèle de regroupement. Vous pouvez par exemple regrouper les endpoints en fonction d'un critère ou d'une combinaison des critères suivants :


- Structure de l'organisation (Ventes, Marketing, Assurance Qualité, Développement logiciel, Gestion etc.).
- Besoins en sécurité (Ordinateurs de bureau, Portables, Serveurs etc.).
- Emplacement (siège, bureaux locaux, travailleurs à distance, bureaux à domicile etc.).

Pour organiser votre réseau en groupes :

1. Sélectionnez **Groupes personnalisés** dans le panneau de gauche.
2. Cliquez sur le bouton **+ Ajouter un groupe** en haut du panneau de gauche.
3. Indiquez un nom explicite pour le groupe et cliquez sur **OK**. Le nouveau groupe apparaîtra sous le dossier **Groupes personnalisés**.

Renommer des groupes

Pour renommer un groupe :

1. Sélectionnez le groupe dans le panneau de gauche.
2. Cliquez sur le bouton  **Éditer le groupe** en haut du panneau de gauche.
3. Saisissez le nouveau nom dans le champ correspondant.
4. Cliquez sur **OK** pour confirmer.

Déplacer des groupes et des ordinateurs

Vous pouvez déplacer des entités vers **Groupes personnalisés** partout à l'intérieur de la hiérarchie du groupe. Pour déplacer une entité, glissez déposez-la du panneau de droite vers le groupe de votre choix du panneau de gauche.




Note

L'entité qui est déplacée héritera des paramètres de la politique du nouveau groupe parent, à moins qu'une autre politique lui ait été affectée directement. Pour plus d'informations sur l'héritage de la politique, reportez-vous à « [Politiques de sécurité](#) » (p. 223).

Supprimer des groupes

La suppression d'un groupe correspond à l'action finale. Suite à cela, l'agent de sécurité installé sur l'endpoint ciblé sera supprimé.

Pour supprimer un groupe :

1. Cliquez sur le groupe vide dans le panneau de gauche de la **page Réseau**.
2. Cliquez sur le bouton  **Supprimer un groupe** en haut du panneau de gauche. Vous devrez confirmer votre action en cliquant sur **Oui**.

6.2.4. Trier, filtrer et rechercher des ordinateurs

En fonction du nombre d'endpoints, le tableau du panneau de droite peut comporter plusieurs pages (seules 20 entrées sont affichées par page, par défaut). Pour parcourir les pages, utilisez les boutons de navigation en bas du tableau. Pour modifier le nombre d'entrées affichées sur une page, sélectionnez une option dans le menu à côté des boutons de déplacement.

S'il y a trop d'entrées, vous pouvez utiliser les zones de recherche sous les en-têtes de colonne ou le menu du **Filtres** en haut de la page afin d'afficher uniquement les entités qui vous intéressent. Vous pouvez, par exemple, rechercher un ordinateur spécifique ou choisir d'afficher uniquement les ordinateurs administrés.

Trier des ordinateurs

Pour trier les données en fonction d'une colonne spécifique, cliquez sur les en-têtes de la colonne. Par exemple, si vous souhaitez classer les ordinateurs par nom, cliquez sur l'en-tête **Nom**. Si vous cliquez de nouveau sur l'en-tête, les ordinateurs s'afficheront dans l'ordre inverse.

Nom	OS	IP	Dernière connexion	Étiquette

Trier des ordinateurs

Filtrer des ordinateurs

Pour filtrer les entités de votre réseau, utilisez le menu **Filtres** en haut de la zone de panneaux du réseau.

1. Sélectionnez le groupe souhaité dans le panneau de gauche.
2. Cliquez sur le menu **Filtres** en haut de la zone de panneaux du réseau.
3. Utilisez les critères de filtrage comme suit :
 - **Type**. Sélectionnez le type d'entités que vous souhaitez afficher (ordinateurs, machines virtuelles, dossiers).

Type	Sécurité	Politique	Profondeur
Filtrer par			
<input type="checkbox"/> Ordinateurs			
<input type="checkbox"/> Machines virtuelles			
<input type="checkbox"/> Groupes / Dossiers			
Profondeur: dans les dossiers sélectionnés			
Enregistrer		Annuler	
Réinitialiser			

Ordinateurs - Filtrer par type

- **Sécurité**. Choisissez d'afficher les ordinateurs par état de protection d'administration, de sécurité ou par activité en cours.



Type	Sécurité	Politique	Profondeur
Management		Problèmes de sécurité	
<input type="checkbox"/>	Administrés (Postes de travail)	<input type="checkbox"/>	Avec des problèmes de sécurité
<input type="checkbox"/>	Gérés (Serveurs Exchange)	<input type="checkbox"/>	Sans problèmes de sécurité
<input type="checkbox"/>	Gérés (Relais)		
<input type="checkbox"/>	Serveurs de sécurité		
<input type="checkbox"/>	Non administré		
Profondeur: dans les dossiers sélectionnés			
Enregistrer		Annuler	Réinitialiser

Ordinateurs - Filtrer par sécurité

- **La politique.** Sélectionnez le modèle de politique à partir duquel vous souhaitez filtrer les ordinateurs, le type d'attribution de la politique (Directe ou Héritée), ainsi que l'état d'attribution de celle-ci (Actif, Affecté ou En attente). Vous pouvez également choisir d'afficher uniquement les entités avec des politiques modifiées en mode Power User.

Type	Sécurité	Politique	Profondeur
Modèle:	<input type="text"/>		
	<input type="checkbox"/> Modifié par le Power User		
Type:	<input type="checkbox"/> Direct		
	<input type="checkbox"/> Hérité		
État:	<input type="checkbox"/> Actif		
	<input type="checkbox"/> Appliqué		
	<input type="checkbox"/> En attente		
Profondeur: dans les dossiers sélectionnés			
Enregistrer		Annuler	Réinitialiser

Ordinateurs - Filtrer par politique

- **Profondeur.** Quand on gère un réseau à structure arborescente, les ordinateurs placés dans des sous-groupes ne s'affichent pas lorsqu'on sélectionne le groupe racine. Sélectionnez **Tous les éléments de manière récurrente** pour afficher tous les ordinateurs se trouvant dans le groupe actuel et tous ses sous-groupes.

Type Sécurité Politique **Profondeur**

Filtrer par


Eléments parmi les dossiers sélectionnés

Tous les éléments de manière récurrente

Profondeur: dans les dossiers sélectionnés

Enregistrer Annuler Réinitialiser

Ordinateurs - Filtrer par profondeur

Lorsque vous choisissez de voir tous les éléments de manière récursive, Control Center les affiche sous forme de liste simple. Pour trouver l'emplacement d'un élément, sélectionnez celui qui vous intéresse puis cliquez sur le bouton  **Aller dans le conteneur** dans la partie supérieure du tableau. Vous serez redirigé vers le conteneur parent de l'élément sélectionné.



Note

Vous pouvez afficher tous les critères de filtrage sélectionnés dans la partie inférieure de la fenêtre **Filtres**.

Si vous souhaitez supprimer tous les filtres, cliquez sur le bouton **Réinitialiser**.

4. Cliquez sur **Enregistrer** pour filtrer les ordinateurs en fonction des critères sélectionnés. Le filtre demeure actif sur la page **Réseau** jusqu'à ce que vous vous déconnectiez ou réinitialisiez le filtre.

Recherche d'ordinateurs

1. Sélectionnez le groupe souhaité dans le panneau de gauche.
2. Saisissez le terme recherché dans la case correspondante sous les en-têtes de colonne (Nom, OS ou IP) dans le panneau de droite. Par exemple, saisissez l'IP de l'ordinateur que vous recherchez dans le champ **IP**. Seul l'ordinateur correspondant apparaîtra dans le tableau.

Décochez la case pour afficher la liste complète d'ordinateurs.

	Nom	FQDN	OS	IP	Dernière connexion	Étiquette
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	192.168.113.1 <input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	SRV2012	srv2012.x13.local	Windows Serv...	192.168.113.1	En ligne	N/D

Recherche d'ordinateurs

6.2.5. Lancer des tâches

La page **Réseau** vous permet d'exécuter à distance un certain nombre de tâches d'administration sur les ordinateurs.

Voici ce que vous pouvez faire :

- « Analyse » (p. 72)
- « Tâches des patches » (p. 82)
- « Analyse Exchange » (p. 85)
- « Installer » (p. 89)
- « Désinstaller Client » (p. 95)
- « Mettre à jour le client » (p. 96)
- « Reconfigurer le client » (p. 97)
- « Réparer le client » (p. 99)
- « Redémarrage machine » (p. 100)
- « Découverte du réseau » (p. 101)
- « Découverte applications » (p. 101)
- « Mettre à jour le Security Server » (p. 102)
- « Injecter l'outil personnalisé » (p. 103)

Vous pouvez choisir de créer des tâches individuellement pour chaque ordinateur ou pour des groupes d'ordinateurs. Vous pouvez par exemple installer à distance l'agent de sécurité sur un groupe d'ordinateurs non administrés. Vous pouvez créer ultérieurement une tâche d'analyse pour un ordinateur du même groupe.

Vous pouvez, pour chaque ordinateur, exécuter uniquement les tâches compatibles. Par exemple, si vous sélectionnez un ordinateur non administré, vous pouvez choisir d'installer uniquement l'agent de sécurité, toutes les autres tâches étant désactivées.


Pour un groupe, la tâche sélectionnée sera créée uniquement pour les ordinateurs compatibles. Si aucun des ordinateurs du groupe n'est compatible avec la tâche sélectionnée, vous serez informé que la tâche n'a pas pu être créée.

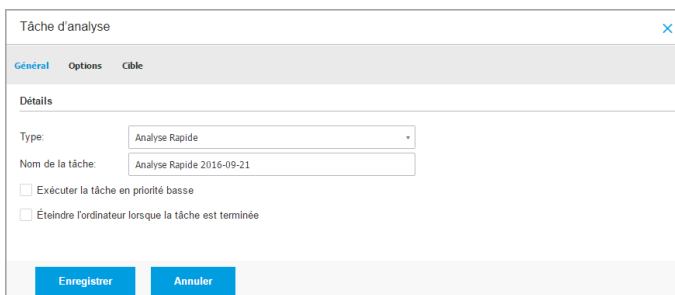
Une fois créée, la tâche commencera à s'exécuter immédiatement sur les ordinateurs en ligne. Si un ordinateur est hors ligne, la tâche s'exécutera dès qu'il sera de nouveau en ligne.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Analyse

Pour exécuter une tâche d'analyse à distance sur un ou plusieurs ordinateurs :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Tous les ordinateurs du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Cochez les cases des ordinateurs ou groupes que vous souhaitez analyser.
5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Analyse**. Une fenêtre de configuration s'affichera.
6. Configurer les options d'analyse :
 - L'onglet **Général**, vous permet de choisir le type d'analyse et de saisir un nom pour la tâche d'analyse. Le nom de la tâche d'analyse est destiné à vous aider à identifier facilement l'analyse en cours dans la page **Tâches**.



The screenshot shows a configuration window titled "Tâche d'analyse" with a close button (X) in the top right corner. Below the title bar are three tabs: "Général" (selected), "Options", and "Cible". Under the "Général" tab, there is a "Détails" section with the following fields and options:

- Type: A dropdown menu with "Analyse Rapide" selected.
- Nom de la tâche: A text input field containing "Analyse Rapide 2016-09-21".
- Exécuter la tâche en priorité basse
- Éteindre l'ordinateur lorsque la tâche est terminée

At the bottom of the window are two buttons: "Enregistrer" (blue) and "Annuler" (grey).

Tâche Analyse des ordinateurs - Configurer les paramètres généraux

Sélectionnez le type d'analyse dans le menu **Type** :

- **Quick Scan** utilise l'analyse dans le Cloud pour détecter les malwares présents sur le système. Ce type d'analyse est préconfiguré pour permettre uniquement l'analyse des emplacements système critiques Windows et Linux. La réalisation d'une analyse rapide dure généralement moins d'une minute et n'utilise qu'une petite partie des ressources du système dont a besoin une analyse antivirus classique.

En cas de détection d'un malware ou d'un rootkit, Bitdefender procède automatiquement à la désinfection. Si pour une raison quelconque le fichier ne peut pas être désinfecté, il est déplacé en quarantaine. Ce type d'analyse ignore les fichiers suspects.

- **L'Analyse Complète** analyse l'ensemble du système afin de détecter tous les types de malwares menaçant sa sécurité : virus, spywares, adwares, rootkits et autres.

Bitdefender essaye automatiquement de désinfecter les fichiers dans lesquels un malware a été détecté. Si le malware ne peut pas être supprimé, il est confiné en quarantaine, où il ne peut pas faire de mal. Les fichiers suspects sont ignorés. Si vous voulez également prendre des mesures pour les fichiers suspects, ou si vous voulez changer les actions par défaut pour les fichiers infectés, choisissez l'Analyse personnalisée.

- **L'analyse de la mémoire** vérifie les programmes en cours d'exécution dans la mémoire de l'ordinateur.
- **L'Analyse du réseau** est un type d'analyse personnalisée, permettant d'analyser les lecteurs réseau à l'aide de l'agent de sécurité de Bitdefender installé sur l'endpoint cible.

Pour que la tâche d'analyse du réseau fonctionne :

- Vous devez affecter la tâche à un seul endpoint de votre réseau.
 - Vous devez indiquer les identifiants d'un compte utilisateur avec des permissions de lecture/écriture sur les lecteurs réseau cibles, afin que l'agent de sécurité soit capable d'accéder et d'appliquer des actions sur ces lecteurs réseau. Les identifiants requis peuvent être configurés dans l'onglet **Cible** de la fenêtre des tâches.
- **Analyse personnalisée** vous permet de sélectionner les emplacements à analyser et de configurer les options d'analyse.

Pour analyses mémoire, réseau et personnalisée, vous avez également les options suivantes :

- **Exécuter la tâche en priorité basse.** Cochez cette case pour diminuer la priorité du processus d'analyse et permettre à d'autres programmes de fonctionner plus rapidement. Cela augmentera le temps nécessaire au processus d'analyse.

**Note**

Cette option ne s'applique qu'à Bitdefender Endpoint Security Tools et Endpoint Security (ancien agent).

- **Éteindre l'ordinateur lorsque la tâche est terminée.** Cochez cette case pour éteindre votre machine si vous ne comptez pas l'utiliser pendant un certain temps.

**Note**

Cette option s'applique à Bitdefender Endpoint Security Tools, Endpoint Security (ancien agent) et Endpoint Security for Mac.

**Note**

Ces deux options ne s'appliquent qu'à Bitdefender Endpoint Security Tools et Endpoint Security (agent héritage).

Pour des analyses personnalisées, configurez les paramètres suivants :

- Allez dans l'onglet **Options** pour définir les options d'analyse. Cliquez sur le niveau de sécurité qui correspond le mieux à vos besoins (Agressif, Normal ou Tolérant). Utilisez la description à droite de l'échelle pour faire votre choix.

Basées sur le profil sélectionné, les options d'analyse de la section **Configuration** sont configurées automatiquement. Vous pouvez cependant, si vous le souhaitez, les configurer en détail. Pour cela, cochez la case **Personnalisé** puis développez la section **Configuration**.

Tâche d'analyse

Général Options Cible

Options d'analyse

Personnalisé - Paramètres définis par l'administrateur

Agressif

Normal

Tolérant

Personnalisé

Configuration

Enregistrer Annuler

Tâche d'analyse des ordinateurs - Configurer une analyse personnalisée

Voici les options proposées :

- **Types de fichiers.** Utilisez ces options pour spécifier les types de fichiers que vous souhaitez analyser. Vous pouvez configurer l'agent de sécurité afin qu'il analyse tous les fichiers (quelle que soit leur extension), ou uniquement les fichiers d'applications ou certaines extensions de fichiers que vous considérez dangereuses. L'analyse de tous les fichiers fournit la meilleure protection, alors que l'analyse des applications uniquement peut être utilisée pour effectuer une analyse plus rapide.



Note

Les fichiers d'applications sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers. Pour plus d'informations, reportez-vous à « [Types de fichiers d'applications](#) » (p. 529).

Si vous souhaitez uniquement que certaines extensions soient analysées, sélectionnez **Extensions personnalisées** dans le menu puis saisissez les extensions dans le champ de saisie, en appuyant sur **Entrée** après chaque extension.



Important

Les agents de sécurité de Bitdefender installés sur les systèmes d'exploitation Windows et Linux analysent la plupart des formats .ISO mais ne leur appliquent aucune action.



Configuration

Types de fichiers

Type: Extensions personnalisées

Extensions: bat, exe

Options de la tâche Analyse des ordinateurs - Ajouter des extensions personnalisées

- **Archives.** Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité du système. Les malwares peuvent affecter le système uniquement si le fichier infecté est extrait de l'archive et exécuté sans que la protection en temps réel ne soit activée. Il est toutefois recommandé d'analyser les archives afin de détecter et de supprimer toute menace potentielle, même si celle-ci n'est pas imminente.



Important

L'analyse des fichiers compressés augmente le temps d'analyse global et demande plus de ressources système.

- **Analyser le contenu compressé.** Sélectionnez cette option si vous souhaitez que les archives fassent l'objet d'une analyse antimalware. Si vous décidez d'utiliser cette option, vous pouvez configurer les options d'optimisation suivantes :
 - **Limiter la taille des archives à (Mo).** Vous pouvez définir une limite de taille pour les archives à analyser. Cochez la case correspondante et tapez la taille maximale des archives (en Mo).
 - **Profondeur maximale des archives (niveaux).** Cochez la case correspondante et sélectionnez la profondeur maximale des archives dans le menu. Pour les meilleures performances, choisissez la valeur la plus faible, pour la protection maximale, choisissez la valeur la plus élevée.

- **Analyser les archives de messagerie.** Sélectionnez cette option si vous souhaitez permettre l'analyse de fichiers de messagerie et de bases de données de messagerie, y compris de formats de fichiers tels que .eml, .msg, .pst, .dbx, .mbx, .tbb et d'autres.



Important

L'analyse des archives de messagerie consomme beaucoup de ressources et peut avoir un impact sur les performances du système.

- **Divers.** Cochez les cases correspondantes pour activer les options d'analyse souhaitées.
 - **Analyser les secteurs d'amorçage.** Pour analyser les secteurs de boot du système. Ce secteur du disque dur contient le code informatique nécessaire pour faire démarrer le processus d'amorçage du système. Quand un virus infecte le secteur d'amorçage, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.
 - **Analyser la base de registre.** Sélectionnez cette option pour analyser les clés de registre. Le registre Windows est une base de données qui contient les paramètres et les options de configuration des composants du système d'exploitation Windows, ainsi que des applications installées.
 - **Rechercher les rootkits.** Sélectionnez cette option pour rechercher des [rootkits](#) et des objets cachés à l'aide de ce logiciel.
 - **Rechercher des enregistreurs de frappe.** Sélectionnez cette option pour rechercher les logiciels [keyloggers](#).
 - **Analyser les volumes partagés.** Cette option analyse les lecteurs de réseau.

Pour l'analyse rapide, cette option est désactivée par défaut. Pour l'analyse complète, elle est activée par défaut. Pour l'analyse personnalisée, si vous définissez le niveau de sécurité sur **Aggressif/Normal**, l'option **Analyser les partages réseau** est activée automatiquement. Si vous définissez le niveau de sécurité sur

- Permissif**, l'option **Analyser les partages réseau** option est automatiquement désactivée.
- **Analyser la mémoire.** Sélectionnez cette option pour analyser les programmes s'exécutant dans la mémoire du système.
 - **Analyser les cookies.** Sélectionnez cette option pour analyser les cookies stockés par les navigateurs sur l'ordinateur.
 - **Analyser uniquement les nouveaux fichiers et ceux modifiés.** En analysant uniquement les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.
 - **Rechercher des applications potentiellement indésirables.** Un Logiciel Potentiellement Indésirable (LPI) est un programme qui peut être indésirable sur l'ordinateur et peut provenir d'un logiciel gratuit. De tels programmes peuvent être installés sans le consentement de l'utilisateur (alors appelés Adware) ou sont inclus par défaut dans le kit d'installation rapide. Les effets possibles de ces programmes sont l'affichage de pop-ups, l'installation indésirable de barre d'outils dans le navigateur par défaut ou le lancement de plusieurs programmes en arrière-plan qui ralentissent les performances du PC.
 - **Analyser les volumes amovibles.** Sélectionnez cette option pour analyser tous les supports de stockage amovibles liés à l'ordinateur.
- **Actions.** En fonction du type de fichier détecté, les actions suivantes sont menées automatiquement :
 - **Quand un fichier infecté est détecté.** Bitdefender détecte les fichiers considérés comme infectés par le biais de divers mécanismes avancés, notamment les technologies basées sur l'intelligence artificielle, l'apprentissage machine et les signatures de logiciels malveillants. L'agent de sécurité de Bitdefender peut généralement supprimer le code malveillant d'un fichier infecté et reconstruire le fichier d'origine. Cette opération est appelée désinfection.

Par défaut, si un fichier infecté est détecté, l'agent de sécurité de Bitdefender tentera automatiquement de le désinfecter. Si la désinfection échoue, le fichier est placé en quarantaine afin de contenir l'infection.



Important

Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

- **Quand un fichier suspect est détecté.** Les fichiers sont considérés comme étant suspicieux par l'analyse heuristique et les autres technologies Bitdefender. Ils offrent un taux de détection élevé, mais les utilisateurs doivent tenir compte de la probabilité de faux résultats positifs (fichiers propres détectés comme étant suspicieux), dans certains cas. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible.

Les tâches d'analyse sont configurées par défaut pour ignorer les fichiers suspects. Vous pouvez modifier l'action par défaut afin de placer des fichiers suspects en quarantaine. Les fichiers en quarantaine sont envoyés régulièrement aux Laboratoires Bitdefender pour y être analysés. Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

- **Quand un rootkit est détecté .** Les rootkits sont des logiciels spécialisés utilisés pour masquer des fichiers au système d'exploitation. Bien que n'étant pas malveillants par nature, les rootkits sont souvent utilisés pour masquer des malwares ou la présence d'un intrus dans le système.

Les rootkits détectés et les fichiers cachés sont ignorés par défaut.

Bien que ce ne soit pas recommandé, vous pouvez modifier les actions par défaut. Vous pouvez spécifier une deuxième action à prendre si la première a échoué, ainsi que d'autres mesures, pour chaque catégorie. Choisissez dans les menus correspondants la première et la seconde actions à prendre pour chaque type de fichier détecté. Les actions suivantes sont disponibles :

Désinfecter

Supprimer le code malveillant des fichiers infectés. Nous vous recommandons de toujours la conserver comme première action à appliquer aux fichiers infectés.

Déplacer en quarantaine

Déplacer les fichiers détectés de l'emplacement actuel vers le dossier de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Vous pouvez gérer les fichiers en quarantaine à partir de la page [Quarantaine](#) de la console.

Supprimer

Supprime les fichiers détectés du disque, sans avertissement. Nous vous recommandons d'éviter d'utiliser cette action.

Ignorer

Aucune action ne sera appliquée aux fichiers détectés. Ces fichiers apparaîtront uniquement dans le journal d'analyse.

- Allez dans l'onglet **Cible** pour configurer les emplacements que vous souhaitez analyser sur les ordinateurs cibles.

La section **Cible de l'analyse** vous permet d'ajouter un nouveau fichier ou dossier à analyser :

- a. Spécifiez un emplacement prédéfini dans le menu déroulant ou saisissez les **Chemins spécifiques** que vous souhaitez analyser.
- b. Indiquez le chemin de l'objet à analyser dans le champ de saisie.
 - Si vous avez choisi un emplacement prédéfini, complétez le chemin selon vos besoins. Par exemple, pour analyser l'ensemble du dossier `Program Files`, il suffit de sélectionner l'emplacement prédéfini correspondant dans le menu déroulant. Pour analyser un dossier spécifique de `Program Files`, vous devez compléter le chemin en ajoutant une barre oblique inverse (`\`) et le nom du dossier.
 - Si vous avez choisi **Chemins spécifiques**, indiquez le chemin complet vers l'objet à analyser. Il est recommandé d'utiliser les variables du système (le cas échéant) afin de s'assurer que le chemin soit valide sur tous les ordinateurs cibles. Pour plus

d'informations sur les variables du système, reportez-vous à « [Variables du système](#) » (p. 530).

c. Cliquez sur le bouton **+ Ajouter** correspondant.

Pour modifier un emplacement existant, cliquez dessus. Pour retirer un emplacement de la liste, cliquez sur le bouton **⊗ Supprimer** correspondant.

Pour les tâches d'analyse du réseau, vous devez indiquer les identifiants d'un compte utilisateur avec des permissions de lecture/écriture sur les lecteurs réseau cibles, afin que l'agent de sécurité soit capable d'accéder et d'appliquer des actions sur ces lecteurs réseau.

Cliquez sur la section **Exclusions** si vous souhaitez définir des exclusions de la cible.

Exclusions		
<input checked="" type="radio"/> Utiliser les exclusions définies dans Politique > Antimalware > Exclusions section		
<input type="radio"/> Définir des exclusions personnalisées pour cette analyse		
Fichier	Chemins spécifiques	+ Action
Type d'exclusions	Fichiers et dossiers à analyser	

Tâche Analyse des ordinateurs - Définir des exclusions

Vous pouvez soit utiliser les exclusions définies par la politique ou définir des exclusions explicites pour l'analyse en cours. Pour plus d'informations sur les exclusions, reportez-vous à « [Exclusions](#) » (p. 294).

7. Cliquez sur **Enregistrer** pour créer la tâche d'analyse. Une message de confirmation s'affichera.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Note

Pour planifier une tâche d'analyse, allez sur la page des **Politiques**, sélectionnez la stratégie affectée aux ordinateurs qui vous intéressent, et ajoutez une tâche d'analyse dans la rubrique **Antimalware > à la demande**. Pour plus d'informations, reportez-vous à « [A la demande](#) » (p. 273).

Tâches des patches

Il est recommandé de fréquemment vérifier si des mises à jour de logiciels sont disponibles et de les installer le plus rapidement possible. GravityZone automatise ce processus par des politiques de sécurité, mais si vous devez immédiatement mettre à jour un logiciel sur certains endpoints, suivez les instructions suivantes :

1. [Analyse des patches](#)
2. [Installation des patches](#)


Configuration nécessaire

- L'agent de sécurité avec le module de Gestion des patches est installé sur les endpoints cibles.
- Pour que les tâches d'analyse et d'installation réussissent, les endpoints Windows doivent remplir les conditions suivantes :
 - **Autorités de certification racines de confiance** stocke le certificat **DigiCert Assured ID Root CA**.
 - **Autorités de certification intermédiaires** contient le **DigiCert SHA2 Assured ID Code Signing CA**.
 - Les correctifs pour Windows 7 et Windows Server 2008 R2 mentionnés dans cet article de Microsoft sont installés sur les endpoints : [Microsoft Security Advisory 3033929](#)

Analyse des patches

Les endpoints dont les logiciels ne sont pas à jour sont vulnérables aux attaques. Il est recommandé de fréquemment les logiciels de vos endpoints et de les mettre à jour le plus rapidement possible. Pour analyser si certains patches ne sont pas installés sur vos endpoints :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Tous les endpoints du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Sélectionnez les endpoints cibles :

5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Analyse des patches**. Une fenêtre de confirmation s'affichera.
6. Cliquez sur **Oui** pour confirmer la tâche d'analyse.

Une fois la tâche terminée, GravityZone ajoute tous les patches dont vos logiciels ont besoin dans l'Inventaire des patches. Pour plus d'informations, reportez-vous à « [Inventaire des patches](#) » (p. 201).



Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Note

Pour planifier une analyse des patches, modifiez les politiques assignées aux endpoints cibles, et configurez les options de la section **Gestion des patches**. Pour plus d'informations, reportez-vous à « [Gestion des correctifs](#) » (p. 343).

Installation des patches

Pour installer un ou plusieurs patches sur les endpoints cibles :

1. Allez sur la page **Réseau**.
 2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
 3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Tous les endpoints du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
 4. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Installer un patch**
- Une fenêtre de configuration s'affichera. Vous pouvez ici voir tous les patches manquants sur les endpoints cibles.
5. Si nécessaire, utilisez les options de tri et de filtre situées en haut du tableau pour trouver certains patches.
 6. Cliquez sur le bouton  **Colonnes** en haut à droite du volet pour voir les informations concernées.
 7. Sélectionnez les patches que vous souhaitez installer.

Certains patches sont dépendant d'autres patches. Dans ce cas, ils sont automatiquement sélectionnés avec le patch.

Cliquez sur numéros de **CVE** ou de **Produits** pour faire apparaître un volet à gauche de l'écran. Le volet contient des informations additionnelles, comme les CVE résolus par le patch, ou les produits auxquels le patch s'applique. Quand vous en aurez pris connaissance, cliquez sur **Fermer** pour masquer le volet.

8. Sélectionnez **Redémarrer les endpoints après l'installation du correctif, si nécessaire** pour redémarrer les endpoints immédiatement après l'installation du correctif, si un redémarrage du système est nécessaire. Veuillez noter que cette action peut perturber l'activité de l'utilisateur.
9. Cliquez sur **Installer**.

La tâche d'installation est créée en parallèle à d'autres sous-tâches pour chaque endpoint cible.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).



Note

- Pour planifier un déploiement de patches, modifiez les politiques assignées aux endpoints cibles, et configurez les options de la section **Gestion des patches**. Pour plus d'informations, reportez-vous à « [Gestion des correctifs](#) » (p. 343).
- Vous pouvez également installer un correctif à partir de la page **Inventaire des correctifs**, en commençant par le correctif qui vous intéresse. Dans ce cas, sélectionnez le correctif dans la liste, cliquez sur le bouton **Installer** situé en haut du tableau et configurez les détails de l'installation du correctif. Pour plus d'informations, reportez-vous à « [Installer des patches](#) » (p. 205).
- Après l'installation du correctif, nous vous recommandons de lancer une tâche d'[Analyse du correctif](#) sur les endpoints cibles. Cette action mettra à jour les informations du correctif stockées dans GravityZone pour vos réseaux gérés.

Vous pouvez désinstaller des correctifs :

- À distance, en lançant une [tâche de désinstallation de correctifs](#) à partir de GravityZone.
- Localement, sur l'endpoint. Dans ce cas, vous devez vous connecter au endpoint en tant qu'administrateur et exécuter le programme de désinstallation manuellement.

Analyse Exchange

Vous pouvez analyser à distance la base de données d'un Serveur Exchange en exécutant une tâche **Analyse Exchange**.

Pour pouvoir analyser la base de données Exchange, vous devez activer l'analyse à la demande en indiquant les identifiants d'un administrateur Exchange. Pour plus d'informations, reportez-vous à « [Analyse de la banque d'informations Exchange](#) » (p. 369).

Pour analyser une base de données Exchange Server :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
3. Dans le panneau de gauche, sélectionnez le groupe contenant le serveur Exchange cible. Vous pouvez voir le serveur dans le panneau de droite.



Note

Vous pouvez également appliquer des filtres pour trouver rapidement le serveur cible :

- Cliquez sur le menu **Filtres** et sélectionnez les options suivantes : **Gérés (Serveurs Exchange)** dans l'onglet **Sécurité** et **Tous les éléments de manière récurrente** dans l'onglet **Profondeur**.
 - Indiquez le nom d'hôte ou l'IP du serveur dans les champs des en-têtes de colonnes correspondants.
4. Cochez la case du Serveur Exchange dont vous souhaitez analyser la base de données.
 5. Cliquez sur le bouton **Tâches** en haut du tableau et sélectionnez **Analyse Exchange**. Une fenêtre de configuration s'affichera.
 6. Configurer les options d'analyse :
 - **Général**. Indiquez un nom explicite pour la tâche.
Pour les bases de données importantes, la tâche d'analyse peut être longue et avoir un impact sur les performances du serveur. Dans ce cas, cochez la case **Arrêter l'analyse si elle dure plus de** et sélectionnez un intervalle adapté dans les menus correspondants.
 - **Cible**. Sélectionnez les conteneurs et objets à analyser. Vous pouvez choisir d'analyser les boîtes aux lettres, les dossiers publics ou les deux. En plus des e-mails, vous pouvez choisir d'analyser d'autres objets tels que les **Contacts**, **Tâches**, **Rendez-vous** et **Éléments de publication**. Vous pouvez en outre définir les restrictions suivantes au contenu à analyser :

- Uniquement les messages non lus
- Uniquement les éléments avec des pièces jointes
- Uniquement les nouveaux éléments, reçus pendant une période donnée

Vous pouvez par exemple choisir d'analyser uniquement les e-mails de boîtes aux lettres d'utilisateurs, reçus au cours des 7 derniers jours.

Cochez la case **Exclusions**, si vous souhaitez définir des exceptions à l'analyse. Pour créer une exception, utilisez les champs de l'en-tête du tableau comme suit :

- Sélectionnez le type de référentiel dans le menu.
- En fonction du type de référentiel, spécifiez l'objet à exclure :

Type de référentiel	Format de l'objet
Boîte de messagerie	Adresse e-mail
Dossier public	Chemin d'accès du dossier, depuis la racine
Base de données	L'identité de la base de données



Note

Pour obtenir l'identité de la base de données, utilisez la commande shell Exchange :

```
Get-MailboxDatabase | fl name,identity
```

Vous ne pouvez saisir qu'un élément à la fois. Si vous avez plusieurs éléments du même type, vous devez définir autant de règles que le nombre d'éléments.

- Cliquez sur le bouton **+ Ajouter** en haut du tableau pour enregistrer l'exception et l'ajouter à la liste.

Pour retirer une règle d'exception de la liste, cliquez sur le bouton **- Supprimer** correspondant.

- **Options.** Configurez les options d'analyse pour les e-mails correspondant à la règle :
 - **Types de fichiers analysés.** Utilisez cette option pour spécifier quels types de fichiers vous souhaitez analyser. Vous pouvez choisir d'analyser tous les fichiers (quelle que soit leur extension), uniquement les fichiers d'applications, ou certaines extensions de fichiers que vous considérez dangereuses. L'analyse de tous les fichiers fournit la meilleure protection,

alors que l'analyse des applications uniquement est recommandée pour une analyse plus rapide.



Note

Les fichiers d'applications sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers. Pour plus d'informations, reportez-vous à « [Types de fichiers d'applications](#) » (p. 529).

Si vous souhaitez uniquement analyser les fichiers avec certaines extensions, vous avez deux possibilités :

- **Extensions définies par l'utilisateur**, où vous devez indiquer uniquement les extensions à analyser.
- **Tous les fichiers, à l'exception d'extensions spécifiques**, où vous devez saisir uniquement les extensions à ne pas analyser.
- **Taille maximale du corps des e-mails/des pièces jointes (Mo)**. Cochez cette case et saisissez une valeur dans le champ correspondant pour définir la taille maximale acceptée d'un fichier joint ou du corps des e-mails à analyser.
- **Profondeur maximale des archives (niveaux)**. Cochez la case et sélectionnez la profondeur maximale des archives dans le champ correspondant. Plus le niveau de profondeur est faible, meilleures sont les performances et plus le degré de protection est faible.
- **Rechercher des applications potentiellement indésirables (PUA)**. Cochez cette case pour rechercher les applications potentiellement malveillantes ou indésirables telles que les adwares, qui peuvent s'installer sur les systèmes sans le consentement des utilisateurs, modifier le comportement de différents logiciels et faire diminuer les performances du système.
- **Actions**. Vous pouvez spécifier les différentes actions que l'agent de sécurité pour exécuter sur les fichiers, selon le type de détection.

Le type de détection sépare les fichiers en trois catégories :

- **Fichier(s) infecté(s)**. Bitdefender détecte les fichiers considérés comme infectés par le biais de divers mécanismes avancés, notamment les technologies basées sur l'intelligence artificielle, l'apprentissage machine et les signatures de logiciels malveillants.
- **Fichiers suspects**. Ces fichiers sont considérés comme étant suspicieux par l'analyse heuristique et les autres technologies Bitdefender. Ils offrent un taux de détection élevé, mais les utilisateurs doivent tenir compte de

la probabilité de faux résultats positifs (fichiers propres détectés comme étant suspects), dans certains cas.

- **Fichiers non analysables.** Ces fichiers ne peuvent pas être analysés. Les fichiers non analysables incluent mais ne se limitent pas aux fichiers protégés par des mots de passe, chiffrés ou compressés.

Pour chaque type de détection, vous avez une action par défaut ou principale et une action alternative en cas d'échec de l'action principale. Bien que ce ne soit pas recommandé, vous pouvez changer ces actions à partir des menus correspondants. Sélectionnez l'action à appliquer :

- **Désinfecter.** Supprime le code malveillant des fichiers infectés et reconstruit le fichier d'origine. Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Nous vous recommandons de toujours la conserver comme première action à appliquer aux fichiers infectés. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible.
- **Rejeter/Supprimer l'e-mail.** Sur les serveurs avec le rôle Transport Edge, l'e-mail détecté est rejeté avec un code d'erreur SMTP 550. Dans tous les autres cas, l'e-mail est supprimé sans avertissement. Nous vous recommandons d'éviter d'utiliser cette action.
- **Supprimer le fichier.** Supprime les pièces jointes présentant des problèmes sans aucun avertissement. Nous vous recommandons d'éviter d'utiliser cette action.
- **Remplacer le fichier.** Supprime les fichiers présentant des problèmes et insère un fichier texte qui informe l'utilisateur des actions appliquées.
- **Placer le fichier en quarantaine.** Place les fichiers détectés dans le dossier de la quarantaine et insère un fichier texte qui informe l'utilisateur des actions appliquées. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Vous pouvez gérer les fichiers de la quarantaine à partir de la page **Quarantaine**.



Note

Veillez noter que 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.

- **Ignorer** Aucune action ne sera appliquée aux fichiers détectés. Ces fichiers apparaîtront uniquement dans le journal d'analyse. Les tâches

d'analyse sont configurées par défaut pour ignorer les fichiers suspects. Vous pouvez modifier l'action par défaut afin de placer des fichiers suspects en quarantaine.

- Par défaut, lorsqu'un e-mail correspond à la portée d'une règle, il est traité exclusivement en fonction de cette règle, sans être comparé à toute autre règle restante. Si vous souhaitez continuer à effectuer une vérification par rapport aux autres règles, décochez la case **Si les conditions de la règle sont remplies, arrêter de traiter d'autres règles**.
7. Cliquez sur **Enregistrer** pour créer la tâche d'analyse. Une message de confirmation s'affichera.
 8. Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Installer

Pour protéger vos ordinateurs avec l'agent de sécurité Bitdefender, vous devez l'installer sur chacun d'eux.



Important

Dans les réseaux isolés n'ayant pas de connectivité directe avec l'appliance GravityZone, vous pouvez installer l'agent de sécurité avec le [rôle Relais](#). Dans ce cas, la communication entre l'appliance GravityZone et les autres agents de sécurité s'effectuera via l'agent Relais, qui aura également le rôle de serveur de mise à jour locale pour les agents de sécurité protégeant le réseau isolé.

Lorsque vous aurez installé un agent Relais, il détectera automatiquement les ordinateurs non protégés du même réseau.



Note

- Nous vous recommandons de maintenir constamment allumé l'ordinateur sur lequel vous installez l'agent Relais.
- Si aucun agent Relais n'est installé dans le réseau, la détection des ordinateurs non protégés peut être réalisée manuellement en envoyant une tâche de **Découverte du réseau** à un endpoint protégé.

La protection Bitdefender peut ensuite être installée sur les ordinateurs à distance à partir de Control Center.

L'installation à distance s'effectue en tâche de fond, sans que l'utilisateur ne le sache.

⊗ Avertissement

Avant l'installation, veillez à désinstaller les logiciels antimalware et pare-feu des ordinateurs. Installer la protection Bitdefender alors que des logiciels de sécurité sont présents peut affecter leur fonctionnement et causer d'importants problèmes avec le système. Windows Defender et le Pare-feu Windows seront automatiquement désactivés lorsque l'installation démarrera.

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](#).

Lors du déploiement de l'agent via un relais Linux, les conditions 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.

i 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.
- Sur les endpoints cibles sous Linux ou Mac, le SSH doit être activé et le firewall désactivé.

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 **Ordinateur / Machine virtuelle** dans le sélecteur d'affichage.
4. 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**.

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

Utilisateur	Mot de passe	Description	Action
<input type="checkbox"/> admin	*****		

Installer Bitdefender Endpoint Security Tools à partir du menu des Tâches

- 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.

8. Si vous souhaitez que les endpoints cibles redémarrent automatiquement pour terminer l'installation, sélectionnez **Redémarrer automatiquement (si nécessaire)**.
9. 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.

10. 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.

11. Sous la section **Système de déploiement**, sélectionnez l'entité à laquelle les endpoints cibles se connecteront pour installer et mettre à jour le client :

- **L'appliance GravityZone**, lorsque les endpoints se connecteront directement à l'appliance GravityZone.

Dans ce cas, vous pouvez également définir :

- Un serveur de communication personnalisé en indiquant son IP ou nom d'hôte, si nécessaire.
 - Les paramètres du proxy, si les endpoints cibles communiquent avec l'appliance GravityZone 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 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

Page 1 de 1 Dernière page 20 1 éléments

- Utilisez la section **Cibles supplémentaires** si vous souhaitez déployer le client sur certaines machines de votre réseau qui n'apparaissent pas dans l'inventaire du réseau. Développez la section et saisissez les adresses IP ou les noms d'hôtes de ces machines dans le champ prévu à cet effet, en les séparant par des virgules. Vous pouvez ajouter autant d'IP que nécessaire.
- 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 votre compte ainsi que le package d'installation disponible par défaut avec Control Center.
- 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 comment modifier les packages d'installation, consultez le Guide d'installation de GravityZone.

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.

- 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`
- `epintegrationservice.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](#).

Mettre à niveau le client


Cette tâche est uniquement disponible lorsque l'agent Endpoint Security est installé et détecté par le réseau. Bitdefender recommande de mettre à niveau Endpoint Security vers le nouveau [Bitdefender Endpoint Security Tools](#), pour bénéficier d'une protection des endpoints de nouvelle génération.

Pour trouver facilement les clients qui ne sont pas à jour, vous pouvez générer un rapport sur l'état de la [mise à niveau](#). Pour en apprendre plus sur la création de rapports, consultez « [Création de rapports](#) » (p. 448).

Désinstaller Client

Pour désinstaller la protection Bitdefender à distance :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Tous les ordinateurs du conteneur sélectionné apparaissent dans le tableau du panneau de droite.

4. Cochez les cases des ordinateurs dont vous souhaitez désinstaller l'agent de sécurité Bitdefender.
5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Désinstaller le client**.
6. Une fenêtre de configuration apparaît, vous permettant d'effectuer les paramètres suivants :
 - Vous pouvez choisir de conserver les éléments en quarantaine sur la machine cliente.
 - Pour les environnements intégrés à vShield, vous devez sélectionner les identifiants requis pour chaque machine, car sinon la désinstallation échouera. Sélectionnez **Utiliser des identifiants pour l'intégration à vShield**, puis vérifiez tous les identifiants appropriés dans le tableau Admin. des authentifications qui apparaît en-dessous.
7. Cliquez sur **Enregistrer** pour créer la tâche. Une message de confirmation s'affichera.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).



Note

Si vous souhaitez réinstaller la protection, vous devez d'abord redémarrer l'ordinateur.


Mettre à jour le client

Consultez régulièrement l'état des ordinateurs administrés. Si vous remarquez un ordinateur avec des problèmes de sécurité, cliquez sur son nom pour afficher la page **Informations**. Pour plus d'informations, reportez-vous à « [État de sécurité](#) » (p. 51).

Les clients ou les contenus de sécurité obsolètes constituent des problèmes de sécurité. Dans ces cas, vous devriez exécuter une mise à jour sur l'ordinateur correspondant. Cette tâche peut être effectuée en local à partir de l'ordinateur ou à distance à partir de Control Center.

Pour mettre à jour le client et les contenus de sécurité à distance, sur les ordinateurs administrés :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).

3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Tous les ordinateurs du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Cochez les cases des ordinateurs sur lesquels vous souhaitez exécuter une mise à jour du client.
5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Mise à jour**. Une fenêtre de configuration s'affichera.
6. Vous pouvez choisir de mettre à jour uniquement le produit, uniquement le contenu de sécurité, ou les deux à la fois.
7. Pour l'OS Linux et les machines intégrées à vShield, il faut également sélectionner les informations d'identification requises. Cochez l'option **Utiliser des identifiants pour l'intégration à Linux et vShield**, puis sélectionnez les identifiants appropriés dans le tableau Admin. des authentifications qui apparaît en-dessous.
8. Cliquez **Mise à jour** pour effectuer la tâche. Un message de confirmation s'affichera.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Reconfigurer le client

Les modules de protection de l'agent de sécurité, les rôles et les modes d'analyse sont configurés au départ dans le package d'installation. Après avoir installé l'agent de sécurité dans votre réseau, vous pouvez modifier les paramètres initiaux à tout moment en envoyant une tâche distante **Reconfigurer le client** aux endpoints administrés qui vous intéressent.



Avertissement

Veillez noter que la tâche **Reconfigurer le client** écrase tous les paramètres d'installation et qu'aucun paramètre initial n'est conservé. Veuillez reconfigurer tous les paramètres d'installation des endpoints cibles lors de l'utilisation de cette tâche.




Note

La tâche **Reconfigurer le client** supprimera tous les modules non pris en charge des installations existantes sur les anciennes versions de Windows.

Vous pouvez modifier les paramètres d'installation depuis la page **Réseau** ou depuis le rapport **État des modules de l'endpoint**.

Pour changer les paramètres d'installation d'un ou plusieurs ordinateurs :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
3. Sélectionnez le groupe souhaité dans le panneau de gauche. Tous les ordinateurs du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Cochez les cases des ordinateurs pour lesquels vous souhaitez modifier les paramètres d'installation.
5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Reconfigurer le client**.
6. Sélectionnez l'une des actions suivantes:
 - **Ajouter**. Ajouter de nouveaux modules en plus des existants.
 - **Supprimer**. Supprimer des modules parmi ceux existants.
 - **Faire correspondre la liste**. Faire correspondre les modules installés à votre sélection.
7. Sélectionnez les modules et les rôles que vous voulez installer ou supprimer des endpoints cibles.



Avertissement

Seuls les modules pris en charge s'installeront. Par exemple, le Pare-Feu s'installe uniquement sur les postes de travail Windows compatibles.

Pour en apprendre plus, consultez la [Disponibilité des couches de protection de GravityZone](#).

8. Sélectionnez **Suppression des solutions concurrentes, si nécessaire** pour veiller à ce que les modules sélectionnés n'entrent pas en conflit avec d'autres solutions de sécurité installées sur les endpoints cibles.
9. Choisissez l'un des modes d'analyse disponibles :
 - **Automatique**. L'agent de sécurité détecte quels moteurs d'analyse sont adaptés selon les ressources de l'endpoint.
 - **Paramètres**. Vous choisissez explicitement quel moteur d'analyse utiliser.

Pour plus d'informations sur les options disponibles, veuillez vous référer à la rubrique Créer des packages d'installation du Guide d'installation.

**Note**

Cette section est seulement disponible avec **Faire correspondre la liste**.

10. Dans la section **Planification**, choisissez quand la tâche sera exécutée :

- **Maintenant**, afin de lancer la tâche immédiatement.
- **Planifié**, afin de planifier la fréquence de la tâche.

Dans ce cas, sélectionnez le temps d'intervalle (par heure, par jour ou par semaine) et configurez le selon vos besoin.

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

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Réparer le client


Utilisez la tâche Réparer le client comme tâche initiale de résolution des problèmes pour n'importe quelle quantité d'endpoints. La tâche télécharge le dernier package d'installation sur l'endpoint cible puis réalise une réinstallation de l'agent.

**Note**

- The modules currently configured on the agent will not be changed.
- La tâche de réparation réinitialisera l'agent de sécurité dans la version indiquée sur la page **Configuration > Mise à jour > Composants**.

Pour envoyer une tâche Réparer le client au client :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Tous les ordinateurs du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Cochez les cases des ordinateurs sur lesquels vous souhaitez exécuter une réparation du client.

5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Réparer le client**. Une fenêtre de confirmation s'affichera.
6. Cochez la case **Je comprends et j'accepte** et cliquez sur le bouton **Enregistrer** pour exécuter la tâche.

**Note**

Pour terminer la tâche de réparation, un redémarrage du client peut être nécessaire.


Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Redémarrage machine

Vous pouvez choisir de faire redémarrer à distance les ordinateurs administrés.

**Note**

Consultez la page [Réseau > Tâches](#) avant de faire redémarrer certains ordinateurs. Les tâches créées auparavant peuvent être encore en cours de traitement sur les ordinateurs cibles.


1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Tous les ordinateurs du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Cochez les cases des ordinateurs que vous souhaitez redémarrer.
5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Redémarrer la machine**.
6. Sélectionnez l'option de planification du redémarrage :
 - Sélectionnez **Redémarrer** pour faire redémarrer les ordinateurs immédiatement.
 - Sélectionnez **Redémarrer le** et utilisez les champs ci-dessous pour planifier le redémarrage à la date et à l'heure souhaitées.
7. Cliquez sur **Enregistrer**. Une message de confirmation s'affichera.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Découverte du réseau

La découverte du réseau est effectuée automatiquement par les agents de sécurité avec le rôle **Relais**. Si vous n'avez pas d'agent Relais d'installé dans votre réseau, vous devez envoyer manuellement une tâche de découverte du réseau à partir d'un endpoint protégé.

Pour exécuter une tâche de découverte du réseau dans votre réseau :


1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Tous les ordinateurs du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Cochez la case de l'ordinateur avec lequel vous souhaitez effectuer la découverte du réseau.
5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Découverte du réseau**.
6. Un message de confirmation s'affichera. Cliquez sur **Oui**.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Découverte applications

Pour découvrir des applications dans votre réseau :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
3. Sélectionnez le groupe souhaité dans le panneau de gauche. Tous les ordinateurs du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Sélectionnez les ordinateurs sur lesquels vous souhaitez effectuer une découverte d'applications.

5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Découverte d'applications**.

**Note**

Bitdefender Endpoint Security Tools avec Contrôle des applications doit être installé et activé sur les ordinateurs sélectionnés. Autrement, la tâche sera grisée. Lorsqu'un groupe sélectionné contient à la fois des cibles valides et des cibles non valides, la tâche ne sera envoyée qu'aux endpoints valides.

6. Cliquez sur **Oui** dans la fenêtre de confirmation pour continuer.

Les applications et les processus découverts sont affichés sur la page **Réseau > Inventaire des applications**. Pour plus d'informations, reportez-vous à « [Inventaire des applications](#) » (p. 195).

**Note**

La tâche **Découverte d'applications** peut prendre un certain temps, en fonction du nombre d'applications installées. Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).


Mettre à jour le Security Server

Le Security Server installé peut également être affiché et géré à partir d'**Ordinateur / Machine virtuelle**, dans le dossier **Groupes personnalisés**.

Si un Security Server n'est pas à jour, vous pouvez lui envoyer une tâche de mise à jour :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
3. Sélectionnez le groupe où est installé le Security Server.

Pour localiser facilement le Security Server, vous pouvez utiliser le menu **Filtres** de la façon suivante :

- Allez dans l'onglet **Sécurité** et sélectionnez **Serveurs de sécurité** uniquement.
 - Allez dans l'onglet **Profondeur** et sélectionnez **Tous les éléments de manière récurrente**.
4. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Mettre à jour le Security Server**.

- Vous devrez confirmer votre action. Cliquez sur **Oui** pour créer la tâche.
Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).




Important

Il est recommandé d'utiliser cette méthode pour mettre à jour le Security Server pour NSX, sinon vous perdrez la quarantaine enregistrée sur l'appareil.

Injecter l'outil personnalisé

Pour injecter des outils dans les systèmes d'exploitation invités, cible :

- Allez sur la page **Réseau**.
- Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
- Sélectionnez le groupe souhaité dans le panneau de gauche. Tous les endpoints du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
- Sélectionnez les cases à cocher des endpoints ciblés.
- Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Injecter l'outil personnalisé**. Une fenêtre de configuration s'affiche.
- Dans le menu déroulant, sélectionnez tous les outils que vous voulez injecter. Pour chaque outil sélectionné, une section apparaît avec ses réglages.

Ces outils étaient auparavant envoyés dans GravityZone. Si vous ne trouvez pas le bon outil dans la liste, rendez-vous dans le **Centre de gestion des outils** et ajoutez-le. Pour plus d'informations, reportez-vous à « [Injection d'outils personnalisés avec HVI](#) » (p. 496).

- Pour chaque outil affiché sur la fenêtre :
 - Cliquez sur le nom de l'outil pour voir ou masquer sa section.
 - Saisissez la ligne de commande de l'outil, avec tous les paramètres nécessaires, exactement comme vous le feriez sur le terminal ou l'invite de commande. Par exemple :

```
bash script.sh <param1> <param2>
```

Pour les outils de réparation BD, vous ne pouvez sélectionner que l'action de réparation et l'action de réparation de secours dans les menus déroulants.

- c. Indiquez l'endroit depuis lequel Security Server doit collecter les journaux :
- **stdout.** Sélectionnez les cases à cocher pour capturer les journaux du canal standard de communication de sortie.
 - **Fichier de sortie.** Cochez cette case pour collecter le fichier journal enregistré sur l'endpoint. Dans ce cas, vous devez saisir un emplacement où Security Server peut trouver le fichier. Vous pouvez utiliser des chemins absolus ou des variables du système.
- Vous disposez ici d'une option supplémentaire : **Supprimer les fichiers journal d'Invité après les avoir transférés.** Sélectionnez-la si vous n'avez plus besoin des fichiers sur l'endpoint.
8. Si vous voulez transférer les fichiers journaux du Security Server à un autre emplacement, vous devez fournir le chemin de l'emplacement de destination et les identifiants d'authentification.
9. L'outil peut parfois nécessiter plus de temps que prévu pour réaliser sa tâche ou peut ne pas répondre. Pour éviter les crashes dans de telles situations, dans la section **Configuration de la sécurité**, choisissez après combien d'heures Security Server doit terminer automatiquement le processus.
10. Cliquez sur **Enregistrer**.
- Vous pourrez voir le statut de la tâche sur la page **Tâches**. Pour obtenir plus d'informations, vous pouvez également consulter le rapport **État de l'injection HVI tiers**.


6.2.6. Créer des rapports rapides

Vous pouvez choisir de créer des rapports instantanés sur les ordinateurs administrés à partir de la page **Réseau** :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
3. Sélectionnez le groupe de votre choix dans le panneau de gauche. Tous les ordinateurs du groupe sélectionné apparaissent dans le tableau du panneau de droite.

Vous pouvez également filtrer le contenu du groupe sélectionné uniquement par ordinateurs administrés.


4. Cochez les cases des ordinateurs que vous souhaitez inclure dans le rapport.

5. Cliquez sur le bouton  **Rapport** en haut du tableau et sélectionnez le type de rapport dans le menu.
Pour plus d'informations, reportez-vous à « [Rapports Ordinateur et Machine virtuelle](#) » (p. 428).
6. Configurer les options de rapports. Pour plus d'informations, reportez-vous à « [Création de rapports](#) » (p. 448).
7. Cliquez sur **Générer**. Le rapport s'affiche immédiatement.
Le temps nécessaire à la création des rapports peut varier en fonction du nombre d'ordinateurs sélectionnés.

6.2.7. Affecter des politiques

Vous pouvez gérer les paramètres de sécurité sur les ordinateurs à l'aide des [politiques](#).

La page **Réseau** vous permet d'afficher, de modifier et d'affecter des politiques à chaque ordinateur ou groupe d'ordinateurs.

 **Note**
Les paramètres de sécurité sont disponibles uniquement pour les ordinateurs gérés. Pour afficher et gérer les paramètres de sécurité plus facilement, vous pouvez [filtrer](#) l'inventaire du réseau uniquement par ordinateurs gérés.


Pour afficher la politique affectée à un ordinateur spécifique :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
3. Sélectionnez le groupe souhaité dans le panneau de gauche. Tous les ordinateurs du groupe sélectionné apparaissent dans le tableau du panneau de droite.
4. Cliquez sur le nom de l'ordinateur administré qui vous intéresse. Une fenêtre d'informations s'affichera.
5. Dans l'onglet **Général**, section **Politique**, cliquez sur le nom de la politique en cours pour afficher ses paramètres.
6. Vous pouvez modifier les paramètres de sécurité en fonction de vos besoins, à condition que le propriétaire de la politique ait autorisé d'autres utilisateurs à modifier cette politique. Veuillez noter que toute modification que vous

effectuez affectera tous les ordinateurs auxquels on a affecté la même politique.

Pour plus d'informations sur les paramètres de la politique de l'ordinateur, reportez-vous à « [Politiques des ordinateurs et machines virtuelles](#) » (p. 239).


Pour affecter une politique à un ordinateur ou à un groupe :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
3. Sélectionnez le groupe souhaité dans le panneau de gauche. Tous les ordinateurs du groupe sélectionné apparaissent dans le tableau du panneau de droite.
4. Cochez la case de l'ordinateur ou du groupe de votre choix. Vous pouvez sélectionner un ou plusieurs objets du même type du même niveau uniquement.
5. Cliquez sur le bouton  **Affecter une politique** en haut du tableau.
6. Effectuez la configuration nécessaire dans la fenêtre **Attribution de la politique**. Pour plus d'informations, reportez-vous à « [Affecter des politiques](#) » (p. 227).

Utiliser Recovery Manager for Encrypted Volumes (système de récupération pour volumes chiffrés)

Lorsque les utilisateurs d'un endpoint oublient les mots de passe de chiffrement et ne peuvent plus accéder aux volumes chiffrés sur leur machine, vous pouvez les aider à retrouver leurs clés de récupération depuis la page **Réseau**.

Pour obtenir une clé de récupération :

1. Allez sur la page **Réseau**.
2. Cliquez sur le bouton  **Gestionnaire de récupération** dans la barre d'outils action du panneau gauche. Une nouvelle fenêtre apparaît.
3. Dans la section **Identifiant** de la fenêtre, saisissez les données suivantes :
 - a. L'ID de la clé de récupération du volume chiffré. L'ID de la clé de récupération est une chaîne de caractère composée de chiffres et de lettres disponibles sur l'endpoint, sur l'écran de récupération de BitLocker.
Sur Windows, l'ID de la clé de récupération est une chaîne de caractère composée de chiffres et de lettres disponibles sur l'endpoint, sur l'écran de récupération de BitLocker.

Autrement, vous pouvez utiliser l'option **Récupération** dans l'onglet **Protection** des [détails sur l'ordinateur](#) pour remplir automatiquement l'ID de la clé de récupération, aussi bien pour les endpoints Windows que macOS.

- b. Le mot de passe de votre compte GravityZone.
4. Cliquez sur **Dévoiler**. La fenêtre s'agrandira.

Dans la fenêtre **Informations sur les volumes**, les données suivantes vous seront présentées :


- a. Nom du volume
 - b. Type de volume (amorçage ou non-amorçage).
 - c. Nom de l'endpoint, tel qu'indiqué dans l'inventaire du réseau.
 - d. Clé de récupération. Sur Windows, la clé de récupération est un mot de passe généré automatiquement lors du chiffrement du volume. Sur Mac, la clé de récupération correspond au mot de passe du compte de l'utilisateur.
5. Envoyez la clé de récupération à l'utilisateur de l'endpoint.

Pour de plus amples informations relatives au chiffrement et déchiffrement de volumes avec GravityZone, veuillez vous référer à « [Chiffrement de disque](#) » (p. 392).

6.2.9. Synchronisation avec Active Directory

L'inventaire du réseau est automatiquement synchronisé avec Active Directory à la fréquence indiquée dans la section de configuration de Control Center. Pour plus d'informations, référez-vous au chapitre Installation et Configuration de GravityZone, dans le Guide d'Installation de GravityZone.

Pour synchroniser manuellement avec Active Directory l'inventaire réseau affiché actuellement :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le [sélecteur d'affichage](#).
3. Cliquez sur le bouton  **Synchroniser avec Active Directory** en haut du tableau.
4. Vous devrez confirmer votre action en cliquant sur **Oui**.



Note

Pour des réseaux Active Directory plus grands, la synchronisation peut prendre un peu plus de temps.

6.3. Machines virtuelles

Pour afficher l'infrastructure virtualisée sous votre compte, allez sur la page **Réseau** et sélectionnez **Machines virtuelles** dans le **sélecteur d'affichage**.



Note

Vous pouvez également gérer les machines virtuelles à partir de l'affichage **Ordinateur / Machine virtuelle** mais vous ne pouvez afficher votre infrastructure virtualisée et filtrer son contenu à l'aide de critères spécifiques qu'à partir de l'affichage **Machines virtuelles**.

Pour plus d'informations sur comment travailler avec les affichages du réseau, référez-vous à « [Travailler avec les affichages réseau](#) » (p. 45).

Nom	OS	IP	Dernière connexion	Étiquette
<input type="checkbox"/> Inventaire VMware			ND	ND
<input type="checkbox"/> Inventaire Citrix			ND	ND
<input type="checkbox"/> Groupes personnalisés			ND	ND
<input type="checkbox"/> Supprimé			ND	ND

L'affichage Réseau - Machines virtuelles

Vous pouvez voir les réseaux de machines virtuelles disponibles dans le panneau de gauche et des informations sur toutes les machines virtuelles dans le panneau de droite.

Pour personnaliser les informations sur une machine virtuelle affichées dans le tableau :

1. Cliquez sur le bouton **III Colonnes** dans l'angle supérieur droit du panneau de droite.
2. Sélectionnez les colonnes que vous souhaitez afficher.
3. Cliquez sur le bouton **Réinitialiser** pour rétablir l'affichage des colonnes par défaut.

Le panneau de gauche affiche une vue arborescente de l'infrastructure virtuelle. La racine de l'arbre s'appelle **Machines virtuelles** et les machines virtuelles sont regroupées sous la racine, dans les catégories suivantes en fonction du fournisseur de technologie de virtualisation :

- **Inventaire Nutanix.** Contient la liste des systèmes Nutanix Prism Element auxquels vous avez accès.
- **Inventaire VMware.** Contient la liste des serveurs vCenter auxquels vous avez accès.
- **Inventaire Citrix.** Contient la liste des systèmes XenServer auxquels vous avez accès.
- **Groupes personnalisés.** Contient les serveurs de sécurité et les machines virtuelles détectés dans votre réseau hors de tout système vCenter Server ou XenServer.

Le panneau de gauche contient également un menu nommé **Affichages** à partir d'où l'utilisateur peut choisir le type d'affichage pour chaque fournisseur de technologie de virtualisation.

Pour accéder à l'infrastructure virtualisée intégrée à Control Center, vous devez indiquer vos identifiants utilisateur pour chaque système vCenter Server disponible. Les authentifiants que vous avez indiqués sont enregistrés dans votre Administrateur des authentifications afin que vous n'ayez pas besoin de les saisir la prochaine fois. Pour plus d'informations, reportez-vous à « [Admin. des authentifications](#) » (p. 219).

La section **Réseau** vous permet de gérer les machines virtuelles comme suit :

- [Vérifier l'état des machines virtuelles](#)
- [Afficher des informations sur les machines virtuelles](#)
- [Organiser les machines virtuelles en groupes](#)
- [Trier, filtrer et rechercher](#)
- [Exécuter des tâches](#)
- [Créer des rapports rapides](#)
- [Affecter des politiques](#)
- [Libérer sièges licence](#)

Dans la section **Configuration > Paramètres réseau**, vous pouvez configurer des [règles planifiées pour nettoyer automatiquement les machines virtuelles](#) de l'Inventaire réseau.

6.3.1. Vérifier l'état des machines virtuelles

Chaque machine virtuelle est représentée sur la page du réseau par une icône spécifique à son type et à son état.





Consultez « États et types d'objets du réseau » (p. 527) pour une liste des types d'icônes et des états existants.

Pour de plus amples informations sur l'état, reportez-vous à :

- [État d'administration](#)
- [État de la connectivité](#)
- [État de sécurité](#)



État d'administration

Les machines virtuelles peuvent avoir les états d'administration suivants :

-  **Administré** - machines virtuelles sur lesquelles la protection Bitdefender est installée.
-  **Redémarrage en attente** - machines virtuelles nécessitant un redémarrage système après l'installation ou la mise à jour de la protection Bitdefender.
-  **Non administrées** - machines virtuelles détectées sur lesquelles la protection Bitdefender n'est pas encore installée.
-  **Supprimé** - les machines virtuelles que vous avez supprimées de Control Center. Pour plus d'informations, reportez-vous à « [Supprimer des endpoints de l'inventaire du réseau](#) » (p. 214).

État de la connectivité

L'état de la connectivité concerne les machines virtuelles administrées et les Security Server. De ce point de vue, les machines virtuelles administrées peuvent être :

-  **En ligne.** Une icône bleue indique que la machine est en ligne.
-  **Hors connexion.** Une icône grise indique que la machine est hors connexion.

Une machine virtuelle est hors connexion si l'agent de sécurité est inactif pendant plus de 5 minutes. Raisons pour lesquelles les machines virtuelles peuvent apparaître hors connexion :

- La machine virtuelle est arrêtée, en veille ou en veille prolongée.



Note

Les machines virtuelles apparaissent comme étant en ligne, même quand elles sont verrouillées ou que l'utilisateur est déconnecté.

- L'agent de sécurité n'a pas de connectivité avec le Serveur de communication de GravityZone :
 - La machine virtuelle peut être déconnectée du réseau.
 - Un routeur ou un pare-feu du réseau peut bloquer la communication entre l'agent de sécurité et Bitdefender Control Center ou le Endpoint Security Relay affecté.
 - La machine virtuelle se trouve derrière un serveur proxy et les paramètres du proxy n'ont pas été configurés correctement dans la politique qui est appliquée.



Avertissement

Pour les machines virtuelles derrière un serveur proxy, les paramètres du proxy doivent être correctement configurés dans le package d'installation de l'agent de sécurité, sans quoi la machine virtuelle ne communiquera pas avec la console GravityZone et apparaîtra toujours comme étant hors connexion, même si une [politique avec les paramètres du proxy adaptés](#) est appliquée après l'installation.

- L'agent de sécurité a été désinstallé manuellement de la machine virtuelle, alors que la machine virtuelle n'avait pas de connectivité avec Bitdefender Control Center ou avec le Endpoint Security Relay affecté. Normalement, lorsque l'agent de sécurité est désinstallé manuellement d'une machine virtuelle, Control Center est informé de cet événement et la machine virtuelle est signalée comme étant non administrée.
- L'agent de sécurité pourrait ne pas fonctionner correctement.

Pour connaître la durée d'inactivité des machines virtuelles :

1. Affichez uniquement les machines virtuelles administrées. Cliquez sur le menu **Filtres** situé au-dessus du tableau, sélectionnez toutes les options « Administré » dont vous avez besoin dans l'onglet **Sécurité**, sélectionnez **Tous les éléments de manière récurrente** dans l'onglet **Profondeur** et cliquez sur **Enregistrer**.
2. Cliquez sur l'en-tête de la colonne **Dernière connexion** pour trier les machines virtuelles par période d'inactivité.

Vous pouvez ignorer les périodes d'inactivité les plus courtes (minutes, heures), car elles sont probablement le résultat d'une condition temporaire. Par exemple, la machine virtuelle est actuellement arrêtée.

De longues périodes d'inactivité (jours, semaines) indiquent en général un problème avec la machine virtuelle.







Note

Nous vous recommandons d'[actualiser](#) le tableau du réseau de temps en temps, afin que les informations sur les endpoints tiennent compte des dernières modifications.

État de sécurité


L'état de sécurité concerne les machines virtuelles administrées et les Security Server. Vous pouvez identifier les machines virtuelles ou les Security Server ayant des problèmes de sécurité en vérifiant les icônes d'état présentant un symbole d'avertissement :

-   Avec des problèmes.
-   Sans problèmes.

Une machine virtuelle ou un Security Server a des problèmes de sécurité si au moins l'une des situations suivantes s'applique :

- La protection antimalware est désactivée (uniquement pour les machines virtuelles).
- La licence est arrivée à expiration.
- Le produit de Bitdefender n'est pas à jour.
- Le contenu de sécurité est périmé.
- Le package complémentaire HVI n'est pas à jour.
- Un malware est détecté (uniquement pour les machines virtuelles).
- La connexion avec les Services Cloud Bitdefender n'a pas pu être établie. Il se peut que cela soit dû à l'une des raisons suivantes :
 - La machine virtuelle a des problèmes de connectivité Internet.
 - Un pare-feu du réseau bloque la connexion avec les Services Cloud Bitdefender.
 - Le port 443, requis pour la communication avec les Services Cloud Bitdefender, est fermé.

Dans ce cas, la protection antimalware repose uniquement sur des moteurs locaux, alors que l'analyse dans le cloud est désactivée, ce qui signifie que l'agent de sécurité ne peut pas fournir une protection en temps réel complète.

Si vous remarquez une machine virtuelle avec des problèmes de sécurité, cliquez sur son nom pour afficher la fenêtre **Informations**. Vous pouvez identifier les problèmes de sécurité par l'icône . Pensez à rechercher les informations de

sécurité dans tous les [onglets de la page des informations](#). Affichez l'info-bulle de l'icône pour plus d'informations. D'autres enquêtes locales peuvent être nécessaires.

Note

Nous vous recommandons d'[actualiser](#) le tableau du réseau de temps en temps, afin que les informations sur les endpoints tiennent compte des dernières modifications. Les endpoints n'ayant reçu aucune mise à jour au cours des 24 dernières heures sont automatiquement signalés **Avec problèmes**, quelle que soit la version des contenus de sécurité présente sur le relais ou sur le Update Server de GravityZone.

6.3.2. Afficher des informations sur les machines virtuelles

Vous pouvez obtenir des informations détaillées sur chaque machine virtuelle à partir de la page **Réseau** comme suit :

- [Consulter la page Réseau](#)
- [Consulter la fenêtre Information](#)

Consulter la page Réseau

Pour en apprendre plus sur une machine virtuelle, consultez les informations disponibles dans le tableau situé à droite de la page **Réseau**.

Vous pouvez supprimer ou ajouter des colonnes d'informations sur la machine virtuelle en cliquant sur le bouton **III Colonnes** situé en haut à droite du panneau.

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Sélectionnez le groupe souhaité dans le panneau de gauche.

Toutes les machines virtuelles du groupe sélectionné sont affichées dans le tableau de droite.

4. Vous pouvez identifier facilement l'état de la machine virtuelle en consultant l'icône correspondante. Pour plus d'informations, reportez-vous à « [Vérifier l'état des machines virtuelles](#) » (p. 109).
5. Consultez les informations affichées sur les colonnes pour chaque machine virtuelle.

Utilisez la ligne d'en-tête pour retrouver au fil de votre saisie le nom des machines virtuelles, en fonction des critères disponibles :

- **Nom** : nom de la machine virtuelle.

- **FQDN** : nom de domaine complet comprenant le nom d'hôte et le nom de domaine.
- **OS** : système d'exploitation installé sur la machine virtuelle.
- **IP** : adresse IP de la machine virtuelle.
- **Dernière connexion** : date et heure auxquelles la machine virtuelle a été vue en ligne pour la dernière fois.



Note

Il est important de surveiller le champ **Dernière connexion** car de longues périodes d'inactivité peuvent signifier qu'il existe un problème de communication ou qu'une machine virtuelle est déconnectée.

- **Étiquette** : une chaîne personnalisée contenant des informations supplémentaires relatives au endpoint. Vous pouvez ajouter une étiquette dans la fenêtre **Information** de la machine virtuelle plus l'utiliser pour vos recherches.
- **Politique** : la politique appliquée à la machine virtuelle, avec un lien pour consulter ou modifier les réglages de la politique.

Consulter la fenêtre Information

Dans la partie droite de la page **Réseau**, cliquez sur le nom de la machine virtuelle que vous voulez voir dans la fenêtre **Information**. La fenêtre n'affiche que les données disponibles pour la machine virtuelle sélectionnée, regroupées en plusieurs onglets.

Vous trouverez ci-après une liste exhaustive des informations que vous pouvez trouver dans la fenêtre **Information**, en fonction du type de machine (machine virtuelle, instance Security Server) et de ses informations de sécurité.

Onglet Général

- Informations générales sur la machine virtuelle, comme le nom, les informations FQDN, l'adresse IP, le système d'exploitation, l'infrastructure, le groupe parent et l'état actuel de connexion.

Dans cette section, vous pouvez affecter une étiquette à une machine virtuelle. Vous pourrez retrouver facilement les machines virtuelles avec la même étiquette et réaliser des actions sur eux, quel que soit leur emplacement sur le réseau.

Pour plus d'informations sur le filtrage des machines virtuelles, consultez « [Trier, filtrer et rechercher des machines virtuelles](#) » (p. 124).

- **Prérequis HVI**, contenant des informations sur la possibilité ou non d'utiliser le Security Server pour déployer la protection HVI. Ainsi, si l'hôte du Security Server est en cours d'exécution sur une version XenServer supportée et que le package de complément est installé, vous pouvez activer HVI sur les machines virtuelles à partir de cet hôte.
- Informations relatives aux couches de sécurité, avec notamment la liste des technologies de sécurité dont vous avez fait l'acquisition pour votre solution GravityZone et le statut de leur licence, qui peut être :
 - **Disponible / Active** – la clé de licence de cette couche de protection est active sur la machine virtuelle.
 - **Expiré** – la clé de licence de cette couche de protection est expirée.
 - **En attente** – la clé de licence n'est pas confirmée pour le moment.

**Note**

Des informations supplémentaires concernant les couches de protection sont disponibles dans l'onglet **Protection**.

- **Connexion du relais**: Le nom, l'IP et l'étiquette du relais auquel la machine virtuelle est connectée, le cas échéant.

Machine virtuelle		Couches de protection	
Nom:	TA_SVE_UBUNTUX64_2	Endpoint:	Actif
FQDN:	ub-installssh		
IP:	N/D		
OS:	N/D		
Étiquette:	<input type="text"/>		
Infrastructure:	VMware		
Groupe:	Clients		
État:	Hors Connexion		
Dernier changement d'état:	26 octobre 2017, 02:21:20		
Nom de l'hôte:	10.17.47.53		
IP de l'hôte:	N/D		

Enregistrer Fermer

Fenêtre Informations - Onglet Général


Onglet Protection


Cet onglet contient des informations sur toutes les couches de protection pour lesquelles l'endpoint a une licence. Les informations concernent :

- Informations relative à l'agent de sécurité telles que le nom et la version du produit, la configuration des moteurs d'analyse et l'état de mise à jour. Pour la Protection Exchange, un moteur antispam et les versions des signatures sont également disponibles.
- Statut de sécurité pour chaque couche de protection. Ce statut apparaît à droite du nom de la couche de protection :
 - **Sécurisé**, quand il n'est fait état d'aucun problème de sécurité sur l'endpoint bénéficiant de la couche de protection.
 - **Vulnérable**, quand il est fait état de problèmes de sécurité sur l'endpoint bénéficiant de la couche de protection. Pour plus d'informations, reportez-vous à « [État de sécurité](#) » (p. 112).
- Security Server associé. Chaque Security Server affecté est affiché en cas de déploiements sans agent ou lorsque les moteurs d'analyse des agents de sécurité sont paramétrés pour utiliser l'analyse à distance. Les informations

relatives au Security Server vous aident à identifier l'appliance virtuelle et à obtenir son état de mise à jour.

- Informations relatives à NSX, telles que l'état du tag virus et le groupe de sécurité auquel appartient la machine virtuelle. Si un tag de sécurité a été appliqué, il vous informe que la machine est infectée. Sinon, soit la machine est propre, soit les tags de sécurité ne sont pas utilisés.
- L'état des modules de protection. Vous pouvez afficher facilement les modules de protection ayant été installés sur l'endpoint ainsi que l'état des modules disponibles (**Activés/Désactivés**) configurés via la politique appliquée.
- Un aperçu rapide concernant l'activité des modules et les rapports sur les malwares dans la journée en cours.

Cliquez sur le lien  **Affichage** pour accéder aux options de rapport puis générer le rapport. Pour plus d'informations, reportez-vous à « [Création de rapports](#) » (p. 448)

- Informations relatives à la couche de protection Sandbox Analyzer :
 - État d'utilisation de Sandbox Analyzer sur la machine virtuelle, affiché à droite de la fenêtre :
 - **Actif** : Sandbox Analyzer dispose d'une licence et est activé via une politique sur la machine virtuelle.
 - **Inactif** : Sandbox Analyzer dispose d'une licence, mais n'est pas activé via une politique sur la machine virtuelle.
 - Nom de l'agent agissant en tant que capteur d'alimentation.
 - État du module sur la machine virtuelle :
 - **Allumé** - Sandbox Analyzer est activé sur la machine virtuelle via une politique.
 - **Éteint** - Sandbox Analyzer n'est pas activé sur la machine virtuelle via une politique.
 - Détection des menaces survenues la semaine précédente, en cliquant sur le lien  **Afficher** afin d'accéder au rapport.
- Informations supplémentaires concernant le module de chiffrement :
 - Volumes détectés (y compris le disque de démarrage).

- L'état de chiffrement de chaque volume (qui peut être **Chiffré**, **Chiffrement en cours**, **Déchiffrement en cours**, **Non chiffré**, **Bloqué** ou **En pause**).

Cliquez sur le lien **Récupération** afin d'obtenir la clé de récupération correspondant au volume chiffré associé. Pour de plus amples informations relatives aux clés de récupérations, veuillez vous référer à « [Utiliser Recovery Manager for Encrypted Volumes \(système de récupération pour volumes chiffrés\)](#) » (p. 167).

Informations

Général Protection Politique Journaux

Protection des postes de travail Vulnérable !

B Agent

Type: BEST

Version du produit: 6.2.4.649

Dernière mise à jour du produit : 21 octobre 2015 09:33:15

Version des signatures: 7.63005 !

Dernière mise à jour des signatures: 21 octobre 2015 09:33:15

Moteur d'analyse principal: Analyse locale

Moteur d'analyse de secours: Aucun(e)

P Présentation

↳ Modules

Antimalware: Activé

Power user: Désactivé

Advanced Threat Control: Activé

↳ Rapport(aujourd'hui)

État des malwares : -> Aucune détection Afficher

Activité des malwares : -> Aucune activité Afficher

Enregistrer Fermer

Fenêtre Informations - Onglet Protection

Pour les Security Server, cet onglet contient des informations relatives au module de Protection du stockage. Les informations concernent :

- Statut Service :
 - **N/A** - La Protection du stockage est autorisée par une licence, mais le service n'a pas encore été configuré.
 - **Activé** - le service est activé dans la politique et fonctionne.
 - **Désactivé** - le service ne fonctionne pas, soit parce qu'il a été désactivé dans la politique, soit parce que la clé de licence a expiré.

- Liste des périphériques de stockage conformes au protocole ICAP connectés avec les informations suivantes :
 - Nom du périphérique de stockage
 - Adresse IP du périphérique de stockage
 - Type du périphérique de stockage
 - The date and time of the last communication between the storage device and Security Server.

Onglet Politique

Une machine virtuelle peut disposer d'une ou de plusieurs politiques, mais seule une politique peut être active à la fois. L'onglet **Politique** affiche des informations sur toutes les politiques qui s'appliquent à la machine virtuelle.

- Le nom de la politique active. Cliquez sur le nom de la politique pour ouvrir le modèle de la politique et afficher ses paramètres.
- Le type de politique active, qui peut être :
 - **Appareil** : lorsque la politique est manuellement affectée à la machine virtuelle par l'administrateur réseau.
 - **Emplacement** : une politique à base de règle assignée à la machine virtuelle si les réglages réseau de la machine virtuelle respectent les conditions d'une [règle d'affectation](#) existante.
 - **Utilisateur** : une politique à base de règle assignée au endpoint s'il respecte l'objectif Active Directory d'une règle d'affectation existante.

Par exemple, une machine peut avoir deux politiques liées à l'utilisateur, une pour les administrateurs et une pour les autres employés. Chaque politique devient active lorsque l'utilisateur avec les privilèges appropriés se connecte.
 - **Externe (NSX)** : lorsque la politique est définie dans l'environnement VMware NSX.
- Le type d'affectation de politique active, qui peut être :
 - **Directe** : lorsque la politique est directement appliquée à la machine virtuelle.
 - **Héritée** : lorsque la machine virtuelle hérite la politique d'un groupe parent.
- **Politiques applicables** : affiche la liste des politiques liées aux règles d'affectation existantes. Ces politiques peuvent s'appliquer à la machine virtuelle lorsqu'elle remplit les conditions des règles d'affectation liées.

Informations
✕

Général Protection Politique Journaux

Résumé

Politique active: Politique par défaut
 Type: Appareil
 Attribution: Hérité de Machines virtuelles

Politiques applicables

Nom de la politique	État	Type	Règles d'affectation
PolicyComplianceReport_tj6	Appliqué	Emplacement	RuleForPolicyComplianceReport_...
Default policy	Appliqué	Appareil	N/D

Première page ← Page de 1 → Dernière page

2 éléments

Enregistrer
Fermer

Fenêtre Informations - Onglet Politique

Pour plus d'informations sur les politiques, reportez-vous à « [Administration des politiques](#) » (p. 224)

Onglet Relais

L'onglet **Relais** est disponible uniquement pour les machines virtuelles avec le rôle relais. Cet onglet affiche des informations sur les endpoints connectés au réseau actuel, comme le nom, l'IP et l'étiquette.

Nom de l'endpoint	IP	Étiquette
CONN-BD	192.168.12.101	
CONN-WIN	192.168.12.222	

Première page ← Page 1 de 1 → Dernière page 20 0 élément

Enregistrer Fermer

Fenêtre Informations - Onglet Relais

Onglet Journaux

L'onglet **Journaux d'analyse** présente des informations détaillées sur toutes les tâches d'analyse effectuées sur la machine virtuelle.

Les journaux sont regroupés par couche de protection et vous pouvez choisir dans le menu déroulant la couche pour laquelle vous souhaitez afficher les journaux.

Cliquez sur la tâche d'analyse qui vous intéresse et le journal s'ouvrira dans une nouvelle page du navigateur.

Lorsque de nombreux journaux d'analyse sont disponibles, ils peuvent occuper plusieurs pages. Pour parcourir les pages, utilisez les options de navigation en bas du tableau. S'il y a trop d'entrées, vous pouvez utiliser les options de filtrage disponibles en haut du tableau .

Informations

Général Protection Politique Journaux

Journaux d'analyse disponibles

Afficher les journaux d'analyse pour : Endpoint Protection

Type	Créé
Analyse rapide	26 octobre 2017, 14:13:51
Analyse complète	05 septembre 2017, 16:16:02

Première page Page 1 de 1 Dernière page 4 éléments

Enregistrer Fermer

Fenêtre Informations - Onglet Journaux d'analyse

Dans cette fenêtre, chaque propriété qui génère des problèmes de sécurité est marquée par l'icône !. Consultez l'info-bulle de l'icône pour plus d'informations. D'autres enquêtes locales peuvent être nécessaires.

6.3.3. Organiser les machines virtuelles en groupes

Vous pouvez gérer des groupes de machines virtuelles dans le panneau de gauche de la page **Réseau**, sous le dossier **Groupes personnalisés**.

Les machines virtuelles importées de Nutanix Prism Element sont regroupées sous le dossier **Inventaire Nutanix**. Les machines virtuelles importées de VMware vCenter sont regroupées sous le dossier **Inventaire VMware**. Les machines virtuelles importées de XenServer sont regroupées sous le dossier **Inventaire Citrix**. Vous ne pouvez pas modifier l'Inventaire Nutanix, l'Inventaire VMware ni l'Inventaire Citrix. Vous pouvez uniquement afficher et gérer les machines virtuelles correspondantes.

Toutes les machines virtuelles qui ne sont pas gérées par les systèmes Nutanix Prism, vCenter ou XenServer sont détectées par la découverte du réseau et placées sous **Groupes personnalisés**, où vous pouvez les classer dans des groupes selon vos préférences. L'un des principaux avantages est que vous pouvez utiliser des politiques de groupes pour répondre à différents besoins en sécurité.

Groupes personnalisés vous permet de [créer](#), [supprimer](#), [renommer](#) et [déplacer](#) des groupes de machines virtuelles dans une structure arborescente personnalisée.

Note


- Un groupe peut contenir à la fois des machines virtuelles et d'autres groupes.
- Lors de la sélection d'un groupe dans le panneau de gauche, vous pouvez afficher toutes les machines virtuelles à l'exception de celles placées dans ses sous-groupes. Pour afficher toutes les machines virtuelles contenus dans le groupe et ses sous-groupes, cliquez sur le menu **Filtres** situé en-haut du tableau et sélectionnez **Tous les éléments de manière récurrente** dans la section **Profondeur**.

Création de groupes

Avant de commencer à créer des groupes, pensez aux raisons pour lesquelles vous en avez besoin et ayez en tête un modèle de regroupement. Vous pouvez par exemple regrouper les machines virtuelles en fonction d'un critère ou d'une combinaison des critères suivants :


- Structure de l'organisation (Ventes, Marketing, Assurance Qualité, Développement logiciel, Gestion etc.).
- Besoins en sécurité (Ordinateurs de bureau, Portables, Serveurs etc.).
- Emplacement (siège, bureaux locaux, travailleurs à distance, bureaux à domicile etc.).

Pour organiser votre réseau en groupes :

1. Sélectionnez **Groupes personnalisés** dans le panneau de gauche.
2. Cliquez sur le bouton  **Ajouter un groupe** en haut du panneau de gauche.
3. Indiquez un nom explicite pour le groupe et cliquez sur **OK**. Le nouveau groupe apparaît sous **Groupes personnalisés**.

Renommer des groupes

Pour renommer un groupe :

1. Sélectionnez le groupe dans le panneau de gauche.
2. Cliquez sur le bouton  **Éditer le groupe** en haut du panneau de gauche.
3. Saisissez le nouveau nom dans le champ correspondant.
4. Cliquez sur **OK** pour confirmer.

Déplacer des groupes et des machines virtuelles

Vous pouvez déplacer des éléments partout à l'intérieur de la hiérarchie **Groupes personnalisés**. Pour déplacer une entité, glissez déposez-la du panneau de droite vers le groupe de votre choix du panneau de gauche.



Note

L'entité qui est déplacée héritera des paramètres de la politique du nouveau groupe parent, à moins que l'héritage de la politique ait été désactivé et qu'une politique différente lui ait été attribuée. Pour plus d'informations sur l'héritage de la politique, reportez-vous à « [Politiques de sécurité](#) » (p. 223).

Supprimer des groupes

Un groupe ne peut pas être supprimé s'il contient au moins une machine virtuelle. Déplacez toutes les machines virtuelles du groupe que vous souhaitez supprimer vers d'autres groupes. Si le groupe comprend des sous-groupes, vous pouvez choisir de déplacer des sous-groupes entiers plutôt que des machines virtuelles individuelles.

Pour supprimer un groupe :

1. Sélectionnez le groupe vide.
2. Cliquez sur le bouton  **Supprimer un groupe** en haut du panneau de gauche. Vous devrez confirmer votre action en cliquant sur **Oui**.

6.3.4. Trier, filtrer et rechercher des machines virtuelles

En fonction du nombre de machines virtuelles, le tableau des machines virtuelles peut comporter plusieurs pages (seules 20 entrées sont affichées par page par défaut). Pour parcourir les pages, utilisez les boutons de navigation en bas du tableau. Pour modifier le nombre d'entrées affichées sur une page, sélectionnez une option dans le menu à côté des boutons de déplacement.

S'il y a trop d'entrées, vous pouvez utiliser les zones de recherche sous les en-têtes de colonne ou le menu du **Filtres** en haut de la page afin d'afficher uniquement les entités qui vous intéressent. Vous pouvez, par exemple, rechercher une machine virtuelle spécifique ou choisir d'afficher uniquement les machines virtuelles administrées.

Trier des machines virtuelles

Pour trier les données en fonction d'une colonne spécifique, cliquez sur les en-têtes de colonne. Par exemple, si vous voulez classer les machines virtuelles par nom, cliquez sur l'en-tête **Nom**. Si vous cliquez de nouveau sur l'en-tête, les machines virtuelles s'afficheront dans l'ordre inverse.

Nom	OS	IP	Dernière connexion	Étiquette

Trier des ordinateurs

Filtrer des machines virtuelles

1. Sélectionnez le groupe souhaité dans le panneau de gauche.
2. Cliquez sur le menu **Filtres** en haut de la zone de panneaux du réseau.
3. Utilisez les critères de filtrage comme suit :
 - **Type**. Sélectionnez le type d'entités virtuelles à afficher.

Type	Sécurité	Politique	Alimentation	Étiquette	Profondeur
Filtrer par					
<input type="checkbox"/> Machines virtuelles	<input type="checkbox"/> Clusters				
<input type="checkbox"/> Hôtes	<input type="checkbox"/> Datacenters				
<input type="checkbox"/> vApps	<input type="checkbox"/> Pools de ressources				
<input type="checkbox"/> Dossiers	<input type="checkbox"/> Pools				
Profondeur: dans les dossiers sélectionnés					
Enregistrer		Annuler		Réinitialiser	

Machines virtuelles - Filtrer par type

- **Sécurité**. Sélectionnez la gestion de protection et/ou l'état de sécurité pour filtrer les objets du réseau. Par exemple, vous pouvez choisir de ne voir que les machines Security Server , ou ne voir que les endpoints avec des problèmes de sécurité.

Type	Sécurité	Politique	Alimentation	Étiquette	Profondeur
Management <input type="checkbox"/> Administrés (Postes de travail) <input type="checkbox"/> Administré avec vShield <input type="checkbox"/> Gérés (Serveurs Exchange) <input type="checkbox"/> Gérés (Relais) <input type="checkbox"/> Serveurs de sécurité <input type="checkbox"/> Non administré		Problèmes de sécurité <input type="checkbox"/> Avec des problèmes de sécurité <input type="checkbox"/> Sans problèmes de sécurité			
Profondeur: récursivement					
Enregistrer		Annuler		Réinitialiser	

Machines virtuelles - Filtrer par sécurité

- **La politique.** Sélectionnez le modèle de politique à partir duquel vous souhaitez filtrer les machines virtuelles, le type d'attribution de la politique (Directe ou Héritée), ainsi que l'état d'attribution de celle-ci (Actif, Affecté ou En attente).

Type	Sécurité	Politique	Alimentation	Étiquette	Profondeur
Modèle: <input type="text"/>		<input type="checkbox"/> Modifié par le Power User			
Type:		<input type="checkbox"/> Direct <input type="checkbox"/> Hérité			
État:		<input type="checkbox"/> Actif <input type="checkbox"/> Appliqué <input type="checkbox"/> En attente			
Profondeur: dans les dossiers sélectionnés					
Enregistrer		Annuler		Réinitialiser	

Machines virtuelles - Filtrer par politique

- **Administrateur.** Vous pouvez choisir d'afficher les machines virtuelles en ligne, hors connexion et suspendues.

Type	Sécurité	Politique	Alimentation	Étiquette	Profondeur
Afficher					
<input type="checkbox"/> En ligne <input type="checkbox"/> Hors Connexion <input type="checkbox"/> Suspendu					
Profondeur: récursivement					
Enregistrer		Annuler		Réinitialiser	

Machines virtuelles - Filtrer par administrateur

- **Tags.** Vous pouvez choisir de filtrer les machines virtuelles en fonction des tags et des attributs que vous avez définis dans votre environnement de virtualisation.

Type	Sécurité	Politique	Alimentation	Étiquette	Profondeur
▼				+	
Type	Attribut	Valeur / Tag	Actions ...		
Profondeur: dans les dossiers sélectionnés					
Enregistrer		Annuler		Réinitialiser	

Machines virtuelles - Filtrer par étiquettes

- **Profondeur.** Lorsque les réseaux de machines virtuelles ont une structure arborescente, les machines virtuelles placées dans des sous-groupes ne s'affichent pas par défaut. Sélectionnez **Tous les éléments de manière récurrente** pour afficher toutes les machines virtuelles comprises dans le groupe actuel et ses sous-groupes.

Type	Sécurité	Politique	Alimentation	Étiquette	Profondeur
Filter par					
<input type="radio"/> Éléments parmi les dossiers sélectionnés					
<input checked="" type="radio"/> Tous les éléments de manière récurrente					
Profondeur: récursivement					
Enregistrer		Annuler		Réinitialiser	

Machines virtuelles - Filtrer par profondeur



Note

Cliquez sur **Réinitialiser** pour effacer le filtre et afficher toutes les machines virtuelles.

4. Cliquez sur **Enregistrer** pour filtrer les machines virtuelles en fonction des critères sélectionnés.

Rechercher des machines virtuelles

1. Sélectionnez le conteneur souhaité dans le panneau de gauche.
2. Saisissez le terme recherché dans la case correspondante sous les en-têtes de colonne (Nom, OS ou IP) dans le panneau de droite. Par exemple, saisissez l'IP de la machine virtuelle que vous recherchez dans le champ **IP**. Seule la machine virtuelle correspondante apparaîtra dans le tableau.

Décochez la case pour afficher la liste complète des machines virtuelles.

6.3.5. Exécuter des tâches sur les machines virtuelles

La page **Réseau** vous permet d'exécuter à distance un certain nombre de tâches d'administration sur les machines virtuelles.

Voici ce que vous pouvez faire :

- « Analyse » (p. 129)
- « Tâches des patches » (p. 139)
- « Analyse Exchange » (p. 142)
- « Installer » (p. 147)
- « Désinstaller Client » (p. 152)
- « Mise à jour » (p. 153)

- « Reconfigurer le client » (p. 154)
- « Découverte du réseau » (p. 155)
- « Découverte applications » (p. 156)
- « Redémarrage machine » (p. 157)
- « Installer le Security Server » (p. 157)
- « Désinstaller le Security Server » (p. 160)
- « Mettre à jour le Security Server » (p. 160)
- « Installer le package de complément HVI » (p. 161)
- « Désinstaller le package de complément HVI » (p. 162)
- « Mettre à jour le package de complément HVI » (p. 163)

Vous pouvez choisir de créer des tâches individuellement pour chaque machine virtuelle ou pour des groupes de machines virtuelles. Vous pouvez par exemple installer à distance Bitdefender Endpoint Security Tools sur un groupe de machines virtuelles non administrées. Vous pouvez créer ultérieurement une tâche d'analyse pour une machine virtuelle du même groupe.

Vous pouvez, pour chaque machine virtuelle, exécuter uniquement les tâches compatibles. Par exemple, si vous sélectionnez une machine virtuelle non administrée, vous pouvez choisir d'installer uniquement l'agent de sécurité, toutes les autres tâches étant désactivées.

Pour un groupe, la tâche sélectionnée sera créée uniquement pour les machines virtuelles compatibles. Si aucune des machines virtuelles du groupe n'est compatible avec la tâche sélectionnée, vous serez informé que la tâche n'a pas pu être créée.


Une fois créée, la tâche commencera à s'exécuter immédiatement sur les machines virtuelles en ligne. Si une machine virtuelle est hors ligne, la tâche s'exécutera dès qu'elle sera de nouveau en ligne.

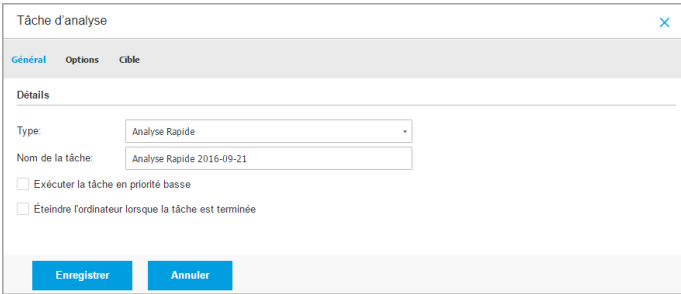
Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Analyse

Pour exécuter une tâche d'analyse à distance sur une ou plusieurs machines virtuelles :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).

3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Toutes les entités contenues dans le groupe sélectionné apparaissent dans le tableau du panneau de droite.
4. Cochez les cases correspondant aux objets que vous souhaitez analyser.
5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Analyse**. Une fenêtre de configuration s'affichera.
6. Configurer les options d'analyse :
 - L'onglet **Général**, vous permet de choisir le type d'analyse et de saisir un nom pour la tâche d'analyse. Le nom de la tâche d'analyse est destiné à vous aider à identifier facilement l'analyse en cours dans la page **Tâches**.



Tâche Analyse des machines virtuelles - Configurer les paramètres généraux

Sélectionnez le type d'analyse dans le menu **Type** :

- L'**Analyse rapide** est préconfigurée pour n'analyser que les emplacements critiques du système et les nouveaux fichiers. La réalisation d'une analyse rapide dure généralement moins d'une minute et n'utilise qu'une petite partie des ressources du système dont a besoin une analyse antivirus classique.

En cas de détection d'un malware ou d'un rootkit, Bitdefender procède automatiquement à la désinfection. Si pour une raison quelconque le fichier ne peut pas être désinfecté, il est déplacé en quarantaine. Ce type d'analyse ignore les fichiers suspects.

- L'**Analyse Complète** analyse l'ensemble du système afin de détecter tous les types de malwares menaçant sa sécurité : virus, spywares, adwares, rootkits et autres.

Bitdefender essaye automatiquement de désinfecter les fichiers dans lesquels un malware a été détecté. Si le malware ne peut pas être supprimé, il est confiné en quarantaine, où il ne peut pas faire de mal. Les fichiers suspects sont ignorés. Si vous voulez également prendre des mesures pour les fichiers suspects, ou si vous voulez changer les actions par défaut pour les fichiers infectés, choisissez l'Analyse personnalisée.

- L'**analyse de la mémoire** vérifie les programmes en cours d'exécution dans la mémoire de la machine virtuelle.
- L'**Analyse du réseau** est un type d'analyse personnalisée, permettant d'analyser les lecteurs réseau à l'aide de l'agent de sécurité de Bitdefender installé sur la machine virtuelle cible.

Pour que la tâche d'analyse du réseau fonctionne :

- Vous devez affecter la tâche à un seul endpoint de votre réseau.
- Vous devez indiquer les identifiants d'un compte utilisateur avec des permissions de lecture/écriture sur les lecteurs réseau cibles, afin que l'agent de sécurité soit capable d'accéder et d'appliquer des actions sur ces lecteurs réseau. Les identifiants requis peuvent être configurés dans l'onglet **Cible** de la fenêtre des tâches.
- **Analyse personnalisée** vous permet de sélectionner les emplacements à analyser et de configurer les options d'analyse.

Pour analyses mémoire, réseau et personnalisée, vous avez également les options suivantes :

- **Exécuter la tâche en priorité basse**. Cochez cette case pour diminuer la priorité du processus d'analyse et permettre à d'autres programmes de fonctionner plus rapidement. Cela augmentera le temps nécessaire au processus d'analyse.



Note

Cette option ne s'applique qu'à Bitdefender Endpoint Security Tools et Endpoint Security (ancien agent).

- **Éteindre l'ordinateur lorsque la tâche est terminée**. Cochez cette case pour éteindre votre machine si vous ne comptez pas l'utiliser pendant un certain temps.



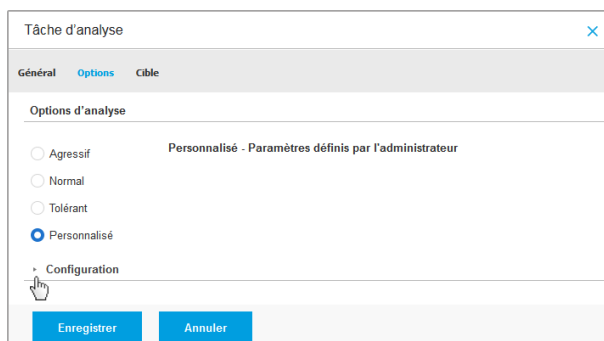
Note

Cette option s'applique à Bitdefender Endpoint Security Tools, Endpoint Security (ancien agent) et Endpoint Security for Mac.

Pour des analyses personnalisées, configurez les paramètres suivants :

- Allez dans l'onglet **Options** pour définir les options d'analyse. Cliquez sur le niveau de sécurité qui correspond le mieux à vos besoins (Agressif, Normal ou Tolérant). Utilisez la description à droite de l'échelle pour faire votre choix.

Basées sur le profil sélectionné, les options d'analyse de la section **Configuration** sont configurées automatiquement. Vous pouvez cependant, si vous le souhaitez, les configurer en détail. Pour cela, sélectionnez l'option **Personnalisé** puis développez la section **Configuration**.



Tâche Analyse des machines virtuelles - Configurer une analyse personnalisée

Voici les options proposées :

- **Types de fichiers.** Utilisez ces options pour spécifier les types de fichiers que vous souhaitez analyser. Vous pouvez configurer l'agent de sécurité afin qu'il analyse tous les fichiers (quelle que soit leur extension), ou uniquement les fichiers d'applications ou certaines extensions de fichiers que vous considérez dangereuses. L'analyse de tous les fichiers fournit la meilleure protection, alors que l'analyse des applications uniquement peut être utilisée pour effectuer une analyse plus rapide.



Note

Les fichiers d'applications sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers. Pour plus d'informations, reportez-vous à « [Types de fichiers d'applications](#) » (p. 529).

Si vous souhaitez uniquement que certaines extensions soient analysées, sélectionnez **Extensions personnalisées** dans le menu puis saisissez les extensions dans le champ de saisie, en appuyant sur **Entrée** après chaque extension.



Important

Les agents de sécurité de Bitdefender installés sur les systèmes d'exploitation Windows et Linux analysent la plupart des formats .ISO mais ne leur appliquent aucune action.

Configuration

Types de fichiers

Type: Extensions personnalisées

Extensions: bat ✕
exe|

Options de la tâche Analyse des machines virtuelles - Ajouter des extensions personnalisées

- **Archives.** Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité du système. Les malwares peuvent affecter le système uniquement si le fichier infecté est extrait de l'archive et exécuté sans que la protection en temps réel ne soit activée. Il est toutefois recommandé d'analyser les archives afin de détecter et de supprimer toute menace potentielle, même si celle-ci n'est pas imminente.



Important

L'analyse des fichiers compressés augmente le temps d'analyse global et demande plus de ressources système.

- **Analyser le contenu compressé.** Sélectionnez cette option si vous souhaitez que les archives fassent l'objet d'une analyse antimalware. Si vous décidez d'utiliser cette option, vous pouvez configurer les options d'optimisation suivantes :
 - **Limiter la taille des archives à (Mo).** Vous pouvez définir une limite de taille pour les archives à analyser. Cochez la case correspondante et tapez la taille maximale des archives (en Mo).
 - **Profondeur maximale des archives (niveaux).** Cochez la case correspondante et sélectionnez la profondeur maximale des archives dans le menu. Pour les meilleures performances, choisissez la valeur la plus faible, pour la protection maximale, choisissez la valeur la plus élevée.
- **Analyser les archives de messagerie.** Sélectionnez cette option si vous souhaitez permettre l'analyse de fichiers de messagerie et de bases de données de messagerie, y compris de formats de fichiers tels que .eml, .msg, .pst, .dbx, .mbx, .tbb et d'autres.



Important

L'analyse des archives de messagerie consomme beaucoup de ressources et peut avoir un impact sur les performances du système.

- **Divers.** Cochez les cases correspondantes pour activer les options d'analyse souhaitées.
 - **Analyser les secteurs d'amorçage.** Pour analyser les secteurs de boot du système. Ce secteur du disque dur contient le code de la machine virtuelle nécessaire pour faire démarrer le processus d'amorçage du système. Quand un virus infecte le secteur d'amorçage, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.
 - **Analyser la base de registre.** Sélectionnez cette option pour analyser les clés de registre. Le registre Windows est une base de données qui contient les paramètres et les options de configuration des composants du système d'exploitation Windows, ainsi que des applications installées.

- **Rechercher les rootkits.** Sélectionnez cette option pour rechercher des [rootkits](#) et des objets cachés à l'aide de ce logiciel.
- **Rechercher des enregistreurs de frappe.** Sélectionnez cette option pour rechercher les logiciels [keyloggers](#). Les keyloggers ne sont pas forcément des applications malveillantes mais ils peuvent être utilisés à des fins malveillantes. Le pirate peut récupérer des informations sensibles à partir des données volées, comme vos numéros de comptes bancaires ou vos mots de passe pour les utiliser à son propre profit.
- **Analyser la mémoire.** Sélectionnez cette option pour analyser les programmes s'exécutant dans la mémoire du système.
- **Analyser les cookies.** Sélectionnez cette option pour analyser les cookies stockés par les navigateurs sur la machine virtuelle.
- **Analyser uniquement les nouveaux fichiers et ceux modifiés.** En analysant uniquement les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.
- **Rechercher des applications potentiellement indésirables.** Un Logiciel Potentiellement Indésirable (LPI) est un programme qui peut être indésirable sur l'ordinateur et peut provenir d'un logiciel gratuit. De tels programmes peuvent être installés sans le consentement de l'utilisateur (alors appelés Adware) ou sont inclus par défaut dans le kit d'installation rapide. Les effets possibles de ces programmes sont l'affichage de pop-ups, l'installation indésirable de barre d'outils dans le navigateur par défaut ou le lancement de plusieurs programmes en arrière-plan qui ralentissent les performances du PC.
- **Analyser les volumes amovibles.** Sélectionnez cette option pour analyser tous les supports de stockage amovibles liés à la machine virtuelle.
- **Actions.** En fonction du type de fichier détecté, les actions suivantes sont menées automatiquement :
 - **Quand un fichier infecté est détecté.** Bitdefender détecte les fichiers considérés comme infectés par le biais de divers

mécanismes avancés, notamment les technologies basées sur l'intelligence artificielle, l'apprentissage machine et les signatures de logiciels malveillants. L'agent de sécurité de Bitdefender peut généralement supprimer le code malveillant d'un fichier infecté et reconstruire le fichier d'origine. Cette opération est appelée désinfection.

Si un fichier infecté est détecté, l'agent de sécurité de Bitdefender tentera automatiquement de le désinfecter. Si la désinfection échoue, le fichier est placé en quarantaine afin de contenir l'infection.



Important

Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

- **Quand un fichier suspect est détecté.** Les fichiers sont considérés comme étant suspects par l'analyse heuristique et les autres technologies Bitdefender. Ils offrent un taux de détection élevé, mais les utilisateurs doivent tenir compte de la probabilité de faux résultats positifs (fichiers propres détectés comme étant suspects), dans certains cas. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible.

Les tâches d'analyse sont configurées par défaut pour ignorer les fichiers suspects. Vous pouvez modifier l'action par défaut afin de placer des fichiers suspects en quarantaine. Les fichiers en quarantaine sont envoyés régulièrement aux Laboratoires Bitdefender pour y être analysés. Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

- **Quand un rootkit est détecté .** Les rootkits sont des logiciels spécialisés utilisés pour masquer des fichiers au système d'exploitation. Bien que n'étant pas malveillants par nature, les rootkits sont souvent utilisés pour masquer des malwares ou la présence d'un intrus dans le système.

Les rootkits détectés et les fichiers cachés sont ignorés par défaut.

Lorsqu'un virus est détecté sur une machine virtuelle NSX, Security Server tag automatiquement la machine virtuelle avec un tag de sécurité, à condition que cette option ait été sélectionnée à l'intégration vCenter Server.

A cette fin, le NSX comprend trois tags de sécurité, spécifiques à la gravité de la menace :

- `ANTI_VIRUS.VirusFound.threat=low`, s'applique sur la machine lorsque Bitdefender classe le malware en risque faible, qu'il peut supprimer.
- `ANTI_VIRUS.VirusFound.threat=medium`, s'applique sur la machine si Bitdefender ne peut pas supprimer les fichiers infectés, mais il les désinfecte.
- `ANTI_VIRUS.VirusFound.threat=high`, s'applique sur la machine si Bitdefender ne peut ni supprimer les fichiers infectés, ni les désinfecte, mais en bloque l'accès.

Vous pouvez isoler des machines infectées en créant des groupes de sécurité avec une appartenance dynamique basée sur les tags de sécurité.



Important

- Si Bitdefender découvre des menaces sur une machine de différents niveaux de sévérité, il lui appliquera les tags coorespondant.
- Un tag de sécurité n'est supprimé d'une machine qu'après une analyse complète et la désinfection de la machine.

Bien que ce ne soit pas recommandé, vous pouvez modifier les actions par défaut. Vous pouvez spécifier une deuxième action à prendre si la première a échoué, ainsi que d'autres mesures, pour chaque catégorie. Choisissez dans les menus correspondants la première et la seconde actions à prendre pour chaque type de fichier détecté. Les actions suivantes sont disponibles :

Désinfecter

Supprimer le code malveillant des fichiers infectés. Nous vous recommandons de toujours la conserver comme première action à appliquer aux fichiers infectés.

Déplacer en quarantaine

Déplacer les fichiers détectés de l'emplacement actuel vers le dossier de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Vous pouvez gérer les fichiers en quarantaine à partir de la page [Quarantaine](#) de la console.

Supprimer


Supprime les fichiers détectés du disque, sans avertissement. Nous vous recommandons d'éviter d'utiliser cette action.


Ignorer

Aucune action ne sera appliquée aux fichiers détectés. Ces fichiers apparaîtront uniquement dans le journal d'analyse.

- Allez dans l'onglet **Cible** pour ajouter les emplacements que vous souhaitez analyser sur les machines virtuelles cibles.

La section **Cible de l'analyse** vous permet d'ajouter un nouveau fichier ou dossier à analyser :

- a. Spécifiez un emplacement prédéfini dans le menu déroulant ou saisissez les **Chemins spécifiques** que vous souhaitez analyser.
- b. Indiquez le chemin de l'objet à analyser dans le champ de saisie.
 - Si vous avez choisi un emplacement prédéfini, complétez le chemin selon vos besoins. Par exemple, pour analyser l'ensemble du dossier `Program Files`, il suffit de sélectionner l'emplacement prédéfini correspondant dans le menu déroulant. Pour analyser un dossier spécifique de `Program Files`, vous devez compléter le chemin en ajoutant une barre oblique inverse (`\`) et le nom du dossier.
 - Si vous avez choisi **Chemins spécifiques**, indiquez le chemin complet vers l'objet à analyser. Il est recommandé d'utiliser les variables du système (le cas échéant) afin de s'assurer que le chemin est valide sur toutes les machines virtuelles cibles. Pour plus d'informations sur les variables du système, reportez-vous à « [Variables du système](#) » (p. 530).
- c. Cliquez sur le bouton  **Ajouter** correspondant.

Pour modifier un emplacement existant, cliquez dessus. Pour retirer un emplacement de la liste, cliquez sur le bouton  **Supprimer** correspondant.

Pour les tâches d'analyse du réseau, vous devez indiquer les identifiants d'un compte utilisateur avec des permissions de lecture/écriture sur les lecteurs réseau cibles, afin que l'agent de sécurité soit capable d'accéder et d'appliquer des actions sur ces lecteurs réseau.

Cliquez sur la section **Exclusions** si vous souhaitez définir des exclusions de la cible.



Fichier	Type d'exclusions	Action
Chemins spécifiques	Fichiers et dossiers à analyser	Action

Tâche Analyse des machines virtuelles - Définir des exclusions

Vous pouvez soit utiliser les exclusions définies par la politique ou définir des exclusions explicites pour l'analyse en cours. Pour plus d'informations sur les exclusions, reportez-vous à « [Exclusions](#) » (p. 294).

7. Cliquez sur **Enregistrer** pour créer la tâche d'analyse. Une message de confirmation s'affichera.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Note

Pour planifier une tâche d'analyse, allez sur la page des **Politiques**, sélectionnez la stratégie affectée aux machines virtuelles qui vous intéressent, et ajoutez une tâche d'analyse dans la rubrique **Antimalware > à la demande**. Pour plus d'informations, reportez-vous à « [A la demande](#) » (p. 273).

Tâches des patches

Il est recommandé de fréquemment vérifier si des mises à jour de logiciels sont disponibles et de les installer le plus rapidement possible. GravityZone automatise ce processus par des politiques de sécurité, mais si vous devez immédiatement

mettre à jour un logiciel sur certaines machines virtuelles, suivez les instructions suivantes :


1. [Analyse des patches](#)
2. [Installation des patches](#)

Configuration nécessaire

- L'agent de sécurité avec le module de Gestion des patches est installé sur les machines cibles.
- Pour que les tâches d'analyse et d'installation réussissent, les machines Windows doivent remplir les conditions suivantes :
 - **Autorités de certification racines de confiance** stocke le certificat **DigiCert Assured ID Root CA**.
 - **Autorités de certification intermédiaires** contient le **DigiCert SHA2 Assured ID Code Signing CA**.
 - Les correctifs pour Windows 7 et Windows Server 2008 R2 mentionnés dans cet article de Microsoft sont installés sur les endpoints : [Microsoft Security Advisory 3033929](#)

Analyse des patches

Les machines virtuelles dont les logiciels ne sont pas à jour sont vulnérables aux attaques. Il est recommandé de contrôler fréquemment les logiciels de vos machines et de les mettre à jour le plus rapidement possible. Pour analyser si certains patches ne sont pas installés sur vos machines virtuelles :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Tous les endpoints du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Sélectionnez les endpoints cibles :
5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Analyse des patches**. Une fenêtre de confirmation s'affichera.
6. Cliquez sur **Oui** pour confirmer la tâche d'analyse.

Une fois la tâche terminée, GravityZone ajoute tous les patches dont vos logiciels ont besoin dans l'Inventaire des patches. Pour plus d'informations, reportez-vous à « [Inventaire des patches](#) » (p. 201).

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).




Note


Pour planifier une analyse des patches, modifiez les politiques assignées aux machines cibles, et configurez les options de la section **Gestion des patches**. Pour plus d'informations, reportez-vous à « [Gestion des correctifs](#) » (p. 343).

Installation des patches

Pour installer un ou plusieurs patches sur les machines virtuelles cibles :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Tous les endpoints du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Installer un patch**

Une fenêtre de configuration s'affichera. Vous pouvez ici voir tous les patches manquants des machines cibles.

5. Si nécessaire, utilisez les options de tri et de filtre situées en haut du tableau pour trouver certains patches.
6. Cliquez sur le bouton  **Colonnes** en haut à droite du volet pour voir les informations concernées.
7. Sélectionnez les patches que vous souhaitez installer.

Certains patches sont dépendant d'autres patches. Dans ce cas, ils sont automatiquement sélectionnés avec le patch.

Cliquez sur numéros de **CVE** ou de **Produits** pour faire apparaître un volet à gauche de l'écran. Le volet contient des informations additionnelles, comme les CVE résolus par le patch, ou les produits auxquels le patch s'applique. Quand vous en aurez pris connaissance, cliquez sur **Fermer** pour masquer le volet.

8. Sélectionnez **Redémarrer les endpoints après l'installation du correctif, si nécessaire** pour redémarrer les endpoints immédiatement après l'installation du correctif, si un redémarrage du système est nécessaire. Veuillez noter que cette action peut perturber l'activité de l'utilisateur.
9. Cliquez sur **Installer**.
La tâche d'installation est créée en parallèle à d'autres sous-tâches pour chaque machine virtuelle cible.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Note

- Pour planifier un déploiement de patches, modifiez les politiques assignées aux machines cibles, et configurez les options de la section **Gestion des patches**. Pour plus d'informations, reportez-vous à « [Gestion des correctifs](#) » (p. 343).
- Vous pouvez également installer un correctif à partir de la page **Inventaire des correctifs**, en commençant par le correctif qui vous intéresse. Dans ce cas, sélectionnez le correctif dans la liste, cliquez sur le bouton **Installer** situé en haut du tableau et configurez les détails de l'installation du correctif. Pour plus d'informations, reportez-vous à « [Installer des patches](#) » (p. 205).
- Après l'installation du correctif, nous vous recommandons de lancer une tâche d'[Analyse du correctif](#) sur les endpoints cibles. Cette action mettra à jour les informations du correctif stockées dans GravityZone pour vos réseaux gérés.

Vous pouvez désinstaller des correctifs :

- À distance, en lançant une [tâche de désinstallation de correctifs](#) à partir de GravityZone.
- Localement sur la machine. Dans ce cas, vous devez vous connecter au endpoint en tant qu'administrateur et exécuter le programme de désinstallation manuellement.

Analyse Exchange

Vous pouvez analyser à distance la base de données d'un Serveur Exchange en exécutant une tâche **Analyse Exchange**.

Pour pouvoir analyser la base de données Exchange, vous devez activer l'analyse à la demande en indiquant les identifiants d'un administrateur Exchange. Pour plus

d'informations, reportez-vous à « [Analyse de la banque d'informations Exchange](#) » (p. 369).

Pour analyser une base de données Exchange Server :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Dans le panneau de gauche, sélectionnez le groupe contenant le serveur Exchange cible. Vous pouvez voir le serveur dans le panneau de droite.



Note

Vous pouvez également appliquer des filtres pour trouver rapidement le serveur cible :

- Cliquez sur le menu **Filtres** et sélectionnez les options suivantes : **Gérés (Serveurs Exchange)** dans l'onglet **Sécurité** et **Tous les éléments de manière récurrente** dans l'onglet **Profondeur**.
 - Indiquez le nom d'hôte ou l'IP du serveur dans les champs des en-têtes de colonnes correspondants.
4. Cochez la case du Serveur Exchange dont vous souhaitez analyser la base de données.
 5. Cliquez sur le bouton **Tâches** en haut du tableau et sélectionnez **Analyse Exchange**. Une fenêtre de configuration s'affichera.
 6. Configurer les options d'analyse :
 - **Général**. Indiquez un nom explicite pour la tâche.
Pour les bases de données importantes, la tâche d'analyse peut être longue et avoir un impact sur les performances du serveur. Dans ce cas, cochez la case **Arrêter l'analyse si elle dure plus de** et sélectionnez un intervalle adapté dans les menus correspondants.
 - **Cible**. Sélectionnez les conteneurs et objets à analyser. Vous pouvez choisir d'analyser les boîtes aux lettres, les dossiers publics ou les deux. En plus des e-mails, vous pouvez choisir d'analyser d'autres objets tels que les **Contacts**, **Tâches**, **Rendez-vous** et **Éléments de publication**. Vous pouvez en outre définir les restrictions suivantes au contenu à analyser :
 - Uniquement les messages non lus
 - Uniquement les éléments avec des pièces jointes
 - Uniquement les nouveaux éléments, reçus pendant une période donnéeVous pouvez par exemple choisir d'analyser uniquement les e-mails de boîtes aux lettres d'utilisateurs, reçus au cours des 7 derniers jours.

Cochez la case **Exclusions**, si vous souhaitez définir des exceptions à l'analyse. Pour créer une exception, utilisez les champs de l'en-tête du tableau comme suit :

- Sélectionnez le type de référentiel dans le menu.
- En fonction du type de référentiel, spécifiez l'objet à exclure :

Type de référentiel	Format de l'objet
Boîte de messagerie	Adresse e-mail
Dossier public	Chemin d'accès du dossier, depuis la racine
Base de données	L'identité de la base de données



Note

Pour obtenir l'identité de la base de données, utilisez la commande shell Exchange :

```
Get-MailboxDatabase | fl name,identity
```

Vous ne pouvez saisir qu'un élément à la fois. Si vous avez plusieurs éléments du même type, vous devez définir autant de règles que le nombre d'éléments.

- Cliquez sur le bouton **+ Ajouter** en haut du tableau pour enregistrer l'exception et l'ajouter à la liste.

Pour retirer une règle d'exception de la liste, cliquez sur le bouton **- Supprimer** correspondant.

- **Options.** Configurez les options d'analyse pour les e-mails correspondant à la règle :
 - **Types de fichiers analysés.** Utilisez cette option pour spécifier quels types de fichiers vous souhaitez analyser. Vous pouvez choisir d'analyser tous les fichiers (quelle que soit leur extension), uniquement les fichiers d'applications, ou certaines extensions de fichiers que vous considérez dangereuses. L'analyse de tous les fichiers fournit la meilleure protection, alors que l'analyse des applications uniquement est recommandée pour une analyse plus rapide.



Note

Les fichiers d'applications sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers. Pour plus d'informations, reportez-vous à « [Types de fichiers d'applications](#) » (p. 529).

Si vous souhaitez uniquement analyser les fichiers avec certaines extensions, vous avez deux possibilités :

- **Extensions définies par l'utilisateur**, où vous devez indiquer uniquement les extensions à analyser.
 - **Tous les fichiers, à l'exception d'extensions spécifiques**, où vous devez saisir uniquement les extensions à ne pas analyser.
- **Taille maximale du corps des e-mails/des pièces jointes (Mo)**. Cochez cette case et saisissez une valeur dans le champ correspondant pour définir la taille maximale acceptée d'un fichier joint ou du corps des e-mails à analyser.
 - **Profondeur maximale des archives (niveaux)**. Cochez la case et sélectionnez la profondeur maximale des archives dans le champ correspondant. Plus le niveau de profondeur est faible, meilleures sont les performances et plus le degré de protection est faible.
 - **Rechercher des applications potentiellement indésirables (PUA)**. Cochez cette case pour rechercher les applications potentiellement malveillantes ou indésirables telles que les adwares, qui peuvent s'installer sur les systèmes sans le consentement des utilisateurs, modifier le comportement de différents logiciels et faire diminuer les performances du système.
- **Actions**. Vous pouvez spécifier les différentes actions que l'agent de sécurité pour exécuter sur les fichiers, selon le type de détection.

Le type de détection sépare les fichiers en trois catégories :

- **Fichier(s) infecté(s)**. Bitdefender détecte les fichiers considérés comme infectés par le biais de divers mécanismes avancés, notamment les technologies basées sur l'intelligence artificielle, l'apprentissage machine et les signatures de logiciels malveillants.
- **Fichiers suspects**. Ces fichiers sont considérés comme étant suspicieux par l'analyse heuristique et les autres technologies Bitdefender. Ils offrent un taux de détection élevé, mais les utilisateurs doivent tenir compte de la probabilité de faux résultats positifs (fichiers propres détectés comme étant suspicieux), dans certains cas.
- **Fichiers non analysables**. Ces fichiers ne peuvent pas être analysés. Les fichiers non analysables incluent mais ne se limitent pas aux fichiers protégés par des mots de passe, chiffrés ou compressés.

Pour chaque type de détection, vous avez une action par défaut ou principale et une action alternative en cas d'échec de l'action principale. Bien que ce

ne soit pas recommandé, vous pouvez changer ces actions à partir des menus correspondants. Sélectionnez l'action à appliquer :

- **Désinfecter.** Supprime le code malveillant des fichiers infectés et reconstruit le fichier d'origine. Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Nous vous recommandons de toujours la conserver comme première action à appliquer aux fichiers infectés. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible.
- **Rejeter/Supprimer l'e-mail.** Sur les serveurs avec le rôle Transport Edge, l'e-mail détecté est rejeté avec un code d'erreur SMTP 550. Dans tous les autres cas, l'e-mail est supprimé sans avertissement. Nous vous recommandons d'éviter d'utiliser cette action.
- **Supprimer le fichier.** Supprime les pièces jointes présentant des problèmes sans aucun avertissement. Nous vous recommandons d'éviter d'utiliser cette action.
- **Remplacer le fichier.** Supprime les fichiers présentant des problèmes et insère un fichier texte qui informe l'utilisateur des actions appliquées.
- **Placer le fichier en quarantaine.** Place les fichiers détectés dans le dossier de la quarantaine et insère un fichier texte qui informe l'utilisateur des actions appliquées. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Vous pouvez gérer les fichiers de la quarantaine à partir de la page **Quarantaine**.



Note

Veillez noter que 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.

- **Ignorer** Aucune action ne sera appliquée aux fichiers détectés. Ces fichiers apparaîtront uniquement dans le journal d'analyse. Les tâches d'analyse sont configurées par défaut pour ignorer les fichiers suspects. Vous pouvez modifier l'action par défaut afin de placer des fichiers suspects en quarantaine.
- Par défaut, lorsqu'un e-mail correspond à la portée d'une règle, il est traité exclusivement en fonction de cette règle, sans être comparé à toute autre règle restante. Si vous souhaitez continuer à effectuer une vérification

par rapport aux autres règles, décochez la case **Si les conditions de la règle sont remplies, arrêter de traiter d'autres règles**.

7. Cliquez sur **Enregistrer** pour créer la tâche d'analyse. Une message de confirmation s'affichera.
8. Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « **Afficher et gérer des tâches** » (p. 210).

Installer

Pour protéger vos machines virtuelles avec Security for Virtualized Environments, vous devez installer l'agent de sécurité de Bitdefender sur chacune d'entre elles. L'agent de sécurité de Bitdefender gère la protection sur les machines virtuelles. Il communique également avec le Control Center pour recevoir les commandes de l'administrateur et envoyer les résultats de ses actions. Une fois que vous avez installé un agent de sécurité Bitdefender dans un réseau, il détectera automatiquement les machines virtuelles non protégées de ce réseau. La protection Security for Virtualized Environments peut ensuite être installée sur ces machines virtuelles à distance à partir de Control Center. L'installation à distance s'effectue en tâche de fond, sans que l'utilisateur ne le sache.

Dans les réseaux isolés n'ayant pas de connectivité directe avec l'appliance GravityZone, vous pouvez installer l'agent de sécurité avec le [rôle Relais](#). Dans ce cas, la communication entre l'appliance GravityZone et les autres agents de sécurité s'effectuera via l'agent Relais, qui aura également le rôle de serveur de mise à jour locale pour les agents de sécurité protégeant le réseau isolé.

Note

Nous vous recommandons de maintenir constamment allumée la machine sur laquelle vous installez l'agent Relais.

Avertissement

Avant l'installation, veillez à désinstaller les logiciels antimalware et pare-feu des machines virtuelles. Installer la protection Bitdefender alors que des logiciels de sécurité sont présents peut affecter leur fonctionnement et causer d'importants problèmes avec le système. Windows Defender et le Pare-feu Windows seront automatiquement désactivés lorsque l'installation démarrera.

Pour installer à distance la protection Security for Virtualized Environments sur une ou plusieurs machines virtuelles :


1. Connectez-vous et identifiez-vous sur le Control Center.

2. Allez sur la page **Réseau**.
3. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
4. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Les entités contenues dans le groupe sélectionné apparaissent dans le tableau du panneau de droite.

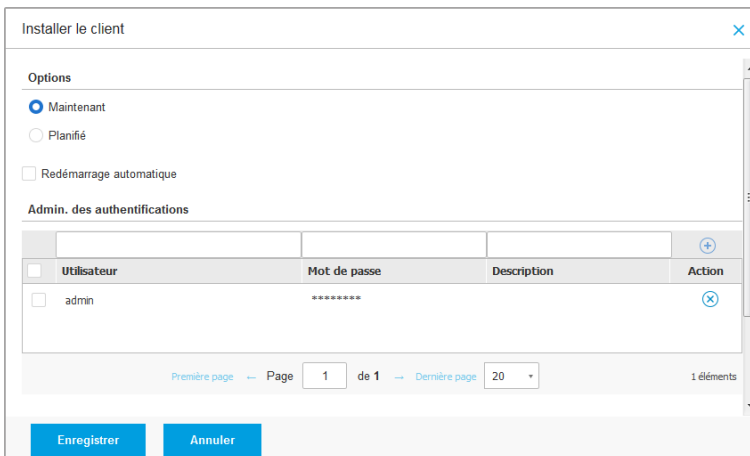


Note

Vous pouvez aussi appliquer des filtres pour afficher uniquement les machines non administrées. 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**.

5. Sélectionnez les entités (machines virtuelles, hôtes, clusters ou groupes) sur lesquelles vous souhaitez installer la protection.
6. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Installer > BEST**.

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	*****		

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

Enregistrer Annuler

Installer Bitdefender Endpoint Security Tools à partir du menu des Tâches

7. 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.

8. Si vous souhaitez que les endpoints cibles redémarrent automatiquement pour terminer l'installation, sélectionnez **Redémarrer automatiquement (si nécessaire)**.
9. 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](#).

 **Note**

Un message d'avertissement s'affiche tant que vous n'avez sélectionné aucun identifiant. Cette étape est obligatoire pour installer à distance Bitdefender Endpoint Security Tools sur les endpoints.

Pour ajouter les identifiants du système d'exploitation requis :

- a. Saisissez le nom d'utilisateur et le mot de passe d'un compte administrateur pour tous les systèmes d'exploitation cibles dans les champs correspondants de l'en-tête du tableau des identifiants. Vous pouvez également ajouter une description qui vous aidera à identifier chaque compte plus facilement.

Si les machines 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.
- 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, cliquez 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.

- c. Cochez les cases correspondant aux comptes que vous souhaitez utiliser.
10. Sous la section **Système de déploiement**, sélectionnez l'entité à laquelle les machines cibles se connecteront pour installer et mettre à jour le client :
- **L'appliance GravityZone**, lorsque les machines se connectent directement à l'appliance GravityZone.
Dans ce cas, vous pouvez également définir un serveur de communication personnalisé en indiquant son IP ou son nom d'hôte, si cela est requis.
 - **Relais Endpoint Security**, si vous souhaitez connecter les machines 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 l'agent relais fonctionne.
- Lors du déploiement de l'agent via un relais Linux, les conditions 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.
- Sur les endpoints cibles sous Linux ou Mac, le SSH doit être activé et le firewall désactivé.

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 trouverez ici tous les packages d'installation créés auparavant pour votre entreprise.

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 comment modifier les packages d'installation, consultez le Guide d'installation de GravityZone.



Avertissement


Veillez noter que le module Pare-feu est disponible uniquement pour les postes Windows.

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.

Désinstaller Client

Pour désinstaller la protection Bitdefender à distance :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Toutes les entités du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Cochez les cases de machines virtuelles dont vous souhaitez désinstaller l'agent de sécurité de Bitdefender.
5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Désinstaller le client**.
6. Une fenêtre de configuration apparaît, vous permettant d'effectuer les paramétrages suivants :
 - Vous pouvez choisir de conserver les éléments en quarantaine sur la machine cliente.
 - Pour les environnements intégrés à vShield, vous devez sélectionner les identifiants requis pour chaque machine, car sinon la désinstallation échouera. Sélectionnez **Utiliser des identifiants pour l'intégration à vShield**, puis vérifiez tous les identifiants appropriés dans le tableau Admin. des authentifications qui apparaît en-dessous.
7. Cliquez sur **Enregistrer** pour créer la tâche. Une message de confirmation s'affichera.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

 **Note**


Si vous souhaitez réinstaller la protection, vous devez d'abord redémarrer l'ordinateur.

Mise à jour

Consultez régulièrement l'état des machines virtuelles administrées. Si vous remarquez une machine virtuelle avec des problèmes de sécurité, cliquez sur son nom pour afficher la page **Informations**. Pour plus d'informations, reportez-vous à « [État de sécurité](#) » (p. 112).

Les clients ou les contenus de sécurité obsolètes constituent des problèmes de sécurité. Dans ces cas, vous devriez exécuter une mise à jour sur les machines virtuelles correspondantes. Cette tâche peut être effectuée en local à partir de la machine virtuelle ou à distance à partir de Control Center.

Pour mettre à jour le client et les contenus de sécurité à distance sur les machines virtuelles administrées :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Toutes les entités du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Cochez les cases des machines virtuelles sur lesquelles vous souhaitez exécuter une mise à jour du client.
5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Mise à jour**. Une fenêtre de configuration s'affichera.
6. Vous pouvez choisir de mettre à jour uniquement le produit, uniquement le contenu de sécurité, ou les deux à la fois.
7. Pour l'OS Linux et les machines intégrées à vShield, il faut également sélectionner les informations d'identification requises. Cochez l'option **Utiliser des identifiants pour l'intégration à Linux et vShield**, puis sélectionnez les identifiants appropriés dans le tableau Admin. des authentifications qui apparaît en-dessous.
8. Cliquez **Mise à jour** pour effectuer la tâche. Une message de confirmation s'affichera.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).


Reconfigurer le client

Les modules de protection de l'agent de sécurité, les rôles et les modes d'analyse sont configurés au départ dans le package d'installation. Après avoir installé l'agent de sécurité dans votre réseau, vous pouvez modifier les paramètres initiaux à tout moment en envoyant une tâche distante **Reconfigurer le client** aux endpoints administrés qui vous intéressent.

Avertissement

Veillez noter que la tâche **Reconfigurer le client** écrase tous les paramètres d'installation et qu'aucun paramètre initial n'est conservé. Veuillez reconfigurer tous les paramètres d'installation des endpoints cibles lors de l'utilisation de cette tâche.

Pour modifier les paramètres d'installation d'une ou plusieurs machines virtuelles :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Toutes les entités du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Cochez les cases des machines virtuelles pour lesquelles vous souhaitez modifier les paramètres d'installation.
5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Reconfigurer le client**.
6. Sous la section **Général**, configurez le moment d'exécution de la tâche :
 - **Maintenant**, afin de lancer la tâche immédiatement.
 - **Planifié**, afin de planifier la fréquence de la tâche. 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 d'autres processus importants doivent également s'exécuter sur la machine cible, vous pouvez planifier la tâche afin qu'elle s'exécute toutes les 2 heures. La tâche démarrera sur chaque machine cible toutes les deux heures jusqu'à ce qu'elle soit réalisée avec succès.

7. Configurez les modules, rôles et modes d'analyse de l'endpoint cible en fonction de vos préférences. Pour plus d'informations, consultez le Guide d'Installation de GravityZone.

Avertissement

- Seuls les modules pris en charge pour chaque système d'exploitation seront installés.
Veuillez noter que le module Pare-feu est disponible uniquement pour les postes Windows.
- Bitdefender Tools (agent héritage) ne supporte que l'analyse centrale.

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

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Découverte du réseau


La découverte du réseau est effectuée automatiquement uniquement par les agents de sécurité avec le rôle **Relais**. Si vous n'avez pas d'agent Relais d'installé dans votre réseau, vous devez envoyer manuellement une tâche de découverte du réseau à partir d'un endpoint protégé.

Pour exécuter une tâche de découverte du réseau dans votre réseau :

Important


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.

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Toutes les entités du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Cochez la case de la machine avec laquelle vous souhaitez effectuer la découverte du réseau.

5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Découverte du réseau**.
6. Un message de confirmation s'affichera. Cliquez sur **Oui**.
Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Découverte applications

Pour découvrir des applications dans votre réseau :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Toutes les machines virtuelles du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Sélectionnez les machines virtuelles sur lesquelles vous souhaitez effectuer une découverte d'applications.
5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Découverte d'applications**.



Note

Bitdefender Endpoint Security Tools avec Contrôle des applications doit être installé et activé sur les machines virtuelles sélectionnées. Autrement, la tâche sera grisée. Lorsqu'un groupe sélectionné contient à la fois des cibles valides et des cibles non valides, la tâche ne sera envoyée qu'aux endpoints valides.

6. Cliquez sur **Oui** dans la fenêtre de confirmation pour continuer.

Les applications et les processus découverts sont affichés sur la page **Réseau > Inventaire des applications**. Pour plus d'informations, reportez-vous à « [Inventaire des applications](#) » (p. 195).



Note

La tâche **Découverte d'applications** peut prendre un certain temps, en fonction du nombre d'applications installées. Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).


Redémarrage machine

Vous pouvez choisir de faire redémarrer à distance les machines virtuelles administrées.



Note

Consultez la page [Réseau > Tâches](#) avant de faire redémarrer certaines machines virtuelles. Les tâches créées auparavant peuvent être encore en cours de traitement sur les machines cibles.

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Toutes les entités du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Cochez les cases des machines virtuelles que vous souhaitez redémarrer.
5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Redémarrer la machine**.
6. Sélectionnez l'option de planification du redémarrage :
 - Sélectionnez **Redémarrer** pour faire redémarrer les machines virtuelles immédiatement.
 - Sélectionnez **Redémarrer le** et utilisez les champs ci-dessous pour planifier le redémarrage à la date et à l'heure souhaitées.
7. Cliquez sur **Enregistrer**. Une message de confirmation s'affichera.
Vous pouvez afficher et gérer la tâche sur la page [Réseau > Tâches](#). Pour plus d'informations, référez-vous à [Afficher et gérer des tâches](#).

Installer le Security Server

Pour installer un Security Server dans votre environnement virtuel :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Parcourez l'inventaire Nutanix, VMware ou Citrix et cochez les cases correspondant aux hôtes ou conteneurs souhaités (Nutanix Prism, vCenter Server, XenServer ou datacenter). Pour une sélection rapide, vous pouvez

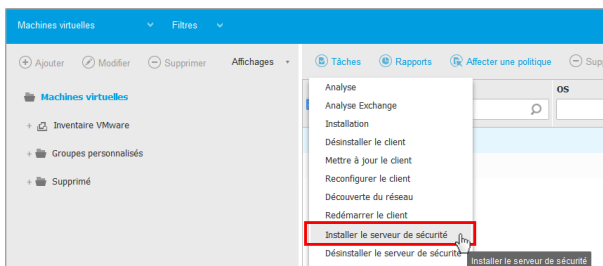
sélectionner directement le conteneur root (Inventaire Nutanix, Inventaire VMware ou Inventaire Citrix). Pour pouvez sélectionner les hôtes individuellement à partir de l'assistant d'installation.



Note

Vous ne pouvez pas sélectionner les hôtes de différents dossiers.

4. Cliquez sur le bouton **Tâches** en haut du tableau et sélectionnez **Installer Security Server** dans le menu. La fenêtre **installation de Security Server** s'affiche.



Installer Security Server à partir du menu Tâches

5. Tous les hôtes détectés dans le conteneur sélectionné apparaîtront dans la liste. Sélectionnez les hôtes sur lesquels vous souhaitez installer les instances de Security Server.
6. Sélectionnez les paramètres de configuration que vous souhaitez utiliser.



Important

Utiliser des paramètres communs tout en déployant plusieurs instances Security Server simultanément nécessite que les hôtes partagent le même emplacement de stockage, aient leurs adresses IP affectées par un serveur DHCP et fassent partie du même réseau.

7. Cliquez sur **Suivant**.
8. Indiquez les identifiants de VMware vShield correspondant à chaque machine vCenter.
9. Indiquez un nom explicite pour le Security Server.

10. Pour les environnements VMware, sélectionnez l'emplacement dans lequel vous souhaitez inclure le Security Server à partir du menu **Dossier de déploiement**.
11. Sélectionnez l'emplacement de stockage de destination.
12. Choisissez le type d'allocation d'espace disque. Il est recommandé de déployer l'appliance en utilisant l'allocation d'espace disque fixe.



Important

Si vous utilisez une allocation d'espace disque dynamique et que l'espace disque de la banque de données vient à manquer, le Security Server se bloquera, et l'hôte demeurera, par conséquent, non protégé.

13. Configurez l'allocation de ressources mémoire et processeur en fonction du ratio de consolidation de la VM sur l'hôte. Sélectionnez **Faible**, **Moyen** ou **Élevé** pour charger les paramètres d'allocation de ressources recommandés ou sur **Manuel** pour configurer l'allocation de ressources manuellement.
14. Vous devez définir un mot de passe administrateur pour la console Security Server. Définir un mot de passe d'administration écrase le mot de passe root par défaut (« sve »).
15. Configurez le fuseau horaire de l'appliance.
16. Sélectionnez le type de configuration réseau pour le réseau Bitdefender. L'adresse IP du Security Server ne doit pas changer puisqu'elle est utilisée par les agents Linux pour la communication.

Si vous choisissez DHCP, veillez à configurer le serveur DHCP afin qu'il réserve une adresse IP à cette appliance.

Si vous choisissez "statique", vous devez indiquer l'adresse IP, le masque de sous-réseau, la passerelle et les informations de DNS.
17. Sélectionnez le réseau vShield et saisissez les identifiants vShield. L'étiquette par défaut du réseau vShield est `vm-service-vshield-pg`.
18. Cliquez sur **Enregistrer** pour créer la tâche. Une message de confirmation s'affichera.



Important

- Les packages du Security Server ne sont pas inclus par défaut dans l'appliance GravityZone. En fonction de la configuration effectuée par l'administrateur

root, le package du Security Server nécessaire à votre environnement sera téléchargé lorsqu'une tâche d'installation du Security Server sera lancée ou l'administrateur sera informé que l'image est manquante et l'installation ne se poursuivra pas. Si le package est manquant, l'administrateur root devra le télécharger manuellement pour que l'installation soit possible.

- L'installation de Security Server sur Nutanix par le biais de la tâche d'installation à distance peut échouer si le cluster Prism Element est enregistré dans Prism Central ou pour une autre raison. Dans ces situations, il est recommandé de réaliser un déploiement manuel de Security Server. Pour plus d'informations, consultez cet [article de la base de connaissances](#) :

19. Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Désinstaller le Security Server

Pour désinstaller un Security Server :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Sélectionnez le datacenter ou le dossier contenant l'hôte sur lequel le Security Server est installé.
4. Cochez la case correspondant à l'hôte sur lequel est installé le Security Server.
5. Cliquez sur le bouton **Tâches** en haut du tableau et sélectionnez **Désinstaller Security Server**.
6. Saisissez les identifiants vShield et cliquez sur **Oui** pour créer la tâche.
7. Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Mettre à jour le Security Server

Pour mettre à jour un Security Server :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'hôte sur lequel est installé le Security Server.

Pour localiser facilement le Security Server, vous pouvez utiliser le menu **Filtres** de la façon suivante :


- Allez dans l'onglet **Sécurité** et sélectionnez **Serveurs de sécurité** uniquement.
- Allez dans l'onglet **Profondeur** et sélectionnez **Tous les éléments de manière récurrente**.



Note

Si vous utilisez un outil de gestion de la virtualisation qui n'est pas intégré actuellement à Control Center, Security Server sera placé dans **Groupes personnalisés**.

Pour plus d'informations concernant les plates-formes de virtualisation supportées, référez-vous au Guide d'installation de GravityZone.

4. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Mettre à jour le Security Server**.
5. Vous devrez confirmer votre action en cliquant sur **Oui**.
6. Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).



Important

Il est recommandé d'utiliser cette méthode pour mettre à jour le Security Server pour NSX, sinon vous perdrez la quarantaine enregistrée sur l'appareil.

Installer le package de complément HVI

Afin de protéger les machines virtuelles avec HVI, vous devez installer le package de complément sur l'hôte. Le rôle de ce package est d'assurer la communication entre l'hyperviseur et Security Server installé sur l'hôte. Une fois installé, HVI va protéger les machines virtuelles qui ont activé HVI dans leur politique.



Important

- HVI protège les machines virtuelles exclusivement sur les hyperviseurs Citrix Xen.
- Vous n'avez pas besoin de désinstaller l'agent de sécurité existant des machines virtuelles.

Pour installer le package de complément sur un hôte :

1. Allez sur la page **Configuration > mise à jour**.
2. Sélectionnez le package de complément dans la liste des **Composants** puis cliquez sur le bouton **Télécharger** en haut du tableau.

3. Aller sur la page **Réseau** et sélectionnez **Machines virtuelles** dans le sélecteur d'affichage.
4. Sélectionnez **Serveur** dans le menu **Aperçus** dans le panneau de gauche.
5. Sélectionnez un ou plusieurs hôtes Xen dans l'inventaire réseau. Vous pouvez facilement voir les hôtes disponibles en sélectionnant l'option **Type > Hôtes** dans le menu **Filtres**.
6. Cliquez sur le bouton **Tâches** sur le panneau de droite et choisissez **Installer le package de complément HVI**. La fenêtre d'installation s'ouvre.
7. Programmez la date de tâche d'installation. Vous pouvez choisir d'exécuter la tâche immédiatement après l'avoir enregistrée, ou à une heure spécifique. Au cas où l'installation ne se termine pas au moment spécifié, la tâche reprend automatiquement selon les paramètres de récurrence. Par exemple, si vous sélectionnez plus d'un hôte et qu'un hôte n'est pas disponible lorsque le package est programmé à être installé, la tâche s'exécutera à nouveau au moment spécifié.
8. L'hôte doit redémarrer pour appliquer les changements et terminer l'installation. Si vous souhaitez que l'hôte redémarre automatiquement, sélectionnez **Redémarrer automatiquement (si besoin)**.
9. Cliquez sur **Enregistrer**. Une message de confirmation s'affichera.
Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**.

Désinstaller le package de complément HVI

Pour désinstaller le package de complément des hôtes :

1. Aller sur la page **Réseau** et sélectionnez **Machines virtuelles** dans le sélecteur d'affichage.
2. Sélectionnez **Serveur** dans le menu **Aperçus** dans le panneau de gauche.
3. Sélectionnez un ou plusieurs hôtes Xen dans l'inventaire réseau. Vous pouvez facilement voir les hôtes disponibles en sélectionnant l'option **Type > Hôtes** dans le menu **Filtres**.
4. Cliquez sur le bouton **Tâches** sur le panneau de droite et choisissez **Désinstaller le package de complément HVI**. La fenêtre de configuration s'affichera.
5. Programmer la suppression du package. Vous pouvez choisir d'exécuter la tâche immédiatement après l'avoir enregistrée, ou à une heure spécifique. Au

cas où la suppression ne se termine pas au moment spécifié, la tâche reprend automatiquement selon les paramètres de récurrence. Par exemple, si vous sélectionnez plus d'un hôte et qu'un hôte n'est pas disponible lorsque le package est programmé à être supprimé, la tâche s'exécutera à nouveau au moment spécifié.

6. L'hôte doit redémarrer pour terminer la suppression. Si vous souhaitez que l'hôte redémarre automatiquement, sélectionnez **Redémarrer automatiquement (si besoin)**.
7. Cliquez sur **Enregistrer**. Une message de confirmation s'affichera.
Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**.

Mettre à jour le package de complément HVI

Pour mettre à jour le package de complément sur les hôtes :


1. Installez le dernier Package complémentaire HVI disponible.
Pour plus d'informations, reportez-vous à « [Installer le package de complément HVI](#) » (p. 161).
2. Allez sur la page **Réseau**.
3. Sélectionnez **Machines virtuelles** dans le sélecteur d'affichage.
4. Sélectionnez **Serveur** dans le menu **Aperçus** dans le panneau de gauche.
5. Sélectionnez un ou plusieurs hôtes Xen dans l'inventaire réseau.
Vous pouvez facilement voir les hôtes disponibles en sélectionnant l'option **Type > Hôtes** dans le menu **Filtres**.
6. Cliquez sur le bouton **Tâches** sur le panneau de droite et choisissez **Mettre à jour le package de complément HVI**. La fenêtre de configuration s'affichera.
7. Programmer la mise à jour du package. Vous pouvez choisir d'exécuter la tâche immédiatement après l'avoir enregistrée, ou à une heure spécifique.

Au cas où la mise à jour ne se termine pas au moment spécifié, la tâche reprend automatiquement selon les paramètres de récurrence. Par exemple, si vous sélectionnez plus d'un hôte et qu'un hôte n'est pas disponible lorsque le package est programmé pour se mettre à jour, la tâche s'exécutera à nouveau au moment spécifié.

8. Sélectionnez **Redémarrer automatiquement (si nécessaire)** si vous voulez redémarrer l'hôte de manière automatique. Sinon, vous devez redémarrer manuellement l'hôte pour appliquer la mise à jour.
9. Cliquez sur **Enregistrer**. Une message de confirmation s'affichera.
Vous pouvez surveiller l'état des tâches sur la page **Réseau > Tâches**.

Injecter l'outil personnalisé

Pour injecter des outils dans les systèmes d'exploitation invités, cible :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Sélectionnez le groupe souhaité dans le panneau de gauche. Tous les endpoints du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Sélectionnez les cases à cocher des endpoints ciblés.
5. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Injecter l'outil personnalisé**. Une fenêtre de configuration s'affiche.
6. Dans le menu déroulant, sélectionnez tous les outils que vous voulez injecter. Pour chaque outil sélectionné, une section apparaît avec ses réglages.

Ces outils étaient auparavant envoyés dans GravityZone. Si vous ne trouvez pas le bon outil dans la liste, rendez-vous dans le **Centre de gestion des outils** et ajoutez-le. Pour plus d'informations, reportez-vous à « [Injection d'outils personnalisés avec HVI](#) » (p. 496).

7. Pour chaque outil affiché sur la fenêtre :
 - a. Cliquez sur le nom de l'outil pour voir ou masquer sa section.
 - b. Saisissez la ligne de commande de l'outil, avec tous les paramètres nécessaires, exactement comme vous le feriez sur le terminal ou l'invite de commande. Par exemple :

```
bash script.sh <param1> <param2>
```

Pour les outils de réparation BD, vous ne pouvez sélectionner que l'action de réparation et l'action de réparation de secours dans les menus déroulants.

- c. Indiquez l'endroit depuis lequel Security Server doit collecter les journaux :

- **stdout.** Sélectionnez les cases à cocher pour capturer les journaux du canal standard de communication de sortie.
- **Fichier de sortie.** Cochez cette case pour collecter le fichier journal enregistré sur l'endpoint. Dans ce cas, vous devez saisir un emplacement où Security Server peut trouver le fichier. Vous pouvez utiliser des chemins absolus ou des variables du système.

Vous disposez ici d'une option supplémentaire : **Supprimer les fichiers journal d'Invité après les avoir transférés.** Sélectionnez-la si vous n'avez plus besoin des fichiers sur l'endpoint.


8. Si vous voulez transférer les fichiers journaux du Security Server à un autre emplacement, vous devez fournir le chemin de l'emplacement de destination et les identifiants d'authentification.
9. L'outil peut parfois nécessiter plus de temps que prévu pour réaliser sa tâche ou peut ne pas répondre. Pour éviter les crashes dans de telles situations, dans la section **Configuration de la sécurité**, choisissez après combien d'heures Security Server doit terminer automatiquement le processus.
10. Cliquez sur **Enregistrer**.

Vous pourrez voir le statut de la tâche sur la page **Tâches**. Pour obtenir plus d'informations, vous pouvez également consulter le rapport **État de l'injection HVI tiers**.

6.3.6. Créer des rapports rapides

Vous pouvez choisir de créer des rapports instantanés sur les machines virtuelles administrées à partir de la page **Réseau** :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Toutes les machines virtuelles du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Filtrez le contenu du groupe sélectionné uniquement par machines virtuelles administrées.
5. Cochez les cases correspondant aux machines virtuelles que vous souhaitez inclure dans le rapport.

6. Cliquez sur le bouton  **Rapport** en haut du tableau et sélectionnez le type de rapport dans le menu. Pour plus d'informations, reportez-vous à « [Rapports Ordinateur et Machine virtuelle](#) » (p. 428).
7. Configurer les options de rapports. Pour plus d'informations, reportez-vous à « [Création de rapports](#) » (p. 448)
8. Cliquez sur **Générer**. Le rapport s'affiche immédiatement. Le temps nécessaire à la création des rapports peut varier en fonction du nombre de machines virtuelles sélectionnées.

6.3.7. Affecter des politiques

Vous pouvez gérer les paramètres de sécurité sur les machines virtuelles à l'aide de [politiques](#).

La page **Réseau** vous permet d'afficher, de modifier et d'affecter des politiques à chaque machine virtuelle ou groupe de machines virtuelles.



Note


Les paramètres de sécurité sont disponibles uniquement pour les machines virtuelles administrées. Pour afficher et gérer les paramètres de sécurité plus facilement, vous pouvez [filtrer](#) l'inventaire du réseau uniquement par machines virtuelles gérées.

Pour afficher les paramètres de sécurité affectés à une machine virtuelle spécifique :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Toutes les machines virtuelles du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Cliquez sur le nom de la machine virtuelle qui vous intéresse. Une fenêtre d'informations s'affichera.
5. Dans l'onglet **Général**, section **Politique**, cliquez sur le nom de la politique en cours pour afficher ses paramètres.
6. Vous pouvez modifier les paramètres de sécurité en fonction de vos besoins, à condition que le propriétaire de la politique ait autorisé d'autres utilisateurs à modifier cette politique. Veuillez noter que toute modification que vous effectuerez affectera toutes les machines virtuelles auxquelles on a affecté la même politique.

Pour plus d'informations sur les paramètres de la politique de la machine virtuelle, reportez-vous à « [Politiques de sécurité](#) » (p. 223)


Pour affecter une politique à une machine virtuelle ou à un groupe de machines virtuelles :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Machines virtuelles** dans le [sélecteur d'affichage](#).
3. Sélectionnez l'emplacement souhaité dans le panneau de gauche. Toutes les machines virtuelles du conteneur sélectionné apparaissent dans le tableau du panneau de droite.
4. Cochez la case de l'entité de votre choix. Vous pouvez sélectionner un ou plusieurs objets du même type du même niveau uniquement.
5. Cliquez sur le bouton  **Affecter une politique** en haut du tableau.
6. Effectuez la configuration nécessaire dans la fenêtre **Attribution de la politique**.

Pour plus d'informations, reportez-vous à « [Affecter des politiques](#) » (p. 227).



Avertissement

Pour les stratégies avec [HVI_LONG] activé, les machines cibles peuvent nécessiter un redémarrage juste après l'affectation des stratégies. Les machines dans cet état sont marquées sur la page **Réseau** avec l'icône  **En attente de redémarrage**.

6.3.8. Utiliser Recovery Manager for Encrypted Volumes (système de récupération pour volumes chiffrés)

Lorsque les utilisateurs d'un endpoint oublie les mots de passe de chiffrement et ne peuvent plus accéder aux volumes chiffrés sur leur machine, vous pouvez les aider à retrouver leurs clés de récupération depuis la page **Réseau**.

Pour obtenir une clé de récupération :

1. Allez sur la page **Réseau**.
2. Cliquez sur le bouton  **Gestionnaire de récupération** dans la barre d'outils action du panneau gauche. Une nouvelle fenêtre apparaît.
3. Dans la section **Identifiant** de la fenêtre, saisissez les données suivantes :
 - a. L'ID de la clé de récupération du volume chiffré. L'ID de la clé de récupération est une chaîne de caractère composée de chiffres et de lettres disponibles sur l'endpoint, sur l'écran de récupération de BitLocker.

Sur Windows, l'ID de la clé de récupération est une chaîne de caractère composée de chiffres et de lettres disponibles sur l'endpoint, sur l'écran de récupération de BitLocker.

Autrement, vous pouvez utiliser l'option **Récupération** dans l'onglet **Protection** des [détails sur la machine virtuelle](#) pour remplir automatiquement l'ID de la clé de récupération, aussi bien pour les endpoints Windows que macOS.

- b. Le mot de passe de votre compte GravityZone.
4. Cliquez sur **Dévoiler**. La fenêtre s'agrandira.

Dans la fenêtre **Informations sur les volumes**, les données suivantes vous seront présentées :

- a. Nom du volume
 - b. Type de volume (amorçage ou non-amorçage).
 - c. Nom de l'endpoint, tel qu'indiqué dans l'inventaire du réseau.
 - d. Clé de récupération. Sur Windows, la clé de récupération est un mot de passe généré automatiquement lors du chiffrement du volume. Sur Mac, la clé de récupération correspond au mot de passe du compte de l'utilisateur.
5. Envoyez la clé de récupération à l'utilisateur de l'endpoint.

Pour de plus amples informations relatives au chiffrement et déchiffrement de volumes avec GravityZone, veuillez vous référer à « [Chiffrement de disque](#) » (p. 392).


6.3.9. Libérer les sièges de licence

Dans les inventaires Active Directory, vCenter Server (sans vShield, NSX ou HVI) et Xen Server, vous pouvez facilement libérer les sièges de licence utilisés par les machines virtuelles où l'agent de sécurité a été enlevé sans faire appel au désinstalleur.

Après cela, les machines cibles deviennent non gérées dans l'inventaire de réseau.

Pour libérer un siège de licence :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Ordinateurs et machines virtuelles** ou **machines virtuelles** du [sélecteur de vues](#).
3. Sélectionnez le groupe de votre choix dans le panneau de gauche. Toutes les machines virtuelles seront affichées dans le tableau latéral de droite.

4. Sélectionnez la machine virtuelle dont vous souhaitez supprimer la licence.
5. Cliquez sur le bouton  **Supprimer licence** en haut du tableau.
6. Cliquez sur **Oui** dans la fenêtre de confirmation pour continuer.

6.4. Appareils mobiles

Pour gérer la sécurité des appareils mobiles utilisés dans votre entreprise, vous devez d'abord les lier à des utilisateurs spécifiques de Control Center puis installer et activer l'application GravityZone Mobile Client sur chacun d'entre eux.

Les appareils mobiles peuvent appartenir à l'entreprise ou être personnels. Vous pouvez installer et activer GravityZone Mobile Client sur tous les appareils mobiles avant de les remettre à leurs utilisateurs. Les utilisateurs peuvent également installer et activer GravityZone Mobile Client par eux-mêmes, en suivant les instructions reçues par e-mail. Pour plus d'informations, consultez le Guide d'Installation de GravityZone.

Pour afficher les appareils mobiles des utilisateurs sous votre compte, allez dans la section **Réseau** et sélectionnez **Appareils Mobiles** dans le [sélecteur de service](#). La page **Réseau** affiche les groupes d'utilisateurs disponibles dans le panneau de gauche et les utilisateurs et appareils correspondants dans le panneau de droite.

Si l'intégration à Active Directory a été configurée, vous pouvez ajouter des appareils mobiles aux utilisateurs Active Directory existants. Vous pouvez également créer des utilisateurs sous **Groupes personnalisés** et leur ajouter des appareils mobiles.

Vous pouvez faire passer l'affichage du panneau de droite sur **Utilisateurs** ou **Appareils** à l'aide de l'onglet **Affichage** du menu **Filtres** situé en-haut du tableau. L'affichage **Utilisateurs** vous permet de gérer les utilisateurs du Control Center, comme ajouter des utilisateurs et des appareils mobiles, vérifier le nombre d'appareils pour chaque utilisateur etc.) Utilisez l'affichage **Appareils** pour gérer et consulter facilement les informations de tous les appareils mobiles du Control Center.

Vous pouvez gérer les utilisateurs et les appareils mobiles du Control Center en effectuant les actions suivantes :

- [Ajouter des utilisateurs personnalisés](#)
- [Ajouter des appareils mobiles aux utilisateurs](#)
- [Organiser les utilisateurs personnalisés dans des groupes](#)
- [Filtrer et rechercher des utilisateurs et des appareils](#)
- [Consulter l'état de l'utilisateur ou de l'appareil et des informations détaillées](#)

- Exécuter des tâches sur les appareils mobiles
- Créer des rapports d'appareils mobiles rapides
- Vérifier et modifier les paramètres de sécurité d'un appareil
- Synchroniser l'inventaire de Control Center avec Active Directory
- Supprimer des utilisateurs et des appareils mobiles


6.4.1. Ajouter des utilisateurs personnalisés

Si l'intégration à Active Directory a été configurée, vous pouvez ajouter des appareils mobiles aux utilisateurs Active Directory existants.

Sans Active Directory, vous devez commencer par créer des utilisateurs personnalisés afin d'avoir un moyen d'identifier les propriétaires d'appareils mobiles.

Il y a deux façons de créer des utilisateurs personnalisés. Vous pouvez soit les ajouter une par une soit importer un fichier CSV.

Pour ajouter un utilisateur personnalisé :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de service](#).
3. Cliquez sur le menu **Filtres** en haut du tableau et rendez-vous dans l'onglet **Afficher** tab. Veillez à ce que l'option **Utilisateur(s)** soit sélectionnée.
4. Dans le panneau de gauche, sélectionnez **Groupes personnalisés**.
5. Cliquez sur le bouton  **Ajouter un utilisateur** en haut du tableau. Une fenêtre de configuration s'affichera.
6. Spécifiez les informations requises de l'utilisateur :
 - Un nom d'utilisateur explicite (par exemple, le nom complet de l'utilisateur)
 - L'adresse e-mail de l'utilisateur



Important

- Veillez à indiquer une adresse e-mail valide. L'utilisateur recevra les instructions d'installation par e-mail lorsque vous ajouterez un appareil.
- Chaque adresse e-mail peut être associée uniquement à un utilisateur.

7. Cliquez sur **OK**.

Pour importer des utilisateurs appareil mobile :

1. Allez sur la page **Réseau**.

2. Sélectionnez **Appareils mobiles** dans le [sélecteur de service](#).
3. Cliquez sur le menu **Filtres** en haut du tableau et rendez-vous dans l'onglet **Afficher** tab. Veillez à ce que l'option **Utilisateur(s)** soit sélectionnée.
4. Dans le panneau de gauche, sélectionnez **Groupes personnalisés**.
5. Cliquez sur **Importer utilisateurs**. Une nouvelle fenêtre s'ouvre.
6. Sélectionnez le fichier CSV et cliquez sur **Importer**. La fenêtre se ferme et le tableau est rempli d'utilisateurs importés.

**Note**

Si une erreur survient, un message s'affiche et le tableau n'est alors rempli que par les utilisateurs valides. Les utilisateurs existants sont passés.

Vous pouvez ensuite [créer des groupes d'utilisateurs](#) sous **Groupes personnalisés**. La politique et les tâches affectées à un utilisateur s'appliqueront à tous les appareils appartenant à cet utilisateur.

6.4.2. Ajouter des appareils mobiles aux utilisateurs

Un utilisateur peut avoir un nombre illimité d'appareils mobiles. Vous pouvez ajouter des appareils à un ou plusieurs utilisateurs, mais seulement un appareil par utilisateur à la fois.

Ajouter un appareil à un seul utilisateur

Pour ajouter un appareil à un utilisateur spécifique :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Localisez l'utilisateur dans le groupe **Active Directory** ou dans **Groupes personnalisés** et cochez la case correspondante dans le panneau de droite.

**Note**

Le menu [Filtres](#) doit être configuré sur **Utilisateurs** dans l'onglet **Afficher**.

4. Cliquez sur le bouton  **Ajouter un appareil** en haut du tableau. Une fenêtre de configuration s'affichera.

Ajouter un appareil

Nom de l'appareil:

Configurer automatiquement le nom

Propriété:

Afficher les identifiants d'activation

Ajouter un appareil mobile à un utilisateur.

5. Configurez les détails de l'appareil mobile :
 - a. Indiquez un nom explicite pour l'appareil.
 - b. Utilisez l'option **Configurer automatiquement le nom** si vous souhaitez que le nom de l'appareil soit généré automatiquement. Lorsqu'il est ajouté, l'appareil a un nom générique. Lorsque l'appareil est activé, il est automatiquement renommé avec les informations correspondantes du fabricant et du modèle.
 - c. Indiquez si l'appareil appartient à l'entreprise ou est personnel. Vous pouvez filtrer les appareils mobiles en fonction de leurs propriétaires et les gérer selon vos besoins.
 - d. Sélectionnez l'option **Afficher les identifiants d'activation** si vous pensez installer GravityZone Mobile Client sur l'appareil de l'utilisateur.
6. Cliquez sur **OK** pour ajouter l'appareil. L'utilisateur reçoit immédiatement un e-mail comportant les instructions d'installation et les détails de l'activation à configurer sur l'appareil. Les détails de l'activation comprennent le jeton d'activation et l'adresse du serveur de communication (ainsi que le code QR correspondant).
7. Si vous avez sélectionné l'option **Afficher les identifiants d'activation**, la fenêtre **Détails de l'activation** apparaît, indiquant le jeton d'activation unique, l'adresse du serveur de communication et le code QR du nouvel appareil.

Détails de l'activation

Jeton d'activation: 4128574892

URL du serveur: 10.10.17.80:8443

Code QR

Fermer

Détails de l'activation des appareils mobiles

Après l'installation de GravityZone Mobile Client, lorsqu'on vous invite à activer l'appareil, indiquez le jeton d'activation et l'adresse du serveur de communication ou scannez le code QR.

Ajouter des appareils à plusieurs utilisateurs


Pour ajouter des appareils mobiles à une sélection d'utilisateurs et de groupes :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Localisez les utilisateurs ou les groupes dans les dossiers **Active Directory** ou dans **Groupes personnalisés** et cochez les cases correspondantes dans le panneau de droite.



Note

Le menu [Filtres](#) doit être configuré sur **Utilisateurs** dans l'onglet **Afficher**.

4. Cliquez sur le bouton  **Ajouter un appareil** à droite du tableau. Dans ce cas, vous devez seulement définir la propriété des appareils dans la fenêtre de configuration.

Si aucune adresse e-mail n'est spécifiée pour certains utilisateurs, vous en serez informé immédiatement par un message. La liste des utilisateurs correspondants sera disponible dans la zone **Notification** de Control Center.

Les appareils mobiles créés par une sélection multiple recevront par défaut un nom générique dans Control Center. Lorsqu'un appareil est activé, il est automatiquement renommé avec les informations correspondantes du fabricant et du modèle.

5. Cliquez sur **OK** pour ajouter les appareils. Les utilisateurs reçoivent immédiatement un e-mail comportant les instructions d'installation et les détails de l'activation à configurer sur les appareils. Les détails de l'activation comprennent le jeton d'activation et l'adresse du serveur de communication (ainsi que le code QR correspondant).

Vous pouvez voir le nombre d'appareils affectés à chaque utilisateur dans le panneau de droite sous la colonne **Appareils**.

6.4.3. Organiser les utilisateurs personnalisés dans des groupes

Vous pouvez voir les groupes d'utilisateurs disponibles dans le panneau de gauche de la page **Réseau**.

Les utilisateurs d'Active Directory sont regroupés sous **Active Directory**. Vous ne pouvez pas modifier les groupes Active Directory. Vous pouvez uniquement afficher et ajouter des appareils aux utilisateurs correspondants.

Vous pouvez placer tous les utilisateurs non Active Directory sous **Groupes personnalisés**, où vous pouvez créer et organiser des groupes comme vous le souhaitez. L'un des principaux avantages est que vous pouvez utiliser des politiques de groupes pour répondre à différents besoins en sécurité.

Groupes personnalisés vous permet de [créer](#), [supprimer](#), [renommer](#) et [déplacer](#) des groupes d'utilisateurs dans une structure arborescente personnalisée.



Important

Veuillez noter ceci :

- Un groupe peut contenir à la fois des utilisateurs et d'autres groupes.
- Lors de la sélection d'un groupe dans le panneau de gauche, vous pouvez afficher tous les utilisateurs à l'exception de ceux placés dans ses sous-groupes. Pour afficher tous les utilisateurs contenus dans le groupe et ses sous-groupes, cliquez

sur le menu **Filtres** situé en-haut du tableau et sélectionnez **Tous les éléments de manière récurrente** dans la section **Profondeur**.

Création de groupes

Pour créer un groupe personnalisé :

1. Sélectionnez **Groupes personnalisés** dans le panneau de gauche.
2. Cliquez sur le bouton **+ Ajouter un groupe** en haut du panneau de gauche.
3. Indiquez un nom explicite pour le groupe et cliquez sur **OK**. Le nouveau groupe apparaît sous **Groupes personnalisés**.

Renommer des groupes

Pour renommer un groupe personnalisé :

1. Sélectionnez le groupe dans le panneau de gauche.
2. Cliquez sur le bouton **✎ Éditer le groupe** en haut du panneau de gauche.
3. Saisissez le nouveau nom dans le champ correspondant.
4. Cliquez sur **OK** pour confirmer.

Déplacer des groupes et des utilisateurs

Vous pouvez déplacer des groupes et des utilisateurs partout à l'intérieur de la hiérarchie **Groupes personnalisés**. Pour déplacer un groupe ou un utilisateur, glissez-déposez-le de l'emplacement actuel vers le nouvel emplacement.



Note

L'entité qui est déplacée héritera des paramètres de la politique du nouveau groupe parent, à moins que l'héritage de la politique ait été désactivé et qu'une politique différente lui ait été attribuée.

Supprimer des groupes

Un groupe ne peut pas être supprimé s'il contient au moins un utilisateur. Déplacez tous les utilisateurs du groupe que vous souhaitez supprimer vers un autre groupe. Si le groupe comprend des sous-groupes, vous pouvez choisir de déplacer tous les sous-groupes plutôt que des utilisateurs individuels.

Pour supprimer un groupe :




1. Sélectionnez le groupe vide.
2. Cliquez sur le bouton  **Supprimer un groupe** en haut du panneau de gauche. Vous devrez confirmer votre action en cliquant sur **Oui**.

6.4.4. Consulter l'état des appareils mobiles

Chaque appareil mobile est représenté sur la page du réseau par une icône spécifique à son type et à son état.

Consultez « [États et types d'objets du réseau](#) » (p. 527) pour une liste des types d'icônes et des états existants.

Les appareils mobiles peuvent avoir les états de'administration suivants :

-  **Administré (Actif)**, lorsque toutes les conditions suivantes sont remplies :
 - Le GravityZone Mobile Client est activé sur l'appareil.
 - Le GravityZone Mobile Client a synchronisé avec le Control Center au cours des dernières 48 heures.
-  **Administré (Inactif)**, lorsque toutes les conditions suivantes sont remplies :
 - Le GravityZone Mobile Client est activé sur l'appareil.
 - Le GravityZone Mobile Client n'a pas synchronisé avec le Control Center depuis plus de 48 heures.
-  **Non administré**, dans les situations suivantes :
 - GravityZone Mobile Client n'a pas encore été installé et activé sur l'appareil mobile.
 - GravityZone Mobile Client a été désinstallé de l'appareil mobile (pour les appareils Android uniquement).
 - Le profil MDM Bitdefender a été supprimé de l'appareil (pour les appareils iOS uniquement).

Pour consulter l'état d'administration des appareils :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Dans le panneau de gauche, sélectionnez le groupe qui vous intéresse.
4. Cliquez sur le menu **Filtres** situé au-dessus du tableau et effectuez les paramètres suivants :

- a. Allez dans l'onglet **Afficher** et sélectionnez **Appareils**.
- b. Allez dans l'onglet **Sécurité** et sélectionnez l'état qui vous intéresse sous la section **Management**. Vous pouvez sélectionner un ou plusieurs critères de filtrage simultanément.
- c. Vous pouvez également choisir d'afficher tous les appareils de manière réursive en sélectionnant l'option correspondante dans l'onglet **Profondeur**.
- d. Cliquez sur **Enregistrer**.

Tous les appareils mobiles correspondant aux critères sélectionnés apparaissent dans le tableau.

Vous pouvez également générer un rapport sur l'état de la synchronisation des appareils sur un ou plusieurs appareils mobiles. Ce rapport fournit des informations détaillées concernant l'état de synchronisation de chaque appareil sélectionné, y compris la date et l'heure de la dernière synchronisation. Pour plus d'informations, reportez-vous à « [Créer des rapports rapides](#) » (p. 191)

6.4.5. Appareils Conformés et Non conformes

Une fois que l'application GravityZone Mobile Client a été activée sur un appareil mobile, le Control Center vérifie que l'appareil correspondant remplit toutes les exigences de conformité. Les appareils mobiles peuvent avoir les états de sécurité suivants :

- **Sans problèmes de sécurité**, quand toutes les exigences de conformité sont remplies.
- **Avec des problèmes de sécurité**, quand au moins une des exigences de conformité n'est pas remplie. Lorsqu'un appareil est déclaré non conforme, l'utilisateur est invité à corriger le problème de non-conformité. L'utilisateur doit effectuer les modifications requises au cours d'une période donnée, sinon l'action pour les appareils non conformes définie dans la politique sera appliquée.

Pour plus d'informations concernant les actions et les critères de non-conformité, reportez-vous à « [Conformité](#) » (p. 407).

Pour consulter l'état de conformité des appareils :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Dans le panneau de gauche, sélectionnez le groupe qui vous intéresse.

4. Cliquez sur le menu **Filtres** situé au-dessus du tableau et effectuez les paramètres suivants :
 - a. Allez dans l'onglet **Afficher** et sélectionnez **Appareils**.
 - b. Allez dans l'onglet **Sécurité** et sélectionnez l'état qui vous intéresse sous la section **Problèmes de sécurité**. Vous pouvez sélectionner un ou plusieurs critères de filtrage simultanément.
 - c. Vous pouvez également choisir d'afficher tous les appareils de manière réursive en sélectionnant l'option correspondante dans l'onglet **Profondeur**.
 - d. Cliquez sur **Enregistrer**.
Tous les appareils mobiles correspondant aux critères sélectionnés apparaissent dans le tableau.
5. Vous pouvez afficher le ratio de conformité des appareils pour chaque utilisateur :
 - a. Cliquez sur le menu **Filtres** situé au-dessus du tableau et sélectionnez **Utilisateurs** dans la catégorie **Afficher**. Tous les utilisateurs du groupe sélectionné apparaissent dans le tableau.
 - b. Consultez la colonne **Conformité** pour savoir combien d'appareils sont conformes parmi le nombre total d'appareils de l'utilisateur.

Vous pouvez également générer un rapport sur la conformité des appareils sur un ou plusieurs appareils mobiles. Ce rapport fournit des informations détaillées concernant l'état de conformité de tous les appareils sélectionnés, y compris le motif de la non-conformité. Pour plus d'informations, reportez-vous à « [Créer des rapports rapides](#) » (p. 191)

6.4.6. Consulter des informations détaillées sur les utilisateurs et les appareils mobiles

Vous pouvez obtenir des informations détaillées sur tous les utilisateurs et appareils mobiles à partir de la page **Réseau**.

Consulter des informations sur un utilisateur

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Sélectionnez le groupe souhaité dans le panneau de gauche.

4. Cliquez sur le menu des **Filtres** situé au-dessus du tableau, allez dans l'onglet **Afficher** et sélectionnez **Utilisateur(s)**. Pour afficher tous les utilisateurs de manière récurrente, allez dans l'onglet **Profondeur** et sélectionnez **Tous les éléments de manière récurrente**. Cliquez sur **Enregistrer**. Tous les utilisateurs du groupe sélectionné apparaissent dans le tableau.
5. Consultez les informations affichées dans les colonnes du tableau pour tous les utilisateurs :
 - **Nom**. Le nom d'utilisateur.
 - **appareils**. Le nombre d'appareils liés à l'utilisateur. Cliquez sur le nombre pour passer à l'affichage **Appareils** et afficher uniquement les appareils correspondants.
 - **Conformité**. Le rapport entre les appareils conformes et l'ensemble des appareils liés à l'utilisateur. Cliquez sur la première valeur pour passer à l'affichage **Appareils** et afficher uniquement les appareils conformes.
6. Cliquez sur le nom de l'utilisateur qui vous intéresse. Une fenêtre de configuration apparaît où vous pouvez voir et modifier le nom et l'adresse e-mail de l'utilisateur.

Consulter des informations sur un appareil

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Sélectionnez le groupe souhaité dans le panneau de gauche.
4. Cliquez sur le menu des **Filtres** situé au-dessus du tableau, allez dans l'onglet **Afficher** et sélectionnez **Appareils**. Cliquez sur **Enregistrer**. Tous les appareils appartenant aux utilisateurs du groupe sélectionné apparaissent dans le tableau.
5. Consultez les informations affichées dans les colonnes du tableau pour tous les appareils :
 - **Nom**. Le nom de l'appareil.
 - **Utilisateur**. Le nom de l'utilisateur possédant l'appareil.
 - **OS**. Le système d'exploitation de l'appareil.
6. Cliquez sur le nom d'un appareil pour obtenir plus d'informations. La fenêtre **Détails des appareils mobiles** apparaît ; elle vous permet de consulter les informations suivantes regroupées sous les onglets **Présentation** et **Détails** :

- **Général.**
 - **Nom.** Le nom spécifié lors de l'ajout de l'appareil au Control Center.
 - **Utilisateur.** Le nom du propriétaire de l'appareil.
 - **Groupe.** Le groupe parent de l'appareil mobile dans l'inventaire du réseau.
 - **OS.** Le système d'exploitation de l'appareil mobile.
 - **Propriété.** Le type d'appareil portable dont il s'agit (appartenant à l'entreprise ou personnel).
- **Sécurité.**
 - **Versión du client.** La version de l'application GravityZone Mobile Client installée sur l'appareil, détectée uniquement après l'inscription.
 - **La politique.** La politique affectée actuellement à l'appareil mobile. Cliquez sur le nom de la politique pour aller sur la page **Politique** correspondante et consulter les paramètres de sécurité.



Important

Par défaut, seul l'utilisateur qui a créé la politique peut la modifier. Pour changer cela, le propriétaire de la politique doit cocher l'option **Autoriser d'autres utilisateurs à modifier cette politique** à partir de la page **Détails** de la politique. Les modifications apportées à une politique affecteront tous les appareils auxquels cette politique a été affectée. Pour plus d'informations, reportez-vous à « [Affecter des politiques](#) » (p. 192).

- **État de la licence.** Afficher les informations de licence de l'appareil correspondant.
- **État de conformité.** L'état de conformité est disponible pour les appareils mobiles administrés. Un appareil mobile peut être Conforme ou Non conforme.



Note

Pour les appareils mobiles non conformes, une icône de notification **!** s'affiche. Consultez l'info-bulle de l'icône pour connaître la raison de la non-conformité.

Pour plus d'informations sur la conformité des appareils mobiles reportez-vous à « [Conformité](#) » (p. 407).

- **Activité des logiciels malveillants (24 dernières heures).** Un aperçu rapide du nombre de détections de malwares pour l'appareil correspondant pour la journée en cours.
- **Mot de passe de verrouillage.** Un mot de passe unique généré automatiquement lors de l'inscription d'un appareil, utilisé pour [verrouiller l'appareil à distance](#) (pour les appareils Android uniquement).
- **Statut du cryptage.** Certains appareils Android 3.0 ou plus récents supportent la fonctionnalité de cryptage de l'appareil. Consultez le statut du cryptage sur la page des détails de l'appareil afin de découvrir si l'appareil correspondant supporte la fonctionnalité de cryptage. Si le cryptage est requis par une politique sur l'appareil, vous pouvez également afficher l'état d'activation du cryptage.

- **Détails de l'activation**

- **Code d'activation.** Le jeton d'activation unique affecté à l'appareil.
- Adresse du serveur de communication.
- **Code QR.** Le code QR unique contenant le jeton d'activation et l'adresse du serveur de communication.

- **Matériel.** Vous pouvez consulter ici les informations matérielles des appareils, disponibles uniquement pour les appareils administrés (activés). Les informations matérielles sont vérifiées toutes les 12 heures et actualisées en cas de changement.



Important

À partir du système d'exploitation Android 10, GravityZone Mobile Client n'a pas accès au numéro de série, aux numéros IMEI et IMSI et à l'adresse MAC de l'appareil. Cette restriction donne lieu aux situations suivantes :

- Si un appareil mobile sur lequel GravityZone Mobile Client est déjà installé passe à Android 10 alors qu'il utilisait une version antérieure, la Control Center affichera toutes ces informations. Avant la mise à jour, l'appareil doit utiliser la dernière version de GravityZone Mobile Client.
- Si GravityZone Mobile Client est installé sur un appareil Android 10, Control Center n'affichera pas les bonnes informations concernant cet appareil en raison des limitations imposées par le système d'exploitation.

- **Réseau.** Vous pouvez consulter ici les informations de connectivité réseau, disponibles uniquement pour les appareils administrés (activés).

6.4.7. Trier, filtrer et rechercher des appareils mobiles

Le tableau d'inventaire des appareils mobiles peut comporter plusieurs pages, en fonction du nombre d'utilisateurs ou d'appareils (seules 10 entrées sont affichées par page par défaut). Pour parcourir les pages, utilisez les boutons de navigation en bas du tableau. Pour modifier le nombre d'entrées affichées sur une page, sélectionnez une option dans le menu à côté des boutons de déplacement.

S'il y a trop d'entrées, vous pouvez utiliser les options de filtrage pour afficher uniquement les entités qui vous intéressent. Vous pouvez, par exemple, rechercher un appareil mobile ou choisir d'afficher uniquement les appareils administrés.

Trier l'inventaire des appareils mobiles

Pour trier les données en fonction d'une colonne spécifique, cliquez sur les en-têtes de la colonne. Par exemple, si vous souhaitez classer les appareils par nom, cliquez sur l'en-tête **Nom**. Si vous cliquez de nouveau sur l'en-tête, les appareils s'afficheront dans l'ordre inverse.

Filtrer l'inventaire des appareils mobiles

1. Sélectionnez le groupe souhaité dans le panneau de gauche.
2. Cliquez sur le menu **Filtres** en haut de la zone de panneaux du réseau.
3. Utilisez les critères de filtrage comme suit :
 - **Type**. Sélectionnez le type d'entités que vous souhaitez afficher (Utilisateurs/Appareils et Dossiers).

Type	Sécurité	Politique	Afficher	Propriété	Profondeur
Filtrer par					
<input type="checkbox"/> Utilisateurs / Périphériques					
<input type="checkbox"/> Dossiers					
Afficher: appareils					
Profondeur: récursivement					
Enregistrer		Annuler		Réinitialiser	

Appareils mobiles - Filtrer par type

- **Sécurité.** Choisissez d'afficher les ordinateurs par état d'administration et de sécurité.

Type	Sécurité	Politique	Afficher	Propriété	Profondeur
Management <input type="checkbox"/> Administré (Actif) <input type="checkbox"/> Administré (Inactif) <input type="checkbox"/> Non administré		Problèmes de sécurité <input type="checkbox"/> Avec des problèmes de sécurité <input type="checkbox"/> Sans problèmes de sécurité			
Type: utilisateurs/appareils Afficher: appareils Profondeur: récursivement					
Enregistrer		Annuler		Réinitialiser	

Appareils mobiles - Filtrer par sécurité

- **La politique.** Sélectionnez le modèle de politique à partir duquel vous souhaitez filtrer les appareils mobiles, le type d'attribution de la politique (Directe ou Héritée), ainsi que l'état d'attribution de celle-ci (Actif, Affecté ou En attente).

Type	Sécurité	Politique	Afficher	Propriété	Profondeur
Modèle: <input type="text"/>					
Type: <input type="checkbox"/> Direct <input type="checkbox"/> Hérité					
État: <input type="checkbox"/> Actif <input type="checkbox"/> Appliqué <input type="checkbox"/> En attente					
Afficher: utilisateurs Profondeur: dans les dossiers sélectionnés					
Enregistrer		Annuler		Réinitialiser	

Appareils mobiles - Filtrer par politique

- **Afficher.** Sélectionnez **Utilisateurs** pour afficher uniquement les utilisateurs du groupe sélectionné. Sélectionnez **Appareils** pour afficher uniquement les appareils du groupe sélectionné.

Type	Sécurité	Politique	Afficher	Propriété	Profondeur
Afficher					
<input type="radio"/> Utilisateur(s)					
<input checked="" type="radio"/> appareils					
Afficher: appareils					
Profondeur: récursivement					
Enregistrer		Annuler		Réinitialiser	

Appareils mobiles - Filtrer par affichage

- **Propriété.** Vous pouvez filtrer les appareils mobiles par propriété, en choisissant d'afficher les appareils appartenant à l'**Entreprise** ou **Personnels**. L'attribut de propriété est défini dans les informations détaillées sur les appareils mobiles.

Type	Sécurité	Politique	Afficher	Propriété	Profondeur
Afficher					
<input type="checkbox"/> Enterprise					
<input type="checkbox"/> Personnel					
Type: utilisateurs/appareils					
Afficher: appareils					
Profondeur: récursivement					
Enregistrer		Annuler		Réinitialiser	

Appareils mobiles - Filtrer par propriété

- **Profondeur.** Quand on gère un réseau à structure arborescente, les utilisateurs ou appareils mobiles placés dans des sous-groupes ne s'affichent pas lorsqu'on sélectionne le groupe racine. Sélectionnez **Tous les éléments de manière récurrente** pour afficher toutes les entités se trouvant dans le groupe actuel et dans ses sous-groupes.

Type Sécurité Politique Afficher Propriété **Profondeur**

Filtrer par

Éléments parmi les dossiers sélectionnés

Tous les éléments de manière récurrente

Type: utilisateurs/appareils
Afficher: appareils
Profondeur: récursivement

Enregistrer Annuler Réinitialiser

Appareils mobiles - Filtrer par profondeur

4. Cliquez sur **Enregistrer** pour filtrer l'inventaire des appareils mobiles en fonction des critères sélectionnés.

Le filtre demeure actif sur la page **Réseau** jusqu'à ce que vous vous déconnectiez ou réinitialisiez le filtre.

Rechercher des appareils mobiles

Le tableau du panneau de droite fournit des informations spécifiques sur les utilisateurs et les appareils mobiles. Vous pouvez utiliser les catégories disponibles sur chaque colonne pour filtrer le contenu du tableau.

1. Sélectionnez le groupe souhaité dans le panneau de gauche.
2. Passez à l'affichage de votre choix (Utilisateurs ou Appareils mobiles) en utilisant le menu **Filtres** en haut de la zone de panneaux du réseau.
3. Recherchez les entités que vous souhaitez utiliser à l'aide des champs de recherche sous chaque en-tête de colonne du panneau de droite :
 - Indiquez le terme recherché de votre choix dans le champ correspondant.
Par exemple, passez à l'affichage **Appareils** et indiquez le nom de l'utilisateur que vous recherchez dans le champ **Utilisateur**. Seuls les appareils mobiles correspondants apparaîtront dans le tableau.
 - Sélectionnez l'attribut à partir duquel vous souhaitez effectuer la recherche dans la liste déroulante correspondante.
Par exemple, passez à l'affichage **Appareils**, cliquez sur la liste **OS** et sélectionnez **Android** pour afficher uniquement les appareils mobiles Android.

**Note**

Pour effacer le terme recherché et afficher toutes les entités, placez le curseur de la souris sur la case correspondante et cliquez sur l'icône

6.4.8. Exécuter des tâches sur les appareils mobiles

La page **Réseau** vous permet d'exécuter à distance plusieurs tâches d'administration sur les appareils mobiles. Voici ce que vous pouvez faire :

- « Verrouiller » (p. 187)
- « Supprimer » (p. 188)
- « Analyse » (p. 189)
- « Localiser » (p. 190)

	appareils	Conformité
Supprimer	1	1/1
Analyse	2	2/2

Tâches des appareils mobiles

Pour exécuter des tâches à distance sur des appareils mobiles, certains prérequis doivent être remplis. Pour plus d'informations, référez-vous au chapitre Configuration requise pour l'installation du Guide d'Installation de GravityZone.

Vous pouvez choisir de créer des tâches individuellement pour chaque appareil mobile, pour chaque utilisateur ou pour des groupes d'utilisateurs. Vous pouvez par exemple vérifier à distance la présence de malwares sur les appareils mobiles d'un groupe d'utilisateurs. Vous pouvez également exécuter une tâche de localisation pour un appareil mobile spécifique.

L'inventaire du réseau peut contenir des appareils mobiles **actifs, inactifs ou non administrés**. Une fois créées, les tâches commenceront à s'exécuter immédiatement sur les appareils mobiles actifs. Pour les appareils inactifs, les tâches démarreront dès qu'ils seront de nouveau en ligne. Les tâches ne seront pas créées pour les

appareils mobiles non administrés. Un message indiquant que la tâche n'a pas pu être créée apparaîtra dans ce cas.

Vous pouvez afficher et gérer les tâches sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Verrouiller

La tâche Verrouiller verrouille immédiatement l'écran des appareils mobiles cibles. Le comportement de la tâche Verrouiller dépend du système d'exploitation :

- Pour les appareils Android (version 7.0 ou supérieure), la tâche Verrouiller force l'utilisation du mot de passe défini dans votre console GravityZone uniquement si aucune autre protection par verrouillage n'est configurée sur l'appareil. Le cas contraire, les options existantes de verrouillage de l'écran telles que Schéma, PIN, Mot de passe, Empreinte digitale ou Smart Lock seront utilisées pour protéger l'appareil.




Note

- Le mot de passe de verrouillage de l'écran généré par le Control Center apparaît dans la fenêtre Détails des appareils mobiles.
 - La tâche Déverrouiller n'est plus disponible pour les appareils Android (version 7.0 ou supérieure). Sinon, les utilisateurs peuvent déverrouiller leurs appareils manuellement. Toutefois, vous devez auparavant vérifier que tous ces appareils permettent de respecter les exigences de complexité du mode de passe de déverrouillage.
 - Pour des raisons de limitation technique, la tâche Verrouiller n'est pas disponible sur Android 11.
- Sous iOS, si l'appareil a un mot de passe de verrouillage de l'écran, il est demandé pour le déverrouillage.

Pour verrouiller des appareils mobiles à distance :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Sélectionnez le groupe souhaité dans le panneau de gauche.
4. Cliquez sur le menu **Filtres** en haut de la zone de panneaux du réseau et sélectionnez **Utilisateurs** dans la catégorie **Afficher**. Cliquez sur **Enregistrer**. Tous les utilisateurs du groupe sélectionné apparaissent dans le tableau.

5. Cochez les cases correspondant aux utilisateurs qui vous intéressent. Vous pouvez sélectionner un ou plusieurs utilisateurs simultanément.
6. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Verrouiller**.
7. Vous devrez confirmer votre action en cliquant sur **Oui**. Un message vous indiquera si la tâche a été ou non créée.
8. Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Supprimer

La tâche **Supprimer** restaure les paramètres d'usine des appareils mobiles cibles. Exécutez cette tâche pour effacer à distance toutes les informations sensibles et les applications stockées sur les appareils mobiles cibles.



Avertissement

Utilisez la tâche **Supprimer** avec précaution. Vérifiez à qui appartiennent les appareils cibles (si vous souhaitez éviter de supprimer des données d'appareils mobiles personnels) et assurez-vous que vous souhaitez réellement effacer les données des appareils sélectionnés. Une fois envoyée, la tâche **Supprimer** ne peut pas être annulée.



Note

Pour des raisons de limitation technique, la tâche Effacer n'est pas disponible sur Android 11.


Pour effacer à distance les données d'un appareil mobile :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Sélectionnez le groupe souhaité dans le panneau de gauche.
4. Cliquez sur le menu **Filtres** en haut de la zone de panneaux du réseau et sélectionnez **Appareils** dans la catégorie **Afficher**. Cliquez sur **Enregistrer**. Tous les appareils du groupe sélectionné apparaissent dans le tableau.



Note

Vous pouvez également sélectionner **Tous les éléments de manière récurrente** sous la section **Profondeur** pour afficher tous les appareils du groupe actuel.

5. Cochez la case correspondant à l'appareil dont vous souhaitez effacer les données.
6. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Supprimer**.
7. Vous devrez confirmer votre action en cliquant sur **Oui**. Un message vous indiquera si la tâche a été ou non créée.
8. Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Analyse

La tâche **Analyse** vous permet de rechercher la présence de malwares sur les appareils mobiles sélectionnés. L'utilisateur de l'appareil est informé des malwares détectés et invité à les supprimer. L'analyse est effectuée dans le cloud et l'appareil doit donc avoir un accès à Internet.

Note


L'analyse à distance ne fonctionne pas sur les appareils iOS (limitation de plateforme).


Pour analyser des appareils mobiles à distance :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Sélectionnez le groupe souhaité dans le panneau de gauche.
4. Cliquez sur le menu **Filtres** en haut de la zone de panneaux du réseau et sélectionnez **Appareils** dans la catégorie **Afficher**. Cliquez sur **Enregistrer**. Tous les appareils du groupe sélectionné apparaissent dans le tableau.

Note

Vous pouvez également sélectionner **Tous les éléments de manière récurrente** sous la section **Profondeur** pour afficher tous les appareils du groupe actuel. Pour afficher uniquement les appareils Android du groupe sélectionné, allez sur l'en-tête de colonne **OS** dans le panneau de droite et sélectionnez **Android** dans la liste correspondante.

5. Cochez les cases correspondant aux appareils que vous souhaitez analyser.
6. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Analyse**.

7. Vous devrez confirmer votre action en cliquant sur **Oui**. Un message vous indiquera si la tâche a été ou non créée.
8. Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Un rapport d'analyse est disponible lorsque la tâche se termine. Cliquez sur l'icône correspondante  dans la colonne **Rapports** pour générer un rapport instantané. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

Localiser

La tâche Localiser ouvre une carte indiquant l'emplacement des appareils sélectionnés. Vous pouvez localiser un ou plusieurs appareils simultanément.

Pour que la tâche Localiser fonctionne, les services de localisation doivent être activés sur les appareils mobiles.


Pour localiser les appareils mobiles :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Sélectionnez le groupe souhaité dans le panneau de gauche.
4. Cliquez sur le menu **Filtres** en haut de la zone de panneaux du réseau et sélectionnez **Appareils** dans la catégorie **Afficher**. Cliquez sur **Enregistrer**. Tous les appareils du groupe sélectionné apparaissent dans le tableau.



Note

Vous pouvez également sélectionner **Tous les éléments de manière réursive** sous la section **Profondeur** pour afficher de façon réursive tous les appareils du groupe actuel.

5. Cochez la case correspondant à l'appareil que vous souhaitez localiser.
6. Cliquez sur le bouton  **Tâches** en haut du tableau et sélectionnez **Localiser**.
7. La fenêtre **Localisation** s'ouvre et affiche les informations suivantes :
 - Une carte affichant l'emplacement des appareils mobiles sélectionnés. Si un appareil n'est pas synchronisé, la carte affichera son dernier emplacement connu.

- Un tableau affichant les informations détaillées des appareils sélectionnés (nom, utilisateur, dernières date et heure de synchronisation). Pour afficher l'emplacement sur la carte d'un appareil listé dans le tableau, cochez simplement sa case. La carte affichera immédiatement l'emplacement de l'appareil correspondant.
 - L'option **AutoActualisation** actualise automatiquement l'emplacement des appareils mobiles sélectionnés toutes les 10 secondes.
8. Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à « [Afficher et gérer des tâches](#) » (p. 210).

6.4.9. Créer des rapports rapides

Vous pouvez choisir de créer des rapports instantanés sur les appareils mobiles à partir de la page **Réseau** :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Sélectionnez le groupe de votre choix dans le panneau de gauche.
4. Cliquez sur le menu **Filtres** en haut de la zone de panneaux du réseau et sélectionnez **Appareils** dans la catégorie **Afficher**. Vous pouvez également sélectionner les options Administré dans l'onglet **Sécurité** pour filtrer le groupe sélectionné uniquement par appareils gérés. Cliquez sur **Enregistrer**. Tous les appareils correspondant aux critères de filtrage du groupe sélectionné apparaissent dans le tableau.
5. Cochez les cases correspondant aux appareils mobiles qui vous intéressent. Vous pouvez sélectionner un ou plusieurs appareils simultanément.
6. Cliquez sur le bouton **📄 Rapport** en haut du tableau et sélectionnez le type de rapport dans le menu. Pour plus d'informations, reportez-vous à « [Rapports Appareils Mobiles](#) » (p. 446)
7. Configurer les options de rapports. Pour plus d'informations, reportez-vous à « [Création de rapports](#) » (p. 448)
8. Cliquez sur **Générer**. Le rapport s'affiche immédiatement. Le temps nécessaire à la création des rapports peut varier en fonction du nombre d'appareils mobiles sélectionnés.

6.4.10. Affecter des politiques

Vous pouvez gérer les paramètres de sécurité sur les appareils mobiles à l'aide de [politiques](#).

La section **Réseau** vous permet d'afficher, de modifier et d'affecter des politiques aux appareils mobiles sous votre compte.

Vous pouvez affecter des politiques à des groupes, des utilisateurs ou certains appareils mobiles.



Note

Une politique attribuée à un utilisateur affecte tous les appareils qu'il possède. Pour plus d'informations, reportez-vous à « [Affecter des politiques locales](#) » (p. 227).


Pour afficher les paramètres de sécurité affectés à un appareil mobile :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Cliquez sur le menu **Filtres** en haut de la zone de panneaux du réseau et sélectionnez **Appareils** dans la catégorie **Afficher**. Cliquez sur **Enregistrer**. Tous les appareils appartenant aux utilisateurs du groupe sélectionné apparaissent dans le tableau.
4. Cliquez sur le nom de l'appareil mobile qui vous intéresse. Une [fenêtre détails](#) apparaîtra.
5. Dans la section **Sécurité** de la page **Présentation**, cliquez sur le nom de la politique affectée actuellement pour afficher ses paramètres.
6. Vous pouvez modifier les paramètres de sécurité selon vos besoins. Veuillez noter que toutes les modifications que vous apporterez s'appliqueront également à tous les autres appareils sur lesquels la politique est active.

Pour plus d'informations, reportez-vous à « [Politiques des appareils mobiles](#) » (p. 401)

Pour affecter une politique à un appareil mobile :


1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Dans le panneau de gauche, sélectionnez le groupe qui vous intéresse.

4. Cliquez sur le menu **Filtres** en haut de la zone de panneaux du réseau et sélectionnez **Appareils** dans la catégorie **Afficher**. Cliquez sur **Enregistrer**. Tous les appareils appartenant aux utilisateurs du groupe sélectionné apparaissent dans le tableau.
5. Dans le panneau de droite, cochez la case de l'appareil mobile qui vous intéresse.
6. Cliquez sur le bouton  **Affecter une politique** en haut du tableau.
7. Effectuez la configuration nécessaire dans la fenêtre **Attribution de la politique**. Pour plus d'informations, reportez-vous à « [Affecter des politiques locales](#) » (p. 227).

6.4.11. Synchronisation avec Active Directory

L'inventaire du réseau est automatiquement synchronisé avec Active Directory à la fréquence indiquée dans la section de configuration de Control Center. Pour plus d'informations, référez-vous au chapitre Installation et Configuration de GravityZone, dans le Guide d'Installation de GravityZone.

Pour synchroniser manuellement les utilisateurs affichés actuellement avec Active Directory :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Cliquez sur le bouton  **Synchroniser avec Active Directory** en haut du tableau.
4. Vous devrez confirmer votre action en cliquant sur **Oui**.



Note

Pour des réseaux Active Directory plus grands, la synchronisation peut prendre un peu plus de temps.

6.4.12. Supprimer des utilisateurs et des appareils mobiles

Lorsque l'inventaire du réseau contient des utilisateurs ou des appareils mobiles obsolètes, il est recommandé de les supprimer.

Supprimer des appareils mobiles de l'inventaire du réseau

Lorsque vous supprimez un appareil de Control Center :

- GravityZone Mobile Client est dissocié mais n'est pas supprimé de l'appareil.

- Pour les appareils iOS, le Profil MDM est supprimé. Si l'appareil n'est pas connecté à Internet, le Profil MDM demeure installé jusqu'à ce qu'une nouvelle connexion soit disponible.
- Tous les journaux liés à l'appareil supprimé sont toujours disponibles.
- Vos informations personnelles et applications ne sont pas affectées.



Avertissement

- Vous ne pouvez pas restaurer les appareils mobiles supprimés.
- Si vous supprimez par erreur un appareil verrouillé, vous devez restaurer ses paramètres d'usine pour le déverrouiller.

Pour supprimer un appareil mobile :

1. Allez sur la page **Réseau**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Dans le panneau de gauche, sélectionnez le groupe qui vous intéresse.
4. Cliquez sur le menu **Filtres** en haut de la zone de panneaux du réseau et sélectionnez **Appareils** dans la catégorie **Afficher**.
5. Cliquez sur **Enregistrer**.
6. Cochez la case correspondant aux appareils mobiles que vous souhaitez supprimer.
7. Cliquez sur le bouton  **Supprimer** en haut du tableau. Vous devrez confirmer votre action en cliquant sur **Oui**.

Supprimer des utilisateurs de l'inventaire du réseau

Les utilisateurs actuellement liés aux appareils mobiles ne peuvent pas être supprimés. Vous devez commencer par supprimer les appareils mobiles correspondants.




Note

Vous pouvez supprimer uniquement les utilisateurs des Groupes personnalisés.

Pour supprimer un utilisateur :

1. Allez sur la page **Réseau**.

2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Dans le panneau de gauche, sélectionnez le groupe qui vous intéresse.
4. Cliquez sur le menu **Filtres** en haut de la zone de panneaux du réseau et sélectionnez **Utilisateurs** dans la catégorie **Afficher**.
5. Cliquez sur **Enregistrer**.
6. Cochez la case correspondant à l'utilisateur que vous souhaitez supprimer.
7. Cliquez sur le bouton  **Supprimer** à droite du tableau. Vous devrez confirmer votre action en cliquant sur **Oui**.


6.5. Inventaire des applications

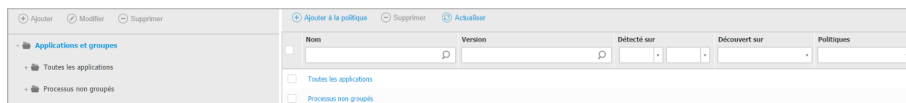
Vous pouvez visualiser toutes les applications découvertes dans votre réseau par la tâche **Découverte d'applications** dans la section **Applications et groupes**. Pour plus d'informations, reportez-vous à « [Découverte applications](#) » (p. 101).

Les applications et processus sont automatiquement ajoutés dans le dossier **Applications et groupes**, sur le panneau de gauche.

Vous pouvez organiser les applications et processus en groupes personnalisés.

Toutes les applications/tous les processus se trouvant dans un dossier sélectionné apparaissent dans le tableau du panneau de droite. Vous pouvez effectuer une recherche par nom, par version, par éditeur/auteur, par utilitaire de mise à jour, par lieu et par politique.

Pour afficher les informations les plus récentes dans le tableau, cliquez sur le bouton  **Actualiser** situé en haut du tableau. Cela peut être nécessaire lorsque vous passez du temps sur la page.



The screenshot shows the Bitdefender GravityZone interface. On the left, there is a sidebar with a tree view under 'Applications et groupes' containing 'Toutes les applications' and 'Processus non groupés'. The main area has a top bar with buttons: 'Ajouter à la politique', 'Supprimer', and 'Actualiser'. Below this is a table with columns: 'Nom', 'Version', 'Détecté sur', 'Découvert sur', and 'Politiques'. There are search filters and checkboxes for 'Toutes les applications' and 'Processus non groupés'.

Inventaire des applications



Important

Les nouvelles applications découvertes chaque fois que vous exécutez la tâche **Découverte d'applications** sont automatiquement placées dans le dossier **Applications non groupées**. Les processus qui ne sont pas liés à des applications spécifiques sont placés dans le dossier **Processus non groupés**.

Arborescence Applications et groupes

Pour ajouter un groupe personnalisé dans l'arborescence **Applications et groupes** :

1. Sélectionnez le dossier **Toutes les applications**.
2. Cliquez sur le bouton **+ Ajouter** situé en haut de l'arborescence.
3. Saisissez un nom dans la nouvelle fenêtre.
4. Cliquez sur **OK** pour créer le nouveau groupe.
5. Sélectionnez le dossier **Applications non groupées**. Toutes les applications groupées dans un dossier sélectionné sont affichées dans le tableau du panneau de droite.
6. Sélectionnez les applications souhaitées dans le tableau du panneau de droite. Effectuez un glisser-déposer des éléments que vous avez sélectionnés dans le panneau de droite vers le groupe personnalisé que vous avez choisi dans le panneau de gauche.

Pour ajouter une application personnalisée :


1. Sélectionnez le dossier cible dans **Toutes les applications**.
2. Cliquez sur le bouton **+ Ajouter** situé en haut de l'arborescence.
3. Saisissez un nom dans la nouvelle fenêtre.
4. Cliquez sur **OK** pour créer l'application personnalisée.
5. Vous pouvez ajouter des processus liés à la nouvelle application personnalisée à partir du dossier **Processus non groupés** ou à partir d'autres dossiers affichés dans l'arborescence **Applications et groupes**. Une fois le dossier sélectionné, tous les processus sont affichés dans le tableau du panneau de droite.
6. Sélectionnez les processus souhaités dans le tableau du panneau de droite. Effectuez un glisser-déposer des éléments que vous avez sélectionnés dans le panneau de gauche afin de les déplacer dans l'application personnalisée.

Note

Une application ne peut faire partie que d'un seul groupe.

Pour éditer le nom d'un dossier ou d'une application :

1. Sélectionnez-le(la) dans l'arborescence **Applications et groupes**.


2. Cliquez sur le bouton  **Éditer** situé en haut de l'arborescence.
3. Remplacez le nom par celui que vous voulez.
4. Cliquez sur **OK**.

Vous pouvez déplacer des groupes et des applications partout à l'intérieur de la hiérarchie **Applications et groupes**. Pour déplacer un groupe ou une application, effectuez un glisser-déposer du groupe ou de l'application de l'emplacement actuel vers le nouvel emplacement.

Pour supprimer un dossier personnalisé ou une application personnalisée, sélectionnez-le(la) dans l'arborescence **Applications et groupes** puis cliquez sur le bouton  **Supprimer** situé en haut de l'arborescence.

Ajouter des applications aux politiques

Pour ajouter une application ou un processus à une règle directement depuis l'Inventaire des applications :

1. Sélectionnez le dossier souhaité dans l'arborescence **Applications et groupes**. Le contenu du dossier est affiché dans le panneau de droite.
2. Sélectionnez les processus ou les applications que vous souhaitez dans le panneau de droite.
3. Cliquez sur le bouton  **Ajouter à la politique** pour ouvrir la fenêtre de configuration.
4. Dans la section **Appliquer la règle à ces politiques**, saisissez un nom de politique existant. Utilisez la boîte de recherche pour effectuer une recherche par nom de politique ou par propriétaire.
5. Dans la section **Informations relatives à la règle**, saisissez un **Nom de la règle**.
6. Sélectionnez la case **Activée** pour activer la règle.
7. Le type de cible est automatiquement reconnu. Si nécessaire, éditez les critères existants :
 - **Processus spécifique(s)**, pour définir un processus qui est autorisé à démarrer ou n'a pas le droit de le faire. Vous pouvez accorder une autorisation par chemin d'accès, par hash ou par certificat. Les conditions au sein de la règle sont liées par des ET logiques.
 - Pour autoriser une application à partir d'un chemin d'accès spécifique :

- a. Sélectionnez **Chemin d'accès** dans la colonne **Type**. Spécifiez le chemin d'accès vers l'objet. Vous pouvez fournir un nom de chemin d'accès absolu ou relatif et utiliser des caractères de remplacement. Le symbole astérisque (*) correspond à n'importe quel fichier au sein d'un répertoire. Un double astérisque (**) correspond à tous les fichiers et répertoires du répertoire défini. Un point d'interrogation (?) correspond à un caractère unique. Vous pouvez également ajouter une description afin d'aider à identifier le processus.
 - b. Dans le menu déroulant **Sélectionner un ou plusieurs contextes**, vous pouvez choisir entre local, CD-ROM, amovible et réseau. Vous pouvez bloquer une application exécutée à partir d'un support amovible, ou l'autoriser si l'application est exécutée localement.
- Pour autoriser une application sur la base d'un hash, sélectionnez **Hash** dans la colonne **Type** et saisissez une valeur de hachage. Vous pouvez également ajouter une description afin d'aider à identifier le processus.

**Important**

Pour générer la valeur de hachage, téléchargez l'outil [Empreinte digitale](#). Pour plus d'informations, reportez-vous à « [Outils du Contrôle des applications](#) » (p. 532)

- Pour accorder une autorisation sur la base d'un certificat, sélectionnez **Certificat** dans la colonne **Type** et saisissez une empreinte numérique de certificat. Vous pouvez également ajouter une description afin d'aider à identifier le processus.

**Important**

Pour obtenir l'empreinte numérique du certificat, téléchargez l'outil [Empreinte numérique](#). Pour plus d'informations, reportez-vous à « [Outils du Contrôle des applications](#) » (p. 532)



Général

Nom de la règle:

Activé

Cibles

Cible:

Type	Match	Description	Contexte	Action
Certificat	Veillez saisir un thumbprint c	Veillez saisir une valeur.	Sélectionnez un ou plusieurs	
Chemin	C:\test*.exe	**wildcard	Local	
Chemin	C:\test\test1*.exe	*wildcard	Local	
Chemin	C:\test\test1\exemp?e.exe	? wildcard	Local	
Hash	aabbccddeeffgghh6789	hash description	N/D	
Certificat	aaddgggyy1234567890	certificat description	N/D	

Règles d'applications

Cliquez sur **Ajouter** pour ajouter la règle. La règle nouvellement créée aura la priorité la plus haute dans cette politique.

- **Inventorier des applications ou des groupes**, pour ajouter un groupe ou une application découvert(e) sur votre réseau. Vous pouvez visualiser les applications en cours d'exécution sur votre réseau sur la page **Réseau > Inventaire des applications**.

Insérez les noms d'applications ou de groupes dans le champ, séparés par une virgule. La fonction remplissage automatique affiche des suggestions à mesure que vous écrivez.

8. Sélectionnez la case **Inclure les sous-processus** pour appliquer la règle aux processus enfant engendrés.

Avertissement


Lorsque vous définissez des règles pour les applications de navigateur, il est recommandé de désactiver cette option afin de prévenir les risques de sécurité.

9. Éventuellement, vous pouvez également définir des exclusions à la règle de démarrage du processus. L'opération d'ajout est identique à celle décrite aux étapes précédentes.

10. Dans la section **Permissions**, choisissez d'autoriser la règle à s'exécuter ou de le lui interdire.

11. Cliquez sur **Enregistrer** pour appliquer les modifications.

Pour supprimer une application ou un processus :

1. Sélectionnez le dossier souhaité dans l'arborescence **Applications et groupes**.
2. Sélectionnez les processus ou les applications que vous souhaitez dans le panneau de droite.
3. Cliquez sur le bouton  **Supprimer**.

Utilitaires de mise à jour


Vous devez définir des utilitaires de mise à jour pour les applications découvertes dans votre réseau.



Avertissement

Si vous ne désignez pas d'utilitaires de mise à jour, les applications figurant sur la liste blanche ne seront pas autorisées à se mettre à jour.


Pour désigner un utilitaire de mise à jour :

1. Sélectionnez le dossier souhaité dans l'arborescence **Applications et groupes**. Le contenu du dossier est affiché dans le panneau de droite.
2. Dans le panneau de droite, sélectionnez le fichier que vous souhaitez utiliser en tant qu'utilitaire de mise à jour.
3. Cliquez sur le bouton  **Désigner des utilitaires de mise à jour**.
4. Cliquez sur **Oui** pour confirmer la désignation. Les utilitaires de mise à jour sont signalés par une icône spécifique :



Utilitaire de mise à jour

Pour oublier un utilitaire de mise à jour :

1. Sélectionnez le dossier souhaité dans l'arborescence **Applications et groupes**. Le contenu du dossier est affiché dans le panneau de droite.
2. Dans le panneau de gauche, sélectionnez l'utilitaire de mise à jour que vous souhaitez oublier.
3. Cliquez sur le bouton  **Oublier l'utilitaire de mise à jour**.
4. Cliquez sur **Oui** pour confirmer.

6.6. Inventaire des patches

GravityZone détecte les correctifs dont vos logiciels ont besoin grâce à des tâches d'**Analyse des correctifs** puis les ajoute à l'inventaire des correctifs.

La page **Inventaire des correctifs** affiche tous les correctifs détectés pour le logiciel installé sur vos endpoints et indique les actions que vous pouvez entreprendre sur ces correctifs.

Utilisez l'**Inventaire des patches** quand vous devez déployer immédiatement certains patches. Cette alternative vous permet de facilement résoudre certains problèmes dont vous pourriez avoir conscience. Par exemple, vous avez lu un article sur une vulnérabilité d'un logiciel et vous connaissez l'identifiant du CVE. Vous pouvez rechercher dans l'inventaire les patches qui corrigent ce CVE puis voir sur quels endpoints ils doivent être appliqués.

Pour accéder à l'inventaire des patches, cliquez sur **Réseau > Inventaire des patches** depuis le menu principal de Control Center.

La page est divisée en deux volets :

- Le volet de gauche affiche les produits logiciels installés sur votre réseau, regroupés par fournisseur.
- Le volet de droite présente un tableau avec les patches disponibles et des informations les concernant.

Dashboard	Search products...	Ignore patches	Install	Patch stats	Refresh					
Network	Display all patches	Patch Name	KB Nu...	CVE	Bullet...	Patch sever...	Category	Installed / Pendi...	Missing / Install...	Affected Pr...
Patch Inventory	+ 7-Zip	<input type="checkbox"/> Windows6.1-SP1-Windows7-KB...	Q24799	1 CVE(s)	MS11-0...	Critical	Security	0 EP / 0 EP	1 EP / 0 EP	7 Product(s)
Application Inventory	+ AIMP DevTeam	<input type="checkbox"/> Windows6.1-SP1-Windows7-KB...	Q25054	0 CVE(s)	MSWU...	None	Non-Security	0 EP / 0 EP	1 EP / 0 EP	6 Product(s)
Packages	+ AOL Inc	<input type="checkbox"/> Windows6.1-SP1-Windows7-KB...	Q24881	0 CVE(s)	MSWU...	None	Non-Security	0 EP / 0 EP	1 EP / 0 EP	6 Product(s)
Tasks	+ AT&T	<input type="checkbox"/> Windows6.1-Windows7-SP1-KB...	Q24916	1 CVE(s)	MS11-0...	Important	Security	0 EP / 0 EP	1 EP / 0 EP	7 Product(s)
Policies	+ Acro Software	<input type="checkbox"/> Windows6.1-Windows7-SP1-KB...	Q25062	1 CVE(s)	MS11-0...	Important	Security	0 EP / 0 EP	1 EP / 0 EP	7 Product(s)
Assignment Rules										

Inventaire des patches

Vous allez ensuite découvrir comment utiliser l'inventaire. Voici ce que vous pouvez faire :

- [Visualiser les détails des correctifs](#)
- [Rechercher et filtrer des correctifs](#)
- [Ignorer les patches](#)
- [Installer des correctifs](#)
- [Désinstaller des correctifs](#)
- [Créer des statistiques sur les correctifs](#)

6.6.1. Consulter les informations des patches

Le tableau des correctifs fournit des informations qui vous aident à identifier les correctifs, à évaluer leur importance et à visualiser leur statut d'installation et leur portée. Ces informations sont présentées ci-dessous :

- **Nom du patch.** Le nom du fichier exécutable contenant le patch.
- **Numéro base de connaissances.** Ce numéro identifie l'article de la base de connaissances qui annonce la publication d'un patch.
- **CVE.** La quantité de CVE corrigée par le patch. En cliquant sur ce numéro, une liste des identifiants de CVE apparaît.
- **ID du bulletin.** L'identifiant du bulletin de sécurité publié par le vendeur. Cet identifiant mène à l'article qui décrit le patch et fournit des informations sur l'installation.
- **Sévérité du patch.** Cette évaluation vous informe de l'importance du patch en ce qui concerne les dommages qu'il permet d'éviter.

- **Catégorie.** En fonction du type de problèmes qu'ils résolvent, les patches sont regroupés en deux catégories : Lié à la sécurité ou Non lié à la sécurité. Ce champ vous indique la catégorie dans laquelle se situe le patch.
- **Installé / Installation en attente.** Ces numéros indiquent sur combien d'endpoints est installé le patch et combien sont en attente d'installation. Le numéro mène à la liste de ces endpoints.
- **Manquant / Installation échouée .** Ces numéros indiquent sur combien d'endpoints le patch n'a pas été installé et sur combien l'installation a échoué. Le numéro mène à la liste de ces endpoints.
- **Produits affectés.** Le numéro des produits pour lesquels le patch a été publié. Le numéro mène à la liste de ces produits logiciels.
- **Annulable.** Si vous devez annuler un certain correctif, vous devez d'abord vérifier que le correctif peut être désinstallé. Utilisez ce filtre pour savoir quels sont les correctifs pouvant être supprimés (annulés). Pour plus d'informations, veuillez consulter [Désinstaller des correctifs](#).

Pour personnaliser les informations contenues dans le tableau :

1. Cliquez sur le bouton **III Colonnes** à droite de la [barre d'action](#).
2. Sélectionnez les colonnes que vous souhaitez afficher.
3. Cliquez sur le bouton **Réinitialiser** pour rétablir l'affichage des colonnes par défaut.

Tant que vous êtes sur cette page, les processus de GravityZone en tâche de fond peuvent affecter la base de données. Veillez à bien consulter les informations les plus récentes du tableau en cliquant sur le bouton ☺ **Actualiser** situé en haut du tableau.

GravityZone examine une fois par semaine la liste des correctifs disponibles et supprime ceux qui n'ont plus de raison d'être car les applications ou les endpoints auxquels ils se réfèrent n'existent plus.

GravityZone examine également chaque jour la liste des correctifs et supprime ceux qui ne sont plus disponibles, même s'ils peuvent être présents sur certains endpoints.

6.6.2. Rechercher et filtrer des patches

Par défaut, Control Center affiche tous les patches disponibles pour votre logiciel. GravityZone dispose de plusieurs options pour trouver rapidement les patches dont vous avez besoin.

Filtrer les patches par produit



1. Localisez le produit dans le volet de gauche.
Pour cela, vous pouvez soit faire défiler la liste pour trouver son fournisseur, ou saisir le nom dans le champ de recherche situé en haut du volet.
2. Cliquez sur le nom du fournisseur pour développer la liste et voir ses produits.
3. Sélectionnez un produit pour voir les patches disponibles ou désélectionnez-le pour masquer les patches.
4. Répétez les étapes précédentes pour tous les produits qui vous intéressent.

Si vous voulez de nouveau voir les patches de tous les produits, cliquez sur le bouton **Afficher tous les patches** situé en haut du volet de gauche.

Filtrer les patches par utilité

Lorsqu'un patch, ou une version plus récente de celui-ci, est déjà déployé sur un endpoint, il devient superflu. Et comme il est parfois possible que des patches de ce type apparaissent dans l'inventaire, GravityZone vous donne la possibilité de les ignorer. Sélectionnez ces patches et cliquez sur le bouton **Ignorer les patches** situé en haut du tableau.

Control Center affiche les patches ignorés sur une page différente. Cliquez sur le bouton **Administré/Ignoré** dans la partie droite de la [barre d'outils d'action](#) pour basculer entre les affichages :

-  pour voir les patches ignorés.
-  pour voir les patches gérés.

Filtrer les patches par détails

Utilisez le système de recherche pour filtrer les patches selon certains critères ou selon les informations dont vous disposez. Saisissez les termes recherchés dans les champs de recherches situé en haut du tableau des patches. Les patches correspondants sont affichés dans le tableau pendant que vous tapez, ou une fois la sélection faite.


Videz les champs pour réinitialiser la recherche.

6.6.3. Ignorer des correctifs




Il vous faudra peut-être ignorer certains correctifs de l'inventaire des correctifs, si vous ne prévoyez pas de les installer sur vos endpoints, en utilisant la commande **Ignorer des correctifs**.

Un correctif ignoré sera exclus des tâches et des rapports de correctifs automatiques, et il ne sera pas considéré comme un correctif manquant.

Pour ignorer un correctif :

1. Sur la page **Inventaire des correctifs**, sélectionnez le ou les correctifs que vous souhaitez ignorer.
2. Cliquez sur le bouton  **Ignorer les patches** en haut du tableau.
Une fenêtre de configuration apparaîtra, dans laquelle vous pourrez visualiser les informations relatives aux correctifs sélectionnés, ainsi que celles relatives aux correctifs secondaires.
3. Cliquez sur **Ignorer**. Le correctif sera supprimé de la liste de l'inventaire des correctifs.

Les correctifs ignorés seront visibles dans un affichage spécifique, à partir duquel vous pourrez entreprendre des actions les concernant :


- Cliquez sur le bouton  **Afficher les correctifs ignorés** situé en haut à droite du tableau. Vous visualiserez la liste de tous les correctifs ignorés.
- Vous pouvez obtenir davantage d'informations sur un correctif ignoré en générant un rapport statistique sur le correctif. Sélectionnez le correctif ignoré de votre choix et cliquez sur le bouton  **Statistiques du correctif** situé en haut du tableau. Pour plus d'informations, veuillez consulter « [Création de statistiques sur les patches](#) » (p. 209)
- Pour restaurer des correctifs ignorés, sélectionnez-les et cliquez sur le bouton  **Restaurer des correctifs** situé en haut du tableau.

Une fenêtre de configuration apparaîtra, dans laquelle vous pourrez visualiser des informations concernant les correctifs sélectionnés.

Cliquez sur le bouton **Restaurer** pour envoyer le correctif vers l'inventaire.


6.6.4. Installer des patches

Pour installer des patches depuis l'Inventaire des patches :

1. Rendez-vous sur **Réseau > Inventaire des correctifs**.
2. Localisez les patches que vous souhaitez installer. Si nécessaire, utilisez les filtres pour les retrouver rapidement.
3. Sélectionnez les patches et cliquez sur le bouton  **Installer** situé en haut du tableau. Une fenêtre de configuration apparaîtra, à partir de laquelle vous pourrez éditer les détails de l'installation du correctif.

Vous visualiserez les correctifs sélectionnés, ainsi que les correctifs secondaires.

- Sélectionnez les groupes d'endpoints cibles.
- **Redémarrez les endpoints après l'installation du patch, si nécessaire..** Cette option redémarrera les endpoints immédiatement après l'installation des correctifs, si un redémarrage du système est nécessaire. Veuillez noter que cette action peut perturber l'activité de l'utilisateur.

Si vous n'activez pas cette option, cela signifie que si un redémarrage du système est nécessaire sur certains endpoints cibles, ces derniers afficheront l' icône de statut redémarrage en attente dans l'inventaire du réseau de GravityZone. Dans ce cas, vous disposez des options suivantes :


- Lancer une tâche **Redémarrer la machine** sur les endpoints en attente de redémarrage au moment de votre choix. Pour plus d'informations, reportez-vous à « [Redémarrage machine](#) » (p. 100).
- Configurer la politique active afin de notifier l'utilisateur de l'endpoint qu'un redémarrage est nécessaire. Pour cela, accédez à la politique active sur l'endpoint cible, allez sur **Général > Notifications** et activez l'option **Notification de redémarrage de l'endpoint**. Dans ce cas, l'utilisateur recevra une alerte pop-up chaque fois qu'un redémarrage sera nécessaire en raison de modifications effectuées par les composants GravityZone spécifiés (dans ce cas, Gestion des correctifs). L'alerte pop-up permettra de choisir de différer le redémarrage. Si l'utilisateur choisit de reporter le redémarrage, la notification de redémarrage apparaîtra régulièrement à l'écran jusqu'à ce que l'utilisateur redémarrage le système ou que le délai défini par l'administrateur de la société expire.

Pour plus d'informations, reportez-vous à « [Notification de redémarrage de l'endpoint](#) » (p. 245).

4. Cliquez sur **Installer**.

La tâche d'installation est créée en parallèle à d'autres sous-tâches pour chaque endpoint cible.

Note

- Vous pouvez également installer un correctif à partir de la page **Réseau**, en commençant par les endpoints spécifiques que vous souhaitez gérer. Dans ce cas, sélectionnez les endpoints dans l'inventaire du réseau, cliquez sur le bouton  **Tâches** situé en haut du tableau et choisissez **Installer des correctifs**. Pour plus d'informations, reportez-vous à « [Installation des patches](#) » (p. 83).
- Après l'installation du correctif, nous vous recommandons de lancer une tâche d'[Analyse du correctif](#) sur les endpoints cibles. Cette action mettra à jour les informations du correctif stockées dans GravityZone pour vos réseaux gérés.

6.6.5. Désinstallation des patches

Il vous faudra peut-être supprimer des correctifs ayant causé des dysfonctionnements sur les endpoints cibles. GravityZone dispose d'une option permettant d'annuler les correctifs installés sur votre réseau, qui restaure le logiciel à son état préalable à l'application du correctif.

La fonction de désinstallation est disponible uniquement pour les correctifs pouvant être annulés. L'inventaire des correctifs de GravityZone inclut une colonne **Annulable**, dans laquelle vous pouvez filtrer les correctifs selon qu'ils sont annulables ou non.

Note


Le caractère d'annulabilité dépend de la façon dont le correctif a été publié par le fabricant ou des modifications apportées par le correctif au logiciel. Pour les correctifs ne pouvant être annulés, il vous faudra peut-être réinstaller le logiciel.

Pour désinstaller un correctif :


1. Rendez-vous sur **Réseau > Inventaire des correctifs**.
2. Sélectionnez le correctif que vous souhaitez désinstaller. Pour rechercher un correctif spécifique, utilisez les filtres disponibles dans les colonnes, tels que le numéro KB ou le CVE. Utilisez la colonne **Annulable** pour afficher uniquement les correctifs disponibles pouvant être désinstallés.

Note

Vous ne pouvez désinstaller qu'un seul correctif à la fois sur un ou plusieurs endpoints.

3. Cliquez sur le bouton  **Désinstaller** en haut du tableau. Une fenêtre de configuration apparaîtra, à partir de laquelle vous pourrez éditer les détails de la tâche de désinstallation.

- **Nom de la tâche.** Vous pouvez modifier le nom par défaut de la tâche de désinstallation du correctif, si vous le souhaitez. Ainsi, vous identifierez plus facilement la tâche dans la page des [Tâches](#).
- **Ajouter un patch à la liste des patches à ignorer.** En règle générale, vous n'aurez plus besoin d'un correctif que vous souhaitez désinstaller. Cette option ajoute automatiquement le correctif à la [liste des correctifs ignorés](#), une fois le correctif désinstallé.
- **Redémarrez les endpoints après la désinstallation du patch, si nécessaire..** Cette option redémarrera les endpoints immédiatement après la désinstallation des correctifs, si un redémarrage du système est nécessaire. Veuillez noter que cette action peut perturber l'activité de l'utilisateur.

Si vous n'activez pas cette option, cela signifie que si un redémarrage du système est nécessaire sur certains endpoints cibles, ces derniers afficheront l' icône de statut redémarrage en attente dans l'inventaire du réseau de GravityZone. Dans ce cas, vous disposez des options suivantes :

- Lancer une tâche **Redémarrer la machine** sur les endpoints en attente de redémarrage au moment de votre choix. Pour plus d'informations, reportez-vous à « [Redémarrage machine](#) » (p. 100).
- Configurer la politique active afin de notifier l'utilisateur de l'endpoint qu'un redémarrage est nécessaire. Pour cela, accédez à la politique active sur l'endpoint cible, allez sur **Général > Notifications** et activez l'option **Notification de redémarrage de l'endpoint**. Dans ce cas, l'utilisateur recevra une alerte pop-up chaque fois qu'un redémarrage sera nécessaire en raison de modifications effectuées par les composants GravityZone spécifiés (dans ce cas, Gestion des correctifs). L'alerte pop-up permettra de choisir de différer le redémarrage. Si l'utilisateur choisit de reporter le redémarrage, la notification de redémarrage apparaîtra régulièrement à l'écran jusqu'à ce que l'utilisateur redémarrage le système ou que le délai défini par l'administrateur de la société expire.

Pour plus d'informations, reportez-vous à « [Notification de redémarrage de l'endpoint](#) » (p. 245).

- Dans le tableau **Cibles de l'annulation**, sélectionnez les endpoints sur lesquels vous souhaitez désinstaller le correctif.

Vous pouvez sélectionner un ou plusieurs endpoints de votre réseau. Utilisez les filtres disponibles pour localiser l'endpoint de votre choix.

**Note**

Le tableau affiche uniquement les endpoints sur lesquels le correctif sélectionné est installé.

4. Cliquez sur **Confirmer**. Une tâche **Désinstallation du correctif** sera créée et lancée sur les endpoints cibles.


Un rapport concernant la **Désinstallation du correctif** est automatiquement généré pour chaque tâche de désinstallation d'un correctif achevée, fournissant des informations relatives au correctif, aux endpoints cibles et au statut de la tâche de désinstallation du correctif.

**Note**

Après la désinstallation d'un correctif, nous vous recommandons de lancer une tâche d'**Analyse du correctif** sur les endpoints cibles. Cette action mettra à jour les informations du correctif stockées dans GravityZone pour vos réseaux gérés.

6.6.6. Création de statistiques sur les patches

Si vous avez besoin d'information sur l'état de certains patches sur tous les endpoints, utilisez la fonctionnalité **Statistiques sur le patch**, qui génère un rapport instantané pour le patch sélectionné :

1. Sur la page **Inventaire des correctifs**, sélectionnez le correctif désiré dans le volet de droite.
2. Cliquez sur le bouton  **Statistiques sur le correctif** en haut du tableau.

Un rapport statistique sur le correctif apparaît, vous donnant de nombreuses informations sur l'état du correctif, avec notamment :

- Un diagramme circulaire, qui présente le pourcentage de correctifs installés, dont l'installation a échoué, manquant ou en attente pour les endpoints concernés par le correctif.
- Un tableau avec les informations suivantes :

- **Nom, FQDN, IP et Système d'exploitation** de chaque endpoint concerné par le correctif.
- **Dernier contrôle** : la date du dernier contrôle du correctif sur l'endpoint.
- **État du correctif** : installé, échec de l'installation, manquant ou ignoré.



Note

La fonctionnalité de statistiques sur le correctif est disponible aussi bien pour les correctifs administrés qu'ignorés.

6.7. Afficher et gérer des tâches

La page **Réseau > Tâches** vous permet d'afficher et de gérer toutes les tâches que vous avez créées.

Une fois que vous avez créé une tâche pour l'un des objets du réseau, vous pouvez la voir dans le tableau des tâches.


Vous pouvez effectuer les actions suivantes à partir de la page **Réseau > Tâches** :

- [Vérifier l'état d'une tâche](#)
- [Afficher les rapports sur les tâches](#)
- [Redémarrer tâches](#)
- [Arrêter les Tâches d'analyse Exchange](#)
- [Supprimer des tâches](#)

6.7.1. Vérifier l'état d'une tâche

Lorsque vous créez une tâche pour un ou plusieurs objets du réseau, vous pouvez suivre son avancement et être informé de la survenue d'erreurs.

Allez sur la page **Réseau > Tâches** et vérifiez la colonne **État** pour chaque tâche qui vous intéresse. Vous pouvez vérifier l'état de la tâche principale et vous pouvez également obtenir des informations détaillées sur chaque sous-tâche.

Redémarrer Supprimer Actualiser				
Nom	Type de tâche	État	Période de début	Rapports
<input type="checkbox"/> Scan Device 2015-06-23	Analyse	En attente (0 / 1)	23 jui 2015, 15:38:02	

La page Tâches

- **Vérifier l'état de la tâche principale.**

La tâche principale concerne l'action lancée sur les objets du réseau (telle que l'installation d'un client ou une analyse) et contient un certain nombre de sous-tâches, une pour chaque objet du réseau sélectionné. Par exemple, une tâche d'installation principale créée pour huit ordinateurs contient huit sous-tâches. Les chiffres entre parenthèses indiquent le nombre de sous-tâches terminées. Par exemple, (2/8) signifie que deux sous-tâches sur huit sont terminées.

L'état de la tâche principale peut être :

- **En attente**, quand aucune des sous-tâches n'a démarré ou lorsque le nombre de déploiements simultanés est dépassé. Le nombre maximal de déploiements simultanés peut être défini à partir du menu **Configuration**. Pour plus d'informations, consultez le Guide d'Installation de GravityZone.
- **En cours**, lorsque toutes les sous-tâches sont en cours d'exécution. L'état de la tâche principale demeure "En cours" tant que la dernière sous-tâche n'a pas été effectuée.
- **Terminé**, lorsque toutes les sous-tâches sont terminées (avec succès ou non). Lorsque les sous-tâches ont échoué, un symbole d'avertissement apparaît.

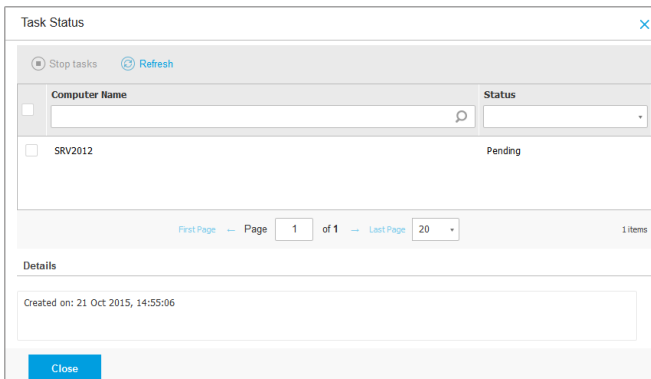
- **Vérifier l'état des sous-tâches.**

Rendez-vous sur la tâche qui vous intéresse et cliquez sur le lien de la colonne **État** pour ouvrir la fenêtre **État**. Vous pouvez voir la liste des objets du réseau auxquels on a affecté la tâche principale et l'état de la sous-tâche correspondante. L'état des sous-tâches peut être :

- **En cours**, lorsque la sous-tâche est toujours en cours d'exécution.
De plus, pour les tâches d'analyse à la demande sur Exchange, vous pouvez également voir l'état d'avancement.

- **Terminé**, lorsque la sous-tâche s'est terminée avec succès.
- **En attente**, lorsque la sous-tâche n'a pas encore démarré. Cela peut se produire dans les situations suivantes :
 - La sous-tâche est en attente dans une file d'attente.
 - Il y a des problèmes de connectivité entre le Control Center et l'objet du réseau cible.
 - L'appareil cible est Inactif (hors ligne) dans le cas d'appareils mobiles. La tâche s'exécutera sur l'appareil cible dès que celui-ci sera de nouveau en ligne.
- **Échec**, lorsque aucune des sous-tâches n'a démarré ou est interrompue en raison d'erreurs, telles que des identifiants incorrects ou un espace mémoire insuffisant.
- **Arrêt**, lorsque l'analyse à la demande prend trop de temps à se terminer et vous avez décidé d'y mettre fin.

Pour afficher les détails de chaque sous-tâche, sélectionnez-la et consultez la section **Détails** en bas du tableau.



Computer Name	Status
SRV2012	Pending

First Page Page 1 of 1 Last Page 20 1 items

Details

Created on: 21 Oct 2015, 14:55:06

Close

Détails sur l'état des tâches


Vous obtiendrez des informations au sujet de :

- La date et l'heure auxquelles la tâche a démarré.
- La date et l'heure auxquelles la tâche s'est terminée.

- La description des erreurs rencontrées.


6.7.2. Afficher les rapports sur les tâches

La page **Réseau > Tâches** vous permet d'afficher des rapports sur les tâches d'analyse rapide.

1. Accédez à la page **Réseau > Tâches**.
2. Sélectionnez l'objet du réseau souhaité dans le [sélecteur d'affichage](#).
3. Cochez la case correspondant à la tâche d'analyse qui vous intéresse.
4. Cliquez sur le bouton  correspondant de la colonne **Rapports**. Attendez que le rapport s'affiche. Pour plus d'informations, reportez-vous à « [Utilisation des rapports](#) » (p. 427).

6.7.3. Relancement des tâches

Pour diverses raisons, les tâches d'installation, de désinstallation ou de mise à jour du client peuvent ne pas se terminer. Vous pouvez choisir de redémarrer les tâches ayant échoué plutôt que d'en créer de nouvelles, en procédant comme suit :

1. Accédez à la page **Réseau > Tâches**.
2. Sélectionnez l'objet du réseau souhaité dans le [sélecteur d'affichage](#).
3. Cochez les cases correspondant aux tâches ayant échoué.
4. Cliquez sur le bouton  **Redémarrer** en haut du tableau. Les tâches sélectionnées redémarreront et l'état des tâches passera à **Nouvelle tentative**.


Note

Pour les tâches avec plusieurs sous-tâches, l'option **Redémarrer** est disponible uniquement lorsque toutes les sous-tâches sont terminées et exécutera uniquement les sous-tâches ayant échoué.

6.7.4. Arrêt des Tâches d'analyse Exchange

Analyser le stockage Exchange peut prendre un temps considérable. Si pour n'importe quelle raison vous souhaitez arrêter une tâche d'analyse à la demande Exchange, suivez les étapes décrites ci-dessous :

1. Accédez à la page **Réseau > Tâches**.
2. Sélectionnez l'aperçu du réseau souhaité dans le [sélecteur d'affichage](#).


3. Cliquez sur le lien dans la colonne **État** pour ouvrir la fenêtre **État tâche**.
4. Sélectionnez la case correspondant à la sous-tâche en cours d'exécution ou en suspens que vous souhaitez arrêter.
5. Cliquez sur le bouton  **Arrêter tâches** en haut du tableau. Vous devrez confirmer votre action en cliquant sur **Oui**.

**Note**

Vous pouvez également arrêter une analyse à la demande du stockage Exchange à partir de la zone événements de Bitdefender Endpoint Security Tools.

6.7.5. Supprimer des tâches

GravityZone supprime automatiquement les tâches en attente au bout de deux jours, et les tâches achevées au bout de 30 jours. S'il vous reste encore de nombreuses tâches, nous vous recommandons de supprimer celles dont vous n'avez plus besoin, afin d'éviter que la liste ne soit encombrée.

1. Accédez à la page **Réseau > Tâches**.
2. Sélectionnez l'objet du réseau souhaité dans le [sélecteur d'affichage](#).
3. Cochez la case correspondant à la tâche que vous souhaitez supprimer.
4. Cliquez sur le bouton  **Supprimer** en haut du tableau. Vous devrez confirmer votre action en cliquant sur **Oui**.

**Avertissement**

Supprimer une tâche en attente annulera également la tâche.

Si une tâche en cours est supprimée, toutes les sous-tâches en attente seront annulées. Dans ce cas, toutes les sous-tâches terminées ne peuvent pas être annulées.

6.8. Supprimer des endpoints de l'inventaire du réseau

L'inventaire du réseau contient par défaut le dossier **Supprimé**, destiné à stocker les endpoints que vous ne voulez pas gérer.

L'action **Supprimer** a les effets suivants :

- Lorsque des endpoints non gérés sont supprimés, ils sont directement déplacés vers le dossier **Supprimé**.
- Lorsque des endpoints gérés sont supprimés :

- Une tâche de désinstallation du client est créée
- Un siège de licence est libéré
- Les endpoints sont déplacés vers le dossier **Supprimé**


Pour supprimer des endpoints de l'inventaire du réseau :

1. Allez sur la page **Réseau**.
2. Sélectionnez l'affichage réseau adapté dans le [sélecteur d'affichage](#).
3. Sélectionnez **Groupes personnalisés** dans le panneau de gauche. Tous les endpoints disponibles dans ce groupe apparaissent dans le tableau du panneau de droite.



Note

Vous pouvez uniquement supprimer les endpoints affichés dans **Groupes personnalisés**, qui sont détectés hors de toute infrastructure réseau intégrée.

4. Dans le panneau de droite, cochez la case du endpoint à supprimer.
5. Cliquez sur le bouton  **Supprimer** en haut du tableau. Vous devrez confirmer votre action en cliquant sur **Oui**.

Si l'endpoint à supprimer est géré, une tâche **Désinstaller le client** est créée sur la page **Tâches** et l'agent de sécurité sera désinstallé de l'endpoint, libérant ainsi un siège de licence.

6. L'endpoint est déplacé vers le dossier **Supprimé**.

Vous pouvez, à tout moment, déplacer les endpoints du dossier **Supprimé** vers **Groupes personnalisés**, à l'aide du glisser-déposer.



Note

- Si vous voulez arrêter de gérer de manière permanente certains endpoints, vous devez les laisser dans le dossier **Supprimé**.
- Si vous supprimez des endpoints du dossier **Supprimé**, ils seront complètement supprimés de la base de données de GravityZone. Néanmoins, les endpoints exclus qui sont en ligne seront détectés par la prochaine tâche de Découverte de réseau et apparaîtront dans l'Inventaire réseau en tant que nouveaux endpoints.

6.9. Configuration des paramètres du réseau

Sur la page **Configuration > Paramètres réseau** page, vous pouvez configurer les paramètres relatifs à l'Inventaire réseau, comme : sauvegarder les filtres, mémoriser le dernier emplacement parcouru, créer et gérer des règles planifiées pour supprimer les machines virtuelles inutilisées.

Les options sont réparties dans les sections suivantes :

- [Paramètres de l'inventaire réseau](#)
- [Nettoyage des machines hors ligne](#)

6.9.1. Paramètres de l'inventaire réseau

Dans la section **paramètres de l'Inventaire réseau**, les options suivantes sont disponibles :

- **Enregistrer les filtres de l'Inventaire réseau.** Cochez cette case pour enregistrer vos filtres sur la page **Réseau** entre deux sessions de Control Center.
- **Se souvenir du dernier emplacement visité dans l'Inventaire réseau jusqu'à ce que je me déconnecte.** Cochez cette case pour enregistrer le dernier emplacement auquel vous avez accédé lorsque vous quittez la page **Réseau**. L'emplacement n'est pas enregistré entre les sessions.
- **Empêcher la création de doublons des endpoints clonés.** Sélectionnez cette option pour activer un nouveau type d'objets réseau dans GravityZone, appelé les images principales. De cette manière, vous pourrez distinguer les endpoints sources de leurs clones. Pour cela, vous devez marquer chaque endpoint que vous clonez comme suit :
 1. Allez sur la page **Réseau**.
 2. Sélectionnez l'endpoint que vous voulez cloner.
 3. Depuis son menu contextuel, sélectionnez **Définir comme image principale**.

6.9.2. Nettoyage des machines hors ligne

Dans la section **Nettoyage des machines hors ligne**, vous pouvez planifier des règles pour supprimer automatiquement les machines virtuelles de l'Inventaire réseau.

Tasks	Offline machines cleanup
Risk Management	Configure rules to automatically delete unused virtual machines from the Network Inventory and clear their license seats.
Policies	+ Add rule X Delete
Assignment Rules	
Reports	
Quarantine	
Accounts	
User Activity	
System Status	
Configuration	
Update	

Rule name	Offline for	Machines name	Location	Deleted(last 24h)	State
<input type="checkbox"/> Rule 3	66 days		Custom Groups	0 machines	<input checked="" type="checkbox"/>
<input type="checkbox"/> Rule 4	78 days		Custom Groups	0 machines	<input type="checkbox"/>

Configuration - Paramètres réseau - Nettoyage des machines hors ligne

Création de règles

Pour créer une règle de nettoyage :

1. Dans la section **Nettoyage des machines hors ligne**, cliquez sur le bouton **Ajouter une règle**.
2. Sur la page Configuration :
 - a. Saisir un nom pour la règle.
 - b. Sélectionnez une heure pour le nettoyage quotidien.
 - c. Définissez les critères de nettoyage :
 - Le nombre de jours depuis lequel les machines sont passées hors ligne (de 1 à 90).
 - Un modèle de nom, qui peut être appliqué à une seule ou à plusieurs machines virtuelles.

Par exemple, utilisez `machine_1` pour supprimer la machine portant ce nom. Vous pouvez aussi utiliser `machine_*` pour supprimer toutes les machines dont le nom commence par `machine_`.

Ce champ est sensible à la casse et n'accepte que les lettres, les chiffres et les caractères spéciaux astérisque (*), tiret bas (_), et tiret (-). Le nom ne peut pas commencer par un astérisque (*).
 - d. Sélectionnez les groupes d'endpoints cibles sur lesquels appliquer la règle dans l'inventaire réseau.
3. Cliquez sur **Enregistrer**.

Afficher et gérer les règles

La section **Paramètres réseau > Nettoyage des machines hors ligne** présente toutes les règles que vous avez créées. Un tableau dédié vous fournit les informations détaillées suivantes :

- Nom de la règle.
- Le nombre de jours depuis quand la machine est hors ligne.
- Modèle de nom des machines.
- Emplacement dans l'inventaire réseau.
- Le nombre de machines supprimées les 24 dernières heures.
- État : activé, désactivé ou invalide.



Note

Une règle est invalide si les cibles ne sont plus valides pour certaines raisons. Par exemple, les machines virtuelles ont été supprimées ou vous n'y avez plus accès.

Une nouvelle règle est activée par défaut. Vous pouvez activer et désactiver des règles n'importe quand en utilisant le bouton On/Off de la colonne **État**.

Si nécessaire, utilisez les options de tri et de filtre situées en haut du tableau pour trouver certaines règles.

Pour modifier une règle :

1. Cliquez sur le nom de la règle.
2. Sur la page de configuration, modifiez les détails de la règle.
3. Cliquez sur **Enregistrer**.

Pour supprimer une ou plusieurs règles :

1. Utilisez les cases à cocher pour sélectionner une ou plusieurs règles.
2. Cliquez sur le bouton **Supprimer** en haut du tableau.

6.10. Configuration des paramètres de Security Server

Les Security Servers utilisent leur mécanisme de mise en cache pour dédupliquer l'analyse antimalware et ainsi optimiser ce processus. Une étape de plus de l'optimisation de l'analyse est de partager ce cache avec d'autres Security Servers.

Le partage du cache ne fonctionne qu'entre Security Servers du même type. Par exemple un Security Server Multi-Platform ne partagera son cache qu'avec un autre Security Server Multi-Platform et pas avec un Security Server for NSX.

Pour activer et configurer le partage de cache :

1. Rendez-vous sur la page **Configuration > Paramètres de Security Server**.
2. Cochez la case **Partage de cache de Security Server**.
3. Choisissez la portée du partage :
 - Tous les Security Servers disponibles.
Il est recommandé d'utiliser cette option si tous les Security Servers sont sur le même réseau.
 - Security Servers disponible dans la liste Affectation.
Utilisez cette option quand les Security Servers sont répartis sur différents réseaux et que le partage de cache pourrait générer une grande quantité de trafic.
4. Pour limiter la portée, créez un groupe de Security Servers. Sélectionnez les Security Servers dans le menu déroulant et cliquez sur **Ajouter**.
Seuls les Security Servers ajoutés au tableau partagera leur cache.



Note

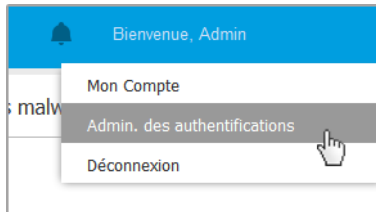
Les Security Servers pour NSX-T et NSX-V échangent des informations en cache qu'au sein du même vCenter Server.

5. Cliquez sur **Enregistrer**.

6.11. Admin. des authentifications

L'Administrateur des authentifications vous aide à définir les identifiants requis pour accéder aux inventaires vCenter Server disponibles et pour l'authentification à distance sur 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

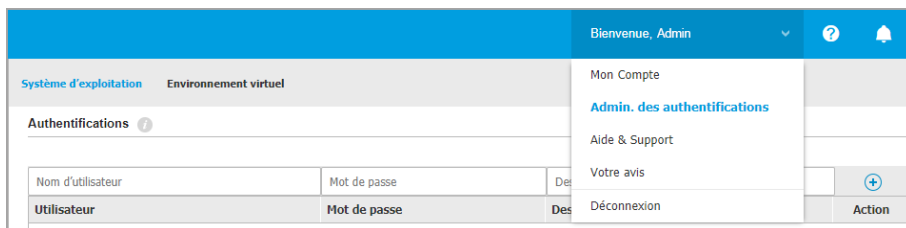
La fenêtre **Admin. des authentifications** comporte deux onglets :

- [Système d'exploitation](#)
- [Environnement virtuel](#)

6.11.1. Système d'exploitation

L'onglet **Système d'exploitation** 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 :



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.

6.11.2. Environnement virtuel

L'onglet Environnement virtuel vous permet de gérer les identifiants des systèmes de serveurs virtualisés disponibles.

Pour accéder à l'infrastructure virtualisée intégrée à Control Center, vous devez indiquer vos identifiants utilisateur pour chaque système de serveur virtualisé disponible. Control Center utilise vos identifiants pour se connecter à l'infrastructure virtualisée, en affichant uniquement les ressources auxquelles vous avez accès (en fonction de ce qui est défini dans le serveur virtualisé).

Pour spécifier les identifiants requis pour se connecter à un serveur virtualisé :

1. Sélectionnez le serveur dans le menu correspondant.

**Note**

Si le menu n'est pas disponible, c'est que l'intégration n'a pas encore été configurée ou que tous les authentifiants requis ont déjà été configurés.

2. Saisissez votre nom d'utilisateur et votre mot de passe ainsi qu'une description explicite.
3. Cliquez sur le bouton **+** **Ajouter**. Le nouveau jeu d'authentifiants est ajouté au tableau.

**Note**


Si vous ne configurez pas vos informations d'authentification dans l'Administrateur des authentifications, on vous demandera de les saisir lorsque vous tenterez de parcourir l'inventaire de tout système de serveur virtualisé. Les authentifiants que vous avez indiqués sont enregistrés dans votre Administrateur des authentifications afin que vous n'ayez pas besoin de les saisir la prochaine fois.

**Important**

Lorsque vous changez le mot de passe utilisateur de votre serveur virtualisé, pensez à l'actualiser dans l'Administrateur des authentifications.

6.11.3. 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.

7. POLITIQUES DE SÉCURITÉ

Une fois installée, la protection Bitdefender peut être configurée et administrée à partir du Control Center à l'aide des politiques de sécurité. Une politique spécifique les paramètres de sécurité à appliquer aux objets de l'inventaire du réseau cible (ordinateurs, machines virtuelles ou appareils mobiles).

Juste après l'installation, les objets de l'inventaire du réseau se voient attribuer la politique par défaut, qui est préconfigurée avec les paramètres de protection recommandés. Si l'intégration NSX est activée, trois autres politiques de sécurité par défaut pour NSX sont disponibles, une pour chaque niveau de sécurité : permissive, normale et agressive. Ces politiques sont pré-configurées avec les paramètres de protection recommandés. Vous ne pouvez pas modifier ou supprimer les politiques par défaut.

Vous pouvez créer autant de politiques que nécessaire en fonction de vos besoins en sécurité, pour chaque type d'objet du réseau administré.

Voici ce que vous avez besoin de savoir au sujet des politiques :

- Les politiques sont créées dans la section **Politiques** et affectées aux objets du réseau de la page **Réseau**.
- Les politiques peuvent hériter de plusieurs paramètres de modules d'autres politiques.
- Vous pouvez configurer une affectation de politique aux endpoints de façon à ce que la politique s'applique seulement sous certaines conditions, selon l'emplacement ou l'utilisateur connecté. Ainsi, un endpoint peut avoir plusieurs politiques qui lui sont assignées.
- Les postes de travail peuvent avoir une politique active à la fois.
- Vous pouvez affecter une politique à des endpoints individuels ou à des groupes d'endpoints. Lorsque vous attribuerez une politique, vous définirez également les options d'héritage de la politique. Par défaut, chaque endpoint hérite de la politique du groupe parent.
- Les politiques sont envoyées aux objets du réseau cibles, immédiatement après leur création ou leur modification. Les paramètres devraient être appliqués aux objets du réseau en moins d'une minute (à condition qu'ils soient en ligne). Si un objet du réseau n'est pas en ligne, les paramètres seront appliqués dès qu'il sera de nouveau en ligne.
- La politique s'applique uniquement aux modules de protection installés.
- La page **Politiques** affiche uniquement les types de politique suivants :
 - Les politiques que vous avez créées.

- D'autres politiques (telles que les modèles ou la politique par défaut créés par d'autres utilisateurs) qui sont affectées à des endpoints sous votre compte.
- Vous ne pouvez pas modifier les politiques créées par d'autres utilisateurs (à moins que les propriétaires des politiques ne l'autorisent dans les paramètres des politiques) mais vous pouvez les écraser en affectant une autre politique aux objets cibles.



Avertissement

Seuls les modules de politiques supportés s'appliqueront aux endpoints cibles. Veuillez noter que seul le module Antimalware est supporté pour les systèmes d'exploitation serveurs.

7.1. Administration des politiques

Vous pouvez afficher et gérer les politiques sur la page **Politiques**.

Nom de la politique	Créé par	Modifié le	Cibles	Appliqué/En attente
<input type="checkbox"/> Politique par défaut (par défaut)	root		196	4/ 357

La page Politiques

Chaque type d'endpoint a des paramètres de politique spécifiques. Pour gérer les politiques, vous devez commencer par sélectionner le type d'endpoint (**Ordinateur / Machine virtuelle** ou **Appareils mobiles**) dans le **sélecteur d'affichage**.

Les politiques existantes s'affichent dans le tableau. Pour chaque politique, vous pouvez voir :

- Nom de la politique.
- L'utilisateur qui a créé la politique.
- La date et l'heure de la dernière modification de la politique.
- Le nombre de cibles sur lequel la politique a été envoyé.*
- Le nombre de cibles sur lequel la politique a été appliqué / est suspendu.*

Pour les politiques ayant le module NSX activé, des informations supplémentaires sont disponibles :

- Le nom de politique NSX, utilisé pour identifier la politique Bitdefender dans VMware vSphere.
- Visibilité de la politique dans les consoles d'administration, vous permettant de filtrer les politiques pour NSX. Ainsi, alors que les politiques **Locales** ne sont visibles que dans Bitdefender Control Center, les politiques **Globales** sont également visibles dans VMware NSX.

Ces détails sont cachés par défaut.

Pour personnaliser les informations sur une politique apparaissant dans le tableau :

1. Cliquez sur le bouton **III Colonnes** à droite de la [barre d'action](#).
2. Sélectionnez les colonnes que vous souhaitez afficher.
3. Cliquez sur le bouton **Réinitialiser** pour rétablir l'affichage des colonnes par défaut.

* En cliquant sur le numéro vous serez redirigé vers la page **Réseau**, où vous pouvez afficher les paramètres correspondants. Il vous sera demandé de choisir [l'affichage réseau](#) . Cette action va créer un [filtre](#) en utilisant les critères de la politique.


Vous pouvez [classer](#) les politiques disponibles et également [rechercher](#) certaines politiques à l'aide des critères disponibles.

7.1.1. Création de politiques

Vous pouvez créer des politiques soit en en ajoutant une nouvelle, soit en dupliquant (clonant) une politique existante.

Pour créer une politique de sécurité :

1. Allez sur la page **Politiques**.
2. Choisissez le type d'endpoint de votre choix dans le [sélecteur d'affichage](#).
3. Choisissez la méthode de création de la politique :
 - **Ajouter une nouvelle politique.**
 - Cliquez sur le bouton **+Ajouter** en haut du tableau. Cette commande crée une nouvelle politique à partir du modèle de politique par défaut.
 - **Cloner une politique existante.**

- a. Cochez la case de la politique que vous souhaitez dupliquer.
 - b. Cliquez sur le bouton  **Cloner** en haut du tableau.
4. Configurez les paramètres de la politique. Pour plus d'informations, reportez-vous à :
- [« Politiques des ordinateurs et machines virtuelles » \(p. 239\)](#)
 - [« Politiques des appareils mobiles » \(p. 401\)](#)

5. Cliquez sur **Enregistrer** pour créer la politique et revenir à la liste des politiques.

Lors de la définition de politiques à utiliser dans VMware NSX, en plus de configurer les paramètres de protection antimalware dans GravityZone Control Center, vous devez aussi créer une politique dans NSX, lui instruisant d'utiliser la politique GravityZone comme profil service. Pour créer une politique de sécurité NSX :

1. Connectez-vous à vSphere Web Client.
2. Allez dans l'onglet **Réseau & Sécurité > Service Composer > Politiques de sécurité**.
3. Cliquez sur le bouton **Créer une politique de sécurité** dans la barre d'outils en haut du tableau des politiques. La fenêtre de configuration s'affiche.
4. Saisissez le nom de la politique puis cliquez sur **Suivant**.
De façon optionnelle, vous pouvez également ajouter une courte description.
5. Cliquez sur le bouton **Ajouter un service d'inspection invité** en haut du tableau. La fenêtre de configuration du Service introspection invité s'affiche.
6. Saisissez le nom et la description du service.
7. Laissez l'action par défaut sélectionnée, pour permettre au profil de service Bitdefender de s'appliquer au groupe de sécurité.
8. Dans le menu **Nom du service** sélectionnez **Bitdefender**.
9. Dans le menu **Nom du service** sélectionnez une politique de sécurité GravityZone existante.
10. Laissez les valeurs par défaut des options **État** et **Appliquer**.



Note

Pour plus d'informations sur les paramètres de stratégie de sécurité, consultez la [documentation VMware NSX](#).

11. Cliquez sur **OK** pour ajouter le service.

12. Cliquez sur **Suivant** jusqu'à la dernière étape puis cliquez sur **Terminer**.

7.1.2. Affecter des politiques

La politique par défaut est attribuée au départ à tous les endpoints. Une fois que vous avez défini les politiques nécessaires dans la page **Politiques**, vous pouvez les assigner aux endpoints.

Le processus d'affectation de politiques est lié aux environnements auxquels GravityZone s'intègre. Pour certaines intégrations, telles que VMware NSX, les politiques sont accessibles en dehors de GravityZone Control Center. Les politiques externes sont également citées.

Affecter des politiques locales

Vous pouvez assigner les politiques locales de deux façons :

- **Affectation basée sur l'appareil**, ce qui signifie que vous sélectionnez manuellement les endpoints cibles auxquels vous affectez les politiques. Ces politiques sont également appelées politiques appareil.
- **Affectation basée sur la règle**, ce qui signifie qu'une politique est affectée à un endpoint géré si les paramètres réseaux sur l'endpoint correspondent aux conditions données d'une règle d'affectation existante.



Note

- Vous pouvez affecter uniquement les politiques que vous avez créées. Pour affecter une politique créée par un autre utilisateur, vous devez commencer par la cloner sur la page **Politiques**.
- Sur les machines virtuelles uniquement protégées par HVI, vous ne pouvez affecter que des politiques appareil. Lorsque Bitdefender Endpoint Security Tools est également installé sur celles-ci, vous pouvez affecter des politiques basées une règle, l'agent de sécurité gérant l'activation de la politique.

Affecter des politiques

Dans GravityZone, vous pouvez attribuer des politiques de plusieurs façons :

- Attribuer la politique directement à la cible.
- Attribuer la politique du groupe parent par le biais de l'héritage.

- Forcer l'héritage de la politique pour la cible.

Par défaut, chaque endpoint ou groupe d'endpoints hérite de la politique du groupe parent. Si vous modifiez la politique du groupe parent, tous les descendants seront affectés, sauf ceux sur lesquels une politique a été appliquée de force.

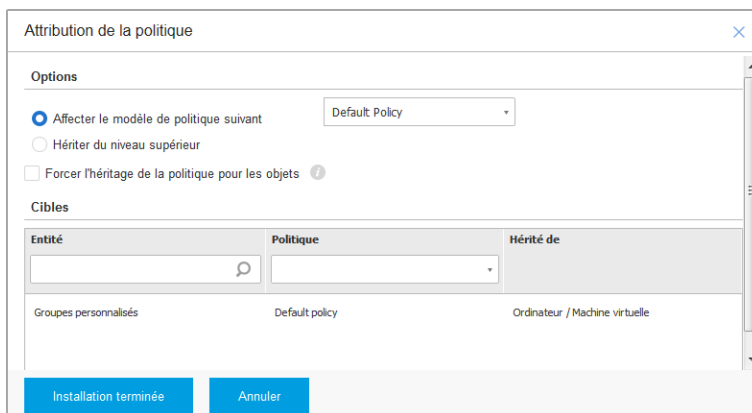
Pour affecter une politique appareil :

1. Allez sur la page **Réseau**.
2. Choisissez l'affichage réseau à partir du [sélecteur d'affichages](#).
3. Sélectionnez les endpoints cibles : Vous pouvez sélectionner un ou plusieurs endpoint(s) ou groupe(s) d'endpoints.

Pour des raisons liées à l'héritage, vous ne pouvez pas changer la politique par défaut du groupe racine. Par exemple, **Ordinateurs et Machines virtuelles** se verra toujours affecter la **politique par défaut**.

4. Cliquez sur le bouton  **Affecter une politique** situé en haut du tableau, ou sélectionnez l'option **Affecter une politique** dans le menu contextuel.

La page **Attribution de la politique** s'affiche :



Attribution de la politique

Options

Affecter le modèle de politique suivant Default Policy

Hériter du niveau supérieur

Forcer l'héritage de la politique pour les objets ⓘ

Cibles

Entité	Politique	Hérité de
<input type="text"/>	<input type="text"/>	
Groupes personnalisés	Default policy	Ordinateur / Machine virtuelle

Installation terminée Annuler

Paramètres de l'affectation de politique

5. Vérifiez le tableau avec les endpoints cibles. Pour chaque endpoint, vous pouvez voir :
 - La politique affectée.

- Le groupe parent à partir duquel la cible hérite de la politique, le cas échéant. Si le groupe applique la politique, vous pouvez cliquer sur son nom pour voir la page **Attribution de la politique** avec ce groupe comme cible.
 - État de l'application.
Cet état indique si la cible force l'héritage de la politique ou est forcée d'hériter de la politique.
Remarquez les cibles sur lesquelles une politique a été appliquée de force (état **forcée**). Leurs politiques ne peuvent être remplacées. En pareil cas, un avertissement est affiché.
6. En cas d'avertissement, cliquez sur le lien **Exclure ces cibles** pour continuer.
 7. Choisissez l'une des options disponibles pour affecter la politique :
 - **Affecter le modèle de politique suivant** - pour attribuer une politique spécifique directement aux endpoints cibles.
 - **Hériter du niveau supérieur** - pour utiliser la politique du groupe parent.
 8. Si vous choisissez d'affecter un modèle de politique :
 - a. Sélectionnez la politique dans la liste déroulante.
 - b. Sélectionnez **Forcer l'héritage de la politique pour les groupes enfants** pour obtenir les résultats suivants :
 - Affecter la politique à tous les descendants des groupes cibles, sans exception.
 - Empêcher sa modification à partir d'un niveau inférieur dans la hiérarchie.Un nouveau tableau affiche de manière réursive tous les endpoints et groupes d'endpoints affectés, ainsi que les politiques qui seront remplacées.
 9. Cliquez sur **Terminer** pour enregistrer et appliquer des modifications. Sinon, cliquez sur **Retour** ou **Annuler** pour revenir à la page précédente.

Une fois que vous avez terminé, les politiques sont aussitôt poussées vers les endpoints cibles. Les paramètres devraient être appliqués aux postes de travail en moins d'une minute (à condition qu'ils soient en ligne). Si un endpoint n'est pas en ligne, les paramètres seront appliqués dès qu'il sera de nouveau en ligne.

Pour vérifier que la politique a été correctement affectée :

1. Sur la page **Réseau**, cliquez sur le nom de l'endpoint qui vous intéresse. Le Control Center affichera la fenêtre **Informations**.
2. Consultez la section **Politique** pour afficher l'état de la politique actuelle. Elle devra afficher **Appliquée**.

Une autre méthode pour vérifier le statut de l'affectation consiste à consulter des détails de la politique :

1. Allez sur la page **Politiques**.
2. Trouvez la politique que vous avez assignée.
Dans la colonne **Active/Appliquée/En attente** vous pouvez voir le nombre d'endpoints pour chacun de ces trois statuts.
3. Cliquez sur n'importe quel nombre pour voir la liste des endpoints avec leur statut respectif sur la page **Réseau**.

Affecter des politiques basées sur règle

La page **Règles d'affectation > de politiques** vous permet de définir des politiques liées à l'utilisateur et à l'emplacement. Par exemple, vous pouvez appliquer des règles de pare-feu plus restrictives lorsque les utilisateurs se connectent à Internet à l'extérieur de l'entreprise, ou vous pouvez activer Web Access Control pour les utilisateurs qui ne font pas partie du groupe administrateurs.

Voici ce que vous avez besoin de savoir au sujet des règles d'affectation :

- Les postes de travail peuvent uniquement avoir une politique active à la fois.
- Une politique appliquée via une règle va écraser la politique d'appareil appliquée sur l'endpoint.
- Si aucune des règles d'affectation n'est applicable, alors la politique appareil est appliquée.
- Les règles sont mises en ordre et traitées selon leur priorité, 1 étant la plus forte. Vous pouvez avoir plusieurs règles pour une même cible. Dans ce cas, la première règle correspondant aux paramètres de connexion active sera appliquée sur l'endpoint cible.

Par exemple, si un endpoint correspond à une règle utilisateur avec une priorité 4 et une règle d'emplacement avec une priorité 3, la règle d'emplacement s'appliquera.



Avertissement

Assurez-vous de bien avoir pris en compte les paramètres tels que les exclusions, les communications ou les détails proxy lors de la création de règles.

Pour une bonne pratique, il est recommandé d'utiliser une politique d'héritage pour conserver les paramètres essentiels de la politique appareil également dans la politique utilisée par les règles d'affectation.

Pour créer une nouvelle règle :

1. Rendez-vous sur la page **Affectation de règles**.
2. Cliquez sur le bouton **+Ajouter** en haut du tableau.
3. Sélectionner le type de règle :
 - Règle de localisation
 - Règle utilisateur
 - Règle de tag
4. Configurez les paramètres de règle selon vos besoins.
5. Cliquez sur **Enregistrer** pour enregistrer les modifications et appliquer la règle aux endpoints cibles de la politique.

Pour modifier les paramètres d'une règle existante :

1. Sur la page **Règles d'affectation**, trouvez la règle que vous cherchez et cliquez dessus pour la modifier.
2. Configurez les paramètres de règle selon vos besoins.
3. Cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre. Pour quitter la fenêtre sans enregistrer les modifications, cliquez sur **Annuler**.

Si vous ne souhaitez plus utiliser une règle, sélectionnez-la et cliquez sur le bouton **- Supprimer** en haut du tableau. Vous devrez confirmer votre action en cliquant sur **Oui**.

Pour afficher les informations les plus récentes, cliquez sur le bouton **🔄 Actualiser** en haut du tableau.


Configuration des règles d'emplacement



Un emplacement est un segment de réseau identifié par un ou plusieurs paramètres réseaux, tel qu'une passerelle spécifique, un DNS spécifique utilisé pour résoudre

des URL, ou un sous-groupe d'IP. Par exemple, vous pouvez définir des emplacements tels que le LAN de la société, le cluster de serveurs ou un service.

Dans la fenêtre de configuration de règle, suivez ces étapes :

1. Indiquez un nom et une description explicites pour la règle que vous souhaitez créer.
2. Configurez la priorité de la règle. Les règles sont classées par ordre de priorité, la première ayant la plus élevée. La même priorité ne peut être accordée deux fois ou plus.
3. Sélectionnez la politique pour laquelle vous créez la règle d'affectation.
4. Définissez les emplacements auxquels la règle doit s'appliquer.
 - a. Sélectionnez le type de paramètres réseau dans le menu en haut du tableau Emplacements. Voici les types disponibles :

Type	Valeur
Étendue de l'adresse IP/IP	Adresses IP spécifiques dans un réseau ou des sous-réseaux. Pour les sous-réseaux, utilisez le format CIDR. Par exemple, 10.10.0.12 ou 10.10.0.0/16
Adresse de la passerelle	L'adresse IP de la passerelle
Adresse du serveur WINS	Adresse IP du serveur WINS
	 Important Cette option ne s'applique pas aux systèmes Linux et Mac.
Adresse du serveur DNS	Adresse IP du serveur DNS
Suffixe DNS connexion DHCP	Nom DNS sans nom d'hôte pour une connexion DHCP spécifique Par exemple : hq.company.biz
L'endpoint peut résoudre l'hôte	Nom d'hôte. Par exemple : fileserv.company.biz

Type	Valeur
L'endpoint peut se connecter à GravityZone	Oui/Non
Type de réseau	Sans fil/Ethernet Lorsque vous choisissez le sans-fil, vous pouvez aussi ajouter le SSID réseau.  Important Cette option ne s'applique pas aux systèmes Linux et Mac.
Nom d'hôte	Nom d'hôte Par exemple : <code>cmp.bitdefender.com</code>  Important Vous pouvez également utiliser des caractères génériques. L'astérisque (*) remplace un ou plusieurs caractères tandis que le point d'interrogation (?) remplace exactement un caractère. Exemples : <code>*.bitdefender.com</code> <code>cmp.bitdefend??.com</code>

- b. Saisissez la valeur du type sélectionné. Là où c'est possible, vous pouvez saisir plusieurs valeurs dans le champs dédié, séparées par un point-virgule (;) et sans espaces supplémentaires. Par exemple, lorsque vous saisissez `10.10.0.0/16;192.168.0.0/24`, la règle s'applique à l'endpoint cible dont l'IP correspond à n'importe lequel de ces sous-réseaux.

**Avertissement**

Vous ne pouvez utiliser qu'un seul type de paramètre réseau par règle d'emplacement. Par exemple, si vous ajoutez un emplacement avec le **préfixe IP/réseau**, vous ne pouvez pas réutiliser ce paramètre dans la même règle.

c. Cliquez sur le bouton **+** **Ajouter** à droite du tableau.

Les paramètres réseau sur les endpoints doivent correspondre à tous les emplacements fournis, pour que la règle s'applique. Par exemple, pour identifier le réseau LAN du bureau vous pouvez passer par la passerelle, le type de réseau et le DNS ; de plus, si vous ajoutez un sous-réseau, vous identifiez un département dans le LAN de la société.

Type	Valeur	Actions p...
Préfixe de réseau/IP	10.10.0.0/16;192.168.0.0/24	X
Adresse de la passerelle	10.10.0.1;192.168.0.1	X

Règle de localisation


Cliquez sur le champ **Valeur** pour modifier les critères existants, puis appuyez sur **Entrée** pour enregistrer les modifications.

Pour effacer un emplacement, sélectionnez-le et cliquez sur le bouton **X** **Supprimer**.

5. Vous souhaitez peut être exclure certains emplacements de la règle. Pour créer une exclusion, définissez les emplacements à exclure de la règle :
 - a. Sélectionnez la case **Exclusions** dans le tableau Emplacements.
 - b. Sélectionnez le type de paramètres réseau dans le menu en haut du tableau Exclusions. Pour plus d'informations sur les options, reportez-vous au « [Configuration des règles d'emplacement](#) » (p. 231).
 - c. Saisissez la valeur du type sélectionné. Vous pouvez saisir plusieurs valeurs dans le champs dédié, séparées par un point-virgule (;) et sans espaces supplémentaires.
 - d. Cliquez sur le bouton **+** **Ajouter** à droite du tableau.

Les paramètres réseaux sur les endpoints doivent remplir toutes les conditions fournies dans le tableau Exclusions pour que l'exclusion soit effective.

Cliquez sur le champ **Valeur** pour modifier les critères existants, puis appuyez sur **Entrée** pour enregistrer les modifications.

Pour supprimer une exclusion, cliquez sur le bouton  **Supprimer** à droite du tableau.

6. Cliquez sur **Enregistrer** pour sauvegarder la règle d'affectation et l'appliquer. Une fois créée, la règle emplacement s'applique automatiquement à tous les endpoints cibles gérés.

Configurer de règles utilisateur



Important

- Vous pouvez créer des règles d'utilisateur si une intégration à Active Directory est disponible.
- Vous pouvez définir des règles utilisateur pour les utilisateurs d'Active Directory et pour les groupes. Les règles basées sur les groupes Active Directory ne sont pas supportées par les systèmes Linux.

Dans la fenêtre de configuration de règle, suivez ces étapes :

1. Indiquez un nom et une description explicites pour la règle que vous souhaitez créer.
2. Configurez la priorité. Les règles sont classées par ordre de priorité, la première ayant la plus élevée. La même priorité ne peut être accordée deux fois ou plus.
3. Sélectionnez la politique pour laquelle vous créez la règle d'affectation.
4. Dans la rubrique **Cibles** sélectionnez les groupes d'utilisateurs et de sécurité auxquels vous voulez que la règle s'applique. Vous pouvez afficher votre sélection dans le tableau à droite.
5. Cliquez sur **Enregistrer**.

Une fois créée, la règle liée à l'utilisateur s'applique aux endpoint gérés cibles au moment de la connexion de l'utilisateur.

Configurer les règles de tag



Important

- Vous pouvez créer des règles de tag uniquement si une intégration Amazon EC2 ou Microsoft Azure est disponible.

Vous pouvez utiliser les tags définis dans les infrastructures cloud pour assigner une politique GravityZone spécifique à vos machines virtuelles hébergées dans le

cloud. Toutes les machines virtuelles dont les tags sont spécifiés dans la règle de tag seront appliquées avec la politique définie par la règle.



Note

D'après l'infrastructure cloud, vous pouvez définir les tags de la machine virtuelle comme suit :

- Pour Amazon EC2 : à partir de l'onglet **Tags** de l'instance EC2.
- Pour Microsoft Azure : à partir de la section **Présentation** de la machine virtuelle.

Une règle de tag peut contenir un ou plusieurs tags. Pour créer une règle de tag :

1. Indiquez un nom et une description explicites pour la règle que vous souhaitez créer.
2. Configurez la priorité de la règle. Les règles sont classées par ordre de priorité, la première ayant la plus élevée. La même priorité ne peut être accordée deux fois ou plus.
3. Sélectionnez la politique pour laquelle vous souhaitez créer la règle de tag.
4. Dans le tableau **Tag**, ajoutez un ou plusieurs tags.

Un tag consiste en une combinaison clé-valeur sensible à la casse. Assurez-vous de saisir les tags tels qu'ils sont définis dans votre infrastructure cloud. Seules les combinaisons clé-valeur valides seront prises en compte.

Pour ajouter un tag :

- a. Dans le champ **Clé du tag**, saisissez le nom de la clé.
- b. Dans le champ **Valeur du tag**, saisissez le nom de la valeur.
- c. Cliquez sur le bouton **+ Ajouter** à droite du tableau.

Affecter des politiques NSX

Dans NSX, les politiques de sécurité sont affectées aux groupes de sécurité. Un groupe de sécurité peut contenir plusieurs objets vCenter variés, tels que des datacenters, des clusters et des machines virtuelles.

Pour affecter une politique de sécurité à un groupe de sécurité :

1. Connectez-vous à vSphere Web Client.
2. Allez dans l'onglet **Réseau & Sécurité > Service Composer** puis cliquez sur l'onglet **Groupes de sécurité**.

3. Créez autant de groupes de sécurité que nécessaire. Pour plus d'informations, veuillez vous référer à la [documentation VMware](#).
Vous pouvez créer des groupes de sécurité dynamiques, selon les tags de sécurité. Ainsi, vous pouvez grouper toutes les machines virtuelles infectées.
4. Cliquez droit sur le groupe de sécurité qui vous intéresse puis cliquez sur **Appliquer Politique**.
5. Sélectionnez la politique à appliquer puis cliquez sur **OK**.

7.1.3. Modification des paramètres de la politique

Les paramètres de la politique peuvent être configurés lors de sa création. Vous pouvez ensuite les modifier selon vos besoins à tout moment.



Note

Par défaut, seul l'utilisateur qui a créé la politique peut la modifier. Pour changer cela, le propriétaire de la politique doit cocher l'option **Autoriser d'autres utilisateurs à modifier cette politique** à partir de la page **Détails** de la politique.

Pour modifier les paramètres d'une politique existante :

1. Allez sur la page **Politiques**.
2. Choisissez le type d'endpoint de votre choix dans le [sélecteur d'affichage](#).
3. Recherchez la politique dans la liste et cliquez sur son nom pour la modifier.
4. Configurez les paramètres de la politique selon vos besoins. Pour plus d'informations, reportez-vous à :
 - [« Politiques des ordinateurs et machines virtuelles » \(p. 239\)](#)
 - [« Politiques des appareils mobiles » \(p. 401\)](#)
5. Cliquez sur **Enregistrer**.

Les politiques sont envoyées aux objets du réseau cibles, immédiatement après la modification des attributions ou après la modification des paramètres. Les paramètres devraient être appliqués aux objets du réseau en moins d'une minute (à condition qu'ils soient en ligne). Si un objet du réseau n'est pas en ligne, les paramètres seront appliqués dès qu'il sera de nouveau en ligne.

7.1.4. Renommer des politiques

Les politiques doivent porter des noms explicites afin que vous, ou un autre administrateur, puissiez les identifier rapidement.

Pour renommer une politique :

1. Allez sur la page **Politiques**.
2. Choisissez le type d'endpoint de votre choix dans le [sélecteur d'affichage](#).
3. Cliquez sur le nom de la politique. Cela ouvrira la page de la politique.
4. Indiquez un nouveau nom de politique.
5. Cliquez sur **Enregistrer**.

i Note

Le nom de la politique est unique. Vous devez saisir un nom différent pour chaque nouvelle politique.

7.1.5. Suppression de politiques

Si vous n'avez plus besoin d'une politique, supprimez-la. Une fois la politique supprimée, les objets du réseau auxquels elle s'appliquait se verront attribuer la politique du groupe parent. Si aucune autre politique ne s'applique, la politique par défaut sera finalement appliquée. Lors de la suppression d'une politique contenant des rubriques héritées d'autres politiques, les paramètres des rubriques héritées sont stockés dans les politiques enfants.


i Note

Par défaut, seul l'utilisateur qui a créé la politique peut la supprimer. Pour changer cela, le propriétaire de la politique doit cocher l'option **Autoriser d'autres utilisateurs à modifier cette politique** à partir de la page **Détails** de la politique.

Pour pouvoir supprimer une politique NSX de GravityZone Control Center, vous devez vous assurer que la politique n'est pas utilisée. Ainsi, affectez le groupe de sécurité cible avec un autre profil de sécurité. Pour plus d'informations, reportez-vous à « [Affecter des politiques NSX](#) » (p. 236).

Pour supprimer une politique :

1. Allez sur la page **Politiques**.
2. Choisissez le type d'endpoint de votre choix dans le [sélecteur d'affichage](#).

3. Cochez la case de la politique que vous souhaitez supprimer.
4. Cliquez sur le bouton  **Supprimer** en haut du tableau. Vous devrez confirmer votre action en cliquant sur **Oui**.

7.2. Politiques des ordinateurs et machines virtuelles

Les paramètres de la politique peuvent être configurés lors de sa création. Vous pouvez ensuite les modifier selon vos besoins à tout moment.

Pour configurer les paramètres d'une politique :

1. Allez sur la page **Politiques**.
 2. Sélectionnez **Ordinateur / Machine virtuelle** dans le sélecteur d'affichage.
 3. Cliquez sur le nom de la politique. Cela ouvrira la page des paramètres de la politique.
 4. Configurez les paramètres de la politique selon vos besoins. Les paramètres sont organisés dans les sections suivantes :
 - [Généraux](#)
 - [HVI](#)
 - [Antimalware](#)
 - [Sandbox Analyzer](#)
 - [Pare-feu](#)
 - [Protection du réseau](#)
 - [Gestion des correctifs](#)
 - [Contrôle des applications](#)
 - [Contrôle des appareils](#)
 - [Relais](#)
 - [Protection Exchange](#)
 - [Chiffrement de disque](#)
 - [NSX](#)
 - [Protection de stockage](#)
- Naviguez dans les sections à l'aide du menu situé à gauche de la page.
5. Cliquez sur **Enregistrer** pour enregistrer les modifications et les appliquer aux ordinateurs cibles. Pour quitter la page de la politique sans enregistrer les modifications, cliquez sur **Annuler**.

**Note**

Pour apprendre à travailler avec les politiques, reportez-vous à « [Administration des politiques](#) » (p. 224).

7.2.1. Généraux

Les paramètres généraux vous aident à gérer les options d'affichage de l'interface utilisateur, la protection par mot de passe, les paramètres du proxy, les paramètres Power User, les options de communication et les préférences en matière de mise à jour des endpoints cibles.

Les paramètres sont organisés dans les sections suivantes :

- [Détails](#)
- [Notifications](#)
- [Réglages](#)
- [Communication](#)
- [Mise à jour](#)

Détails

La page **Détails** présente des informations générales sur la politique :

- Nom de la politique
- L'utilisateur qui a créé la politique
- La date et l'heure auxquelles la politique a été créée
- La date et l'heure de la dernière modification de la politique

Détails de la politique	
Nom: *	special
<input type="checkbox"/>	Autoriser d'autres utilisateurs à modifier cette politique
Historique	
Créé par :	Admin
Créé le :	28 oct 2014, 22:52:41
Modifié le :	28 déc 2014, 22:15:08

Politiques des ordinateurs et machines virtuelles

Vous pouvez renommer la politique en indiquant le nouveau nom dans le champ correspondant et en cliquant sur le bouton **Enregistrer** en bas de la page. Les politiques doivent porter des noms explicites afin que vous, ou un autre administrateur, puissiez les identifier rapidement.




Note

Par défaut, seul l'utilisateur qui a créé la politique peut la modifier. Pour changer cela, le propriétaire de la politique doit cocher l'option **Autoriser d'autres utilisateurs à modifier cette politique** à partir de la page **Détails** de la politique.

Règles d'héritage

Vous pouvez configurer des rubriques devant être héritées d'autre politiques. Pour ce faire :

1. Sélectionnez le module et la rubrique dont vous souhaitez que la politique hérite. Toutes les rubriques peuvent être héritées, sauf **Détails > Généraux**.
2. Spécifiez la politique dont vous souhaitez hériter de la rubrique.
3. Cliquez sur le bouton  **Ajouter** à droite du tableau.

Si une politique source supprimée, le principe d'héritage est rompu et les paramètres des rubriques héritées sont stockées dans la politique enfant.

Les rubriques héritées ne peuvent pas être héritées par d'autres politiques. Considérez l'exemple suivant :

La politique A hérite de la rubrique **Antimalware > à la Demande** de la politique B. La politique C ne peut pas hériter de la rubrique **Antimalware > à la Demande** de la politique A.

Informations de support technique

Vous pouvez personnaliser le support technique et les informations de contact disponibles dans la fenêtre **À propos de** de l'agent de sécurité en complétant les champs correspondants.

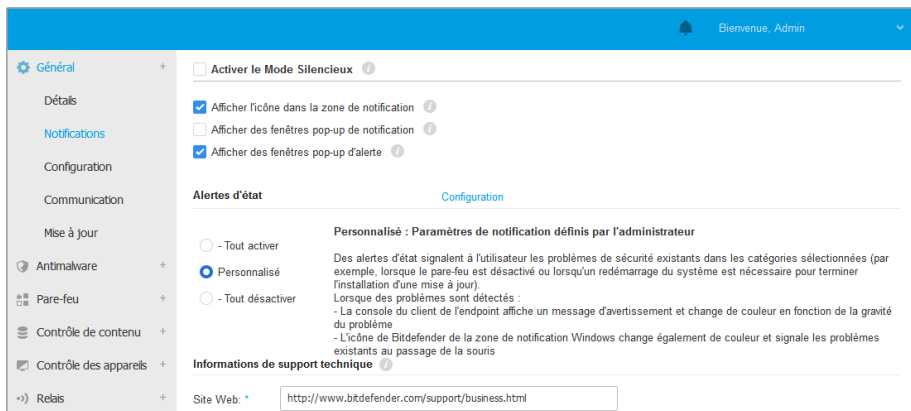
Pour configurer une adresse e-mail dans la fenêtre **A propos** de sorte qu'elle ouvre l'application de messagerie par défaut du endpoint, vous devez l'ajouter dans le champ **Email** avec le préfixe « mailto: ». Exemple : `mailto: nom@domaine.com`.

Les utilisateurs peuvent accéder à ces informations à partir de la console de l'agent de sécurité en faisant un clic droit sur l'icône Bitdefender **B** de la zone de notification et en sélectionnant **À propos de**.

Notifications

Dans cette section, vous pouvez configurer les options d'affichage de l'interface utilisateur de l'agent de sécurité de Bitdefender de façon complète et intuitive.

D'un seul clic, vous pouvez activer ou désactiver toute une catégorie de notifications et ne conserver que ce qui vous importe réellement. De plus, sur la même page, vous pouvez contrôler intégralement la visibilité des problèmes liés aux endpoints.



Politiques - Paramètres d'affichage

- **Mode Silencieux.** Utilisez cette case pour activer ou désactiver le Mode Silencieux. Le Mode Silencieux est conçu pour vous aider à désactiver facilement l'interaction de l'utilisateur dans l'agent de sécurité. Lorsque le Mode Silencieux est activé, les modifications suivantes sont apportées à la configuration de la politique :
 - Les options **Afficher l'icône dans la zone de notification**, **Afficher les fenêtres pop-up de notification** et **Afficher les fenêtres pop-up d'alertes** seront désactivées dans cette section.
 - Si le **niveau de protection du pare-feu** a été réglé sur **Ensemble de règles et demander** ou sur **Ensemble de règles, fichiers connus et demander**, il passera à **Ensemble de règles, fichiers connus et autoriser**. Sinon, le paramètre niveau de protection demeurera inchangé.
- **Afficher l'icône dans la zone de notification.** Sélectionnez cette option pour afficher l'icône de Bitdefender **B** dans la zone de notification (également

appelée barre d'état système). L'icône informe les utilisateurs de leur état de protection en modifiant son apparence et en affichant une fenêtre pop-up de notification. Les utilisateurs peuvent également faire un clic droit dessus et ouvrir rapidement la fenêtre principale de l'agent de sécurité ou la fenêtre **À propos de**.

- **Afficher des fenêtres pop-up d'alerte.** Des fenêtres pop-up d'alerte informent les utilisateurs des événements de sécurité nécessitant une intervention de leur part. Si vous choisissez de ne pas afficher de pop-up d'alerte, l'agent de sécurité applique automatiquement l'action recommandée. Les pop-ups sont générés dans les situations suivantes :
 - Si le pare-feu est configuré pour demander à l'utilisateur quelle action effectuer lorsque des applications inconnues demandent l'accès au réseau ou Internet.
 - Si Advanced Threat Control / le système de détection d'intrusion est activé lorsqu'une application potentiellement dangereuse est détectée.
 - Si l'analyse des périphériques est activée elle se lancera à chaque fois qu'un périphérique est connecté au PC. Vous pouvez configurer ce paramètre dans la section **Antimalware > A la demande**
- **Afficher des fenêtres pop-up de notification.** Distinctes des fenêtres pop-up d'alerte, les fenêtres pop-up de notification informent les utilisateurs de divers événements de sécurité. Les fenêtres pop-up disparaissent automatiquement après quelques secondes sans intervention de l'utilisateur.

Sélectionnez **Afficher les fenêtres pop-up de notification**, puis cliquez sur le lien **Affichez les paramètres modulaires** afin de choisir les événements dont vous souhaitez que les utilisateurs soient informés, fournis par module. Il existe trois types de fenêtres pop-up de notification, en fonction de la gravité des événements :

- **Informations.** Les utilisateurs sont informés des événements de sécurité importants mais ne présentant pas de danger. Par exemple, une application qui s'est connectée à Internet.
- **Faible.** Les utilisateurs sont informés des événements de sécurité pouvant nécessiter leur attention. Par exemple, l'Analyse à l'accès a détecté une menace et le fichier a été supprimé ou placé en quarantaine.
- **Critique.** Ces fenêtres pop-up de notification informent les utilisateurs de situations dangereuses. Par exemple, l'Analyse à l'accès a détecté une

menace et l'action par défaut est **Ne rien faire**, le malware est donc encore présent sur le endpoint, ou bien un processus de mise à jour n'a pas pu s'achever.

Sélectionnez la case associée au nom du type pour activer ce type de fenêtres pop-up pour tous les modules à la fois. Cochez les cases associées à des modules individuels afin d'activer ou de désactiver des notifications spécifiques.

La liste des modules peut varier en fonction de votre licence.

- **Visibilité problèmes endpoint.** Les utilisateurs sont informés que leur poste de travail présente des problèmes de configuration de la sécurité grâce aux alertes d'état. Les utilisateurs peuvent par exemple voir les problèmes liés à leur protection antimalware comme la désactivation du module d'analyse à l'accès ou un retard de l'analyse complète du système. Les utilisateurs sont informés de l'état de leur protection de deux façons :
 - En vérifiant la zone d'état de la fenêtre principale, qui affiche un message d'état approprié et change de couleur en fonction de la gravité des problèmes de sécurité. Les utilisateurs peuvent également consulter les problèmes en détail, en cliquant sur le bouton correspondant.
 - En vérifiant l'icône Bitdefender **B** de la barre d'état système, dont l'aspect change lorsque des problèmes sont détectés.

L'agent de sécurité de Bitdefender utilise les couleurs suivantes pour la zone de notification :

- Vert : aucun problème n'est détecté.
- Jaune : L'endpoint présente des problèmes non critiques affectant sa sécurité. Les utilisateurs n'ont pas à interrompre leur travail pour régler ces problèmes.
- Rouge : le poste de travail présente des problèmes critiques requérant une action immédiate de l'utilisateur.

Sélectionnez **Visibilité des problèmes liés aux endpoints**, puis cliquez sur le lien **Afficher les paramètres modulaires** afin de personnaliser les alertes d'état affichées sur l'interface utilisateur de l'agent de Bitdefender.

Pour chaque module, vous pouvez choisir d'afficher l'alerte en tant qu'avertissement ou en tant que problème critique, ou bien de ne pas l'afficher du tout. Les options sont décrites ci-après :

- **Général.** L'alerte d'état est générée lorsqu'un redémarrage du système est requis pendant ou après l'installation du produit, ainsi que lorsque l'agent de sécurité n'a pas pu se connecter aux Services Cloud de Bitdefender.
- **Antimalware.** Les alertes d'état sont générées dans les situations suivantes :
 - L'analyse à l'accès est activée mais de nombreux fichiers locaux sont ignorés.
 - Un certain nombre de jours se sont écoulés depuis la dernière analyse complète du système sur la machine.
Vous pouvez choisir l'affichage des alertes et définir le nombre de jours maximal sans analyse complète du système.
 - Un redémarrage est nécessaire pour terminer un processus de désinfection.
- **Pare-feu.** Cette alerte d'état est générée lorsque le module Pare-feu est désactivé.
- **Contrôle des applications.** Cette alerte d'état est générée lorsque le module Contrôle des application est modifié.
- **Contrôle de contenu.** Cette alerte d'état est générée lorsque le module Contrôle de contenu est désactivé.
- **Mise à jour.** Cette alerte d'état est générée lorsqu'un redémarrage du système est requis pour terminer une opération de mise à jour.
- **Notification de redémarrage de l'endpoint.** Cette option affiche une alerte de redémarrage sur l'endpoint chaque fois qu'un redémarrage du système est nécessaire en raison de modifications apportées à l'endpoint par les modules GravityZone sélectionnés au titre des paramètres modulaires.



Note

Les endpoints nécessitant un redémarrage du système sont identifiés par une icône de statut spécifique () dans l'inventaire de GravityZone.

Vous pouvez personnaliser les alertes de redémarrage en cliquant sur **Afficher paramètres modulaires**. Voici les options proposées :

- **Mettre à jour** - Sélectionnez cette option pour activer les notifications de redémarrage pour la mise à jour de l'agent.

- **Patch Management** - Sélectionnez cette option pour activer les notifications de notification de redémarrage pour l'installation de patch.



Note

Vous pouvez également un délai maximum de report du redémarrage par l'utilisateur. Pour cela, sélectionnez **Redémarrer automatiquement la machine après** et saisissez une valeur comprise entre 1 et 46.

L'alerte de redémarrage nécessite que l'utilisateur entreprenne l'une des actions suivantes :

- **Redémarrer maintenant.** Dans ce cas, le système redémarrera immédiatement.
- **Reporter le redémarrage.** En ce cas, une notification de redémarrage apparaîtra régulièrement à l'écran jusqu'à ce que l'utilisateur redémarrage le système ou que le délai défini par l'administrateur de la société expire.

Réglages

Cette section vous permet de configurer les paramètres suivants :

- **Configuration du mot de passe.** Pour empêcher que les utilisateurs avec des droits d'administration ne désinstallent la protection, vous devez définir un mot de passe.

Le mot de passe de désinstallation peut être configuré avant l'installation en personnalisant le package d'installation. Si vous avez procédé ainsi, sélectionnez **Conserver les paramètres d'installation** pour conserver le mot de passe actuel.

Pour définir le mot de passe, ou pour modifier le mot de passe actuel, sélectionnez **Activer le mot de passe** et saisissez le mot de passe souhaité. Pour supprimer la protection par mot de passe, sélectionnez **Désactiver le mot de passe**.

- **Configuration du proxy**

Si votre réseau se trouve derrière un serveur proxy, vous devez définir les paramètres du proxy qui permettront à vos endpoints de communiquer avec les composants de la solution GravityZone. Vous devez dans ce cas activer l'option **Configuration du proxy** et complétez les paramètres requis :

- **Serveur** - saisissez l'adresse IP du serveur proxy
- **Port** - saisissez le port utilisé pour se connecter au serveur proxy.
- **Nom d'utilisateur** - indiquez un nom d'utilisateur reconnu par le serveur proxy.

- **Mot de passe** - indiquez le mot de passe valide de l'utilisateur spécifié

- **Power User**

Le module Power User fournit des droits d'administration au niveau de l'endpoint, permettant à l'utilisateur de l'endpoint d'accéder et de modifier les paramètres de la politique via une console locale et à travers l'interface Bitdefender Endpoint Security Tools.

Si vous souhaitez que certains endpoints disposent de droits Power User, vous devez d'abord inclure ce module dans l'agent de sécurité installé sur les endpoints cibles. Vous devez ensuite configurer les paramètres Power User dans la politique appliquée à ces endpoints :

**Important**

Le module Power User est disponible uniquement pour les systèmes d'exploitation des postes de travail et serveurs Windows pris en charge.

1. Activez l'option **Power User**.
2. Définissez un mot de passe Power User dans les champs ci-dessous.

Les utilisateurs qui accèdent au mode Power User à partir de l'endpoint local devront saisir le mot de passe défini.

Pour accéder au module Power User, les utilisateurs doivent faire un clic droit sur l'icône de Bitdefender **B** de la zone de notification et sélectionner **Power User** dans le menu contextuel. Après avoir indiqué le mot de passe dans la fenêtre de connexion, une console contenant les paramètres de la politique appliquée actuellement apparaîtra, dans laquelle l'utilisateur de l'endpoint peut afficher et modifier les paramètres de la politique.

**Note**

Seules certaines fonctionnalités de sécurité sont accessibles en local via la console Power User, concernant les modules Antimalware, Pare-Feu, Contrôle de Contenu et Contrôle des appareils.

Pour annuler les modifications réalisées en mode Power User :

- Dans Control Center, ouvrez le modèle de politique affecté à l'endpoint avec les droits Power User et cliquez sur **Enregistrer**. Les paramètres d'origine seront ainsi réappliqués à l'endpoint cible.
- Affectez une nouvelle politique à l'endpoint avec les droits Power User.

- Connectez-vous à l'endpoint local, ouvrez la console Power User et cliquez sur **Resync**.

Pour trouver facilement les endpoints ayant des politiques modifiées en mode Power User :

- Sur la page **Réseau**, cliquez sur le menu **Filtres** et sélectionnez l'option **Modifié par le Power User** de l'onglet **Politique**.
- Sur la page **Réseau**, cliquez sur l'endpoint qui vous intéresse pour faire apparaître la fenêtre **Informations**. Si la politique a été modifiée en mode Power User, une notification apparaîtra dans l'onglet **Général** > section **Politique**.



Important

Le module Power User est spécifiquement conçu pour résoudre les problèmes, ce qui permet à l'administrateur réseau d'afficher et de modifier facilement les paramètres de politiques sur les ordinateurs locaux. L'affectation de droits Power User à d'autres utilisateurs de la société doit être limité au personnel autorisé, afin de garantir que les politiques de sécurité soient toujours appliquées à tous les endpoints du réseau de la société.

● Options

Cette section vous permet de définir les paramètres suivants :

- **Supprimer les événements de plus de (jours)**. L'agent de sécurité de Bitdefender tient un journal détaillé des événements concernant son activité sur l'ordinateur (comprenant également les activités surveillées par le Contrôle de contenu). Par défaut, les événements sont supprimés du journal après 30 jours. Si vous souhaitez modifier cet intervalle, choisissez une option différente dans le menu.
- **Envoyer les rapports de plantage à Bitdefender**. Sélectionnez cette option afin que les rapports soient envoyés aux Laboratoires Bitdefender afin d'y être analysés en cas de plantage de l'agent de sécurité. Les rapports aideront nos ingénieurs à découvrir la cause du problème et à éviter qu'il ne se reproduise. Aucune donnée personnelle ne sera envoyée.
- **Soumettre des fichiers exécutables suspects pour analyse**. Sélectionnez cette option afin que les fichiers qui n'ont pas l'air fiables ou qui ont un comportement suspect soient envoyés aux Laboratoires Bitdefender pour analyse.

- **Envoyer les violations de mémoire HVI à Bitdefender.** Par défaut, HVI envoie des informations anonymes aux serveurs cloud de Bitdefender sur les violations détectées, afin de les utiliser à des fins statistiques ou pour améliorer les taux de détection du produit. Vous pouvez décocher cette case si vous ne voulez pas envoyer ces informations depuis votre réseau.

Communication

Cette section vous permet d'affecter une ou plusieurs machines relais aux endpoints cibles, puis de configurer les préférences en matière de proxy pour la communication entre les endpoints cibles et GravityZone.

Affectation des serveurs de communication aux postes de travail

Lorsque plusieurs serveurs de communication sont installés sur l'appliance GravityZone, vous pouvez affecter aux ordinateurs cibles un ou plusieurs serveurs de communication via la politique. Les endpoints relais disponibles, utilisés comme serveurs de communication, sont également pris en compte.

Pour affecter des serveurs de communication aux ordinateurs cibles :

1. Dans le tableau **Affectation des serveurs de communication aux postes de travail**, cliquez sur le champ **Nom**. La liste des serveurs de communication détectés s'affiche.
2. Sélectionnez une entité.

Priorité	ECS (10.10.17.80)	IP	Nom personnalisé/IP
	MASTER-PC		

Politiques des ordinateurs et machines virtuelles - Paramètres de communication

3. Cliquez sur le bouton **+** **Ajouter** à droite du tableau.
Le serveur de communication est ajouté à la liste. Tous les ordinateurs cibles communiqueront avec Control Center via le serveur de communication spécifié.
4. Procédez de la même façon pour ajouter plusieurs serveurs de communication, si possible.
5. Vous pouvez configurer la priorité des serveurs de communication à l'aide des flèches se trouvant à droite de chaque élément. La communication avec les ordinateurs cibles s'effectuera via l'entité se trouvant en haut de la liste. Lorsque la communication avec cet élément ne peut pas être établie, le suivant sera pris en compte.
6. Pour retirer un élément de la liste, cliquez sur le bouton **×** **Supprimer** correspondant à droite du tableau.

Communication entre les endpoints et Le Relais / entre les endpoints et GravityZone

Cette section vous permet de configurer les préférences en matière de proxy pour la communication entre les endpoints cibles et les machines relais affectées, ou entre les endpoints cibles et l'appliance GravityZone (quand aucun relais n'a été affecté) :

- **Conserver les paramètres d'installation**, pour utiliser les mêmes paramètres proxy que ceux du package d'installation.
- **Utiliser le proxy défini dans la section Général**, pour utiliser les paramètres du proxy définis dans la politique actuelle, sous la section **Général > Configuration**.
- **Ne pas utiliser**, lorsque les endpoints cibles ne communiquent pas avec les composants GravityZone spécifiques via proxy.

Communication entre les endpoints et les Services Cloud

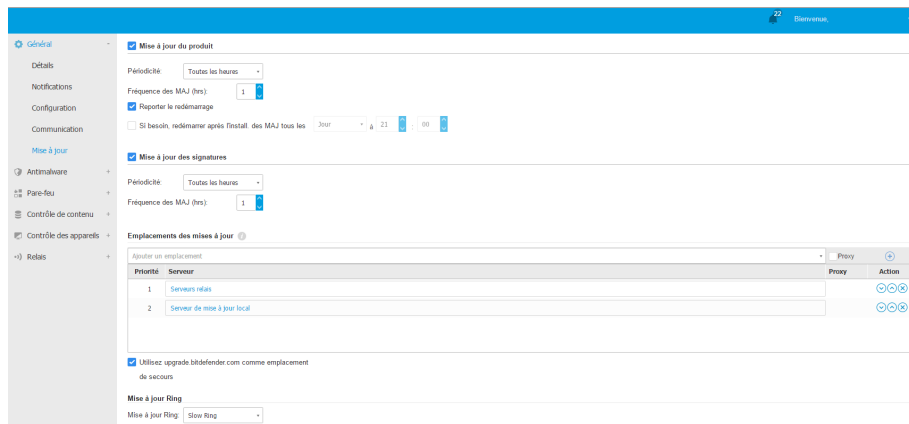
Cette rubrique vous permet de configurer les préférences en matière de proxy pour la communication entre les endpoints cibles et les Services Cloud Bitdefender (nécessitant une connexion à Internet) :

- **Conserver les paramètres d'installation**, pour utiliser les mêmes paramètres proxy que ceux du package d'installation.
- **Utiliser le proxy défini dans la section Général**, pour utiliser les paramètres du proxy définis dans la politique actuelle, sous la section **Général > Configuration**.

- **Ne pas utiliser**, lorsque les endpoints cibles ne communiquent pas avec les composants GravityZone spécifiques via proxy.

Mise à jour

Les mises à jour sont très importantes car elles permettent de contrer les nouvelles menaces. Bitdefender publie l'ensemble des mises à jour de produits et contenus de sécurité, par le biais des serveurs Bitdefender sur Internet. Toutes les mises à jour sont chiffrées et numériquement signées pour qu'elles ne puissent pas être altérées. Lorsqu'une nouvelle mise à jour est disponible, l'agent de sécurité de Bitdefender vérifie la signature numérique de la mise à jour et le contenu du package, afin de contrôler respectivement leur authenticité et leur intégrité. Ensuite, chaque mise à jour est analysée et la nouvelle version est comparée à celle qui est déjà installée. Les fichiers les plus récents sont téléchargés localement et comparés à leur empreinte MD5, afin de s'assurer qu'ils n'ont pas été modifiés. Cette rubrique vous permet de configurer les paramètres de mise à jour des contenus de sécurité et de l'agent de sécurité de Bitdefender.



The screenshot displays the 'Mise à jour' (Updates) configuration page in the Bitdefender GravityZone console. The page is divided into several sections:

- Mise à jour du produit (Product Updates):** Includes a dropdown for 'Périodicité' (All hours), a 'Fréquence des MAJ (hrs)' spinner set to 1, and a checked 'Rapporter le redémarrage' (Report restart) option. There is also an unchecked option for 'Si besoin, redémarrer après l'install. des MAJ tous les' followed by a time picker set to 30m.
- Mise à jour des signatures (Signature Updates):** Similar to the product updates section, with 'Périodicité' set to 'Toutes les heures' and 'Fréquence des MAJ (hrs)' set to 1.
- Emplacements des mises à jour (Update Locations):** A table with columns for 'Priorité' (Priority), 'Serveur' (Server), and 'Action'. It lists two servers: 'Serveurs relais' (Priority 1) and 'Serveur de mise à jour local' (Priority 2).
- Utilisez l'upgrade bitdefender.com comme emplacement de secours (Use bitdefender.com upgrade as backup location):** A checked checkbox.
- Mise à jour Ring:** A dropdown menu currently set to 'Slow Ring'.

Politiques des ordinateurs et machines virtuelles - Options de mise à jour

- **Mise à jour du produit.** L'agent de sécurité de Bitdefender recherche, télécharge et installe automatiquement des mises à jour toutes les heures (configuration par défaut). Les mises à jour automatiques s'effectuent en silence, en tâche de fond.

- **Périodicité.** Afin de changer les mises à jour automatique récurrente, choisissez une option différente à partir du menu et configurez la, en fonction de vos besoins, dans les champs adéquats.
- **Reporter le redémarrage.** Certaines mises à jour requièrent un redémarrage du système pour s'installer et fonctionner correctement. Par défaut, le produit continuera à fonctionner avec les anciens fichiers jusqu'à ce que l'ordinateur soit redémarré. Les dernières mises à jour seront ensuite appliquées. Une notification dans l'interface utilisateur demandera à l'utilisateur de redémarrer le système lorsqu'une mise à jour le nécessite. Il est recommandé de garder le cryptage activé. Autrement, le système redémarrera automatiquement, après avoir installé une mise à jour qui nécessite un redémarrage. Les utilisateurs recevront une notification leur indiquant de sauvegarder leur travail, mais le redémarrage ne pourra pas être annulé.
- Si vous choisissez de reporter un redémarrage, vous pouvez définir une heure qui vous convient, à laquelle les ordinateurs redémarreront automatiquement si besoin. Cela peut être très utile pour les serveurs. Sélectionnez **Redémarrer après l'installation des mises à jour si besoin** et spécifiez quand redémarrer (tous les jours ou toutes les semaines, un certain jour, ou à une certaine heure de la journée).
- **Mise à jour du contenu relatif à la sécurité.** Par contenu de sécurité, on entend tous les moyens dynamiques et statiques de détecter les menaces, tels qu'entre autres les moteurs d'analyse, les modèles de Machine Learning, l'heuristique, les règles, les signatures et les listes noires. L'agent de sécurité de Bitdefender recherche automatiquement les mises à jour du contenu de sécurité, toutes les heures (configuration par défaut). Les mises à jour automatiques s'effectuent en silence, en tâche de fond. Afin de changer les mises à jour automatique récurrente, choisissez une option différente à partir du menu et configurez la, en fonction de vos besoins, dans les champs adéquats.
- **Emplacements des mises à jour.** L'emplacement de mise à jour par défaut de l'agent de sécurité de Bitdefender est le serveur de mise à jour local de GravityZone. Ajouter une mise à jour emplacement soit en choisissant les emplacements prédéfinis dans le menu déroulant, soit en saisissant l'adresse IP ou le nom d'hôte d'un ou plusieurs serveurs mise à jour dans votre réseau. Configurer leur priorité à l'aide des boutons haut/bas s'affichant au passage de la souris. Si le premier emplacement de mise à jour n'est pas disponible, l'on utilise le suivant et ainsi de suite.

Pour configurer une adresse de mise à jour locale :

1. Indiquez l'adresse du serveur de mise à jour dans le champ **Ajouter un emplacement**. Vous pouvez :

– Choisir un emplacement prédéfini :

- **Serveurs relais**. L'endpoint se connectera automatiquement au Serveur relais qui lui est affecté.



Avertissement

Les serveurs Relay ne sont pas pris en charge sur les anciens systèmes d'exploitation. Pour plus d'informations, veuillez vous référer au Guide d'installation.



Note

Vous pouvez voir le Serveur relais affecté dans la fenêtre **Informations**. Pour plus de détails, veuillez vous référer à [Voir détails ordinateur](#).

- **Serveur de mise à jour local**

– Entrez l'adresse IP ou le nom d'hôte d'un ou plusieurs serveurs mise à jour dans votre réseau. Utilisez l'une des syntaxes suivantes :

- `ip_du_serveur_de_mise_à_jour : port`
- `nom_du_serveur_de_mise_à_jour : port`


Le port par défaut est 7074.

La case **Utiliser les serveurs de Bitdefender comme emplacement de secours** est cochée par défaut. Si les emplacements de mise à jour ne sont pas disponibles, les emplacements de secours seront utilisés.



Avertissement

La désactivation des emplacements de secours arrêtera les mises à jour automatiques, laissant votre réseau vulnérable lorsque les emplacements prévus ne sont pas disponibles.

2. Si des ordinateurs clients se connectent au serveur local de mise à jour via un serveur proxy, sélectionnez **Utiliser un proxy**.
3. Cliquez sur le bouton  **Ajouter** à droite du tableau.

- Utilisez les flèches vers le ⬆ Haut / ⬇ et vers le Bas de la colonne **Action** pour définir les emplacements de mise à jour prioritaires. Si le premier emplacement de mise à jour n'est pas disponible, le suivant est pris en compte et ainsi de suite.

Pour retirer un emplacement de la liste, cliquez sur le bouton **Supprimer** correspondant. Bien que vous puissiez supprimer l'emplacement des mises à jour par défaut, cela n'est pas recommandé.

- **Mise à jour Ring.** Vous pouvez déployer des mises à jour de produits en phases, en utilisant la mise à jour des rings :
 - **Slow Ring.** Les machines avec une politique de slow ring recevront des mises à jour à une date ultérieure, en fonction de la réponse reçue d'endpoints fast ring. C'est une mesure de précaution dans le processus de mise à jour. Il s'agit des paramètres par défaut et ils doivent être utilisés pour les machines critiques.
 - **Fast Ring.** Les machines avec une politique fast ring reçoivent les toutes premières mises à jour disponibles. Ce paramètre est recommandé pour les machines non critiques dans l'environnement de production.



Important

- Dans le cas improbable où un problème se produit sur le fast ring sur les machines avec une configuration particulière, il sera corrigé avant la mise à jour du slow ring.
- BEST for Windows Legacy ne permet pas un déploiement par phase. Les anciens endpoints en déploiement par phase doivent être déplacés en production.



Note

Pour plus de détails sur la façon dont la sélection mise à jour des rings affecte le mode pré-production, veuillez vous référer au chapitre **Mise à jour GravityZone > Mode pré-production** du Guide d'installation GravityZone.

7.2.2. HVI



Note

HVI ne fournit de la protection que pour les machines virtuelles dans les hyperviseurs Citrix Xen.

Hypervisor Memory Introspection protège les machines virtuelles des menaces avancées contre lesquelles moteurs basés sur signatures ne peuvent lutter. Cela assure une détection des attaques en temps réel, en surveillant les processus depuis l'extérieur des systèmes d'exploitation. Le mécanisme de protection inclut plusieurs options pour bloquer les attaques au moment où elles surviennent et supprimer la menace immédiatement.

Dans le cadre du principe de séparation de mémoire du système d'exploitation, HVI inclut deux modules de protection organisés dans les catégories suivantes :

- **Espace utilisateur**, concernant les processus normaux des applications utilisateur.
- **Espace noyau**, concernant les processus réservés au noyau du système d'exploitation.

En outre, la politique HVI contient deux fonctionnalités pour vous aider à gérer la sécurité et à assurer que les machines virtuelles restent protégées :

- **Exclusions**, pour voir et gérer les processus exclus de l'analyse.
- **Outils personnalisés**, pour injecter les outils qui sont nécessaires aux activités opérationnelles et forensiques sur les systèmes d'exploitation invités.

Espace utilisateur

Dans cette rubrique, vous pouvez configurer les paramètres de protection pour les processus qui s'exécutent dans l'espace mémoire utilisateur.

Utiliser la case **Introspection mémoire espace utilisateur** pour activer ou désactiver la protection.

La fonctionnalité de ce module s'appuie sur des règles, ce qui vous permet de configurer la protection séparément pour différents groupes de processus. De plus, vous pouvez choisir de collecter davantage de données d'investigation.

- **Règles applicables à l'espace utilisateur**
- **Données d'investigation**

Règles applicables à l'espace utilisateur

Le module contient un nombre de règles prédéfinies concernant les applications les plus vulnérables. Le tableau dans cette rubrique liste les règles existantes, fournissant d'importantes informations sur chacune d'elles :

- Nom de la règle

- Processus auxquels s'applique la règle.
- Mode surveillance
- Action bloquant l'attaque détectée
- Actions pour supprimer la menace

Vous pouvez également fournir une liste de règles personnalisées pour les processus que vous souhaitez surveiller. Pour créer une nouvelle règle :

1. Cliquez sur le bouton **+Ajouter** en haut du tableau. Cette action ouvre la fenêtre de configuration de règle.
2. Configurer le module à l'aide des paramètres de règle suivants :
 - **Nom de la règle** . Indiquez le nom sous lequel la règle figurera dans le tableau des règles. Par exemple, pour les processus tels que `firefox.exe` ou `chrome.exe`, vous pouvez nommer la règle `Navigateurs`.
 - **Processus**. Saisissez les noms de processus que vous souhaitez surveiller, séparés par un point virgule (;).
 - **Mode de surveillance**. Pour une configuration rapide, cliquez sur le niveau de sécurité qui correspond le mieux à vos besoins (**Agressif**, **Normal** ou **Tolérant**). Utilisez la description à droite de l'échelle pour faire votre choix.

Vous pouvez configurer les paramètres du module en détails en choisissant le niveau de protection **Personnalisé** et en sélectionnant l'une ou plusieurs des options suivantes :

- **Les hooks configurés dans les DLL mode utilisateur critiques**. Détecter les injections DLL, qui chargent du code malveillant dans les processus d'appel.
- **Ouverture/déchiffrement des tentatives dans l'exécutable principal**. Détecte les tentatives de déchiffrement de code dans le principal processus exécutable, et protège le processus de toute altération par des instructions malveillantes.
- **Écritures étrangères à l'intérieur du processus cible**. Protège contre l'injection de code dans le processus protégé.
- **Exploits**. Détecte des comportements processus fortuits causés par l'exploitation d'un bug ou d'une vulnérabilité précédemment dévoilée.

Utilisez cette option si vous souhaitez surveiller l'exécution de code à partir du segment de mémoire et de la pile des applications protégées.

- **Raccordement de WinSock.** Bloque les interceptions de bibliothèques réseau (DLL) utilisées par le système d'exploitation, assurant une communication TCP/IP sûre.
- **Actions.** Vous pouvez appliquer plusieurs actions aux menaces détectées. Chaque action dispose également de plusieurs options possibles ou actions secondaires. Voici leur description :
 - **Action principale.** Ceci est l'action immédiate que vous pouvez exécuter lorsqu'une attaque est détectée sur la machine invitée, vous permettant de bloquer l'attaque. Vous avez le choix entre les options suivantes :
 - **Journal.** N'enregistre l'événement que dans la base de données. Dans ce cas vous recevrez simplement une notification (si elles sont configurées) et pourrez voir l'incident dans le rapport **Activités HVI**.
 - **Refus.** Rejet de toute tentative de menace d'altération du processus cible.
 - **Arrêt de la machine.** Arrêt de la machine virtuelle sur laquelle le processus cible s'exécute.



Important

Il est recommandé de définir en premier l'action prioritaire pour **Log**. Puis utilisez la politique pendant un certain temps pour valider que tout fonctionne comme prévu. Ensuite, vous pouvez définir quelle action vous souhaitez réaliser en cas de détection d'une violation de la mémoire.

- **Action de réparation.** Selon l'option sélectionnée, le Security Server injecte un outil de réparation dans le système d'exploitation invité. L'outil commence automatiquement à analyser à la recherche de malwares, et lorsqu'une menace est détectée, il effectue l'action sélectionnée. Vous avez le choix entre les options suivantes :
 - **Désinfection.** Supprimer le code malveillant des fichiers infectés. Nous vous recommandons de toujours la conserver comme première action à appliquer aux fichiers infectés.

- **Suppression.** Supprime les fichiers détectés du disque, sans avertissement. Nous vous recommandons d'éviter d'utiliser cette action.
- **Ignorer.** L'outil de réparation détecte et ne rapporte que les fichiers détectés.
- **Aucun.** L'outil de réparation ne sera pas injecté dans le système d'exploitation invité.

**Note**

La fermeture de l'outil le supprimera également du système, ne laissant aucune trace dans le système d'exploitation invité.

- **Action de réparation de secours.** Lorsque l'action de réparation a échoué, vous pouvez choisir une autre action de réparation dans les options disponibles.

3. Cliquez sur **Enregistrer**.

Une fois créée, vous pouvez modifier une règle à tout moment. Cliquez sur le nom de la règle va ouvrir la fenêtre de configuration de la règle.

GravityZone vous permet également de configurer rapidement le comportement d'Introspection mémoire après détection, en changeant plusieurs règles en même temps. Pour configurer plusieurs règles avec les mêmes actions :

1. Sélectionnez les règles que vous souhaitez modifier.
2. Cliquez sur le bouton **Action et réparation** en haut du tableau.
3. Sélectionnez l'option que vous voulez pour chaque action :
4. Cliquez sur **Enregistrer**. Les nouvelles actions vont devenir effectives une fois que vous aurez enregistré la politique, pourvu que les machines cibles soient connectées à Internet.

Pour retirer une ou plusieurs règle de la liste, sélectionnez-les puis cliquez sur le bouton **Supprimer** en haut du tableau.

Données d'investigation

Cochez la case **Évènements liés au plantage des applications** située sous le tableau des règles de l'espace utilisateur afin de permettre la collecte d'informations détaillées en cas de fermeture inopinée des applications.

Vous pouvez visualiser cette information dans le Rapport d'activité HVI et trouver la raison qui a provoqué la fermeture inopinée de l'application. Dans le cas où l'évènement serait lié à une attaque, les informations s'y rattachant apparaîtraient regroupées avec celles d'autres évènements sous l'incident correspondant ayant conduit à l'évènement.

Espace noyau

HVI protège les éléments clés du système d'exploitation, tels que :

- Les pilotes de noyaux critiques et les objets de pilotes liés, impliquant des tableaux de répartition rapide I/O associés aux pilotes noyaux.
- Les pilotes réseau, dont les altérations pourraient permettre à un malware d'intercepter du trafic et d'injecter des composants malveillants dans le flux du trafic.
- L'image noyau du système d'exploitation, impliquant : la section de code, la section de données et la section lecture seule, dont le Import Address Table (IAT), Export Address Table (EAT) et les ressources.

Dans cette rubrique, vous pouvez configurer les paramètres de protection pour les processus qui s'exécutent dans l'espace mémoire noyau.

Utiliser la case **Introspection mémoire espace noyau** pour activer ou désactiver la protection.

Pour une configuration rapide, cliquez sur le niveau de sécurité qui correspond le mieux à vos besoins (**Agressif**, **Normal** ou **Tolérant**). Utilisez la description à droite de l'échelle pour faire votre choix.

Vous pouvez configurer les paramètres du module en détails en choisissant le niveau de protection **Personnalisé** et en sélectionnant l'une ou plusieurs des options suivantes :

- **Control registers.** Les Control Registers (RC) sont des registres processeurs qui contrôlent le comportement général d'un processeur ou d'un autre appareil numérique. Sélectionnez cette option pour détecter des tentatives de chargement de valeurs non valides dans des Control Registers spécifiques.
- **Model Specific Registers.** Ces registres font référence à n'importe lequel des Control Registers variés dans les instructions x86 concernant le débogage, le traçage de programmes d'exécution, la surveillance de la performance de l'ordinateur, et la manipulation de certaines fonctionnalités CPU. Sélectionnez cette option pour détecter les tentatives de modification de ces registres.

- **Intégrité IDT/GDT** . Les tableaux Global ou Interrupt Descriptor (IDT/GDT) sont utilisés par le processeur pour déterminer la bonne attitude à avoir face aux interruptions et exceptions. Sélectionnez cette option pour détecter toute tentative de modification de ces tableaux.
- **Protection antimalware pour pilotes**. Sélectionnez cette option pour détecter les tentatives de modification de pilotes utilisés par des logiciels antimalwares.
- **Protection pour pilotes Xen**. Sélectionnez cette option pour détecter les tentatives de modification de l'hyperviseur Citrix XenServer.

Vous pouvez appliquer plusieurs actions aux menaces détectées. Chaque action dispose également de plusieurs options possibles ou actions secondaires. Voici leur description :

- **Action principale.**

- **Journal**. N'enregistre l'événement que dans la base de données. Dans ce cas vous recevrez simplement une notification (si elles sont configurées) et pourrez voir l'incident dans le rapport **Activités introspection mémoire**.
- **Refus**. Rejet de toute tentative de menace d'altération du processus cible.
- **Arrêt de la machine**. Arrêt de la machine virtuelle sur laquelle le processus cible s'exécute.



Important

Il est recommandé de définir en premier l'action prioritaire pour **Log**. Puis utilisez la politique pendant un certain temps pour valider que tout fonctionne comme prévu. Ensuite, vous pouvez définir quelle action vous souhaitez réaliser en cas de détection d'une violation de la mémoire.

- **Action de réparation.**

- **Désinfection**. Supprimer le code malveillant des fichiers infectés. Nous vous recommandons de toujours la conserver comme première action à appliquer aux fichiers infectés.
- **Suppression**. Supprime les fichiers détectés du disque, sans avertissement. Nous vous recommandons d'éviter d'utiliser cette action.
- **Ignorer**. L'outil de réparation détecte et ne rapporte que les fichiers détectés.
- **Aucun**. L'outil de réparation ne sera pas injecté dans le système d'exploitation invité.

- **Action de réparation de secours.** Lorsque l'action de réparation a échoué, vous pouvez choisir une autre action de réparation dans les options disponibles.

De plus, vous pouvez choisir de recueillir des informations qui enrichiront les données fournies aux équipes d'investigation. Cochez les cases **Évènements liés à des défaillances du système d'exploitation** et **Évènements liés à des pilotes** afin de permettre la collecte d'informations relatives à des défaillances du système d'exploitation invité ou à des évènements générés par des modules supplémentaires chargés par le système d'exploitation. Ces évènements, qui précèdent un incident, aideront les investigations informatiques à déterminer plus rapidement la source de l'attaque.

Ces évènements sont compilés dans le Rapport d'activité HVI, sous l'incident qui a conduit à ceux-ci.

Exclusions

GravityZone vous permet d'exclure des processus de l'analyse HVI, en utilisant les rapports **Applications bloquées** et **Activité HVI**. La section **Exclusions** regroupe tous les processus des rapports mentionnés et les affiche sous forme de tableau.

Pour chaque processus exclu, vous pouvez voir un commentaire avec la raison de l'exclusion.

Si vous changez d'avis à propos d'un processus exclu, cliquez sur le bouton **Supprimer** en haut du tableau pour l'ajouter aux analyses futures.

Outils Personnalisés

Dans cette section, vous pouvez configurer l'injection d'outils dans les systèmes d'exploitation invités cibles. Ces outils doivent être envoyés à GravityZone avant de pouvoir les utiliser. Pour plus d'informations, reportez-vous à « [Injection d'outils personnalisés avec HVI](#) » (p. 496).

Pour configurer les injections :

1. Utilisez la case **Activer les injections** pour activer ou désactiver la fonctionnalité.
2. Cliquez sur le bouton **+** **Ajouter** en haut du tableau pour ajouter un nouvel outil. Une fenêtre de configuration s'affiche.
3. Sélectionnez l'outil que vous voulez utiliser dans le menu déroulant **Choisir un outil**.

Ces outils étaient auparavant envoyés dans GravityZone. Si vous ne trouvez pas le bon outil dans la liste, rendez-vous dans le **Centre de gestion des outils** et ajoutez-le. Pour plus d'informations, reportez-vous à « [Injection d'outils personnalisés avec HVI](#) » (p. 496).

4. Dans **Description de l'outil**, saisissez l'utilisation prévue de l'outil ou toute autre information utile.
5. Saisissez la ligne de commande de l'outil, avec tous les paramètres nécessaires, exactement comme vous le feriez sur le terminal ou l'invite de commande. Par exemple :

```
bash script.sh <param1> <param2>
```

Pour les outils de réparation BD, vous ne pouvez sélectionner que l'action de réparation et l'action de réparation de secours dans les menus déroulants.

6. Indiquez l'endroit depuis lequel Security Server doit collecter les journaux :
 - **stdout**. Sélectionnez les cases à cocher pour capturer les journaux du canal standard de communication de sortie.
 - **Fichier de sortie**. Cochez cette case pour collecter le fichier journal enregistré sur l'endpoint. Dans ce cas, vous devez saisir un emplacement où Security Server peut trouver le fichier. Vous pouvez utiliser des chemins absolus ou des variables du système.

Vous disposez ici de deux options supplémentaires :

 - a. **Supprimer les fichiers journal de l'invité après les avoir transférés**. Sélectionnez cette option si vous n'avez plus besoin des fichiers sur l'endpoint.
 - b. **Transférer les journaux vers**. Sélectionnez cette option pour déplacer les fichiers journaux de Security Server vers un autre emplacement. Dans ce cas, vous devez fournir le chemin de l'emplacement de destination et les identifiants d'authentification.
7. Sélectionner comment l'injection sera déclenchée. Vous disposez des options suivantes :
 - **après qu'une violation a été détectée sur une machine virtuelle invitée**. L'outil est injecté dès qu'une menace est détectée sur la machine virtuelle.

- **selon un planning spécifique.** Utilisez les options de planification pour configurer un calendrier d'injection. Vous pouvez choisir d'exécuter l'outil de manière régulière, à partir d'une date et d'une heure spécifiées.

Gardez à l'esprit que la machine virtuelle doit être allumée au moment de la planification. Une injection planifiée ne s'exécutera pas si la machine est éteinte ou en pause. Dans de telles situations, il est recommandé de cocher la case **Si le moment de l'injection planifiée a été manqué, exécuter la tâche dès que possible.**

- L'outil peut parfois nécessiter plus de temps que prévu pour réaliser sa tâche ou peut ne pas répondre. Pour éviter les crashes dans de telles situations, dans la section **Configuration de la sécurité**, choisissez après combien d'heures Security Server doit terminer automatiquement le processus.
- Cliquez sur **Enregistrer**. L'outil sera ajouté dans le tableau.

Vous pouvez ajouter autant d'outils que nécessaire en suivant les étapes susmentionnées.

7.2.3. Antimalware



Note

Ce module est disponible pour :

- Windows pour postes de travail
- Windows pour serveurs
- Linux
- macOS

Le module Antimalware protège le système contre tous les types de malwares (virus, chevaux de Troie, spywares, rootkits, adwares, etc.). La protection est divisée en trois catégories :

- Analyse à l'accès : empêche les nouvelles menaces d'infecter le système.
- Analyse à l'exécution : protection proactive contre les menaces.
- Analyse à la demande : permet de détecter et de supprimer les logiciels malveillants déjà présents dans le système.

Lorsqu'il détecte un virus ou un autre malware, l'agent de sécurité de Bitdefender tente automatiquement de supprimer le code malveillant du fichier infecté et de reconstruire le fichier d'origine. Cette opération est appelée désinfection. Les

fichiers qui ne peuvent pas être désinfectés sont placés en quarantaine afin d'isoler l'infection. Quand un virus est en quarantaine, il ne peut causer aucun dommage car il ne peut ni être exécuté ni être lu.

Les utilisateurs avancés peuvent configurer des exceptions d'analyse s'ils ne souhaitent pas que certains fichiers ou types de fichiers soient analysés.

Les paramètres sont organisés dans les sections suivantes :

- [À l'accès](#)
- [À l'exécution](#)
- [A la demande](#)
- [HyperDetect](#)
- [Anti-exploit avancé](#)
- [Réglages](#)
- [Serveurs de sécurité](#)

À l'accès

Dans cette section, vous pouvez configurer les composants qui assurent la protection lors d'un accès à un fichier ou à une application :

- [Analyse à l'accès](#)
- [Vaccin anti-ransomware](#)

The screenshot shows the Bitdefender GravityZone configuration window for 'Analyse à l'accès'. The left sidebar contains a navigation menu with categories like 'Tableau de bord', 'Réseau', 'Packages', 'Tâches', 'Politiques', 'Règles d'affichage', 'Rapports', 'Quarantaine', 'Comptes', 'Activité des utilisateurs', 'Configuration', 'Mise à jour', and 'Licence'. The main content area is titled 'Analyse à l'accès' and includes a 'Configuration' tab. It features two main sections: 'Normal - Sécurité standard, faible utilisation des ressources' and 'Advanced Threat Control'. The 'Normal' section has radio buttons for 'Agresif', 'Normal' (selected), 'Tolérant', and 'Personnalisé', with a description: 'Cette option est conçue pour fournir un équilibre optimal entre la sécurité et les performances. Protège contre tous les types de malwares en analysant tous les fichiers, auxquels on accède à partir de fichiers locaux (à l'exception des fichiers archivés) et des fichiers ne présentant quasiment aucun risque.' The 'Advanced Threat Control' section has a dropdown for 'Action par défaut pour les applications infectées' set to 'Désinfecter', and radio buttons for 'Agresif', 'Normal' (selected), and 'Vaccin ransomware', with a description: 'Normal - Recommandé pour la plupart des systèmes. Cette option régule le taux de détection de Bitdefender Advanced Threat Control sur moyen et affiche des alertes susceptibles de contenir des faux positifs (applications considérées à tort comme étant malveillantes).'

Politiques - Paramètres à l'accès

Analyse à l'accès

L'analyse à l'accès empêche que de nouveaux malwares accèdent au système en analysant les fichiers locaux et du réseau (lorsqu'ils sont ouverts, déplacés, copiés ou exécutés), les secteurs d'amorçage et les applications potentiellement indésirables.

 **Note**

Cette fonctionnalité a certaines restrictions sur les systèmes Linux. Pour en savoir plus, consultez le chapitre sur les prérequis du Guide d'installation de GravityZone.

Pour configurer l'analyse à l'accès :

1. Utilisez cette case pour activer ou désactiver l'analyse à l'accès.

 **Avertissement**

Si vous désactivez l'analyse à l'accès, les endpoints seront vulnérables aux malwares.

2. Pour une configuration rapide, cliquez sur le niveau de sécurité qui correspond le mieux à vos besoins (Agressif, Normal ou Tolérant). Utilisez la description à droite de l'échelle pour faire votre choix.
3. Vous pouvez configurer les paramètres d'analyse en détail en sélectionnant le niveau de protection **Personnalisé** et en cliquant sur le lien **Configuration**. La fenêtre **Paramètres de l'analyse à l'accès** s'affichera ; elle contient plusieurs options organisées sous deux onglets, **Général** et **Avancé**.

Les options sous l'onglet **General** sont décrites ci-dessous :

- **Emplacement du fichier.** Utilisez ces options pour spécifier les types de fichiers que vous souhaitez analyser. Les préférences d'analyse peuvent être configurées pour les fichiers locaux (stockés sur l'endpoint local) ou les fichiers réseau (stockés sur les partages réseau). Si la protection antimalware est installée sur tous les ordinateurs du réseau, vous pouvez désactiver l'analyse des fichiers du réseau pour permettre un accès plus rapide au réseau.

Vous pouvez configurer l'agent de sécurité afin qu'il analyse tous les fichiers à l'accès (quelle que soit leur extension), ou uniquement les fichiers d'applications ou certaines extensions de fichiers que vous considérez dangereuses. L'analyse de tous les fichiers accédés offre une protection maximale alors que l'analyse des applications uniquement peut être utilisée pour obtenir de meilleures performances du système.

 **Note**

Les fichiers d'applications sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers. Pour plus d'informations, reportez-vous à « [Types de fichiers d'applications](#) » (p. 529).

Si vous souhaitez uniquement que certaines extensions soient analysées, sélectionnez **Extensions définies par l'utilisateur** dans le menu puis saisissez les extensions dans le champ de saisie, en appuyant sur **Entrée** après chaque extension.

i Note

Sur les systèmes Linux, les extensions de fichiers sont sensibles à la casse et les fichiers ayant les mêmes noms, mais des extensions différentes, sont des objets distincts. Par exemple, `fichier.txt` est différent de `fichier.TXT`.

Afin d'améliorer les performances du système, vous pouvez également exclure de l'analyse les fichiers volumineux. Cochez la case **Taille maximale (Mo)** et indiquez la taille maximale des fichiers qui seront analysés. Utilisez cette option de façon avisée car les malwares peuvent affecter également des fichiers volumineux.

- **Analyse.** Cochez les cases correspondantes pour activer les options d'analyse souhaitées.
 - **Uniquement les fichiers nouveaux ou modifiés.** En analysant uniquement les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.
 - **Secteurs de boot .** Pour analyser les secteurs de boot du système. Ce secteur du disque dur contient le code nécessaire pour faire démarrer le processus d'amorçage du système. Quand un virus infecte le secteur d'amorçage, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.
 - **Keyloggers.** Les enregistreurs de frappe enregistrent ce que vous tapez sur votre clavier et envoient des rapports sur Internet à une personne malveillante (un pirate informatique). Le pirate peut récupérer des informations sensibles à partir des données volées, comme vos numéros de comptes bancaires ou vos mots de passe pour les utiliser à son propre profit.
 - **Applications potentiellement indésirables (PUA).** Un Logiciel Potentiellement Indésirable (LPI) est un programme qui peut être indésirable sur l'ordinateur et peut provenir d'un logiciel gratuit. De tels programmes peuvent être installés sans le consentement de l'utilisateur (alors appelés Adware) ou sont inclus par défaut dans le kit d'installation rapide. Les effets possibles de ces programmes sont l'affichage de

pop-ups, l'installation indésirable de barre d'outils dans le navigateur par défaut ou le lancement de plusieurs programmes en arrière-plan qui ralentissent les performances du PC.

- **Archives.** Sélectionnez cette option si vous souhaitez activer l'analyse à l'accès des fichiers archivés. L'analyse des fichiers compressés est un processus lent et consommant beaucoup de ressources, qui n'est donc pas recommandé pour une protection en temps réel. Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité du système. Les malwares peuvent affecter le système uniquement si le fichier infecté est extrait de l'archive et exécuté sans que l'analyse à l'accès ne soit activée.

Si vous décidez d'utiliser cette option, vous pouvez configurer les options d'optimisation suivantes :

- **Taille maximale des archives (Mo).** Vous pouvez définir une limite de taille pour les archives à analyser à l'accès. Cochez la case correspondante et tapez la taille maximale des archives (en Mo).
- **Profondeur maximale des archives (niveaux).** Cochez la case correspondante et sélectionnez la profondeur maximale des archives dans le menu. Pour les meilleures performances, choisissez la valeur la plus faible, pour la protection maximale, choisissez la valeur la plus élevée.
- **Analyse différée.** L'analyse différée améliore vos performances système lorsqu'elle exécute des opérations d'accès au fichier. Par exemple, les ressources du système ne sont pas affectées lorsque des fichiers volumineux sont copiés. Cette option est activée par défaut.
- **Action d'analyse.** En fonction du type de fichier détecté, les actions suivantes sont menées automatiquement :
 - **Pour les fichiers infectés.** Bitdefender détecte les fichiers considérés comme infectés par le biais de divers mécanismes avancés, notamment les technologies basées sur l'intelligence artificielle, l'apprentissage machine et les signatures de logiciels malveillants. L'agent de sécurité de Bitdefender peut généralement supprimer le code malveillant d'un fichier infecté et reconstruire le fichier d'origine. Cette opération est appelée désinfection.

Par défaut, si un fichier infecté est détecté, l'agent de sécurité de Bitdefender tentera automatiquement de le désinfecter. Si la désinfection échoue, le fichier est placé en quarantaine afin de contenir l'infection. Vous pouvez modifier le flux recommandé en fonction de vos besoins.



Important

Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

- **Pour les fichiers suspects.** Les fichiers sont considérés comme étant suspicieux par l'analyse heuristique et les autres technologies Bitdefender. Ils offrent un taux de détection élevé, mais les utilisateurs doivent tenir compte de la probabilité de faux résultats positifs (fichiers propres détectés comme étant suspicieux), dans certains cas. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible.

Lorsqu'un fichier suspect est détecté, les utilisateurs ne peuvent pas y accéder afin d'éviter une infection potentielle.

Bien que ce ne soit pas recommandé, vous pouvez modifier les actions par défaut. Vous pouvez définir deux actions pour chaque type de fichier. Les actions suivantes sont disponibles :

Refuser l'accès

Refuser l'accès aux fichiers détectés.



Important

Pour les endpoints MAC, l'action **Quarantaine** est appliquée au lieu de **Refuser l'accès**.

Désinfecter

Supprimer le code malveillant des fichiers infectés. Nous vous recommandons de toujours la conserver comme première action à appliquer aux fichiers infectés.

Supprimer

Supprime les fichiers détectés du disque, sans avertissement. Nous vous recommandons d'éviter d'utiliser cette action.

Déplacer en quarantaine

Déplacer les fichiers détectés de l'emplacement actuel vers le dossier de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Vous pouvez gérer les fichiers en quarantaine à partir de la page [Quarantaine](#) de la console.

Ne rien faire



Rapporte seulement les fichiers détectés par Bitdefender.

L'onglet **Advanced** permet d'effectuer les analyses à l'accès sur les machines Linux. Utilisez cette case pour l'activer ou le désactiver.

Dans le tableau ci-dessous, vous pouvez configurer les répertoires Linux que vous souhaitez analyser. Par défaut, il existe cinq entrées, dont chacune correspond à un emplacement spécifique sur les terminaux : `/home`, `/bin`, `/sbin`, `/usr`, `/etc`.

Pour ajouter plus d'entrées :

- Tapez le nom de l'emplacement personnalisé dans la barre de recherche, sur la partie supérieure du tableau.
- Sélectionnez les répertoires prédéfinis dans la liste qui s'affiche, lorsque que vous cliquez sur la flèche en bas à droite de la barre de recherche.

Cliquez sur le bouton  **Add** pour enregistrer un emplacement sur le tableau et sur le bouton  **Delete** pour le supprimer.

Vaccin anti-ransomware

Le vaccin anti-ransomware immunise vos machines contre les ransomwares **connus** en bloquant le processus de cryptage, même si l'ordinateur est infecté. Utilisez cette case pour activer ou désactiver le vaccin anti-ransomware.

La fonctionnalité vaccin anti-ransomware est désactivée par défaut. Les Labs Bitdefender analysent le comportement des ransomwares répandus et de nouvelles signatures sont livrées avec chaque mise à jour de contenus de sécurité relatifs aux malwares, pour faire face aux menaces les plus récentes.



Avertissement

Pour augmenter encore la protection contre les infections ransomwares, soyez prudent avec les pièces jointes non sollicitées ou suspectes et vérifiez que le contenu de sécurité est à jour.



Note

Le vaccin anti-ransomware est uniquement disponible avec Bitdefender Endpoint Security Tools pour Windows.

À l'exécution

Dans cette section, vous pouvez configurer la protection contre les processus malveillants lorsqu'ils sont exécutés. Elle couvre les couches de protection suivantes :

Advanced Threat Control

Note

Ce module est disponible pour :

- Windows pour postes de travail
- Windows pour serveurs
- macOS

Bitdefender Advanced Threat Control est une technologie de détection proactive qui utilise des méthodes heuristiques de pointe pour détecter de nouvelles menaces potentielles en temps réel.

Advanced Threat Control surveille en permanence les applications en cours d'exécution sur l'endpoint, à la recherche d'actions ressemblant à celles des malwares. Chacune de ces actions est notée et un score global est calculé pour chaque processus. Lorsque la note globale d'un processus atteint un seuil donné, le processus est considéré comme malveillant.

Advanced Threat Control essaiera de désinfecter automatiquement le fichier détecté. Si la routine de désinfection échoue, Advanced Threat Control supprimera le fichier.

Note

Avant d'appliquer la désinfection, une copie du fichier est envoyée en quarantaine afin que vous puissiez restaurer le fichier ultérieurement, en cas de faux positif. Cette action peut être configurée à l'aide de l'option **Copier les fichiers en quarantaine avant d'appliquer l'action de désinfection** disponible dans l'onglet **Antimalware > Configuration** des paramètres de la politique. Cette option est activée par défaut dans les modèles de politique.

Pour configurer Advanced Threat Control :

1. Utilisez cette case pour activer ou désactiver Advanced Threat Control.



Avertissement

Si vous désactivez Advanced Threat Control, les ordinateurs seront vulnérables aux malwares inconnus.

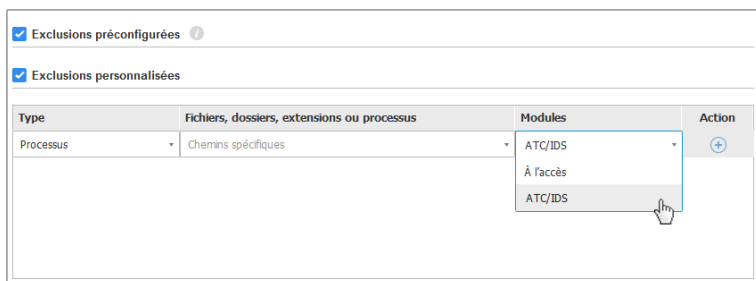
2. L'action par défaut pour les applications infectées, détectée par Advanced Threat Control, est désinfectée. Vous pouvez définir une autre action par défaut, avec le menu disponible :
 - **Bloquer**, pour refuser l'accès à l'application infectée.
 - **Ne rien faire** pour signaler uniquement les applications infectées détectées par Bitdefender.
3. Cliquez sur le niveau de sécurité qui correspond le mieux à vos besoins (**Agressif**, **Normal** ou **Tolérant**). Utilisez la description à droite de l'échelle pour faire votre choix.



Note

Si vous élevez le niveau de protection, Advanced Threat Control aura besoin de moins de signes de comportements similaires à ceux des malwares pour signaler un processus. Cela conduira au signalement d'un nombre plus important d'applications et, en même temps, à un risque plus élevé de faux positifs (des applications saines détectées comme étant malveillantes).

Nous vous recommandons vivement de créer des règles d'exclusion pour les applications fréquemment utilisées ou connues afin d'éviter les faux positifs (applications légitimes détectées à tort comme étant malveillantes). Allez dans l'onglet [Antimalware > Configuration](#) et configurez les règles d'exclusion des processus ATC/IDS pour les applications de confiance.



Politiques des ordinateurs et machines virtuelles - Exclusion des processus ATC/IDS

Limitation des dégâts des ransomwares

Ransomware Mitigation utilise des technologies de détection et de réparation pour protéger vos données contre les attaques de ransomware. Que le ransomware soit connu ou non, GravityZone détecte les processus de chiffrement anormaux et les

bloque. Ensuite, la solution restaure les fichiers à leur emplacement d'origine depuis des copies de sauvegarde.



Important

Ransomware Mitigation nécessite Active Threat Control.



Note

Ce module est disponible pour :

- Windows pour postes de travail
- Windows pour serveurs

Pour configurer Ransomware Mitigation :

1. Cochez la case **Ransomware Mitigation** dans la section **Antimalware > À l'exécution** de la politique pour activer la fonctionnalité.
2. Sélectionnez les modes de surveillance que vous souhaitez utiliser :
 - Local. GravityZone surveille les processus et détecte les attaques de ransomwares initiées en local sur l'endpoint. Cela est recommandé pour les postes de travail. À utiliser avec précaution sur les serveurs à cause de l'impact sur les performances.
 - À distance. GravityZone surveille les chemins de partage réseau et détecte les attaques de ransomware qui sont initiées sur d'autres machines. Utilisez cette option si l'endpoint est un serveur de fichiers ou si des partages réseau sont activés sur celui-ci.
3. Sélectionnez la méthode de récupération :
 - A la demande. Vous sélectionnez manuellement les attaques dont vous voulez récupérer les fichiers. Vous pouvez le faire depuis la page **Rapports > Activité de ransomware** au moment de votre choix, mais au plus tard 30 jours après l'attaque. Après ce délai, la récupération ne sera plus possible.
 - Automatique. GravityZone récupère automatiquement les fichiers juste après la détection d'un ransomware.

Pour que la récupération réussisse, les endpoints doivent être disponibles.

Une fois activé, vous avez plusieurs options pour vérifier si votre réseau subit une attaque de ransomware :

- Consultez les notifications et cherchez **Détection de ransomware**.

Pour plus d'informations sur cette notification, reportez-vous au « [Types de notifications](#) » (p. 498).

- Consulter le rapport **Audit de sécurité**.
- Consultez la page **Activité de ransomware**.

Depuis cette page, vous pouvez exécuter si nécessaire des tâches de récupération. Pour plus d'informations, reportez-vous à ???.

Si vous remarquez qu'une détection est un processus de chiffrement légitime, qu'il comprend certains emplacements où vous autorisez le chiffrement ou l'accès à distance depuis certaines machines, ajoutez l'exclusion dans la section **Antimalware > Paramètres > Exclusions personnalisées** de la politique. Ransomware Mitigation autorise les exclusions de dossiers, de processus, et d'IP/de masque. Pour plus d'informations, reportez-vous à « [Exclusions](#) » (p. 294).

A la demande

Cette section vous permet d'ajouter et de configurer les tâches d'analyse antimalware qui s'exécuteront régulièrement sur les ordinateurs cibles, en fonction de la planification définie.

Général +

Antimalware +

À l'accès

A la demande

Configuration

Serveurs de sécurité

Pare-feu +

Contrôle de contenu +

Contrôle des appareils +

Relais +

Protection Exchange +

Tâches d'analyse

+ Ajouter - Supprimer Actualiser

<input type="checkbox"/>	Nom de la tâche	Type de tâche	Répéter l'intervalle	Première exécution
--------------------------	-----------------	---------------	----------------------	--------------------

Analyse des périphériques ⓘ

Média CD/DVD

Mémoires USB

Lecteurs réseau mappés

Ne pas analyser les appareils contenant des données de plus de (Mo)

Politiques des ordinateurs et machines virtuelles - Tâches d'analyse à la demande

L'analyse est exécutée discrètement en arrière-plan, que l'utilisateur soit connecté au système ou non.

Bien que ce ne soit pas obligatoire, nous vous recommandons de planifier l'exécution hebdomadaire d'une analyse complète sur tous les endpoints. Analyser

les endpoints régulièrement est une mesure de sécurité proactive qui peut aider à détecter et bloquer les malwares susceptibles d'échapper aux fonctionnalités de protection en temps réel.

Outre les analyses régulières, vous pouvez également configurer la [détection et l'analyse automatiques](#) des supports de stockage externes.

Gestion des tâches d'analyse

Le tableau Tâches d'analyse vous informe des tâches d'analyse existantes et fournit d'importantes informations sur chacun d'entre elles :

- Nom et type de tâche.
- Planification à partir de laquelle la tâche s'exécute régulièrement (périodicité).
- Heure à laquelle la tâche a été lancée en premier.

Vous pouvez ajouter et configurer les types de tâches d'analyse suivants :

- **Quick Scan** utilise l'analyse dans le Cloud pour détecter les malwares présents sur le système. La réalisation d'une analyse rapide dure généralement moins d'une minute et n'utilise qu'une petite partie des ressources du système dont a besoin une analyse antivirus classique.

En cas de détection d'un malware ou d'un rootkit, Bitdefender procède automatiquement à la désinfection. Si pour une raison quelconque le fichier ne peut pas être désinfecté, il est déplacé en quarantaine. Ce type d'analyse ignore les fichiers suspects.

L'Analyse rapide est une tâche d'analyse par défaut avec des options préconfigurées qui ne peuvent pas être modifiées. Vous pouvez ajouter uniquement une tâche d'analyse rapide pour la même politique.

- **L'Analyse Complète** analyse l'ensemble de votre endpoint afin de détecter tous les types de malwares menaçant sa sécurité : virus, spywares, adwares, rootkits et autres.

Bitdefender essaie automatiquement de désinfecter les fichiers dans lesquels un malware a été détecté. Si le malware ne peut pas être supprimé, il est confiné en quarantaine, où il ne peut pas faire de mal. Les fichiers suspects sont ignorés. Si vous voulez également prendre des mesures pour les fichiers suspects, ou si vous voulez changer les actions par défaut pour les fichiers infectés, choisissez l'Analyse personnalisée.

L'Analyse complète est une tâche d'analyse par défaut avec des options préconfigurées qui ne peuvent pas être modifiées. Vous pouvez ajouter uniquement une tâche d'analyse complète pour la même politique.

- L'**analyse personnalisée** vous permet de sélectionner les emplacements à analyser et de configurer les options d'analyse.
- **Analyse du réseau** est un type d'analyse personnalisée, qui permet d'affecter un endpoint administré unique pour analyser les lecteurs du réseau, avant de configurer les options d'analyse et les emplacements spécifiques à analyser. Pour les tâches d'analyse du réseau, vous devez indiquer les identifiants d'un compte utilisateur avec des permissions de lecture/écriture sur les lecteurs réseau cibles, afin que l'agent de sécurité soit capable d'accéder et d'appliquer des actions sur ces lecteurs réseau.

La tâche d'analyse du réseau récurrente sera envoyée uniquement à l'endpoint scanner sélectionné. Si l'endpoint sélectionné n'est pas disponible, les paramètres d'analyse locale s'appliqueront.



Note

Vous pouvez créer des tâches d'analyse du réseau uniquement dans une politique qui est déjà appliquée à un endpoint pouvant être utilisé comme scanner.

En plus des tâches d'analyse par défaut (que vous ne pouvez pas supprimer ou dupliquer), vous pouvez créer autant de tâches d'analyse personnalisées et du réseau que vous le souhaitez.

Pour créer et configurer une nouvelle tâche d'analyse personnalisée ou du réseau, cliquez sur le bouton **+ Ajouter** à droite du tableau. Pour modifier les paramètres d'une tâche d'analyse existante, cliquez sur le nom de cette tâche. Reportez-vous à la rubrique suivante pour savoir comment configurer les paramètres de la tâche.

Pour retirer une tâche de la liste, sélectionnez la tâche et cliquez sur le bouton **- Supprimer** à droite du tableau.

Configuration des tâches d'analyse

Les paramètres de la tâche d'analyse sont organisés sous trois onglets :

- **Général** : définissez le nom de la tâche et planifiez son exécution.
- **Options** : choisissez un profil d'analyse pour une configuration rapide des paramètres d'analyse et définissez les paramètres d'analyse pour une analyse personnalisée.

- **Cible** : sélectionnez les fichiers et les dossiers à analyser et définissez des exceptions d'analyse.

Les options sont décrites ci-après du premier au dernier onglet :

Modifier la tâche

Général Options Cible

Détails

Nom de la tâche: Ma Tâche

Exécuter la tâche en priorité basse

Éteindre l'ordinateur lorsque la tâche est terminée

Planificateur

Date et heure de début: 09/22/2016 11:16

Périodicité

Planifier la tâche pour qu'elle s'exécute une fois tous les: 1 jour(s)

Exécuter la tâche tous les: Dim Lun Mar Mer Jeu Ven Sam

Si le moment de l'exécution planifiée a été manqué, exécuter la tâche dès que possible

Ignorer si la prochaine analyse planifiée doit commencer dans moins de: 1 jour(s)

Enregistrer Annuler

Politiques des ordinateurs et machines virtuelles - Configurer les paramètres généraux des tâches d'analyse à la demande

- **Détails.** Choisissez un nom de tâche explicite afin de l'identifier facilement. Lorsque vous choisissez un nom, prenez en compte la cible de la tâche d'analyse, et, éventuellement, les paramètres de l'analyse.

Par défaut, les tâches d'analyse fonctionnent avec une priorité moindre. De cette façon, Bitdefender permet à d'autres programmes de fonctionner plus rapidement, mais augmente le temps nécessaire au processus d'analyse pour finir. Utilisez la case **Exécutez la tâche avec une faible priorité** pour désactiver ou réactiver cette fonctionnalité.



Note

Cette option ne s'applique qu'à Bitdefender Endpoint Security Tools et Endpoint Security (ancien agent).

Cochez la case **Éteindre l'ordinateur une fois la tâche terminée** pour éteindre votre machine si vous ne comptez pas l'utiliser pendant un certain temps.

**Note**

Cette option s'applique à Bitdefender Endpoint Security Tools, Endpoint Security (ancien agent) et Endpoint Security for Mac.

- **Planificateur.** Utilisez les options de planification pour configurer la planification de l'analyse. Vous pouvez configurer l'analyse pour une exécution régulière, à partir d'une date et d'une heure spécifiées.

Les endpoints doivent être allumés au moment planifié. Les analyses planifiées ne s'exécuteront pas si la machine est éteinte, en veille prolongée ou en veille. Dans l'un de ces cas, l'analyse sera reportée intérieurement.

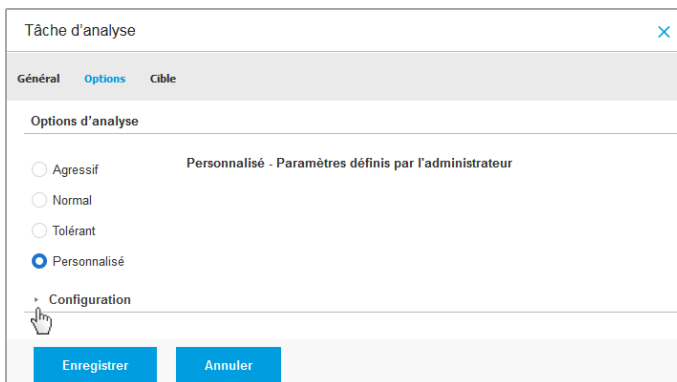
**Note**

L'analyse planifiée s'exécutera à l'heure locale du poste de travail cible. Par exemple, si l'analyse planifiée est configurée pour démarrer à 18h et que le poste de travail se trouve dans un autre fuseau horaire que Control Center, l'analyse démarrera à 18h00 (heure du poste de travail).

Vous pouvez également indiquer ce qu'il doit se passer lorsque la tâche d'analyse ne peut pas s'activer à l'heure prévue (si l'endpoint était éteint ou hors ligne). Utilisez l'option **Si le temps d'exécution planifié est manqué, exécutez la tâche le plus tôt possible** en fonction de vos besoins :

- Si vous laissez cette option décochée, la tâche d'analyse essaiera de s'exécuter de nouveau lors du prochain moment planifié.
 - Si vous sélectionnez cette option, vous forcez l'analyse à s'exécuter le plus tôt possible. Pour personnaliser le meilleur moment pour l'analyse et éviter de déranger les utilisateurs pendant leurs heures de travail, sélectionner **Ignorer si la prochaine analyse planifiée doit commencer dans moins de**, puis indiquez l'intervalle désiré.
- **Options d'analyse.** Cliquez sur le niveau de sécurité qui correspond le mieux à vos besoins (Agressif, Normal ou Tolérant). Utilisez la description à droite de l'échelle pour faire votre choix.

Basées sur le profil sélectionné, les options d'analyse de la section **Configuration** sont configurées automatiquement. Vous pouvez cependant, si vous le souhaitez, les configurer en détail. Pour cela, cochez la case **Personnalisé** puis allez dans la section **Configuration**.



Tâche d'analyse

Général Options Cible

Options d'analyse

Agressif Personnalisé - Paramètres définis par l'administrateur

Normal

Tolérant

Personnalisé

► Configuration

Enregistrer Annuler

Tâche d'analyse des ordinateurs - Configurer une analyse personnalisée

- **Types de fichiers.** Utilisez ces options pour spécifier les types de fichiers que vous souhaitez analyser. Vous pouvez configurer l'agent de sécurité afin qu'il analyse tous les fichiers (quelle que soit leur extension), ou uniquement les fichiers d'applications ou certaines extensions de fichiers que vous considérez dangereuses. L'analyse de tous les fichiers fournit la meilleure protection, alors que l'analyse des applications uniquement peut être utilisée pour effectuer une analyse plus rapide.



Note

Les fichiers d'applications sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers. Pour plus d'informations, reportez-vous à « [Types de fichiers d'applications](#) » (p. 529).

Si vous souhaitez uniquement que certaines extensions soient analysées, sélectionnez **Extensions définies par l'utilisateur** dans le menu puis saisissez les extensions dans le champ de saisie, en appuyant sur **Entrée** après chaque extension.

- **Archives.** Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité du système. Les malwares peuvent affecter le système uniquement si le fichier infecté est extrait de l'archive et exécuté sans que la protection en temps réel ne soit activée. Il est toutefois recommandé d'utiliser cette option afin de détecter et de supprimer toute menace potentielle, même si celle-ci n'est pas imminente.

**Note**

L'analyse des fichiers compressés augmente le temps d'analyse global et demande plus de ressources système.

- **Analyser le contenu compressé.** Sélectionnez cette option si vous souhaitez que les archives fassent l'objet d'une analyse antimalware. Si vous décidez d'utiliser cette option, vous pouvez configurer les options d'optimisation suivantes :
 - **Limitier la taille des archives à (Mo).** Vous pouvez définir une limite de taille pour les archives à analyser. Cochez la case correspondante et tapez la taille maximale des archives (en Mo).
 - **Profondeur maximale des archives (niveaux).** Cochez la case correspondante et sélectionnez la profondeur maximale des archives dans le menu. Pour les meilleures performances, choisissez la valeur la plus faible, pour la protection maximale, choisissez la valeur la plus élevée.
- **Analyser les archives de messagerie.** Sélectionnez cette option si vous souhaitez permettre l'analyse de fichiers de messagerie et de bases de données de messagerie, y compris de formats de fichiers tels que .eml, .msg, .pst, .dbx, .mbx, .tbb et d'autres.

**Note**

L'analyse des archives de messagerie consomme beaucoup de ressources et peut avoir un impact sur les performances du système.

- **Divers.** Cochez les cases correspondantes pour activer les options d'analyse souhaitées.
 - **Analyser les secteurs d'amorçage.** Pour analyser les secteurs de boot du système. Ce secteur du disque dur contient le code nécessaire pour faire démarrer le processus d'amorçage du système. Quand un virus infecte le secteur d'amorçage, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.
 - **Analyser la base de registre.** Sélectionnez cette option pour analyser les clés de registre. Le registre Windows est une base de données qui contient les paramètres et les options de configuration des composants du système d'exploitation Windows, ainsi que des applications installées.

- **Rechercher les rootkits.** Sélectionnez cette option pour rechercher des **rootkits** et des objets cachés à l'aide de ce logiciel.
- **Rechercher des enregistreurs de frappe.** Sélectionnez cette option pour rechercher les logiciels **keyloggers**.
- **Analyser les volumes partagés.** Cette option analyse les lecteurs de réseau. Pour l'analyse rapide, cette option est désactivée par défaut. Pour l'analyse complète, elle est activée par défaut. Pour l'analyse personnalisée, si vous définissez le niveau de sécurité sur **Aggressif/Normal**, l'option **Analyser les partages réseau** est activée automatiquement. Si vous définissez le niveau de sécurité sur **Permissif**, l'option **Analyser les partages réseau** option est automatiquement désactivée.
- **Analyser la mémoire.** Sélectionnez cette option pour analyser les programmes s'exécutant dans la mémoire du système.
- **Analyser les cookies.** Sélectionnez cette option pour analyser les cookies stockés par les navigateurs sur l'endpoint.
- **Analyser uniquement les nouveaux fichiers et ceux modifiés.** En analysant uniquement les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.
- **Rechercher des applications potentiellement indésirables.** Un Logiciel Potentiellement Indésirable (LPI) est un programme qui peut être indésirable sur l'ordinateur et peut provenir d'un logiciel gratuit. De tels programmes peuvent être installés sans le consentement de l'utilisateur (alors appelés Adware) ou sont inclus par défaut dans le kit d'installation rapide. Les effets possibles de ces programmes sont l'affichage de pop-ups, l'installation indésirable de barre d'outils dans le navigateur par défaut ou le lancement de plusieurs programmes en arrière-plan qui ralentissent les performances du PC.
- **Actions.** En fonction du type de fichier détecté, les actions suivantes sont menées automatiquement :
 - **Pour les fichiers infectés.** Bitdefender détecte les fichiers considérés comme infectés par le biais de divers mécanismes avancés, notamment les technologies basées sur l'intelligence artificielle, l'apprentissage machine et les signatures de logiciels malveillants. L'agent de sécurité de peut

généralement supprimer le code malveillant d'un fichier infecté et reconstruire le fichier d'origine. Cette opération est appelée désinfection.

Si un fichier infecté est détecté, l'agent de sécurité de tentera automatiquement de le désinfecter. Si la désinfection échoue, le fichier est placé en quarantaine afin de contenir l'infection.



Important

Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

- **Pour les fichiers suspects.** Les fichiers sont considérés comme étant suspicieux par l'analyse heuristique et les autres technologies Bitdefender. Ils offrent un taux de détection élevé, mais les utilisateurs doivent tenir compte de la probabilité de faux résultats positifs (fichiers propres détectés comme étant suspicieux), dans certains cas. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible.

Les tâches d'analyse sont configurées par défaut pour ignorer les fichiers suspects. Vous pouvez modifier l'action par défaut afin de placer des fichiers suspects en quarantaine. Les fichiers en quarantaine sont envoyés régulièrement aux Laboratoires Bitdefender pour y être analysés. Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

- **Action par défaut pour les rootkits.** Les rootkits sont des logiciels spécialisés utilisés pour masquer des fichiers au système d'exploitation. Bien que n'étant pas malveillants par nature, les rootkits sont souvent utilisés pour masquer des malwares ou la présence d'un intrus dans le système.

Les rootkits détectés et les fichiers cachés sont ignorés par défaut.

Bien que ce ne soit pas recommandé, vous pouvez modifier les actions par défaut. Vous pouvez spécifier une deuxième action à prendre si la première a échoué, ainsi que d'autres mesures, pour chaque catégorie. Choisissez dans les menus correspondants la première et la seconde actions à prendre pour chaque type de fichier détecté. Les actions suivantes sont disponibles :

Ne rien faire

Aucune action ne sera appliquée aux fichiers détectés. Ces fichiers apparaîtront uniquement dans le journal d'analyse.

Désinfecter

Supprimer le code malveillant des fichiers infectés. Nous vous recommandons de toujours la conserver comme première action à appliquer aux fichiers infectés.

Supprimer

Supprime les fichiers détectés du disque, sans avertissement. Nous vous recommandons d'éviter d'utiliser cette action.


Déplacer en quarantaine

Déplacer les fichiers détectés de l'emplacement actuel vers le dossier de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Vous pouvez gérer les fichiers en quarantaine à partir de la page [Quarantaine](#) de la console.

- **Analyser la cible.** Ajouter la liste de tous les emplacements que vous souhaitez analyser sur les ordinateurs cibles.

Pour ajouter un nouveau fichier, ou dossier, à analyser :

1. Spécifiez un emplacement prédéfini dans le menu déroulant ou saisissez les **Chemins spécifiques** que vous souhaitez analyser.
2. Indiquez le chemin de l'objet à analyser dans le champ de saisie.
 - Si vous avez choisi un emplacement prédéfini, complétez le chemin selon vos besoins. Par exemple, pour analyser l'ensemble du dossier `Program Files`, il suffit de sélectionner l'emplacement prédéfini correspondant dans le menu déroulant. Pour analyser un dossier spécifique de `Program Files`, vous devez compléter le chemin en ajoutant une barre oblique inverse (`\`) et le nom du dossier.
 - Si vous avez choisi **Chemins spécifiques**, indiquez le chemin complet vers l'objet à analyser. Il est recommandé d'utiliser les variables du système (le cas échéant) afin de s'assurer que le chemin soit valide sur tous les ordinateurs cibles.
3. Cliquez sur le bouton **+ Ajouter** correspondant.

Pour modifier un emplacement existant, cliquez dessus. Pour retirer un emplacement de la liste, placez le curseur dessus et cliquez sur le bouton  **Supprimer** correspondant.

- Pour les tâches d'analyse du réseau, vous devez indiquer les identifiants d'un compte utilisateur avec des permissions de lecture/écriture sur les lecteurs réseau cibles, afin que l'agent de sécurité soit capable d'accéder et d'appliquer des actions sur ces lecteurs réseau.
- **Exclusions.** Vous pouvez soit utiliser l'exclusion définie dans la section **Antimalware > Exclusions** de la politique actuelle, soit définir des exclusions personnalisées pour la tâche d'analyse en cours. Pour plus d'informations sur les exclusions, reportez-vous à « [Exclusions](#) » (p. 294).

Analyse des périphériques

Vous pouvez configurer l'agent de sécurité pour détecter et analyser automatiquement les périphériques de stockage externe quand ils sont connectés à l'endpoint. Les périphériques détectés appartiennent à l'une des catégories suivantes :

- CD ou DVD
- Des supports USB, tels que des clés flash et des disques durs externes
- Appareils contenant plus de données que la quantité spécifiée.

Les analyses des périphériques tentent de désinfecter automatiquement les fichiers détectés comme infectés ou tentent de les déplacer vers la quarantaine si la désinfection est impossible. Veuillez noter que certains périphériques, comme les CD/DVD, ne sont disponibles qu'en lecture seule. Aucune mesure ne peut être prise pour les fichiers infectés contenus sur ces supports de stockage.

Note

Lors d'une analyse des périphériques, l'utilisateur peut accéder à toutes les données de l'appareil.

Si les fenêtres pop-up d'alertes sont activées dans la section **Général > Notifications**, l'utilisateur devra décider d'analyser ou non le périphérique détecté au lieu de commencer l'analyse automatiquement.

Quand une analyse de périphérique est commencée :

- Un pop-up informe l'utilisateur sur l'analyse des périphériques, à condition que la notification des pop-ups soient activés dans la section **Général > Notifications**

Une fois l'analyse terminée, l'utilisateur doit vérifier les menaces détectées, le cas échéant.

Sélectionnez l'option **Analyse des périphériques** pour activer la détection et l'analyse automatiques des dispositifs de stockage. Pour configurer l'analyse de périphérique individuellement pour chaque type d'appareil, utilisez les options suivantes :

- **Média CD/DVD**
- **Mémoires USB**
- **Ne pas analyser les appareils contenant des données de plus de (Mo)**. Utilisez cette option pour ne pas analyser automatiquement un périphérique détecté si la taille des données stockées est supérieure à la taille spécifiée. Tapez la taille maximale (en mégaoctets) dans le champ correspondant. Zéro signifie qu'aucune restriction de taille n'est imposée.

HyperDetect

Note

Ce module est disponible pour :

- Windows pour postes de travail
- Windows pour serveurs
- Linux

HyperDetect agrmente les technologies d'analyse (analyse à l'accès, à la demande et du trafic) d'une couche de sécurité supplémentaire, afin de lutter contre la nouvelle génération de cyberattaques, notamment les menaces persistantes avancées. HyperDetect améliore les modules de protection antimalware et de contrôle du contenu, à l'aide de puissantes techniques heuristiques s'appuyant sur l'intelligence artificielle et l'apprentissage machine.

Capable d'anticiper les attaques ciblées et de détecter les malware les plus sophistiqués, HyperDetect dévoile les menaces bien plus rapidement que les technologies d'analyse comportementales et basées sur signature.

Pour configurer HyperDetect :

1. Cochez la case **HyperDetect** pour activer ou désactiver le module.

2. Sélectionnez les types de menaces desquelles vous souhaitez protéger votre réseau. Par défaut, la protection est activée pour tous les types de menaces : attaques ciblées, fichiers et trafic de réseaux suspects, exploits, ransomware ou **grayware**.

**Note**

Les techniques heuristiques pour le trafic de réseau nécessitent l'activation de **l'analyse du trafic et du contrôle de contenu**.

3. Personnalisez votre niveau de protection en fonction des types de menaces sélectionnés.

Utilisez le commutateur principal en haut de la liste de menaces, afin de choisir un niveau de protection unique pour tous les types de menaces, ou sélectionnez des niveaux individuels afin de personnaliser la protection.

Le fait de paramétrer le module à un certain niveau se traduira par la mise en œuvre d'actions conformes à ce même niveau. Par exemple, s'il est paramétré en mode **Normal**, le module détectera et contiendra les menaces qui déclenchent les niveaux de sécurité **Tolérant** et **Normal**, mais pas le seuil **Agressif**.

La protection passe d'un seuil **Tolérant** à **Agressif**.

Gardez en tête d'un niveau de détection agressif peut vous diriger vers de faux résultats positifs, tandis qu'un seuil tolérant peut exposer votre réseau à quelques menaces. Il est recommandé de définir un niveau de protection maximum dans un premier temps, puis de l'abaisser dans la mesure où de faux résultats positifs surviendraient, jusqu'à trouver l'équilibre optimal.

**Note**

Lorsque vous activez une protection pour un certain type de menaces, la détection est automatiquement réglée à la valeur par défaut (niveau **Normal**).

4. Dans la section **Actions**, configurez la manière dont HyperDetect doit réagir en cas de détection. Utilisez les options du menu déroulant afin de définir les actions à mettre en œuvre face aux menaces :
 - Pour les fichier : refuser l'accès, supprimer, mettre en quarantaine ou simplement signaler le fichier.
 - Pour le trafic du réseau : bloquer ou simplement signaler les fichiers suspects.

5. Cochez la case **Étendre le reporting à des niveaux supérieurs** juste à côté du menu déroulant, si vous souhaitez visualiser les menaces détectées à des niveaux de protection supérieurs à ceux définis.

Si vous n'êtes pas sûr de votre configuration actuelle, vous pouvez facilement réinitialiser les paramètres en cliquant sur la touche **Réglages par défaut** en bas de la page.

Anti-exploit avancé

Note

Ce module est disponible pour :

- Windows pour postes de travail

L'Anti-exploit avancé est une technologie proactive de détection des exploits en temps réel. Basée sur le Machine Learning, elle protège de tout un ensemble d'exploits connus et inconnus, y compris des attaques sans fichier en mémoire.

Pour activer la protection contre les exploits, cochez la case **Anti-exploit avancé**.

L'anti-exploit avancé est configuré pour fonctionner avec les paramètres recommandés. Vous pouvez modifier la protection si nécessaire. Pour réinitialiser les paramètres par défaut, cliquez sur le lien **Rétablir les paramètres par défaut** situé à droite du titre de la section.

Les paramètres anti-exploits de GravityZone sont organisés en trois sections :

- **Détections sur tout le système**

Les techniques anti-exploits de cette section surveillent les processus système pouvant être la cible d'exploits.

Pour plus d'informations sur les techniques disponibles et sur la manière de les configurer, consultez « [Configurer la mitigation pour tout le système](#) » (p. 287).

- **Applications prédéfinies**

Le module Anti-exploit avancé est préconfiguré avec une liste des applications communes telles que Microsoft Office, Adobe Reader ou Flash Player, qui sont les plus exposées aux exploits.

Pour plus d'informations sur les techniques disponibles et sur la manière de les configurer, consultez « [Configurer les techniques spécifiques à certaines applications](#) » (p. 288).

● Applications supplémentaires

Dans cette section, vous pouvez ajouter et configurer la protection pour toutes les autres applications que vous voulez.

Pour plus d'informations sur les techniques disponibles et sur la manière de les configurer, consultez « [Configurer les techniques spécifiques à certaines applications](#) » (p. 288).

Vous pouvez développer ou réduire chaque section en cliquant sur son titre. De cette manière, vous atteindrez rapidement les paramètres que vous voulez configurer.

Configurer la mitigation pour tout le système

Sous cette section, vous disposez des options suivantes :

Technique	Description
Élévation des privilèges	Empêche les processus d'obtenir des privilèges non autorisés et d'accéder à des ressources. Action par défaut : Terminer le processus
Protection d'un processus LSASS	Empêche le processus LSASS de laisser fuir des informations sensibles telles que les sommes de contrôles de mots de passe ou les paramètres de sécurité. Action par défaut : Bloquer le processus

Ces techniques anti-exploits sont activées par défaut. Pour en désactiver une, décochez la case correspondante.

Vous pouvez également changer l'action appliquée automatiquement en cas de détection. Sélectionnez une des actions disponibles dans le menu associé :

- **Terminer le processus** : met immédiatement un terme au processus victime de l'exploit.
- **Bloquer le processus** : empêche le processus malveillant d'accéder à des ressources non autorisées.
- **Rapport uniquement** : GravityZone fait état de l'événement sans prendre aucune mesure. Vous pouvez voir les informations détaillées relatives à un événement

dans la notification **Anti-exploit avancé** et dans les rapports Applications bloquées et Audit de sécurité.

Configurer les techniques spécifiques à certaines applications

Qu'il s'agisse d'applications prédéfinies ou additionnelles, toutes partagent le même ensemble de technique anti-exploits. En voici une description :

Technique	Description
ROP Emulation	Détecte les tentatives de rendre exécutable les pages mémoire des données en utilisant la technique ROP (Return-Oriented Programming). Action par défaut : Terminer le processus
ROP Stack Pivot	Détecte les tentatives de détournement des flux du code par la technique ROP, en validant l'emplacement de la pile. Action par défaut : Terminer le processus
ROP Illegal Call	Détecte les tentatives de détournement des flux du code par la technique ROP, en validant les instructions d'appel des fonctions système sensibles. Action par défaut : Terminer le processus
ROP Stack Misaligned	Détecte les tentatives de corruption de la pile par la technique ROP, en validant l'alignement mémoire. Action par défaut : Terminer le processus
ROP Return To Stack	Détecte les tentatives d'exécution directe de code depuis la pile par la technique ROP, en validant la plage d'adresses retour. Action par défaut : Terminer le processus
ROP Make Stack Executable	Détecte les tentatives de corruption de la pile par la technique ROP, en validant la page de garde pour la pile. Action par défaut : Terminer le processus
Flash Generic	Détecte les tentatives d'exploitation de Flash Player. Action par défaut : Terminer le processus
Charge active flash	Détecte les tentatives d'exécution de code malveillant via Flash Player, en analysant les objets Flash en mémoire.

Technique	Description
	Action par défaut : Terminer le processus
VBScript Generic	Détecte les tentatives d'exploit par VBScript. Action par défaut : Terminer le processus
Exécution de code shell	Détecte les tentatives de création de nouveaux processus ou de téléchargement de fichiers par shellcode. Action par défaut : Terminer le processus
Shellcode LoadLibrary	Détecte les tentatives d'exécution de code via des chemins d'accès réseau, en utilisant du shellcode. Action par défaut : Terminer le processus
Anti-détour	Détecte les tentatives de contournement des contrôles de sécurité pour créer de nouveaux processus. Action par défaut : Terminer le processus
Shellcode EAF (Filtrage de la table des adresses d'exportations)	Détecte les tentatives d'accès à des fonctions système sensibles par du code malveillant depuis des exportations d'une DLL. Action par défaut : Terminer le processus
Thread shellcode	Détecte les tentatives d'injection de code malveillant en validant les threads nouvellement créés. Action par défaut : Terminer le processus
Anti-meterpreter	Détecte les tentatives de création d'un reverse shell en analysant les pages mémoire exécutables. Action par défaut : Terminer le processus
Création de processus obsolète	Détecte les tentatives de création de nouveau processus à l'aide d'une technique obsolète. Action par défaut : Terminer le processus
Création de processus enfants	Bloque la création de tout processus enfant. Action par défaut : Terminer le processus
Forcer le DEP Windows	Force la prévention de l'exécution des données (DEP) pour bloquer l'exécution de code depuis les pages de données. Par défaut : Désactivé

Technique	Description
Forcer la relocalisation du module (ASLR)	Empêche le chargement de code depuis des emplacements prévisibles en déplaçant les modules mémoire. Par défaut : Activé
Exploits émergents	Protège contre les menaces et les exploits, nouveaux ou émergents. Des mises à jour rapides sont utilisées pour cette catégorie avant que des changements plus complets puissent être réalisés. Par défaut : Activé

Pour surveiller les applications autres que celles qui sont prédéfinies, cliquez sur le bouton **Ajouter une application** situé en haut et en bas de la page.

Pour configurer les paramètres anti-exploits pour une application :

1. Pour les applications existantes, cliquez sur le nom de l'application. Pour les nouvelles applications, cliquez sur le bouton **Ajouter**.

Une nouvelle page présente toutes les techniques et les paramètres associés pour l'application sélectionnée.



Important

Soyez prudent lors de l'ajout de nouvelles applications à surveiller. Bitdefender ne peut garantir la compatibilité avec toutes les applications. Il est donc recommandé de tester dans un premier temps la fonctionnalité sur quelques endpoints non critiques avant de la déployer sur tout le réseau.

2. Lors de l'ajout d'une nouvelle application, saisissez son nom et les noms de ses processus dans les champs dédiés. Utiliser le point-virgule (;) pour séparer les noms de processus.
3. Pour consulter rapidement la description d'une technique, cliquez sur la flèche située à côté de son nom.
4. Cochez ou décochez la case correspondant aux techniques d'exploitation en fonction des besoins.

Utilisez l'option **Tout** si vous souhaitez cocher toutes les techniques à la fois.

5. Si nécessaire, vous pouvez modifier les actions automatiques prises en cas de détection. Sélectionnez une des actions disponibles dans le menu associé :

- **Terminer le processus** : met immédiatement un terme au processus victime de l'exploit.
- **Rapport uniquement** : GravityZone fait état de l'événement sans prendre aucune mesure. Vous pouvez voir les informations détaillées relatives à un événement dans la notification **Anti-exploit avancé** et dans les rapports.

Par défaut, toutes les techniques pour les applications prédéfinies sont configurées de sorte à circonscrire le problème, tandis que les applications additionnelles sont paramétrées de sorte que l'événement fasse uniquement l'objet d'une notification.

Pour changer rapidement la mesure prise pour toutes les techniques à la fois, sélectionnez l'action dans le menu associé avec l'option **Tout**.

Cliquez sur le bouton **Retour** en haut de la page pour retourner aux paramètres généraux de l'Anti-exploit.

Réglages

Cette section vous permet de configurer les paramètres de la quarantaine et les règles d'exclusion d'analyse.

- [Configuration des paramètres de la quarantaine](#)
- [Configurer des exceptions d'analyse](#)

Mise en quarantaine

Vous pouvez configurer les options suivantes pour les fichiers en quarantaine des endpoints cibles :

- **Suppr. les fichiers de + de (j.)** : Par défaut, les fichiers placés en quarantaine depuis plus de 30 jours sont automatiquement supprimés. Si vous souhaitez modifier cet intervalle, choisissez une option différente dans le menu.
- **Envoyer les fichiers en quarantaine aux Laboratoires Bitdefender toutes les (heures)**. Par défaut, les fichiers en quarantaine sont automatiquement envoyés aux Laboratoires Bitdefender toutes les heures. Vous pouvez modifier la fréquence d'envoi des fichiers en quarantaine (une heure par défaut). Les échantillons seront analysés par les spécialistes malwares de Bitdefender. Si

la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer.

- **Analyser de nouveau la quarantaine après la mise à jour des contenus de sécurité relatifs aux malwares.** Maintenez cette option sélectionnée pour analyser automatiquement les fichiers en quarantaine après chaque mise à jour des contenus de sécurité relatifs aux malwares. Les fichiers nettoyés sont automatiquement remis à leur emplacement d'origine.
- **Copier les fichiers en quarantaine avant d'appliquer l'action de désinfection.** Sélectionnez cette option pour éviter de perdre des données en cas de faux positifs et copier chaque fichier détecté comme étant infecté dans la quarantaine avant d'appliquer la désinfection. Vous pouvez restaurer ensuite les fichiers légitimes à partir de la page **Quarantaine**.
- **Autoriser l'utilisateur à intervenir sur la quarantaine locale.** Cette option contrôle les actions que les utilisateurs d'un endpoint peuvent réaliser sur les fichiers locaux en quarantaine via l'interface de Bitdefender Endpoint Security Tools. Par défaut, les utilisateurs locaux peuvent restaurer ou supprimer les fichiers en quarantaine de leur ordinateur en utilisant les options disponibles dans Bitdefender Endpoint Security Tools. En désactivant cette option, les utilisateurs n'auront plus accès aux boutons d'action sur les fichiers en quarantaines de l'interface de Bitdefender Endpoint Security Tools.

Quarantaine centralisée

Si vous voulez conserver les fichiers en quarantaine des endpoints que vous gérez pour une analyse approfondie, utilisez l'option **Quarantaine centralisée**, qui enverra une copie archivée de chaque fichier en quarantaine à un emplacement de partage réseau.

Après avoir activé cette option, chaque fichier en quarantaine des endpoints gérés est copié et compressé dans une archive ZIP protégée par mot de passe à un emplacement réseau défini. Le nom de l'archive est la somme de contrôle du fichier en quarantaine.



Important

La taille limite de l'archive est de 100 Mo. L'archive ne sera pas enregistrée sur l'emplacement réseau si elle dépasse 100 Mo.

Pour configurer la quarantaine centralisée, remplissez les champs suivants :

- **Mot de passe de l'archive** : saisissez le mot de passe requis pour l'archive contenant les fichiers en quarantaine. Le mot de passe doit contenir au moins une majuscule, une minuscule et un chiffre ou un caractère spécial. Confirmer le mot de passe dans le champ suivant.
- **Emplacement de partage** : saisissez le chemin réseau où vous voulez stocker les archives (par exemple `\\ordinateur\dossier`).
- **Nom d'utilisateur et mot de passe nécessaire pour se connecter au partage réseau**. Les formats pris en charge pour le nom d'utilisateur sont les suivants :
 - `utilisateur@domaine`
 - `domain\username`
 - `nom d'utilisateur`.

Pour que la quarantaine centralisée fonctionne correctement, veillez à remplir les conditions suivantes :

- L'emplacement partagé est accessible par le réseau.
- Les endpoints sont connectés au partage réseau.
- Les informations de connexion sont valides et donnent un accès en écriture au partage réseau.
- Le partage réseau dispose de suffisamment d'espace disque.

**Note**

La quarantaine centralisée ne s'applique pas à la quarantaine des serveurs de messagerie.

Bitdefender GravityZone

Tableau de bord

Réseau

Inventaire des applications

Packages

Tâches

Politiques

Règles d'affectation

Rapports

Quarantaine

Comptes

Activité des utilisateurs

Configuration

Mise à jour

Licence

Général

Antimalware

À l'accès

À la demande

Configuration

Serveurs de sécurité

Pare-feu

Contrôle de contenu

Contrôle des applications

Contrôle des appareils

Relais

Quarantaine

Suppr. les fichiers de plus de (j.) :

30

1

Envoyer les fichiers en quarantaine aux Laboratoires Bitdefender toutes les (heures)

Analyser de nouveau la quarantaine après la mise à jour des signatures de malwares

Copier les fichiers en quarantaine avant d'appliquer l'action de désinfection

Autoriser l'utilisateur à intervenir sur la quarantaine locale

Quarantaine centralisée

Archiver le mot de passe:

Confirmer:

Chemin d'accès du partage: \\computer\folder

Partager le nom d'utilisateur: domain\userj

Partager le mot de passe:

Quarantaine centralisée

Si vous avez une instance locale de Sandbox Analyzer de configurée dans la section **Sandbox Analyzer > Capteur de l'endpoint**, vous pouvez cocher la case **Envoyer automatiquement les éléments en quarantaine à Sandbox Analyzer**. Attention, les éléments envoyés ne peuvent pas faire plus que 50 Mo.

Exclusions

L'agent de sécurité de Bitdefender peut exclure de l'analyse certains types d'objets. Les exceptions de l'antimalware sont à utiliser dans des circonstances spécifiques ou selon les recommandations de Microsoft ou de Bitdefender. Pour une liste actualisée des exclusions recommandées par Microsoft, veuillez vous référer à cet [article](#).

Cette section vous permet de configurer l'utilisation de différents types d'exclusions disponibles avec l'agent de sécurité de Bitdefender.

- Les **Exclusions préconfigurées** sont activées et incluses par défaut dans l'agent de sécurité de Bitdefender.

Vous pouvez choisir de désactiver les exclusions préconfigurées, si vous souhaitez analyser tous les types d'objets, mais cette option aura un impact considérable sur les performances de la machine et augmentera la durée de l'analyse.

- Vous pouvez également définir des **Exclusions personnalisées** pour les applications développées en interne ou les outils personnalisés en fonction de vos besoins.

Les exclusions antimalware personnalisées s'appliquent à une ou plusieurs des méthodes d'analyse suivantes :

- Analyse à l'accès
- Analyse à la demande
- Advanced Threat Control
- Protection contre les attaques sans fichier
- Limitation des dégâts des ransomwares



Important

- Si vous avez un fichier test EICAR que vous utilisez régulièrement pour tester la protection antimalware, vous devriez l'exclure de l'analyse à l'accès.
- Si vous utilisez VMware Horizon View 7 et l'application Volumes AppStacks, veuillez vous référer à ce [document VMware](#).

Pour exclure des éléments spécifiques de l'analyse, sélectionnez l'option **Exclusions personnalisées** puis ajoutez des règles dans le tableau situé en-dessous.

The screenshot shows the 'Quarantaine' settings in the Bitdefender GravityZone interface. The left sidebar contains navigation options: Général, Antimalware, À l'accès, A la demande, Configuration, Pare-feu, Contrôle de contenu, and Contrôle des appareils. The main panel is titled 'Quarantaine' and includes a dropdown for 'Suppr. les fichiers de plus de (j.):' set to 30. There are three checked options: 'Envoyer les fichiers en quarantaine aux Laboratoires Bitdefender toutes les (heures)' set to 1, 'Analyser de nouveau la quarantaine après la mise à jour des signatures de malwares', and 'Copier les fichiers en quarantaine avant d'appliquer l'action de désinfection'. Below these, there are two checkboxes: 'Exclusions préconfigurées' and 'Exclusions personnalisées', with the latter being highlighted by a red box. At the bottom, a table lists exclusion rules with columns for Type, Fichiers, dossiers, extensions ou processus, Modules, and Action.

Type	Fichiers, dossiers, extensions ou processus	Modules	Action
Fichier	Chemins spécifiques	A la demande	+

Politiques des ordinateurs et machines virtuelles - Exclusions personnalisées

Pour ajouter une règle d'exclusion personnalisée :

1. Sélectionnez le type d'exclusion dans le menu:

- **Fichier** : uniquement le fichier indiqué
- **Dossier** : tous les fichiers et processus contenus dans le dossier indiqué et dans ses sous-dossiers
- **Extension** : tous les éléments présentant l'extension indiquée
- **Processus** : tous les objets auxquels accèdent les processus exclus
- **Somme de contrôle du fichier** : le fichier présentant la somme de contrôle indiquée
- **Somme de contrôle du certificat** : toutes les applications répondant à un certificat, identifié par sa somme de contrôle (empreinte)
- **Nom de la menace**: tous les éléments ayant le nom de la détection (non disponible pour les systèmes d'exploitation Linux)
- **Ligne de commande**: la ligne de commande indiquée (disponible uniquement pour les systèmes d'exploitation Windows)



Avertissement

Dans les environnements VMware sans agent intégré avec vShield, vous ne pouvez exclure que les dossiers et les extensions. En installant Bitdefender Tools sur les machines virtuelles, vous pouvez également exclure les fichiers et les processus.

Au cours du processus d'installation, lors de la configuration du package, vous devez cocher la case **Déployer l'endpoint with vShield quand un environnement VMware intégré à vShield est détecté**. Pour plus d'informations, veuillez vous référer à la rubrique **Créer des packages d'installation** du Guide d'installation.

2. Indiquez des informations spécifiques au type d'exclusion sélectionné :

Fichier, dossier ou processus

Saisissez le chemin d'accès de l'élément à exclure de l'analyse. Pour indiquer le chemin d'accès, vous disposez de plusieurs méthodes :

- Indiquer explicitement le chemin d'accès.

Par exemple : C : emp

Pour ajouter des exclusions pour des chemins d'accès inconnus, utilisez l'une des syntaxes suivantes :

```
\\hostName\shareName\filePath
```

```
\\IPAddress\shareName\filePath
```

- Utiliser les variables système disponibles dans le menu déroulant.

Pour les exclusions de processus, vous devez ajouter le nom du fichier exécutable de l'application.

Par exemple :

```
%ProgramFiles% - exclut le dossier Program Files
```

```
%WINDIR%\system32 - exclut le dossier system32 contenu dans le dossier Windows
```



Note

Il est recommandé d'utiliser les [variables du système](#) (le cas échéant) afin de s'assurer que le chemin soit valide sur tous les ordinateurs cibles.

- Utiliser des caractères génériques.

L'astérisque (*) remplace zéro caractère ou plus. Le point d'interrogation (?) remplace exactement un caractère. Vous pouvez utiliser plusieurs points d'interrogation pour définir toute combinaison d'un nombre spécifique de caractères. Par exemple, ??? remplace toute combinaison de 3 caractères précisément.

Par exemple :

Exclusions de fichier :

```
C:\Test\* - exclut tous les fichiers du dossier Test
```

```
C:\Test\*.png - exclut tous les fichiers PNG du dossier Test
```

Exclusion d'un dossier :

```
C:\Test\* - exclut tous les dossiers du dossier Test
```

Exclusion de processus :

```
C:\Program Files\WindowsApps\Microsoft.Not???.exe - exclut les processus Microsoft Notes.
```



Note

L'exclusion de processus ne prend pas en charge les caractères génériques sur les systèmes d'exploitation Linux.

Extension

Indiquez la ou les extensions de fichiers à exclure de l'analyse, séparées par un point-virgule ";" Vous pouvez saisir les extensions en les faisant précéder ou non d'un point. Par exemple, saisissez txt pour exclure les fichiers texte.



Note

Sur les systèmes Linux, les extensions de fichiers sont sensibles à la casse et les fichiers ayant les mêmes noms, mais des extensions différentes, sont des objets distincts. Par exemple, `fichier.txt` est différent de `fichier.TXT`.

Somme de contrôle de fichier, somme de contrôle de certificat, nom de la menace ou ligne de commande

Entrez la somme de contrôle du fichier, l'empreinte du certificat (somme de contrôle), le nom exact de la menace ou la ligne de commande correspondant à la règle d'exclusion. Vous pouvez utiliser un élément par exclusion.

3. Sélectionnez les méthodes d'analyse auxquelles la règle s'applique. Certaines exclusions peuvent être pertinentes pour l'analyse à l'accès, l'analyse à la demande ou l'ATC/IDS, tandis que d'autres peuvent être recommandés pour les trois modules.
4. Si vous le souhaitez, vous pouvez cliquer sur le bouton **Afficher les remarques** pour en ajouter une dans la colonne **Remarques** relative à la règle.
5. Cliquez sur le bouton **Ajouter**.

La nouvelle règle sera ajoutée à la liste.

Pour retirer une règle de la liste, cliquez sur le bouton **Supprimer** correspondant.



Important

Veillez noter que les exclusions d'analyse à la demande ne s'appliqueront pas à l'analyse contextuelle. L'analyse contextuelle se lance en faisant un clic droit sur un fichier ou un dossier et en sélectionnant **Analyser avec Bitdefender Endpoint Security Tools**.

Importer et exporter les Exclusions

Si vous comptez réutiliser les règles dans d'autres politiques, vous pouvez choisir de les exporter et de les importer.

Exporter les Exclusions personnalisées :

1. Cliquez sur **Exporter** dans le coin supérieur du tableau des exclusions.
2. Enregistrez le fichier CSV sur votre ordinateur. En fonction des paramètres de votre navigateur, le fichier peut être téléchargé automatiquement, ou on vous demandera de l'enregistrer vers un emplacement de téléchargement par défaut.

Chaque ligne dans le fichier CSV correspond à une seule règle, avec les champs dans l'ordre suivant :

```
<exclusion type>, <object to be excluded>, <modules>
```

Voici les valeurs disponibles pour les champs CSV :

Type d'exclusion :

- 1, pour exclusions de fichier
- 2, pour exclusions de dossier
- 3, pour exclusions d'extension
- 4, pour exclusions de processus
- 5, pour les exclusions de sommes de contrôle de fichier
- 6, pour les exclusions de somme de contrôle de certificat
- 7, pour les exclusions de nom de menace
- 8, pour les exclusions de ligne de commande

Objet à exclure :

Extension ou chemin d'accès fichier.

Modules :

- 1, pour analyse à la demande
- 2, pour analyse à l'accès
- 3, pour tous les modules
- 4, pour ATC/IDS

Par exemple, un fichier CSV contenant des exclusions malwares peut ressembler à ça :

```
1, "d:\\temp", 1
1, %WinDir%, 3
4, "%WINDIR%\\system32", 4
```



Note

Les chemins d'accès Windows doivent contenir le caractère (\) doublé. Par exemple, %WinDir%\\System32\\LogFiles.

Importer les Exclusions personnalisées :

1. Cliquez sur **Importer**. La fenêtre **Importer Exclusions de politique** s'ouvre.
2. Cliquez sur **Ajouter** et sélectionnez le fichier CSV.
3. Cliquez sur **Enregistrer**. Le tableau est rempli avec des règles valides. Si le fichier CSV contient des règles non valides, un message d'avertissement vous informe des numéros de rang correspondants.

Security Server

Dans cette section, vous pouvez configurer :

- [Affectation du Security Server](#)
- [Paramètres spécifiques de Security Server](#)

Politique - Ordinateurs et machines virtuelles - Antimalware - Serveurs de sécurité

Affectation du Security Server

Vous pouvez affecter un ou plusieurs Security Server à des endpoints cibles, et définir la priorité avec laquelle les endpoints choisiront un Security Server auquel envoyer les demandes d'analyse.

Note

Il est recommandé d'utiliser les Security Server pour analyser les machines virtuelles ou les ordinateurs avec peu de ressources.

Pour affecter un Security Server aux endpoints cibles, ajouter les Security Server que vous voulez utiliser dans le tableau **Affectation du Security Server**, comme suit :

1. Cliquez sur le menu déroulant **Security Server** et sélectionnez un Security Server.
2. Si le Security Server est dans la DMZ ou derrière un serveur NAT, saisissez le FQDN ou l'IP du serveur NAT dans le champ **Nom/IP du serveur personnalisé**.

Important

Vérifiez que la redirection de port est correctement configurée sur le serveur NAT pour que le trafic des endpoints puisse atteindre le Security Server.

3. Cliquez sur le bouton **+ Ajouter** dans la colonne **Actions**.
Le Security Server est ajouté à la liste.

4. Répétez les instructions précédentes pour ajouter si besoin d'autres Security Server.

Pour définir la priorité des Security Server :

1. Utilisez les flèches haut et bas dans la colonne **Actions** pour augmenter ou diminuer la priorité du Security Server.

Lors de l'affectation de plusieurs Security Server, celui en haut de la liste est celui qui a la priorité la plus élevée, et qui sera donc sélectionné en premier. Si ce Security Server est indisponible ou surchargé, le Security Server suivant est sélectionné. Le trafic d'analyse est redirigé vers le premier Security Server disponible et présentant une charge adaptée.

2. Sélectionnez **Commencez par vous connecter au Security Server installé sur le même hôte physique, s'il est disponible, quelle que soit la priorité affectée** pour une distribution uniforme des endpoints et pour optimiser la latence. Si ce Security Server est indisponible, un autre Security Server de la liste est choisi, par ordre de priorité.



Important

Cette option ne fonctionne qu'avec Security Server multiplateforme et que si GravityZone est intégré à l'environnement virtualisé.

Pour supprimer un Security Server de la liste, cliquez sur le bouton  **Supprimer** dans la colonne **Actions**.

Paramètres du Security Server

Lors de l'affectation de la politique aux Security Server, pour pouvez modifier les paramètres suivants :

- **Limiter le nombre d'analyses à la demande simultanées.**

Exécuter plusieurs tâches d'analyse à la demande sur des machines virtuelles partageant la même banque de données peut entraîner des [conflits de ressources d'analyse antimalware](#). Pour empêcher cela et pour n'autoriser qu'une quantité limitée de tâches d'analyse en simultanée :

1. Sélectionnez l'option **Limiter le nombre d'analyses à la demande simultanées**.
2. Sélectionnez le niveau de tâches d'analyse simultanées autorisées dans le menu déroulant. Vous pouvez choisir un niveau prédéfini ou saisir une valeur personnalisée.

La formule pour trouver la limite maximale de tâches d'analyse pour chaque niveau prédéfini est la suivante : $N = a \times \text{MAX}(b ; \text{vCPU} - 1)$, où :

- N = limite maximale des tâches d'analyse
- a = coefficient multiplicateur, avec les valeurs suivantes : 1 - pour Bas ; 2 - pour Moyen ; 4 - pour Élevé
- $\text{MAX}(b ; \text{vCPU} - 1)$ = une fonction qui renvoie le nombre maximal de slots d'analyse disponibles sur le Security Server.
- b = le nombre par défaut de slots d'analyse à la demande, actuellement réglé sur quatre.
- vCPU = nombre de processeurs virtuels affectés au Security Server

Par exemple :

Pour un Security Server avec 12 processeurs et un niveau Élevé d'analyses simultanées, nous avons une limite de :

$N = 4 \times \text{MAX}(4 ; 12 - 1) = 4 \times 11 = 44$ tâches d'analyse à la demande simultanées.

● Activez les règles d'affinité pour Security Server Multi-Platform

Choisissez le comportement voulu pour le Security Server lorsque son hôte passe en mode maintenance :

- Si activé, le Security Server reste lié à l'hôte et GravityZone l'arrête. Lorsque la maintenance est terminée, GravityZone redémarre automatiquement le Security Server.

Il s'agit du comportement par défaut.

- Si désactivé, le Security Server est déplacé vers un autre hôte et continue de fonctionner. Dans ce cas, le nom du Security Server change dans Control Center pour indiquer l'ancien hôte. Ce changement de nom persiste jusqu'à ce que le Security Server soit redéplacé vers son hôte d'origine.

Si les ressources le permettent, le Security Server peut être déplacé vers un hôte sur lequel un Security Server est déjà installé.



Important

Cette option n'a aucun effet si le Security Server est également utilisée par HVI.

- **Utiliser le protocole SSL**

Activez cette option si vous souhaitez chiffrer la connexion entre les endpoints cibles et les appliances Security Server spécifiées.

Par défaut, GravityZone utilise des certificats de sécurité auto-signés. Vous pouvez les remplacer par vos propres certificats sur la page **Configuration > Certificats** de Control Center. Pour plus d'informations, veuillez vous référer au chapitre "Configurer les paramètres de Control Center" du Guide d'installation.

- **Communication entre les Security Server et GravityZone**

Choisissez une des options disponibles pour définir vos préférences en matière de proxy pour la communication entre les machines Security Servers sélectionnées et GravityZone .

- **Conserver les paramètres d'installation**, pour utiliser les mêmes paramètres proxy que ceux du package d'installation.
- **Utiliser le proxy défini dans la section Général**, pour utiliser les paramètres du proxy définis dans la politique actuelle, sous la section **Général > Configuration**.
- **Ne pas utiliser de proxy**, lorsque les endpoints cibles ne communiquent pas avec les composants Bitdefender spécifiques via proxy.

7.2.4. Sandbox Analyzer



Note

Ce module est disponible pour :

- Windows pour postes de travail
- Windows pour serveurs

Offrant une puissante couche de protection contre les menaces avancées, Sandbox Analyzer effectue des analyses automatiques détaillées des fichiers suspects, qui n'ont pas encore été signalés par les moteurs antimalware de Bitdefender.

Dans cette section, vous pouvez configurer les éléments suivants :

- [Envoi via capteur de l'endpoint](#)
- [Envoi via capteur réseau](#)
- [Envoi via capteur ICAP](#)

● Paramètres de Sandbox Manager

Dans les paramètres de la politique, vous pouvez également configurer l'envoi automatique depuis la quarantaine centralisée. Pour plus d'informations, veuillez consulter « [Quarantaine centralisée](#) » (p. 292)

Pour en apprendre plus sur les envois manuels, rendez-vous sur « [Envoi manuel](#) » (p. 487). Pour en apprendre plus sur l'envoi via l'API, consultez les chapitres **Sandbox** et **Portail Sandbox** du [Guide des API GravityZone \(On-Premises\)](#).

Capteur endpoint

Sur les endpoints Windows, Bitdefender Endpoint Security Tools peut faire office de capteur d'alimentation pour Sandbox Analyzer.

The screenshot displays the configuration interface for the Endpoint Collector. On the left, a navigation pane lists various security features, with 'Sandbox Analyzer' and 'Capteur endpoint' selected. The main content area is divided into several sections:

- Soumission automatique d'échantillon des endpoints gérés**: A checkbox is checked, with a description: 'Activer le capteur intégré d'un endpoint pour soumettre des échantillons contenant des objets suspects à Sandbox Analyzer pour procéder à une analyse comportementale approfondie.'
- Mode analyse**: A sub-section with the text 'Réaliser l'analyse dans l'un de ces deux modes :'. Two options are listed: '- Surveiller - les objets sont toujours accessibles par l'utilisateur.' and '- Bloquer - l'utilisateur ne peut pas accéder aux objets jusqu'à réception du résultat de l'analyse.' Below this, the 'Surveiller' radio button is selected.
- Actions de réparation**: A section with the text 'Choisissez comment traiter les menaces détectées. Si l'agent de sécurité ne peut pas réaliser l'action par défaut, il appliquera la mesure de secours.' It contains two dropdown menus: 'Action par défaut' set to 'Rapport uniquement' and 'Action de secours' set to 'Mettre en Quarantaine'.
- Informations**: A section with a blue information icon and the text 'L'objectif de soumissions et les exclusions seront appliqués comme défini dans Antimalware > Analyse à l'accès et Antimalware > Paramètres'.
- Préfiltrage du contenu**: A section at the bottom of the configuration area.

Politiques > Sandbox Analyzer > Capteur endpoint

Pour configurer l'envoi automatique via le capteur de l'endpoint :

1. Sous **Paramètres de la connexion**, sélectionnez l'une des options :

- **Utiliser Cloud Sandbox Analyzer** - le capteur de l'endpoint enverra les échantillons à une instance Sandbox Analyzer hébergée par Bitdefender, en fonction de votre région.

- **Utiliser l'instance locale de Sandbox Analyzer** - le capteur de l'endpoint enverra les échantillons à une instance Sandbox Analyzer On-Premises. Choisissez votre instance Sandbox Analyzer dans le menu déroulant.

Si votre réseau se trouve derrière un serveur proxy ou un pare-feu, vous pouvez configurer un proxy afin de connecter Sandbox Analyzer, en sélectionnant la case **Utiliser la configuration proxy**.

Vous devez compléter les champs suivants :

- **Serveur** - saisissez l'adresse IP du serveur proxy
 - **Port** - saisissez le port utilisé pour se connecter au serveur proxy.
 - **Utilisateur** - indiquez un nom d'utilisateur reconnu par le serveur proxy.
 - **Mot de passe** - indiquez le mot de passe valide de l'utilisateur spécifié
2. Cochez la case **Envoi automatique d'échantillons des endpoints gérés** afin d'activer l'envoi automatique d'éléments suspects vers Sandbox Analyzer.



Important

- Sandbox Analyzer requiert l'analyse à l'accès. Assurez-vous que votre module **antimalware et d'analyse à l'accès** soit activé.
 - Sandbox Analyzer utilise les mêmes cibles et exclusions que celles définies par **l'antimalware et l'analyse à l'accès**. Examinez attentivement les paramètres de l'analyse à l'accès, lors de la configuration de Sandbox Analyzer.
 - Afin d'éviter les faux résultats positifs (détection incorrecte d'applications légitimes), vous pouvez définir des exclusions par nom de fichier, extension, taille de fichier et chemin de fichier. Pour plus d'informations sur l'analyse à l'accès, reportez-vous à « [Antimalware](#) » (p. 263).
 - La limite de téléchargement pour n'importe quel fichier ou dossier est de 50 Mo.
3. Choisissez le **Mode analyse**. Vous avez deux options :
- **Surveillance**. L'utilisateur peut accéder au fichier pendant l'analyse sandbox, mais il est recommandé de ne pas l'ouvrir avant d'avoir reçu les résultats de l'analyse.
 - **Blocage**. L'utilisateur ne peut pas exécuter le fichier, tant que les résultats d'analyse n'ont pas été renvoyés vers l'endpoint depuis Sandbox Analyzer Cluster via Sandbox Analyzer Portal.

4. Indiquer les **actions de réparation**. Celles-ci sont appliquées lorsque Sandbox Analyzer détecte une menace. Pour chaque mode d'analyse, une double configuration vous est fournie, composée d'une action par défaut et d'une action de secours. Sandbox Analyzer exécute l'action par défaut dans un premier temps, puis l'action de secours, si la précédente n'a pas pu être réalisée.

Lorsque vous accédez à cette section pour la toute première fois, les configurations suivantes sont disponibles :

**Note**

Conformément aux bonnes pratiques, il est recommandé d'appliquer des actions de réparation dans cette configuration.

- Avec le mode **Surveillance**, l'action par défaut consiste à **Signaler exclusivement**, et l'action de secours est désactivée.
- Avec le mode **Blocage**, l'action par défaut consiste à **Mettre en quarantaine**, et l'action de secours est **Supprimer**.

Sandbox Analyzer vous propose les actions de réparation suivantes :

- **Désinfecter**. Il supprime le code malveillant des fichiers infectés.
- **Supprimer**. Il supprime l'ensemble des fichiers infectés du disque.
- **Quarantaine**. Il déplace les fichiers détectés de l'emplacement actuel vers le dossier de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Vous pouvez gérer les fichiers mis en quarantaine à partir de la page **Quarantaine** de Control Center.
- **Rapport uniquement**. Sandbox Analyzer rapporte uniquement les menaces détectées, sans appliquer aucune action supplémentaire.

**Note**

En fonction de l'action définie par défaut, l'action de repli sera peut-être indisponible.

5. Les actions de réparation par défaut et de secours sont configurées en mode **Rapport uniquement**.
6. Dans **Préfiltrage du contenu**, personnalisez le niveau de protection contre les menaces potentielles. Le capteur de l'endpoint embarque un mécanisme de

filtrage des contenus qui détermine si un fichier suspect doit être détoné dans Sandbox Analyzer.

Les types d'objets pris en charge sont : les applications, les documents, les scripts, les archives, les e-mails. Pour en apprendre plus sur les types d'objet pris en charge, consultez « [Types de fichier pris en charge par le préfiltrage de contenu lors de l'envoi automatique](#) » (p. 534).

Utilisez le commutateur principal en haut de la liste de menaces, afin de choisir un niveau de protection unique pour tous les types d'objets, ou sélectionnez des niveaux individuels afin de personnaliser la protection.

En fonction du niveau défini, la quantité d'échantillons envoyés variera :

- **Tolérant.** Le capteur de l'endpoint envoie automatiquement à Sandbox Analyzer uniquement les objets dont la probabilité d'être malveillant est la plus élevée, et ignore les autres objets.
- **Normal.** Le capteur de l'endpoint est équilibré entre fichiers envoyés et fichiers ignorés, et envoie à Sandbox Analyzer des objets dont la probabilité d'être malveillant est très élevée et moins élevée.
- **Agressif.** Le capteur de l'endpoint envoie à Sandbox Analyzer pratiquement tous les objets, quel que soit leur risque potentiel.

Dans un champ dédié, vous pouvez définir des exceptions pour les types d'objet que vous ne voulez pas envoyer à Sandbox Analyzer.

Vous pouvez également définir des limites de taille pour les objets envoyés en sélectionnant la case à cocher et en entrant la valeur désirée, comprise entre 1 ko et 50 Mo.

7. Dans **Profil de détonation**, ajustez le niveau de complexité de l'analyse comportementale, qui affecte les performances de Sandbox Analyzer. Par exemple, avec un niveau **Élevé**, Sandbox Analyzer réalisera une analyse plus poussée sur moins d'échantillons que ce qu'il traiterait au niveau **Moyen** ou **Faible**.

Sandbox Analyzer prend en charge l'envoi de fichiers locaux via des endpoints faisant office de relais, capables de connecter différentes adresses Sandbox Analyzer Portal, en fonction de votre région. Pour plus de détails concernant les paramètres de configuration de relais, veuillez vous référer à « [Relais](#) » (p. 358).

**Note**

Un proxy configuré dans les paramètres de connexion de Sandbox Analyzer outrepassera les endpoints dotés d'un rôle de relais.

Capteur réseau

Dans cette section, vous pouvez configurer l'envoi automatique d'échantillons du trafic réseau à Sandbox Analyzer via le capteur réseau. Ce module nécessite que Network Security Virtual Appliance soit déployé et configuré avec Sandbox Analyzer On-Premises.

Pour configurer l'envoi automatique via le capteur réseau :

1. Cochez la case **Envoi automatique d'échantillons des capteurs réseau** afin d'activer l'envoi automatique d'éléments suspects vers Sandbox Analyzer.
2. Dans **Préfiltrage du contenu**, personnalisez le niveau de protection contre les menaces potentielles. Le capteur réseau embarque un mécanisme de filtrage des contenus qui détermine si un fichier suspect doit être détoné dans Sandbox Analyzer.

Les types d'objets pris en charge sont : les applications, les documents, les scripts, les archives, les e-mails. Pour en apprendre plus sur les types d'objet pris en charge, consultez « [Types de fichier pris en charge par le préfiltrage de contenu lors de l'envoi automatique](#) » (p. 534).

Utilisez le commutateur principal en haut de la liste de menaces, afin de choisir un niveau de protection unique pour tous les types d'objets, ou sélectionnez des niveaux individuels afin de personnaliser la protection.

En fonction du niveau défini, la quantité d'échantillons envoyés variera :

- **Tolérant.** Le capteur réseau envoie automatiquement à Sandbox Analyzer uniquement les objets dont la probabilité d'être malveillant est la plus élevée, et ignore les autres objets.
- **Normal.** Le capteur réseau est équilibré entre fichiers envoyés et fichiers ignorés, et envoie à Sandbox Analyzer des objets dont la probabilité d'être malveillant est très élevée et moins élevée.
- **Agressif.** Le capteur réseau envoie à Sandbox Analyzer pratiquement tous les objets, quel que soit leur risque potentiel.

Dans un champ dédié, vous pouvez définir des exceptions pour les types d'objet que vous ne voulez pas envoyer à Sandbox Analyzer.

Vous pouvez également définir des limites de taille pour les objets envoyés en sélectionnant la case à cocher et en entrant la valeur désirée, comprise entre 1 ko et 50 Mo.

3. Sous **Paramètres de connexion**, sélectionnez l'instance Sandbox Analyzer à privilégier pour l'envoi de contenus réseau.

Si votre réseau se trouve derrière un serveur proxy ou un pare-feu, vous pouvez configurer un proxy afin de connecter Sandbox Analyzer, en sélectionnant la case **Utiliser la configuration proxy**.

Vous devez compléter les champs suivants :

- **Serveur** - saisissez l'adresse IP du serveur proxy
 - **Port** - saisissez le port utilisé pour se connecter au serveur proxy.
 - **Utilisateur** - indiquez un nom d'utilisateur reconnu par le serveur proxy.
 - **Mot de passe** - indiquez le mot de passe valide de l'utilisateur spécifié
4. Dans **Profil de détonation**, ajustez le niveau de complexité de l'analyse comportementale, qui affecte les performances de Sandbox Analyzer. Par exemple, avec un niveau **Élevé**, Sandbox Analyzer réalisera une analyse plus poussée sur moins d'échantillons que ce qu'il traiterait au niveau **Moyen** ou **Faible**.

Capteur ICAP

Dans cette section, vous pouvez configurer la soumission automatique à Sandbox Analyzer via le capteur ICAP.

Note

Sandbox Analyzer nécessite qu'un Security Server soit configuré pour analyser les serveurs de stockage en réseau (NAS) qui utilisent le protocole ICAP. Pour plus d'informations, veuillez consulter « [Protection de stockage](#) » (p. 397)

1. Cochez la case **Envoi automatique d'échantillons du capteur ICAP** afin d'activer l'envoi automatique d'éléments suspects vers Sandbox Analyzer.
2. Dans **Préfiltrage du contenu**, personnalisez le niveau de protection contre les menaces potentielles. Le capteur réseau embarque un mécanisme de filtrage des contenus qui détermine si un fichier suspect doit être détoné dans Sandbox Analyzer.

Les types d'objets pris en charge sont : les applications, les documents, les scripts, les archives, les e-mails. Pour en apprendre plus sur les types d'objet pris en charge, consultez « [Types de fichier pris en charge par le préfiltrage de contenu lors de l'envoi automatique](#) » (p. 534).

Utilisez le commutateur principal en haut de la liste de menaces, afin de choisir un niveau de protection unique pour tous les types d'objets, ou sélectionnez des niveaux individuels afin de personnaliser la protection.

En fonction du niveau défini, la quantité d'échantillons envoyés variera :

- **Tolérant.** Le capteur de l'ICAP envoie automatiquement à Sandbox Analyzer uniquement les objets dont la probabilité d'être malveillant est la plus élevée, et ignore les autres objets.
- **Normal.** Le capteur ICAP est équilibré entre fichiers envoyés et fichiers ignorés, et envoie à Sandbox Analyzer des objets dont la probabilité d'être malveillant est très élevée et moins élevée.
- **Agressif.** Le capteur de ICAP envoie à Sandbox Analyzer pratiquement tous les objets, quel que soit leur risque potentiel.

Dans un champ dédié, vous pouvez définir des exceptions pour les types d'objet que vous ne voulez pas envoyer à Sandbox Analyzer.

Vous pouvez également définir des limites de taille pour les objets envoyés en sélectionnant la case à cocher et en entrant la valeur désirée, comprise entre 1 ko et 50 Mo.

3. Sous **Paramètres de connexion**, sélectionnez l'instance Sandbox Analyzer à privilégier pour l'envoi de contenus réseau.

Si votre réseau se trouve derrière un serveur proxy ou un pare-feu, vous pouvez configurer un proxy afin de connecter Sandbox Analyzer, en sélectionnant la case **Utiliser la configuration proxy**.

Vous devez compléter les champs suivants :

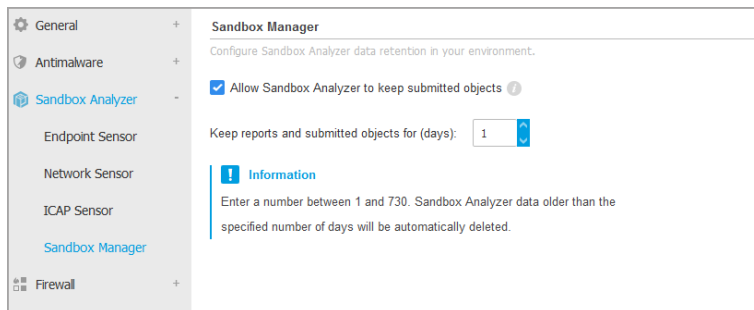
- **Serveur** - saisissez l'adresse IP du serveur proxy
 - **Port** - saisissez le port utilisé pour se connecter au serveur proxy.
 - **Utilisateur** - indiquez un nom d'utilisateur reconnu par le serveur proxy.
 - **Mot de passe** - indiquez le mot de passe valide de l'utilisateur spécifié
4. Dans **Profil de détonation**, ajustez le niveau de complexité de l'analyse comportementale, qui affecte les performances de Sandbox Analyzer. Par

exemple, avec un niveau **Élevé**, Sandbox Analyzer réalisera une analyse plus poussée sur moins d'échantillons que ce qu'il traiterait au niveau **Moyen** ou **Faible**.

Sandbox Manager

Dans cette section, vous pouvez configurer la rétention des données pour vos instances Sandbox Analyzer :

- Cochez la case **Autoriser Sandbox Analyzer à conserver les objets envoyés**. Ce paramètre vous permet d'utiliser l'option **Envoyer de nouveau en analyse** de la zone des fiches d'envoi de l'interface de reporting de Sandbox Analyzer.
- Indiquez le nombre de jours pendant lesquels Sandbox Analyzer doit conserver les rapports et les objets envoyés dans le datastore. Vous pouvez entrer un maximum de 730 données. Une fois la période définie expirée, toutes les données seront supprimées.



Politiques > Sandbox Analyzer > Sandbox Manager

7.2.5. Pare-feu



Note

Ce module est disponible pour les postes Windows.

Le pare-feu protège votre endpoint contre les tentatives de connexions entrantes et sortantes non autorisées.

La fonctionnalité du Pare-feu se fonde sur les profils du réseau. Les profils sont basés sur des niveaux de confiance, qui doivent être définis pour chaque réseau.

Le Pare-feu détecte chaque nouvelle connexion, compare les informations de l'adaptateur pour cette connexion avec les informations des profils existants, et applique le profil correct. Pour des informations détaillées sur la manière dont les profils s'appliquent, consultez « [Paramètres des réseaux](#) » (p. 316).



Important

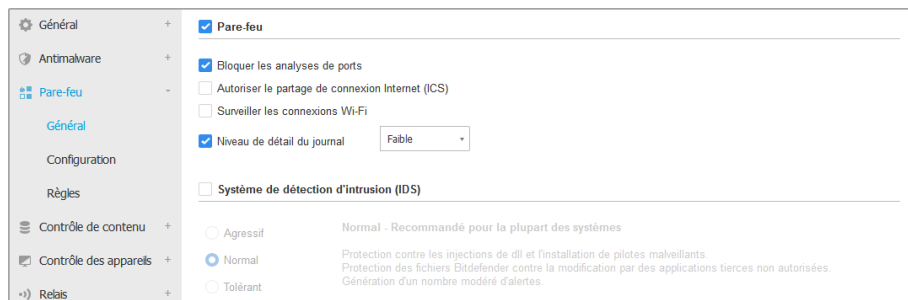
Le module Pare-feu est disponible uniquement pour les postes Windows.

Les paramètres sont organisés dans les sections suivantes :

- [Généraux](#)
- [Réglages](#)
- [Règles](#)

Généraux

Dans cette section, vous pouvez activer ou désactiver le pare-feu de Bitdefender et configurer les paramètres généraux.



Politiques des ordinateurs et machines virtuelles - Paramètres généraux du pare-feu

- **Pare-feu.** Utilisez cette case pour activer ou désactiver le pare-feu.



Avertissement

Si vous désactivez le pare-feu, les ordinateurs seront vulnérables aux attaques via le réseau et l'Internet.

- **Bloquer les analyses de ports.** Les analyses de ports sont fréquemment utilisées par les pirates pour découvrir quels ports sont ouverts sur un ordinateur. Ils

peuvent alors s'introduire dans l'ordinateur s'ils découvrent un port vulnérable ou moins sécurisé.

- **Autoriser le partage de connexion Internet (ICS).** Sélectionnez cette option pour paramétrer le pare-feu pour qu'il autorise le trafic de partage de connexion Internet.



Note

Cette option n'active pas automatiquement le partage de connexion Internet sur le système de l'utilisateur.

- **Surveiller les connexions Wi-Fi.** L'agent de sécurité de Bitdefender peut informer les utilisateurs connectés à un réseau Wifi lorsqu'un nouvel ordinateur rejoint le réseau. Pour afficher ces notifications sur l'écran de l'utilisateur, sélectionnez cette option.
- **Niveau de détail du journal.** L'agent de sécurité de Bitdefender dispose d'un journal d'événements concernant l'utilisation du module Pare-feu (activer/désactiver le pare-feu, bloquer le trafic, modifier les paramètres) ou des événements générés par les activités détectées par ce module (analyse des ports, bloquer les tentatives de connexion ou le trafic selon les règles). Choisissez une option du **Niveau de précision du journal** afin de spécifier la quantité d'informations devant figurer dans le journal.
- **Système de détection d'intrusion .** Le système de détection d'intrusion surveille le système à la recherche d'activités suspectes (par exemple, des tentatives non autorisées de modification de fichiers Bitdefender, des injections de DLL, des tentatives de keylogging etc.).



Note

Les paramètres de la politique Système de détection d'intrusion (IDS) ne s'appliquent qu'à Endpoint Security (ancien agent de sécurité). L'agent Bitdefender Endpoint Security Tools agent intègre un système de détection d'intrusion basé sur l'hôte dans son module Advanced Threat Control (ATC).

Pour configurer le système de détection d'intrusion :

1. Utilisez cette case pour activer ou désactiver le système de détection d'intrusion.

2. Cliquez sur le niveau de sécurité qui correspond le mieux à vos besoins (Agressif, Normal ou Tolérant). Utilisez la description à droite de l'échelle pour faire votre choix.

Pour éviter qu'une application légitime ne soit détectée par le système de détection d'intrusion, merci d'ajouter une **règle d'exclusion du processus ATC/IDS** pour cette application, dans la section [Antimalware > Configuration > Exclusions personnalisées](#).



Important

Le Système de détection d'intrusion est seulement disponible pour les clients Endpoint Security.

Réglages

Le pare-feu applique automatiquement un profil en fonction du niveau de confiance. Vous pouvez avoir différents niveaux de confiance pour les connexions réseau, selon l'architecture du réseau ou le type d'adaptateur utilisé pour établir la connexion réseau. Par exemple, si vous avez des sous-réseaux dans le réseau de votre entreprise, vous pouvez mettre en place un niveau de confiance pour chaque sous-réseau.

Les paramètres sont organisés dans les tableaux suivants :

- Réseaux
- Adaptateurs

Général																		
<ul style="list-style-type: none"> Général Antimalware Pare-feu Général Configuration Règles Contrôle de contenu Contrôle des appareils Relais 																		
Réseaux																		
<table border="1"> <thead> <tr> <th>Nom</th> <th>Type</th> <th>Identification</th> <th>MAC</th> <th>IP</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td colspan="6"> </td> </tr> </tbody> </table>							Nom	Type	Identification	MAC	IP	Action						
Nom	Type	Identification	MAC	IP	Action													
Adaptateurs																		
Type	Type de Réseau	Invisibilité du réseau																
Connecté	Domicile/Bureau	Désactivé																
Sans fil	Public	Désactivé																
Virtual	De confiance	Désactivé																

Politiques - Paramètres du pare-feu

Paramètres des réseaux

Si vous souhaitez que le Pare-feu applique des profils différents à plusieurs segments du réseau au sein de votre entreprise, vous devez spécifier les réseaux info gérés dans le tableau **Réseaux**. Remplissez les champs dans le tableau **Networks** comme décrit ci-dessous :

- **Nom.** Entrez le nom par lequel vous souhaitez reconnaître le réseau dans la liste.
- **Type.** Sélectionnez dans le menu le type de profil affecté au réseau.
L'agent de sécurité de Bitdefender applique automatiquement l'un des quatre profils réseau à chaque connexion réseau détectée sur l'endpoint pour définir les options de filtrage de trafic de base. Les types de profil sont :
 - Réseau **de confiance**. Désactive le Pare-feu pour les adaptateurs concernés.
 - Réseau **domestique/d'entreprise**. Permet le trafic entrant et sortant des ordinateurs dans le réseau local pendant que l'autre trafic est filtré.
 - Réseau **public**. Tout le trafic est filtré.
 - Réseau **non fiable**. Bloque complètement le trafic réseau et Internet via les adaptateurs respectifs.
- **Identification.** Sélectionnez dans le menu la méthode d'identification du réseau de l'agent de sécurité de Bitdefender. Les réseaux peuvent être identifiés par trois méthodes : **DNS**, **Passerelle** et **Réseau**.
 - **DNS**: identifie tous les endpoints à l'aide du DNS spécifié.
 - **Gateway**: identifie tous les endpoints communiquant par la passerelle spécifiée.
 - **Réseau**: identifie tous les endpoints à partir du segment réseau spécifié, défini par son adresse réseau.
- **MAC.** Utilisez ce champ pour spécifier l'adresse MAC d'un serveur DNS ou d'une passerelle qui délimite le réseau, selon la méthode d'identification choisie.
Vous devez entrer l'adresse MAC dans le format hexadécimal, séparé par des tirets (-) et des deux points (:). Par exemple : 00-50-56-84-32-2b et 00:50:56:84:32:2b sont toutes deux des adresses valides.
- **IP.** Utilisez ce champ pour définir des adresses IP spécifiques dans un réseau. Le format IP dépend de la méthode d'identification qui suit :

- **Réseau.** Entrez le numéro de réseau dans le format CIDR. Par exemple, 192.168.1.0/24 où 192.168.1.0 est l'adresse réseau et /24 est le masque réseau.
- **Passerelle.** Entrez l'adresse IP de la passerelle.
- **DNS.** Indiquez l'adresse IP du serveur DNS.

Après avoir défini un réseau, cliquez sur le bouton **Ajouter** à droite du tableau pour l'ajouter à la liste.

Paramètres des adaptateurs

Si un réseau qui n'est pas défini dans le tableau **Réseaux** est détecté, l'agent de sécurité de Bitdefender détecte le type d'adaptateur réseau et applique un profil correspondant à la connexion.

Les champs du tableau **Adaptateurs** sont décrits comme suit :

- **Type.** Affiche le type d'adaptateurs réseau. L'agent de sécurité de Bitdefender peut détecter trois types d'adaptateurs prédéfinis : **Câblé**, **Sans fil** et **Virtuel** (Réseau privé virtuel).
- **Type de Réseau.** Décrit le profil de réseau affecté à un type d'adaptateur spécifique. Les profils de réseau sont décrits dans la [section des paramètres réseau](#). Cliquez sur le champ « type de réseau » pour modifier le paramètre.

Si vous sélectionnez **Laisser Windows décider**, pour toute nouvelle connexion au réseau détectée après l'application de la politique, l'agent de sécurité de Bitdefender applique un profil de pare-feu en fonction de la classification du réseau dans Windows, en ignorant les paramètres du tableau **Adaptateurs**.

Si la détection basée sur le Gestionnaire de réseau Windows échoue, une détection de base est tentée. Un profil générique est utilisé où le profil de réseau est considéré comme **Public** et les paramètres de furtivité sont réglés sur **Activé**.

Lorsque l'endpoint joint dans Active Directory se connecte au domaine, le profil du Pare-feu passe automatiquement sur **Domicile/Pro** et les paramètres du mode furtif sur **À distance**. Si l'ordinateur n'est pas dans un domaine, cette condition n'est pas applicable.

- **Découverte du réseau.** Masque l'ordinateur face aux logiciels malveillants et pirates du réseau et face à Internet. Configurez, si besoin, la visibilité de l'ordinateur sur le réseau pour chaque type d'adaptateur en sélectionnant l'une des options suivantes :

- **Oui.** N'importe qui sur le réseau local ou sur Internet peut détecter l'ordinateur (via la commande ping).
- **non.** L'ordinateur n'est pas visible depuis le réseau local et Internet.
- **Distant.** L'ordinateur ne peut pas être détecté depuis Internet. N'importe qui sur le réseau local peut détecter l'ordinateur via la commande ping.

Règles

Cette section vous permet de configurer les règles de trafic des données et d'accès au réseau des applications gérées par le pare-feu. Veuillez noter que les paramètres disponibles s'appliquent uniquement aux **profils Domicile/Bureau** et **Public**.

Configuration

Protection: Ensemble de règles, fichiers connus et autoriser

Créer des règles agressives

Créer des règles pour les applications bloquées par l'IDS

Surveiller les modifications des processus

Ignorer les processus signés

Règles

+ Ajouter Haut Bas Exporter + Importer Supprimer

Priorité	Nom	Type de règle	Réseau	Protocole	Permission
----------	-----	---------------	--------	-----------	------------

Politiques des ordinateurs et machines virtuelles - Paramètres des règles du pare-feu

Réglages

Vous pouvez configurer les paramètres suivants :

- **Protection.** Le niveau de protection sélectionné définit la logique de prise de décisions du pare-feu utilisée lorsque des applications demandent l'accès à des services réseau et Internet. Voici les options proposées :

Ensemble de règles et autoriser

Appliquer les règles de pare-feu existantes et autoriser automatiquement toutes les autres tentatives de connexion. À chaque nouvelle tentative de connexion, une règle est créée et ajoutée à l'ensemble des règles.

Ensemble de règles et demander

Appliquer les règles de pare-feu existantes et demander à l'utilisateur de spécifier l'action à appliquer à toutes les autres tentatives de connexion. Une fenêtre d'alerte contenant des informations détaillées sur la tentative de connexion inconnue apparaît sur l'écran de l'utilisateur. À chaque nouvelle

tentative de connexion, une règle est créée et ajoutée à l'ensemble des règles.

Ensemble de règles et refuser

Appliquer les règles de pare-feu existantes et refuser automatiquement toutes les autres tentatives de connexion. À chaque nouvelle tentative de connexion, une règle est créée et ajoutée à l'ensemble des règles.

Ensemble de règles, fichiers connus et autoriser

Appliquer les règles de pare-feu existantes, autoriser automatiquement les tentatives de connexion faites par des applications connues et autoriser automatiquement toutes les autres tentatives de connexion inconnues. À chaque nouvelle tentative de connexion, une règle est créée et ajoutée à l'ensemble des règles.

Ensemble de règles, fichiers connus et demander

Appliquer les règles de pare-feu existantes, autoriser automatiquement les tentatives de connexion faites par des applications connues et demander à l'utilisateur l'action à appliquer à toutes les autres tentatives de connexion inconnues. Une fenêtre d'alerte contenant des informations détaillées sur la tentative de connexion inconnue apparaît sur l'écran de l'utilisateur. À chaque nouvelle tentative de connexion, une règle est créée et ajoutée à l'ensemble des règles.

Ensemble de règles, fichiers connus et refuser

Appliquer les règles de pare-feu existantes, autoriser automatiquement les tentatives de connexion faites par des applications connues et refuser automatiquement toutes les autres tentatives de connexion inconnues. À chaque nouvelle tentative de connexion, une règle est créée et ajoutée à l'ensemble des règles.



Note

Les fichiers connus constituent un vaste ensemble d'applications sûres, de confiance, établi et actualisé en permanence par Bitdefender.

- **Créer des règles agressives.** Si cette option est sélectionnée, le pare-feu Bitdefender va créer des règles pour chaque processus qui ouvre une application demandant un accès au réseau ou à Internet.

- **Créer des règles pour les applications bloquées par l'IDS.** Lorsque cette option est sélectionnée, le pare-feu crée automatiquement une règle **Refuser** à chaque fois que le Système de détection d'intrusion bloque une application.
- **Surveiller les modifications des processus.** Sélectionnez cette option si vous souhaitez que toute application essayant de se connecter à Internet soit examinée, de manière à voir si elle a été modifiée depuis l'ajout de la règle contrôlant ses accès Internet. Si l'application a été modifiée, une nouvelle règle sera créée en fonction du niveau de protection existant.



Note

De manière générale, ce sont les mises à jours qui modifient les applications. Il existe toutefois un risque qu'elles soient modifiées par des logiciels malveillants ayant pour objectif d'infecter ordinateur local ainsi que d'autres ordinateurs du réseau.

Les applications signées sont en principe fiables et présentent un niveau de sécurité plus élevé. Vous pouvez sélectionner **Ignorer les processus signés** pour autoriser automatiquement les applications signées modifiées à se connecter à Internet.

Règles

Le tableau Règles dresse la liste des règles de pare-feu existantes, fournissant des informations importantes sur chacune d'entre elles :

- Nom de la règle ou application à laquelle il se réfère.
- Protocole auquel s'applique la règle.
- Action de la règle (autoriser ou refuser les paquets).
- Actions que vous pouvez appliquer à cette règle.
- Priorité de la règle.



Note

Voici les règles de pare-feu appliquées expressément par la politique. Des règles supplémentaires peuvent être configurées sur les ordinateurs suite à l'application des paramètres du pare-feu.

Certaines règles de pare-feu par défaut vous aident à autoriser ou refuser facilement les types de trafic les plus courants. Sélectionnez l'option souhaitée dans le menu **Permission**.

ICMP / ICMPv6 entrants

Autoriser ou refuser les messages ICMP / ICMPv6. Les messages ICMP sont souvent utilisés par des pirates pour perpétrer des attaques contre les réseaux informatiques. Par défaut, ce type de trafic est autorisé.

Connexions bureau à distance entrantes

Autoriser ou refuser l'accès à d'autres ordinateurs sur des connexions bureau à distance. Par défaut, ce type de trafic est autorisé.

Envoi d'e-mails

Autoriser ou refuser l'envoi d'e-mails sur SMTP. Par défaut, ce type de trafic est autorisé.

HTTP navigation Web

Autoriser ou refuser la navigation Web HTTP. Par défaut, ce type de trafic est autorisé.

Impression réseau

Autoriser ou refuser l'accès aux imprimantes dans un autre réseau local. Par défaut, ce type de trafic est refusé.

Trafic Windows Explorer sur HTTP / FTP

Autoriser ou refuser le trafic HTTP et FTP de Windows Explorer. Par défaut, ce type de trafic est refusé.

Outre les règles par défaut, vous pouvez créer des règles de pare-feu supplémentaires pour d'autres applications installées sur des endpoints. Cette configuration est cependant réservée aux administrateurs avec de fortes compétences réseaux.

Pour créer et configurer une nouvelle règle, cliquez sur le bouton **+** **Ajouter** en haut du tableau. Reportez-vous à la [rubrique suivante](#) pour davantage d'informations.

Pour retirer une règle de la liste, sélectionnez-la et cliquez sur le bouton **-** **Supprimer** en haut du tableau.



Note

Vous ne pouvez ni supprimer ni modifier les règles par défaut du pare-feu.

Configuration des règles personnalisées

Vous pouvez configurer deux types de règles de pare-feu :

- **Les règles basées sur les applications.** Ces règles s'appliquent à certains logiciels détectés sur les ordinateurs clients.
- **Les règles basées sur la connexion.** Ces règles s'appliquent à toute application ou service qui utilise une connexion spécifique.

Pour créer et configurer une nouvelle règle, cliquez sur le bouton **+ Ajouter** en haut du tableau et sélectionnez le type de règle souhaité dans le menu. Pour modifier une règle existante, cliquez sur le nom de la règle.

Les paramètres suivants peuvent être configurés :

- **Nom de la règle.** Indiquez le nom sous lequel la règle apparaîtra dans le tableau des règles (par exemple, le nom de l'application à laquelle la règle s'applique).
- **Chemin de l'application** (uniquement pour les règles basées sur les applications). Vous devez spécifier le chemin du fichier exécutable de l'application sur les ordinateurs cibles.
 - Choisissez un emplacement prédéfini dans le menu et complétez le chemin selon vos besoins. Par exemple, pour une application installée dans le dossier `Program Files`, sélectionnez `%ProgramFiles%` et complétez le chemin en ajoutant une barre oblique inverse (`\`) et le nom du dossier de l'application.
 - Indiquez le chemin complet dans le champ de saisie. Il est recommandé d'utiliser les variables du système (le cas échéant) afin de s'assurer que le chemin soit valide sur tous les ordinateurs cibles.
- **Ligne de commande** (uniquement pour les règles basées sur les applications). Si vous souhaitez que la règle soit appliquée uniquement quand l'application spécifiée est ouverte à l'aide d'une commande spécifique dans l'interface de commande en ligne Windows, entrez la commande respective dans le champ de saisie. Sinon laissez-le vide.
- **MD5 de l'application** (uniquement pour les règles basées sur les applications). Si vous souhaitez que la règle vérifie l'intégrité des données du fichier de l'application en fonction de son code de hachage MD5, indiquez-le dans le champ de saisie. Dans le cas contraire, laissez le champ vide.
- **Adresse locale.** Spécifiez l'adresse IP locale et le port auxquels s'applique la règle. Si vous avez plus d'un adaptateur réseau, vous pouvez décocher la case

Tous et entrer une adresse IP spécifique. De même, pour filtrer les connexions sur un port ou une plage de ports spécifique, décochez la case **Tous** et indiquez le port ou la plage de ports souhaité dans le champ correspondant.

- **Adresse distante.** Spécifiez l'adresse IP distante et le port auxquels s'applique la règle. Pour filtrer le trafic depuis et vers un ordinateur spécifique, décochez la case **Tous** et entrez son adresse IP.
- **Appliquer la règle uniquement pour les ordinateurs connectés directement.** Vous pouvez filtrer l'accès en fonction de l'adresse Mac.
- **Protocole.** Sélectionnez le protocole IP auquel s'applique la règle.
 - Si vous voulez que la règle s'applique à tous les protocoles, sélectionnez **Toutes**.
 - Si vous souhaitez que la règle s'applique au protocole TCP, sélectionnez **TCP**.
 - Si vous souhaitez que la règle s'applique au protocole UDP, sélectionnez **UDP**.
 - Si vous souhaitez que la règle s'applique à un protocole spécifique, sélectionnez ce protocole dans le menu **Autre**.



Note

Les numéros des protocoles IP sont attribués par l'IANA (Internet Assigned Numbers Authority, l'organisation de gestion de l'adressage IP sur Internet). Vous pouvez obtenir la liste complète des numéros de protocoles IP attribués à l'adresse <http://www.iana.org/assignments/protocol-numbers>.

- **Direction.** Sélectionnez la direction du trafic à laquelle s'applique la règle.

Direction	Description
Sortant	La règle s'applique seulement pour le trafic sortant.
Entrant	La règle s'applique seulement pour le trafic entrant.
Tous les deux	La règle s'applique dans les deux directions.

- **Version IP.** Sélectionnez la version du protocole IP (IPv4, IPv6 ou autre) à laquelle s'applique la règle.

- **Réseau.** Sélectionnez le type de réseau auquel s'applique la règle.
- **Permission.** Sélectionnez l'une des permissions disponibles :

Permission	Description
✓	L'application spécifiée se verra autoriser l'accès réseau/Internet dans les circonstances spécifiées.
✗	L'application spécifiée se verra refuser l'accès réseau/Internet dans les circonstances spécifiées.

Cliquez sur **Enregistrer** pour ajouter la règle.

Pour les règles que vous avez créées, utilisez les flèches à la droite du tableau pour définir chaque priorité de règle. La règle ayant le plus haut niveau de priorité est la plus proche du haut de la liste.

Importer et exporter des règles

Vous pouvez exporter et importer des règles du Pare-Feu pour les utiliser dans d'autres politiques ou pour d'autres entreprises. Pour exporter des règles :

1. Cliquez sur **Exporter** dans le coin supérieur du tableau des règles.
2. Enregistrez le fichier CSV sur votre ordinateur. En fonction des paramètres de votre navigateur, le fichier peut être téléchargé automatiquement, ou on vous demandera de l'enregistrer vers un emplacement de téléchargement par défaut.

Important

- Chaque ligne dans le fichier CSV correspond à une seule règle, et a des multiples champs.
- La priorité des règles du Pare-Feu est déterminée par leur position dans le fichier CSV. Vous pouvez modifier la priorité de la règle en déplaçant la ligne entière.

Pour les règles par défaut, vous ne pouvez modifier que les éléments suivants :

- **Priorité** : Définissez la priorité désirée de la règle en déplaçant les lignes du fichier CSV.
- **Permission** : Modifiez le champ `set.Permission` en utilisant les permissions disponibles :

- 1 pour **Autoriser**
- 2 pour **Refuser**

Toute autre modification sera supprimée à l'importation.

Pour les règles personnalisées de Pare-Feu, toutes les valeurs de champs sont configurables comme suit :

Champ	Nom et valeur
ruleType	Type de règle: 1 pour Règle d'applications 2 pour Règle de connexion
type	La valeur de ce champ est optionnelle.
details.name	Nom de la règle
details.applicationPath	Chemin de l'application (uniquement pour les règles basées sur les applications)
details.commandLine	Ligne de commande (uniquement pour les règles basées sur les applications)
details.applicationMd5	MD5 de l'application (uniquement pour les règles basées sur les applications)
settings.protocol	Protocole 1 pour N'importe lequel 2 pour TCP 3 pour UDP 4 pour Autre
settings.customProtocol	Uniquement nécessaire si Protocole est configuré sur Autre . Pour saisir des valeurs spécifiques, consultez cette

Champ	Nom et valeur
	page . Les valeurs 0, 4, 6, 41, 61, 63, 68, 99, 114, 124, 34-37, 141-143 ne sont pas prises en charge.
<code>settings.direction</code>	Direction : 1 pour Les deux 2 pour Entrant 3 pour Sortant
<code>settings.ipVersion</code>	Version IP: 1 pour N'importe lequel 2 pour IPv4 3 pour IPv6
<code>settings.localAddress.any</code>	Adresse locale est configuré sur N'importe laquelle : 1 pour Vrai 0 ou vide pour Faux
<code>settings.localAddress.ipMask</code>	Adresse locale est configuré sur IP ou IP/Masque
<code>settings.remoteAddress.portRange</code>	Adresse distante est configurée sur Port ou plage de ports
<code>settings.directlyConnected.enable</code>	Appliquer la règle uniquement pour les ordinateurs connectés directement: 1 pour Activé 0 ou vide pour Désactivé
<code>settings.directlyConnected.remoteMac</code>	Appliquer la règle uniquement pour les ordinateurs connectés directement avec le filtre Adresse MAC.

Champ	Nom et valeur
<code>permission.home</code>	Le Réseau auquel la règle s'applique est Domicile/Bureau : : 1 pour Vrai 0 pour vide ou Faux
<code>permission.public</code>	Le Réseau auquel la règle s'applique est Public : : 1 pour Vrai 0 pour vide ou Faux
<code>permission.setPermission</code>	Permissions disponibles : 1 pour Autoriser 2 pour Refuser

Pour importer des règles :

1. Cliquez sur **Importer** en haut du tableau des Règles.
2. Dans la nouvelle fenêtre, cliquez sur **Ajouter** et sélectionnez le fichier CSV.
3. Cliquez sur **Enregistrer**. Le tableau est rempli avec des règles valides.

7.2.6. Protection du réseau

Utilisez la section Protection du réseau pour configurer vos préférences en ce qui concerne le filtrage du contenu, la protection des données relatives à l'activité des utilisateurs, comme la navigation sur le web, les e-mails et les applications logicielles, et la détection des techniques d'attaque réseau tentant d'accéder à un endpoint spécifique. Vous pouvez limiter ou autoriser l'accès à Internet et l'utilisation des applications, configurer l'analyse du trafic, l'antiphishing et les règles de protection des données.

Veillez noter que les paramètres configurés de la Protection du réseau s'appliqueront à tous les utilisateurs qui se connecteront aux ordinateurs cibles.

Les paramètres sont organisés dans les sections suivantes :

- [Généraux](#)
- [Contrôle de contenu](#)

- [Protection Web](#)
- [Attaques de réseau](#)

Note

- Le module Contrôle de contenu est disponible pour :
 - Windows pour postes de travail
 - macOS
- Le module Network Attack Defense est disponible pour :
 - Windows pour postes de travail

Important

Pour macOS, le Contrôle des contenus s'appuie sur une extension de noyau. L'installation d'une extension de noyau nécessite votre accord sur macOS High Sierra (10.13) et supérieur. Le système notifie l'utilisateur qu'une extension système de Bitdefender a été bloquée. L'utilisateur peut l'autoriser à partir des préférences relatives à la **Sécurité & à la Vie privée**. Tant que l'utilisateur n'aura pas approuvé l'extension système de Bitdefender, ce module ne fonctionnera pas et l'interface utilisateur de Endpoint Security for Mac affichera une erreur critique demandant un accord.

Afin d'éviter l'intervention de l'utilisateur, vous pouvez pré-approuver l'extension de noyau Bitdefender en l'inscrivant sur une liste blanche à l'aide d'un outil de gestion des appareils mobiles. Pour plus d'informations concernant les extensions de noyau Bitdefender, reportez-vous à [cet article de la base de connaissances](#).

Généraux

Sur cette page, vous pouvez configurer des options en activant ou désactivant certaines fonctionnalités et configurer les exclusions.


Les paramètres sont organisés dans les sections suivantes :

- [Paramètres généraux](#)
- [Exclusions globales](#)



Politiques des ordinateurs et machines virtuelles - Protection réseau - Généralités

Paramètres généraux

- **Analyse SSL.** Sélectionnez cette option si vous souhaitez que le trafic web SSL (Secure Sockets Layer) soit inspecté par les modules de protection de l'agent de sécurité de Bitdefender.
- **Afficher la barre d'outils du navigateur (ancienne version).** La barre d'outils de Bitdefender informe les utilisateurs de la note attribuée aux pages web qu'ils consultent. La barre d'outils de Bitdefender n'est pas votre barre d'outils de navigateur typique. La seule chose qu'il ajoute au navigateur est un petit bouton  en haut de chaque page web. Cliquer sur le bouton ouvre la barre d'outils.

En fonction de la façon dont Bitdefender classe la page web, l'un des résultats suivants s'affiche dans la partie gauche de la barre d'outils :

- Le message "Cette page n'est pas sûre" apparaît sur un fond rouge.
- Le message "Nous vous recommandons d'être vigilant" apparaît sur un fond orange.
- Le message "Cette page est sûre" apparaît sur un fond vert.



Note

- Cette option n'est pas disponible pour macOS.
- Cette option est supprimée de Windows à compter des nouvelles installations de Bitdefender Endpoint Security Tools version 6.6.5.82.

- **Search Advisor du navigateur (ancienne version).** Search advisor évalue les résultats des recherches Google, Bing et Yahoo!, ainsi que tous les liens Facebook et Twitter en plaçant une icône devant chaque résultat. Icônes utilisées et leur signification :
 - ✖ Nous vous déconseillons de consulter cette page Web.
 - ⚠ Cette page Web peut contenir du contenu dangereux. Soyez prudent si vous décidez de le consulter.
 - ✔ Cette page peut être consultée en toute sécurité.



Note

- Cette option n'est pas disponible pour macOS.
- Cette option est supprimée de Windows à compter des nouvelles installations de Bitdefender Endpoint Security Tools version 6.6.5.82.

Exclusions globales

Vous pouvez choisir de ne pas analyser une partie du trafic à la recherche de malwares lorsque les options **Network Protection** sont activées.



Note

Ces exclusions s'appliquent à l'**Analyse du trafic** et à l'**Antiphishing**, dans la section **Protection Web**, et à **Network Attack Defense**, dans la section **Attaques de réseau**. Les exclusions de **Protection des données** se configurent séparément, dans la section **Contrôle de contenu**.

Pour définir une exclusion :

1. Sélectionnez le type d'exclusion dans le menu.
2. En fonction du type d'exception, spécifiez comme suit l'élément du trafic à exclure de l'analyse :
 - **IP/Masque.** Saisissez l'adresse IP ou le masque d'adresses IP pour lequel vous ne voulez pas que les trafics entrant et sortant soient analysés, ce qui comprend les techniques d'attaque du réseau.
 - **URL.** Exclut de l'analyse les adresses Internet spécifiées. N'oubliez pas que les exclusions d'analyse basées sur les URL s'appliquent différemment pour les connexions HTTP et les connexions HTTPS, comme cela est expliqué plus loin.

Pour définir une exclusion basée sur un URL, procédez de la manière suivante :

- Saisissez une URL spécifique telle que `www.exemple.com/exemple.html`
 - Dans le cas des connexions HTTP, seul l'URL saisi est exclu de l'analyse.
 - Dans le cas des connexions HTTPS, l'intégralité du domaine de l'URL et tous les sous-domaines éventuels sont exclus. Par conséquent, dans ce cas, vous pouvez indiquer directement le domaine à exclusion de l'analyse.
- Utilisez des caractères génériques pour définir les schémas d'adresse web (uniquement pour les connexions HTTP).



Important

Les exceptions reposant sur des caractères génériques ne fonctionnent pas pour les connexions HTTPS.

Vous pouvez utiliser les symboles suivants :

- L'astérisque (*) remplace zéro caractère ou plus.
- Le point d'interrogation (?) remplace exactement un caractère. Vous pouvez utiliser plusieurs points d'interrogation pour définir toute combinaison d'un nombre spécifique de caractères. Par exemple, (?) remplace toute combinaison de 3 caractères précisément.

Dans le tableau suivant, vous trouverez plusieurs exemples de syntaxe pour spécifier les adresses Internet (URL).

Syntaxe	Application des exceptions
<code>www.exemple*</code>	Toute URL débutant par <code>www.exemple</code> (quelle que soit l'extension de domaine). L'exclusion ne s'appliquera pas aux sous-domaines du site web spécifié, comme <code>sousdomaine.exemple.com</code> .
<code>*exemple.com</code>	Toute URL se terminant par <code>exemple.com</code> , y compris les sous-domaines de celle-ci.

Syntaxe	Application des exceptions
exemple.com	Toute URL contenant la chaîne spécifiée.
*.com	Tout site Internet ayant l'extension de domaine .com, y compris les sous-domaines de celui-ci. Utilisez cette syntaxe pour exclure de l'analyse des domaines entiers de premier niveau.
www.exemple?.com	Toute adresse web débutant par www.exemple?.com, où ? peut être remplacé par n'importe quel caractère unique. Ces sites Web pourraient inclure : www.exemple1.com ou www.exempleA.com.




Note

Vous pouvez utiliser des URL relatives au protocole.

- **Application.** Exclut de l'analyse le processus ou l'application spécifié. Pour définir une exception à l'analyse des applications :
 - Saisissez le chemin de l'application complet. Par exemple, `C:\Program Files\Internet Explorer\iexplore.exe`
 - Utilisez les variables d'environnement pour spécifier le chemin de l'application. Par exemple : `%programfiles%\Internet Explorer\iexplore.exe`
 - Utilisez des caractères génériques pour spécifier des applications dont le nom correspond à un certain schéma. Par exemple :
 - `c*.exe` pour toutes les applications commençant par un « c » (chrome.exe).
 - `?????.exe` pour toutes les applications ayant un nom à six caractères (chrome.exe, safari.exe, etc.).
 - `[^c]*.exe` pour toutes les applications à l'exception de celles commençant par un « c ».
 - `[^ci]*.exe` pour toutes les applications à l'exception de celles commençant par un « c » ou un « i ».

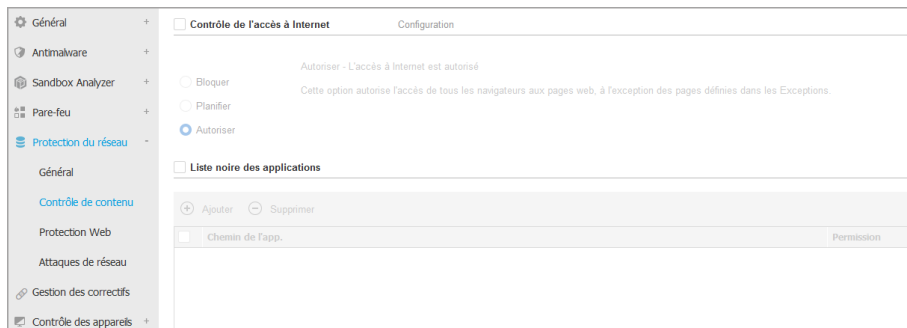
3. Cliquez sur le bouton  **Ajouter** à droite du tableau.

Pour retirer un élément de la liste, cliquez sur le bouton  **Supprimer** correspondant.

Contrôle de contenu

Les paramètres du Contrôle de contenu sont organisés sous les sections suivantes :

- [Contrôle de l'accès à Internet](#)
- [Liste noire des applications](#)
- [Protection des données](#)



Contrôle de l'accès à Internet

Le Contrôle de l'accès à Internet vous permet d'autoriser ou de bloquer l'accès à Internet pour des utilisateurs ou des applications aux moments indiqués.

Les pages Web bloquées par le Contrôle de l'accès à Internet ne s'affichent pas dans le navigateur. Une page Web est affichée par défaut et informe l'utilisateur que la page Web demandée a été bloquée par Contrôle de l'accès à Internet.

Utilisez ce bouton pour activer ou désactiver le **Contrôle de l'accès à Internet**.

Vous avez trois options de configuration :

- Sélectionnez **Autoriser** pour toujours accorder l'accès à Internet.
- Sélectionnez **Bloquer** pour toujours refuser l'accès à Internet.
- Sélectionnez **Planifier** afin d'activer des restrictions horaires pour l'accès à Internet à partir d'un planning détaillé.

Que vous choisissiez d'autoriser ou de bloquer l'accès à Internet, vous pouvez définir des exceptions à ces actions pour l'ensemble des catégories web ou

uniquement pour certaines adresses web. Cliquez sur **Configuration** pour configurer votre planification de l'accès à Internet et les exceptions comme suit :

Planificateur

Pour limiter l'accès à Internet à certaines heures de la journée sur une base hebdomadaire :

1. Sélectionnez dans la grille les intervalles pendant lesquels vous souhaitez bloquer l'accès à Internet.

Vous pouvez cliquer sur des cellules individuelles pour choisir des heures ou cliquer et faire glisser la souris sur plusieurs cellules pour bloquer de plus longues périodes. Cliquez de nouveau dans la cellule pour annuler la sélection.

Pour effectuer une nouvelle sélection, cliquez sur **Tout autoriser** ou **Tout bloquer**, en fonction du type de restriction que vous souhaitez mettre en place.

2. Cliquez sur **Enregistrer**.



Note

L'agent de sécurité de Bitdefender effectuera des mises à jour toutes les heures même si l'accès à Internet est bloqué.

Catégories

Le Filtrage par catégories filtre de façon dynamique l'accès aux sites Web en fonction de leur contenu. Vous pouvez utiliser le Filtrage par catégories afin de définir des exceptions à l'action du Contrôle de l'accès à Internet sélectionnée (Autoriser ou Bloquer) pour l'ensemble des catégories web (telles que les Jeux, Contenu pour Adultes ou réseaux sociaux).

Pour configurer le filtrage par catégories web :

1. Activez **Filtrage par catégories web**.
2. Pour une configuration rapide, cliquez sur l'un des profils prédéfinis (**Agressif**, **Normal** ou **Tolérant**). Utilisez la description à droite de l'échelle pour faire votre choix. Vous pouvez afficher les actions prédéfinies pour les catégories web disponibles en développant la section **Règles Internet** placée ci-dessous.
3. Si vous n'êtes pas satisfait des paramètres par défaut, vous pouvez définir un filtre personnalisé :

- a. Sélectionnez **Personnalisé**.
 - b. Cliquez sur **Règles Internet** pour développer la section correspondante.
 - c. Recherchez la catégorie qui vous intéresse dans la liste et sélectionnez l'action souhaitée dans le menu. Pour en apprendre plus sur les catégories de sites web disponibles, consultez [cet article de la base de connaissances](#).
4. Sélectionnez l'option **Traiter les catégories Web comme des exceptions pour l'accès Internet** si vous souhaitez ignorer les paramètres actuels de l'Accès Web et appliquer uniquement le Filtrage par catégories web.
 5. Le message par défaut affiché aux utilisateurs essayant d'accéder à des sites Internet bloqués contient également la catégorie correspondant au site. Désélectionnez l'option **Afficher des alertes détaillées sur le client** si vous souhaitez cacher ces informations à l'utilisateur.

Note

Cette option n'est pas disponible pour macOS.

6. Cliquez sur **Enregistrer**.

Note

- La permission **Autoriser** pour certaines catégories Web est également prise en compte lors des intervalles pendant lesquels l'accès à Internet est bloqué par le Contrôle de l'accès à Internet.
- **Autoriser** ne fonctionne que lorsque l'accès à Internet est bloqué par le Contrôle de l'accès à Internet, tandis que **Bloquer** ne fonctionne que lorsque l'accès à Internet est autorisé par le Contrôle de l'accès à Internet.
- Vous pouvez écraser la permission de la catégorie d'adresses Web individuelles en les ajoutant avec la permission opposée dans **Contrôle de l'accès à Internet > Configuration > Exclusions**. Par exemple, si une adresse Web est bloquée par le Filtrage par catégories web, ajoutez une règle Internet pour cette adresse avec la mention **Autoriser**.

Exclusions

Vous pouvez également définir des règles Web pour bloquer ou autoriser expressément certaines adresses Internet, écrasant ainsi les paramètres existants du Contrôle de l'accès à Internet. Les utilisateurs pourront ainsi

accéder à une page web spécifique même lorsque la navigation sur Internet est bloquée par le Contrôle de l'accès à Internet.

Pour créer une règle Internet :

1. Activez l'option **Utiliser des exceptions**.
2. Saisissez l'adresse que vous souhaitez autoriser ou bloquer dans le champ **Adresse Web**.
3. Sélectionnez **Autoriser** ou **Bloquer** dans le menu **Permission**.
4. Cliquez sur le bouton **+ Ajouter** à droite du tableau pour ajouter l'adresse à la liste d'exceptions.
5. Cliquez sur **Enregistrer**.

Pour éditer une règle Internet :

1. Cliquez sur l'adresse web que vous souhaitez éditer.
2. Modifiez l'URL existante.
3. Cliquez sur **Enregistrer**.

Pour supprimer une règle Internet, cliquez sur le bouton **⊗ Supprimer** correspondant.

Liste noire des applications


Cette section vous permet de configurer le Blocage des applications, lequel vous aide à bloquer complètement ou à limiter l'accès des utilisateurs à des applications sur leurs ordinateurs. Les jeux, logiciels de messagerie, comme d'autres catégories de logiciels (y compris malveillants) peuvent être bloqués de cette façon.

Pour configurer le Blocage des applications :

1. Activez l'option **Blocage des applications**.
2. Spécifiez les applications auxquelles vous souhaitez limiter l'accès. Pour limiter l'accès à une application :
 - a. Cliquez sur le bouton **+ Ajouter** en haut du tableau. Une fenêtre de configuration s'affiche.
 - b. Vous devez spécifier le chemin du fichier exécutable de l'application sur les ordinateurs cibles. Il y a deux façons de procéder :
 - Choisissez un emplacement prédéfini dans le menu et complétez le chemin selon vos besoins dans le champ de saisie. Par exemple, pour une application installée dans le dossier `Program Files`, sélectionnez

%ProgramFiles et complétez le chemin en ajoutant une barre oblique inverse (\) et le nom du dossier de l'application.

- Indiquez le chemin complet dans le champ de saisie. Il est recommandé d'utiliser les [variables du système](#) (le cas échéant) afin de s'assurer que le chemin soit valide sur tous les ordinateurs cibles.
- c. **Accéder au Planificateur.** Planifiez l'accès aux applications à certaines heures de la journée sur une base hebdomadaire :
- Sélectionnez dans la grille les intervalles pendant lesquels vous souhaitez bloquer l'accès à cette application. Vous pouvez cliquer sur des cellules individuelles pour choisir des heures ou cliquer et faire glisser la souris sur plusieurs cellules pour bloquer de plus longues périodes. Cliquez de nouveau dans la cellule pour annuler la sélection.
 - Pour effectuer une nouvelle sélection, cliquez sur **Tout autoriser** ou **Tout bloquer**, en fonction du type de restriction que vous souhaitez mettre en place.
 - Cliquez sur **Enregistrer**. La nouvelle règle sera ajoutée à la liste.

Pour retirer une règle de la liste, sélectionnez-la et cliquez sur le bouton  **Supprimer** en haut du tableau. Pour modifier une règle existante, cliquez dessus pour ouvrir sa fenêtre de configuration.

Protection des données

La Protection des données empêche la divulgation non autorisée de données sensibles grâce à des règles définies par l'administrateur.



Note

Cette fonctionnalité n'est pas disponible pour macOS.


Vous pouvez créer des règles pour protéger toute information personnelle ou confidentielle, telle que :

- Informations personnelles du client
- Noms et informations clés des produits et technologies en cours de développement
- Informations de contact de cadres de l'entreprise

Les informations protégées peuvent contenir des noms, des numéros de téléphone, des informations de cartes et de comptes bancaires, des adresses e-mail etc.

En fonction des règles de protection des données que vous créez, Bitdefender Endpoint Security Tools analyse le trafic web et de messagerie sortant à la recherche de chaînes de caractères spécifiques (par exemple, un numéro de carte bancaire). Si une correspondance est trouvée, la page web ou l'e-mail est alors bloqué afin d'empêcher l'envoi des données protégées. L'utilisateur est immédiatement informé de l'action prise par Bitdefender Endpoint Security Tools par une page web d'alerte ou un e-mail.

Pour configurer la protection des données :

1. Utilisez cette case pour activer la Protection des données.
2. Créez des règles de protection des données pour toutes les données sensibles que vous souhaitez protéger. Pour créer une règle :
 - a. Cliquez sur le bouton  **Ajouter** en haut du tableau. Une fenêtre de configuration s'affiche.
 - b. Indiquez le nom sous lequel la règle figurera dans le tableau des règles. Choisissez un nom explicite afin que la règle soit facilement identifiable par vous ou un autre administrateur.
 - c. Sélectionnez le type de données que vous souhaitez protéger.
 - d. Saisissez les données que vous souhaitez protéger (par exemple, le numéro de téléphone d'un cadre de l'entreprise ou le nom interne d'un nouveau produit sur lequel l'entreprise travaille). Toute combinaison de mots, chiffres ou chaînes de caractères alphanumériques et spéciaux (tels que @, # or \$) est acceptée.



Important

Les données fournies sont stockées de manière chiffrée sur les endpoints protégés mais sont visibles à partir de votre compte Control Center. Pour plus de sécurité, n'indiquez pas toutes les données que vous souhaitez protéger. Dans ce cas, vous devez décocher l'option **Chercher les mots entiers**.

- e. Configurez les options d'analyse du trafic selon vos besoins.
 - **Analyse web (trafic HTTP)** - analyse le trafic Web (HTTP) et bloque les données sortantes correspondant aux données de la règle.

- **Analyse email (trafic SMTP)** - analyse le trafic mail (SMTP) et bloque les emails sortants qui contiennent les éléments déterminés dans la règle de gestion des données.

Vous pouvez choisir d'appliquer la règle uniquement si les données de la règle correspondent à tous les mots ou à la chaîne de caractères détectée.

- f. Cliquez sur **Enregistrer**. La nouvelle règle sera ajoutée à la liste.
3. Configurez des exceptions aux règles de protection des données afin que les utilisateurs puissent envoyer des données protégées aux sites web et aux destinataires autorisés. Les exclusions peuvent s'appliquer globalement (à toutes les règles) ou uniquement à certaines règles. Pour ajouter une exclusion :
 - a. Cliquez sur le bouton **+Ajouter** en haut du tableau. Une fenêtre de configuration s'affiche.
 - b. Indiquez l'adresse web ou e-mail à laquelle les utilisateurs sont autorisés à divulguer des données protégées.
 - c. Sélectionnez le type d'exclusion (adresse web ou e-mail).
 - d. Dans le tableau **Règles**, sélectionnez la/les règle(s) de protection des données à laquelle/auxquelles cette exclusion doit s'appliquer.
 - e. Cliquez sur **Enregistrer**. La nouvelle règle d'exclusion sera ajoutée à la liste.



Note

Si un e-mail contenant des données bloquées est adressé à plusieurs destinataires, ceux pour lesquels des exclusions ont été définies le recevront.

Pour retirer une règle ou une exclusion de la liste, cliquez sur le bouton **⊗ Supprimer** correspondant à droite du tableau.

Protection Web

Sur cette page, les paramètres sont répartis dans les sections suivantes :

- [Antiphishing](#)
- [Analyse du trafic web](#)



Politiques des ordinateurs et machines virtuelles - Protection du réseau - Protection Web

Antiphishing

La protection antiphishing bloque automatiquement les pages web de phishing connues afin d'empêcher les utilisateurs de divulguer par inadvertance des informations privées ou confidentielles à des fraudeurs en ligne. La page web de phishing est remplacée une page d'avertissement spéciale, s'affichant dans le navigateur, afin d'informer l'utilisateur que la page web requise est dangereuse.

Sélectionnez **Antiphishing** pour activer la protection antiphishing. Vous pouvez affiner le paramétrage de l'antiphishing en configurant les paramètres suivants :

- **Protection contre les escroqueries.** Sélectionnez cette option si vous souhaitez étendre la protection à d'autres types d'arnaques que le phishing. Par exemple, les sites web représentant de fausses sociétés, qui ne requièrent pas directement de données personnelles, mais qui essaient de se faire passer pour des entreprises légitimes afin de réaliser des profits en tentant de convaincre les utilisateurs de faire appel à leurs services.
- **Protection contre le phishing.** Maintenez cette option sélectionnée pour protéger les utilisateurs contre les tentatives de phishing.

Si une page web légitime est détectée à tort comme étant une page de phishing et est bloquée, vous pouvez l'ajouter à la liste blanche afin de permettre aux utilisateurs d'y accéder. La liste ne doit contenir que des sites web de confiance.


Pour gérer les exceptions de l'antiphishing :

1. Rendez-vous dans les paramètres **Général** et cliquez sur **Exclusions globales**.
2. Saisissez l'adresse web et cliquez sur le bouton **+ Ajouter**.

Si vous souhaitez exclure un site Web complet, indiquez le nom de domaine, tel que `http://www.bitdefender.fr`, et si vous souhaitez exclure uniquement une page Web, indiquez l'adresse web exacte de cette page.

**Note**

Les caractères génériques ne sont pas acceptés pour créer les URL.

3. Pour retirer une exception de la liste, cliquez sur le bouton  **Supprimer** correspondant.
4. Cliquez sur **Enregistrer**.

Analyse du trafic web

Les e-mails entrants (POP3) et le trafic web sont analysés en temps réel pour empêcher le téléchargement de malwares sur l'endpoint. Les e-mails sortants (SMTP) sont analysés afin d'éviter que des malwares n'infectent d'autres endpoints. L'analyse du trafic Web peut ralentir un peu la navigation sur Internet, mais elle bloquera les logiciels malveillants provenant d'Internet, y compris les téléchargements de type "drive-by".

Lorsqu'un e-mail infecté est détecté, il est remplacé automatiquement par un e-mail standard informant le destinataire que l'e-mail original était infecté. Si une page Web contient ou distribue des malwares, elle est automatiquement bloquée. Une page d'avertissement spéciale s'affiche à la place afin d'informer l'utilisateur que la page web requise est dangereuse.

Bien que ce ne soit pas recommandé, vous pouvez désactiver l'analyse du trafic de messagerie et web pour améliorer les performances du système. Il ne s'agit pas d'une menace majeure tant que l'analyse à l'accès des fichiers locaux demeure activée.

**Note**

Les options **E-mails entrants** et **E-mails sortants** ne sont pas disponibles pour macOS.

Attaques de réseau

Network Attack Defense fournit une couche de sécurité basée sur une technologie de Bitdefender qui détecte et prend des mesures contre les attaques réseau conçues pour accéder à des endpoints via des techniques spéciales comme : la force brute, les exploits réseau et les password stealers.

Network Attack Defense

Il s'agit d'une couche de sécurité conçue pour détecter sur le réseau les tentatives d'attaque visant à accéder à des endpoints spécifiques de votre entreprise.

Techniques Attack

<input checked="" type="checkbox"/>	Accès initial	Bloquer
<input checked="" type="checkbox"/>	Accès aux informations d'identification	Bloquer
<input checked="" type="checkbox"/>	Découverte	Bloquer
<input checked="" type="checkbox"/>	Déplacement latéral	Bloquer
<input checked="" type="checkbox"/>	Crimeware	Bloquer

Rétablir les paramètres par défaut

Politiques des ordinateurs et machines virtuelles - Protection réseau - Attaques du réseau

Pour configurer Network Attack Defense :

1. Cochez la case **Network Attack Defense** pour activer le module.
2. Sélectionnez la case correspondant à la protection contre chaque catégorie d'attaques réseau. Les techniques d'attaques réseau sont regroupées conformément à la base de connaissances MITRE ATT&CK, comme suit :
 - **Accès initial** - l'attaquant pénètre sur un réseau de diverses manières, notamment les vulnérabilités des serveurs web publics. Par exemple, les exploits de divulgation d'informations, par injection SQL et les vecteurs d'injection drive-by download.
 - **Accès aux informations d'authentification** - l'attaquant vole des informations d'authentification telles que les noms d'utilisateur et les mots de passe pour accéder aux systèmes. Par exemple : attaques par force brute, exploits par authentification non autorisée, password stealers.
 - **Découverte** - l'attaquant, une fois infiltré, essaie d'obtenir des informations sur les systèmes et le réseau interne avant de décider de la marche à suivre. Par exemple : exploits par traversée de répertoire, exploits par traversée de répertoire HTTP.
 - **Déplacement latéral** - l'attaquant explore le réseau, souvent en se déplaçant entre de multiples systèmes pour trouver sa cible principale. L'attaquant peut utiliser des outils spécifiques pour atteindre son objectif. Par exemple : exploits par injection de commande, exploits Shellshock, exploits par doubles extensions.

- **Crimeware** - cette catégorie contient les techniques conçues pour automatiser le cybercrime. Exemple de techniques de type crimeware : exploits nucléaires, divers malwares comme les chevaux de Troie et les bots.
3. Sélectionnez les mesures que vous voulez prendre pour chaque catégorie d'attaque réseau parmi les options suivantes :
- a. **Bloquer** - Network Attack Defense bloque la tentative d'attaque dès la détection.
 - b. **Rapport uniquement** - Network Attack Defense vous informe de la tentative d'attaque détectée, mais n'essaie pas de l'empêcher.

Vous pouvez facilement réinitialiser les paramètres en cliquant sur la touche **Réglages par défaut** en bas de la page.

Des informations détaillées sur les tentatives d'attaque du réseau sont disponibles dans le rapport Incidents réseau et dans la notification de l'événement Incidents du réseau.

7.2.7. Gestion des correctifs

Note Ce module est disponible pour :

- Windows pour postes de travail
- Windows pour serveurs

Le module Gestion des patchs simplifie les tâches de tenue à jour des endpoints avec les derniers patchs logiciels, en distribuant et en installant automatiquement les patchs d'un grand nombre de produits.

Note Vous pouvez consulter la liste des fournisseurs et produits pris en charge dans [cet article de la base de connaissances](#).

Cette section politique contient les paramètres de déploiement automatique des patchs. Vous devrez d'abord configurer comment les endpoints téléchargent les patchs, puis quels patchs installer et quand.

Configurer les Paramètres de téléchargement des patches

La procédure de diffusion des patches utilise des serveurs de mise en cache des patches pour optimiser le trafic réseau. Les endpoints se connectent à ces serveurs et téléchargent les patches via le réseau local. Pour assurer la meilleure disponibilité possible des patches, il est recommandé d'utiliser plusieurs serveurs.

Pour affecter des serveurs de mise en cache des patches à des endpoints cibles :

1. Dans la section **Paramètres de téléchargement des patches**, cliquez sur le champ situé en haut du tableau. Une liste des serveurs de mise en cache des patches détectés apparaît.

Si la liste est vide, il vous faut installer le rôle de serveurs de mise en cache des patches sur un relais de votre réseau. Pour plus d'informations, veuillez vous référer au Guide d'installation.

2. Sélectionnez le serveur désiré dans la liste.
3. Cliquez sur le bouton **+ Ajouter**.
4. Répétez si nécessaires ces étapes pour ajouter d'autres serveurs.
5. Utilisez les flèches haut et bas situées à droite du tableau pour définir la priorité de chaque serveur. Les serveurs prioritaires sont situés en haut de la liste.

Un endpoint demande un patch à ses serveurs par ordre de priorité. L'endpoint télécharge le patch sur le premier serveur où il le trouve. Lorsqu'un patch demandé n'est pas disponible sur un serveur, celui-ci le télécharge automatiquement auprès du fournisseur pour pouvoir répondre aux futures requêtes.

Pour supprimer un serveur dont vous n'avez plus besoin, cliquez sur le bouton Supprimer **-** situé à droite du tableau.

Sélectionnez l'option **Utiliser le site du fournisseur comme emplacement de secours pour le téléchargement des patches** pour veiller à ce que vos endpoints reçoivent les patches logiciels si les serveurs de mise en cache des patches ne sont pas disponibles.

Configurer l'analyse et l'installation des patches

GravityZone déploie les patches via deux phases indépendantes :

1. Évaluation. Lorsque la console de gestion le leur demande, les endpoints cherchent les correctifs qui leur manquent et les signalent.

2. Installation. La console envoie aux agents une liste des patches que vous voulez installer. L'endpoint télécharge les patches depuis le serveur de mise en cache des patches puis les installe.

La politique contient les réglages d'automatisation de ces procédures, partiellement ou entièrement, pour qu'elles s'exécutent périodiquement en fonction du calendrier défini.

Pour configurer l'analyse automatique des patches :

1. Cochez la case **Analyse automatique des patches**.
2. Utilisez les options de planification pour configurer la récurrence des analyses. Vous pouvez configurer l'analyse pour qu'elle soit réalisée tous les jours ou certains jours de la semaine, à l'heure de votre choix.
3. Cochez la case **Analyse intelligente après l'installation d'une nouvelle application/d'un nouveau programme** pour détecter l'installation de toute nouvelle application sur l'endpoint et identifier les patches disponibles.

Pour configurer l'installation automatique des patches :

1. Cochez la case **Installer automatiquement les patches après l'analyse**.
2. Choisissez les types de patches à installer : liés ou non à la sécurité, ou les deux.
3. Utilisez les options de planification pour configurer quand exécuter les tâches d'installation. Vous pouvez configurer l'analyse pour qu'elle soit réalisée immédiatement après la fin de l'analyse, tous les jours ou certains jours de la semaine, à l'heure de votre choix. Nous vous recommandons d'installer les correctifs de sécurité immédiatement après qu'ils ont été détectés.
4. Par défaut, tous les produits sont éligibles au processus d'installation des patches. Si vous voulez mettre à jour automatiquement uniquement certains produits, que vous considérez comme étant essentiels pour vos activités, suivez les instructions suivantes :
 - a. Cochez la case **Fournisseur et produit spécifiques**.
 - b. Cliquez sur le bouton **Fournisseur** en haut du tableau. Une liste avec tous les fournisseurs pris en charge apparaît.
 - c. Faites défiler la liste et sélectionnez un fournisseur de produits que vous voulez mettre à jour.
 - d. Cliquez sur le bouton **Produits** en haut du tableau. Une liste avec tous produits du fournisseur sélectionné apparaît.

- e. Sélectionnez tous les produits que vous voulez mettre à jour.
 - f. Cliquez sur le bouton **+** **Ajouter**.
 - g. Répétez les étapes précédentes pour les autres fournisseurs et produits.
Si vous avez oublié d'ajouter un produit, ou souhaitez au contraire en retirer un, trouvez le fournisseur dans le tableau, double-cliquez sur le champ **Produits**, et sélectionnez ou désélectionnez le produit dans la liste.
Pour supprimer un fournisseur avec tous ses produits, trouvez-le dans le tableau et cliquez sur le bouton **-** **Supprimer** correspondant à droite du tableau.
5. Pour diverses raisons, un endpoint peut être hors ligne au moment où l'installation d'un patch est planifiée. Sélectionnez l'option **Si manqué, exécuter dès que possible** pour installer les patches immédiatement après que l'endpoint soit de nouveau en ligne.
 6. Certains patches peuvent nécessiter un redémarrage du système pour finaliser l'installation. Si vous souhaitez vous en charger manuellement, sélectionnez l'option **Reporter le redémarrage**.



Important

Pour garantir la réussite de l'évaluation et de l'installation sur les endpoints Windows, vous devez veiller à respecter les prérequis suivants :

- **Autorités de certification racines de confiance** stocke le certificat **DigiCert Assured ID Root CA**.
- **Autorités de certification intermédiaires** contient le **DigiCert SHA2 Assured ID Code Signing CA**.
- Les correctifs pour Windows 7 et Windows Server 2008 R2 mentionnés dans cet article de Microsoft sont installés sur les endpoints : [Microsoft Security Advisory 3033929](#)

7.2.8. Contrôle des applications



Note

Ce module est disponible pour :

- Windows pour postes de travail
- Windows pour serveurs

Le module Contrôle des applications ajoute une autre couche de protection contre toutes sortes de menaces de logiciels malveillants (ransomwares, attaques de type zero-day, exploits visant des applications tierces, chevaux de Troie, logiciels espions, rootkits, publiciels, etc.) en empêchant les applications et les processus non autorisés de s'exécuter. Le Contrôle des applications réduit la surface d'attaque dont peuvent tirer parti les menaces de logiciels malveillants au niveau du endpoint et empêche l'installation et l'exécution de toute application non désirée, non fiable ou malveillante.

Le Contrôle des applications applique des politiques flexibles qui vous permettent d'ajouter des applications sur la liste blanche et de gérer les autorisations de mise à jour.



Contrôle des applications



Important

- Pour activer le **Contrôle des applications** pour vos clients actuellement installés, lancez la tâche **Reconfigurer le client**. Une fois le module installé, vous pouvez visualiser son état dans la fenêtre **Informations**.
- Le Contrôle des applications a une incidence majeure sur le mode Power use une fois effectuées les mises à jour des applications. Par exemple, lorsqu'une application figurant sur la liste blanche est mise à jour, l'endpoint transmet la nouvelle information. GravityZone met à jour la règle avec les nouvelles valeurs et renvoie la politique.

Vous devez exécuter la tâche **Découverte d'applications** afin de visualiser les applications et les processus en cours d'exécution sur votre réseau. Pour plus d'informations, reportez-vous à « [Découverte applications](#) » (p. 101). Ensuite, vous pouvez définir les règles du Contrôle des applications.

Le contrôle des applications possède deux modes d'exécution :

- **Mode test.** Le Contrôle des applications se contente de détecter et de signaler les applications de la Control Center, en les laissant s'exécuter comme

d'habitude. Vous pouvez configurer et tester vos règles et politiques de listes blanches, mais les applications ne seront pas bloquées.

- **Mode production.** Le Contrôle des applications bloque toutes les applications inconnues. Les processus du système d'exploitation de Microsoft et les processus de Bitdefender sont placés dans une liste blanche par défaut. Les applications définies figurant dans une liste blanche seront autorisées à s'exécuter. Pour mettre à jour les applications placées dans une liste blanche, vous devez définir des utilitaires de mise à jour. Il existe des processus spécifiques qui sont autorisés à modifier les applications existantes. Pour plus d'informations, reportez-vous à « [Inventaire des applications](#) » (p. 195).

Avertissement

- Afin de vous assurer que les applications légitimes ne sont pas limitées par le Contrôle des applications, vous devez d'abord exécuter le Contrôle des applications en mode test. De cette façon, vous pouvez vous assurer que les règles et politiques de listes blanches sont correctement définies.
- Les processus qui sont déjà en cours d'exécution au moment où le Contrôle des applications est réglé sur **Mode production** seront bloqués après le prochain redémarrage du processus.

Pour gérer l'autorisation d'exécution des applications :

1. Sélectionnez la case **Contrôle des applications** afin d'activer ce module.
2. Utilisez la case **Exécuter en mode test** pour activer ou désactiver le mode test.

Note

- En mode test, vous recevez une notification lorsque le Contrôle des applications aurait bloqué une application spécifique. Pour plus d'informations, reportez-vous à « [Types de notifications](#) » (p. 498).
- Les notifications **Application bloquée** sont affichées dans la Zone de notification lorsque de nouvelles applications sont détectées et lorsque des applications placées dans une liste noire sont bloquées.

3. Définir les règles de démarrage du processus.

Règles de démarrage du processus

Le Contrôle des applications vous permet d'autoriser manuellement des applications et processus spécifiques, sur la base du hash de l'exécutable, de l'empreinte numérique du certificat de signature et du chemin d'accès de l'application. Vous pouvez également définir des exclusions à une règle.



Note

Pour obtenir les valeurs personnalisées du hash de l'exécutable et de l'empreinte numérique du certificat utilisez « [Outils du Contrôle des applications](#) » (p. 532)

Le tableau **Règles de démarrage du processus** vous informe des règles existantes, en vous fournissant des informations importantes :

- Priorité de la règle. La règle ayant le plus haut niveau de priorité est la plus proche du haut de la liste.
- Nom et état de la règle.
- Applications cibles et leurs autorisations d'exécution. La cible représente le nombre de conditions devant être couvertes pour que la règle s'applique, ou le nombre d'applications ou de groupes auxquels la règle s'applique.

Pour créer une règle de démarrage du processus :

1. Cliquez sur le bouton **+** **Ajouter** en haut du tableau pour ouvrir la fenêtre de configuration.
2. Dans la section **Général**, saisissez un **Nom de la règle**.
3. Sélectionnez la case **Activée** pour activer la règle.
4. Dans la section **Cibles**, spécifiez la destination de la règle :
 - **Processus spécifique(s)**, pour définir un processus qui est autorisé à démarrer ou n'a pas le droit de le faire. Vous pouvez accorder une autorisation par chemin d'accès, par hash ou par certificat. Les conditions au sein de la règle sont liées par des ET logiques.
 - Pour autoriser une application à partir d'un chemin d'accès spécifique :
 - a. Sélectionnez **Chemin d'accès** dans la colonne **Type**. Spécifiez le chemin d'accès vers l'objet. Vous pouvez fournir un nom de chemin d'accès absolu ou relatif et utiliser des caractères de remplacement. Le symbole astérisque (*) correspond à n'importe quel fichier au sein d'un répertoire. Un double astérisque (**) correspond à tous les

fichiers et répertoires du répertoire défini. Un point d'interrogation (?) correspond à un caractère unique. Vous pouvez également ajouter une description afin d'aider à identifier le processus.

- b. Dans le menu déroulant **Sélectionner un ou plusieurs contextes**, vous pouvez choisir entre local, CD-ROM, amovible et réseau. Vous pouvez bloquer une application exécutée à partir d'un support amovible, ou l'autoriser si l'application est exécutée localement.
- Pour autoriser une application sur la base d'un hash, sélectionnez **Hash** dans la colonne **Type** et saisissez une valeur de hachage. Vous pouvez également ajouter une description afin d'aider à identifier le processus.



Important

Pour générer la valeur de hachage, téléchargez l'outil [Empreinte digitale](#). Pour plus d'informations, reportez-vous à « [Outils du Contrôle des applications](#) » (p. 532)

- Pour accorder une autorisation sur la base d'un certificat, sélectionnez **Certificat** dans la colonne **Type** et saisissez une empreinte numérique de certificat. Vous pouvez également ajouter une description afin d'aider à identifier le processus.



Important

Pour obtenir l'empreinte numérique du certificat, téléchargez l'outil [Empreinte numérique](#). Pour plus d'informations, reportez-vous à « [Outils du Contrôle des applications](#) » (p. 532)

Général

Nom de la règle:

Activé

Cibles

Cible:

Type	Match	Description	Contexte	Action
Certificat	Veillez saisir un thumbprint c	Veillez saisir une valeur.	Sélectionnez un ou plusieurs	
Chemin	C:\test*.exe	**wildcard	Local	
Chemin	C:\test\test1*.exe	*wildcard	Local	
Chemin	C:\test\test1\exemp?e.exe	? wildcard	Local	
Hash	aabbccddeeffgghh6789	hash description	N/D	
Certificat	aaddggyy1234567890	certificat description	N/D	

Règles d'applications

Cliquez sur **Ajouter** pour ajouter la règle.

- **Inventorier des applications ou des groupes**, pour ajouter un groupe ou une application découvert(e) sur votre réseau. Vous pouvez visualiser les applications en cours d'exécution sur votre réseau sur la page **Réseau > Inventaire des applications**. Pour plus d'informations, reportez-vous à « [Inventaire des applications](#) » (p. 195).

Insérez les noms d'applications ou de groupes dans le champ, séparés par une virgule. La fonction remplissage automatique affiche des suggestions à mesure que vous écrivez.

5. Sélectionnez la case **Inclure les sous-processus** pour appliquer la règle aux processus enfant engendrés.



Avertissement

Lorsque vous définissez des règles pour les applications de navigateur, il est recommandé de désactiver cette option afin de prévenir les risques de sécurité.

6. Éventuellement, vous pouvez également définir des exclusions à la règle de démarrage du processus. L'opération d'ajout est identique à celle décrite aux étapes précédentes.



7. Dans la section **Permissions**, choisissez d'autoriser la règle à s'exécuter ou de le lui interdire.

8. Cliquez sur **Enregistrer** pour appliquer les modifications.


Pour modifier une règle :

1. Cliquez sur le nom de la règle pour ouvrir la fenêtre de configuration.
2. Saisissez les nouvelles valeurs des options que vous souhaitez modifier.
3. Cliquez sur **Enregistrer** pour appliquer les modifications.

Pour définir la priorité de la règle :

1. Sélectionnez la case correspondant à la règle souhaitée.
2. Utilisez les boutons de priorité à droite du tableau :
 - Cliquez sur le bouton  **Haut** pour relever le niveau de la règle sélectionnée.
 - Cliquez sur  **la flèche vers le bas** pour le faire descendre.

Vous pouvez supprimer une ou plusieurs règles à la fois. Vous devez simplement :

1. Sélectionnez les règles que vous souhaitez supprimer.
2. Cliquez sur le bouton  **Supprimer** en haut du tableau. Lorsqu'une règle est supprimée, vous ne pouvez pas la récupérer.

7.2.9. Contrôle des appareils

Note

Ce module est disponible pour :

- Windows pour postes de travail
- Windows pour serveurs
- macOS

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

Important

Pour macOS, le Contrôle des appareils s'appuie sur une extension de noyau. L'installation d'une extension de noyau nécessite l'accord de l'utilisateur sur macOS

High Sierra (10.13) et supérieur. Le système notifie l'utilisateur qu'une extension système de Bitdefender a été bloquée. L'utilisateur peut l'autoriser à partir des préférences relatives à la **Sécurité & à la Vie privée**. Tant que l'utilisateur n'aura pas approuvé l'extension système de Bitdefender, ce module ne fonctionnera pas et l'interface utilisateur de Endpoint Security for Mac affichera une erreur critique demandant un accord.

Afin d'éviter l'intervention de l'utilisateur, vous pouvez pré-approuver l'extension de noyau Bitdefender en l'inscrivant sur une liste blanche à l'aide d'un outil de gestion des appareils mobiles. Pour plus d'informations concernant les extensions de noyau Bitdefender, reportez-vous à [cet article de la base de connaissances](#).

Pour utiliser le module Contrôle des appareils, vous devez d'abord l'inclure dans l'agent de sécurité installé sur les endpoints cibles, avant d'activer l'option **Contrôle des appareils** dans la politique appliquée à ces endpoints. Ensuite, à chaque fois qu'un périphérique sera connecté à un endpoint administré, l'agent de sécurité enverra des informations concernant cet événement à Control Center, dont le nom de l'appareil, la classe, l'ID, la date et l'heure de la connexion.

Dans le tableau suivant, vous trouverez les types d'appareils pris en charge par le Contrôle des appareils sur les systèmes Windows et macOS :

Type d'appareil	Windows	macOS
Adaptateurs Bluetooth	x	x
Appareils CD-ROM	x	x
Lecteurs de disquettes	x	N/A
IEEE 1284.4	x	
IEEE 1284.4	x	
Périphériques de traitement d'images	x	x
Modems	x	Gérés sous Adaptateurs réseau
Lecteurs de bande	x	N/A
Mobile Windows	x	x
Ports COM/LPT	x	Ports LPT vers ports série pris en charge
SCSI RAID	x	

Type d'appareil	Windows	macOS
Imprimantes	x	Ne prend en charge que les imprimantes connectées localement
Adaptateur de réseau	x	x (y compris les clés de sécurité Wi-Fi)
Adaptateurs réseau sans fil	x	x
Stockage interne	x	
Stockage externe	x	x



Note

- Sur macOS, si la permission **Personnalisé** est sélectionnée pour une classe spécifique d'appareils, seule la permission configurée pour la sous-catégorie **Autre** s'appliquera.
- Sur Windows et macOS, le Contrôle des appareils autorise ou interdit l'accès à l'adaptateur Bluetooth au niveau du système, en fonction de la politique définie. Il est impossible de définir des exclusions plus précises pour les appareils jumelés.

Le Contrôle des appareils permet de gérer les permissions des appareils comme suit :

- [Définir des règles d'autorisations](#)
- [Définir des exclusions de permissions](#)

Règles

La section **Règles** vous permet de définir les permissions des appareils connectés aux endpoints cibles.

Pour définir des autorisations pour le type d'appareil de votre choix :

1. Allez dans **Contrôle des appareils > Règles**.
2. Cliquez sur le nom de l'appareil dans le tableau disponible.
3. Sélectionnez un type de permission dans les options disponibles. Veuillez noter que l'ensemble de permissions disponible peut varier en fonction du type d'appareils :
 - **Autorisé** : l'appareil peut être utilisé sur l'endpoint cible.

- **Bloqué** : l'appareil ne peut pas être utilisé sur l'endpoint cible. Dans ce cas, à chaque fois que l'appareil sera connecté à l'endpoint, l'agent de sécurité déclenchera une notification indiquant que l'appareil a été bloqué.



Important

Les appareils connectés préalablement bloqués ne sont pas automatiquement débloqués lorsque le statut de la permission est modifié en **Autorisé**. L'utilisateur doit redémarrer le système ou reconnecter l'appareil afin de pouvoir l'utiliser.

- **Lecture seule** : seules les fonctions de lecture peuvent être utilisées avec l'appareil.
- **Personnalisé** : définissez différentes permissions pour chaque type de port du même appareil, tel que Firewire, ISA Plug & Play, PCI, PCMCIA, USB, etc. Dans ce cas, la liste de composants disponibles pour l'appareil sélectionné s'affiche et vous pouvez définir les permissions souhaitées pour chaque composant.

Par exemple, pour le Stockage externe, vous pouvez bloquer uniquement le port USB et permettre l'utilisation de tous les autres ports.

Stockage externe Règle	
Permission: *	Personnalisé
Description: *	External Storage
Permissions personnalisées	
Firewire:	Autorisé
ISA Plug & Play:	Autorisé
PCI:	Autorisé
PCMCIA:	Autorisé
SCSI:	Autorisé
Carte SD:	Autorisé
USB:	Autorisé
Other:	Autorisé
Enregistrer Annuler	

Politiques des ordinateurs et machines virtuelles - Contrôle des appareils - Règles

Exclusions

Lorsque les règles d'autorisations ont été définies pour différents types d'appareils, vous pouvez souhaiter exclure certains appareils ou types d'appareils de ces règles.

Vous pouvez définir des exclusions d'appareils :

- Par ID de périphérique (ou ID matériel) pour désigner les appareils individuels que vous souhaitez exclure.
- Par ID de produit (ou PID), pour désigner un ensemble de périphériques produits par le même fabricant.

Pour définir des exclusions de règles de périphériques :

1. Allez dans **Contrôle des appareils > Exclusions**.
2. Activez l'option **Exclusions**.
3. Cliquez sur le bouton **+Ajouter** en haut du tableau.
4. Sélectionnez la méthode que vous souhaitez utiliser pour ajouter des exclusions :
 - **Manuellement**. Dans ce cas, vous avez besoin de saisir chaque ID de périphérique ou ID de produit que vous souhaitez exclure, à condition que vous disposiez de la liste d'ID appropriée :
 - a. Sélectionnez le type d'exclusion (par ID de produit ou par ID de périphérique).
 - b. Sélectionnez les ID que vous souhaitez exclure dans le champ **Exceptions**.
 - c. Dans le champ **Description**, indiquez un nom qui vous aidera à identifier l'appareil ou l'ensemble d'appareils.
 - d. Sélectionnez le type de permission pour les appareils spécifiés (**Autorisé** ou **Bloqué**).
 - e. Cliquez sur **Enregistrer**.

Note

Vous pouvez configurer manuellement les exclusions de caractères génériques basées sur l'ID de l'appareil, en utilisant la syntaxe `wildcards:deviceID`. Utilisez le point d'interrogation (?) pour remplacer un caractère, et l'astérisque (*) pour remplacer un nombre quelconque de caractères dans l'ID de l'appareil. Par exemple, avec `wildcards:PCI\VEN_8086*`, tous les appareils dont l'ID contient la chaîne `PCI\VEN_8086` seront exclus de la règle de politique.

- **À partir des appareils détectés.** Vous pouvez dans ce cas sélectionner les ID d'appareils ou les ID de produits à exclure d'une liste de tous les appareils détectés dans votre réseau (concernant les endpoints administrés uniquement) :
 - a. Sélectionnez le type d'exclusion (par ID de produit ou par ID de périphérique).
 - b. Sélectionnez les ID que vous souhaitez exclure dans le tableau **Exclusions** :
 - Pour les ID de périphériques, sélectionnez tous les périphériques à exclure de la liste.
 - Pour les ID de produit, en sélectionnant un appareil, vous excluez tous les appareils ayant le même ID de produit.
 - c. Dans le champ **Description**, indiquez un nom qui vous aidera à identifier l'appareil ou l'ensemble d'appareils.
 - d. Sélectionnez le type de permission pour les appareils spécifiés (**Autorisé** ou **Bloqué**).
 - e. Cliquez sur **Enregistrer**.



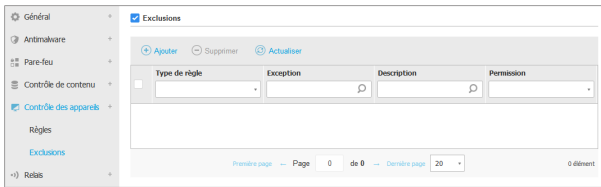
Important

- Les appareils déjà connectés aux endpoints lors de l'installation de Bitdefender Endpoint Security Tools seront détectés uniquement après le redémarrage des endpoints correspondants.
- Les appareils connectés préalablement bloqués ne sont pas automatiquement débloqués par la définition d'une exception avec la permission **Autorisé**. L'utilisateur doit redémarrer le système ou reconnecter l'appareil afin de pouvoir l'utiliser.

Toutes les exclusions d'appareils apparaîtront dans le tableau **Exclusions**.

Pour supprimer une exclusion :

1. Sélectionnez-la dans le tableau.
2. Cliquez sur le bouton  **Supprimer** en haut du tableau.



Politiques des ordinateurs et machines virtuelles - Contrôle des appareils - Exclusions

7.2.10. Relais



Note

Ce module est disponible pour :

- Windows pour postes de travail
- Windows pour serveurs
- Linux

Cette section vous permet de définir les paramètres de mise à jour et de communication des endpoints cibles auxquels on a affecté le rôle relais :

Les paramètres sont organisés dans les sections suivantes :

- [Communication](#)
- [Mise à jour](#)

Communication

L'onglet **Communication** contient les préférences en matière de proxy pour la communication entre les endpoints relais et les composants de GravityZone.

Si besoin, vous pouvez configurer séparément la communication entre les endpoints relais cibles et les Services Cloud Bitdefender / GravityZone à l'aide des paramètres suivants :

- **Conserver les paramètres d'installation**, pour utiliser les mêmes paramètres proxy que ceux du package d'installation.
- **Utiliser le proxy défini dans la section Général**, pour utiliser les paramètres du proxy définis dans la politique actuelle, sous la section **Général > Configuration**.
- **Ne pas utiliser**, lorsque les endpoints cibles ne communiquent pas avec les composants Bitdefender spécifiques via proxy.

Mise à jour

Cette section vous permet de définir les paramètres de mise à jour des endpoints cibles avec le rôle relais :

- La section **Mise à jour** vous permet de configurer les paramètres suivants :
 - La fréquence à laquelle les endpoints relais recherchent des mises à jour.
 - Le dossier situé sur un endpoint relais où les mises à jour des produits et des signatures sont téléchargées et répliquées. Si vous souhaitez définir un dossier de téléchargement spécifique, indiquez son chemin complet dans le champ correspondant.



Important

Nous vous recommandons de définir un dossier dédié aux mises à jour des produits et des signatures. Évitez de choisir un dossier contenant des fichiers système ou personnels.



- **Définir des emplacements de mise à jour personnalisés.** L'emplacement de mise à jour par défaut des agents relais est le serveur de mise à jour local de GravityZone. Vous pouvez spécifier d'autres emplacements de mise à jour en saisissant l'IP ou le nom d'hôte local d'un ou plusieurs serveurs de mise à jour de votre réseau, puis configurer leur priorité à l'aide des boutons vers le haut et vers le bas qui apparaissent au passage de la souris. Si le premier emplacement de mise à jour n'est pas disponible, l'on utilise le suivant et ainsi de suite.


Pour définir un emplacement de mise à jour personnalisé :

1. Activez l'option **Définir des emplacements de mise à jour personnalisés**
2. Indiquez l'adresse du nouveau serveur de mise à jour dans le champ **Ajouter un emplacement**. Utilisez l'une des syntaxes suivantes :
 - `ip_du_serveur_de_mise_à_jour : port`
 - `nom_du_serveur_de_mise_à_jour : port`

Le port par défaut est 7074.

3. Si l'endpoint relais communique avec le serveur local de mise à jour via un serveur proxy, sélectionnez **Utiliser un proxy**. Les paramètres proxy définis dans la section **Général > Configuration** seront pris en compte.
4. Cliquez sur le bouton **+** **Ajouter** à droite du tableau.

5. Utilisez les flèches vers le  Haut /  et vers le Bas de la colonne **Action** pour définir les emplacements de mise à jour prioritaires. Si le premier emplacement de mise à jour n'est pas disponible, le suivant est pris en compte et ainsi de suite.

Pour retirer un emplacement de la liste, cliquez sur le bouton  **Supprimer** correspondant. Bien que vous puissiez supprimer l'emplacement des mises à jour par défaut, cela n'est pas recommandé.

7.2.11. Protection Exchange



Note

Ce module est disponible pour Windows pour serveurs.

Security for Exchange dispose de paramètres extrêmement configurables, protégeant les Serveurs Microsoft Exchange contre des menaces telles que les malwares, le spam et le phishing. Lorsque la Protection Exchange est installée sur votre serveur de messagerie, vous pouvez également filtrer les e-mails contenant des pièces jointes ou du contenu considérés comme dangereux en fonction des politiques de sécurité de votre entreprise.

Pour conserver des niveaux normaux de performances, le trafic de messagerie est traité par les filtres Security for Exchange dans l'ordre suivant :

1. Filtrage antispam
2. Contrôle de contenu > Filtrage du contenu
3. Contrôle de contenu > Pièces jointes
4. Filtrage Antimalware

Les paramètres d'Security for Exchange sont répartis dans les sections suivantes :

- [Généraux](#)
- [Antimalware](#)
- [Antispam](#)
- [Contrôle de contenu](#)

Généraux

Cette section vous permet de créer et de gérer des groupes de comptes de messagerie, de définir l'ancienneté des éléments en quarantaine et d'interdire certains expéditeurs.

Groupes d'utilisateurs

Control Center permet de créer des groupes d'utilisateurs, afin d'appliquer différentes politiques d'analyse et de filtrage à différentes catégories d'utilisateurs. Vous pouvez par exemple créer des politiques adaptées au service informatique, à l'équipe commerciale ou aux dirigeants de votre entreprise.

Les groupes d'utilisateurs sont disponibles partout, quelle que soit la politique ou l'utilisateur les ayant créés.

Pour faciliter la gestion des groupes, Control Center importe automatiquement les groupes d'utilisateurs à partir de Windows Active Directory.

Pour créer un groupe d'utilisateurs :

1. Cliquez sur le bouton **+Ajouter** en haut du tableau. La fenêtre des détails s'affiche.
2. Saisissez le nom du groupe, la description et les adresses e-mail des utilisateurs.



Note

- Pour une grande liste d'adresses e-mail, vous pouvez copier-coller la liste à partir d'un fichier texte.
- Séparateurs de listes acceptés : espace, virgule, point-virgule et entrée.

3. Cliquez sur **Enregistrer**.

Les groupes personnalisés peuvent être modifiés. Cliquez sur le nom du groupe pour ouvrir la fenêtre de configuration où vous pouvez modifier les détails du groupe ou la liste d'utilisateurs.

Pour retirer un groupe personnalisé de la liste, sélectionnez le groupe et cliquez sur le bouton **- Supprimer** en haut du tableau.



Note

Vous ne pouvez pas modifier ou supprimer les groupes Active Directory.

Réglages

- **Supprimer les fichiers en quarantaine de plus de (jours)** Par défaut, les fichiers placés en quarantaine depuis plus de 30 jours sont automatiquement supprimés. Si vous souhaitez modifier ce délai, indiquez une autre valeur dans le champ correspondant.
- **Liste noire de connexion.** Lorsque cette option est activée, Exchange Server rejette tous les e-mails provenant des expéditeurs en liste noire.

Pour créer une liste noire :

1. Cliquez sur le lien **Modifier les éléments en liste noire**.
2. Indiquez les adresses e-mail que vous souhaitez bloquer. Lors de la modification de la liste, vous pouvez également utiliser des caractères génériques pour définir un domaine e-mail entier ou un modèle pour les adresses e-mails :
 - Astérisque (*), remplace zéro, un caractère ou plus
 - Le point d'interrogation (?) remplace n'importe quel caractère.Par exemple, si vous saisissez `*@boohouse.com`, toutes les adresses e-mails de `boohouse.com` seront bloquées.
3. Cliquez sur **Enregistrer**.

Vérification du domaine IP (Anti-spoofing)

Utilisez ce filtre pour empêcher les spammers de copier l'adresse e-mail de l'expéditeur et faire passer l'expéditeur de l'e-mail en question pour quelqu'un de fiable. Vous pouvez spécifier les adresses IP autorisées à envoyer des e-mails à votre domaine d'e-mails et, si nécessaire, à d'autres domaines d'e-mails connus. Si un e-mail semble venir d'un domaine listé, mais que l'adresse IP de l'expéditeur ne correspond pas à l'une des adresses IP spécifiées, l'e-mail est rejeté.



Avertissement

N'utilisez pas ce filtre si vous utilisez un smart host, un service de filtrage d'e-mails ou bien une solution de filtrage d'e-mails passerelles à l'avant de vos serveurs Exchange.



Important

- Le filtre ne vérifie que les connexions e-mails non authentifiées.
- Utilisation optimale :
 - Il est recommandé d'utiliser ce filtre uniquement sur les filtres Exchange qui sont directement en face d'Internet. Par exemple, si vous avez à la fois un serveur Edge Transport et Hub Transport, configurez ce filtre uniquement sur les serveurs Edge.
 - Ajoutez à votre liste de domaines toutes les adresses IP internes autorisées à envoyer des e-mails via des connexions SMTP non authentifiées. Cela peut inclure des systèmes de notifications automatisées, de l'équipement réseau comme des imprimantes, etc.

- Dans une configuration Exchange qui utilise des groupes de disponibilité de base de données, veuillez ajouter également à votre liste de domaine les adresses IP de tous vos serveurs Hub Transport et Boîte de messagerie.
- Soyez prudent si vous souhaitez configurer les adresses IP autorisées pour les domaines d'e-mails externes spécifiques qui ne sont pas administrés par vous. Si vous ne parvenez pas à maintenir la liste d'adresses IP à jour, les e-mails de ces domaines seront rejetés. Si vous utilisez une sauvegarde MX, vous devez ajouter à tous les domaines d'e-mails externes configurés les adresses IP à partir desquelles la sauvegarde MX transfère les e-mails à votre serveur de messagerie primaire.

Pour configurer le filtrage anti-spoofing, suivez les étapes décrites ci-dessous :

1. Sélectionnez la case **Vérification du Domaine IP(Antispoofing)** pour activer le filtre.
2. Cliquez sur le bouton **+Ajouter** en haut du tableau. La fenêtre de configuration s'affichera.
3. Indiquez les domaines e-mail dans le champ correspondant.
4. Fournissez l'éventail d'adresses IP autorisées pour le domaine spécifié précédemment, à l'aide du format CIDR (masque IP/réseau).
5. Cliquez sur le bouton **+ Ajouter** à droite du tableau. Les adresses IP sont ajoutées au tableau.
6. Pour retirer un élément IP de la liste, cliquez sur le bouton **⊗ Supprimer** correspondant à droite du tableau.
7. Cliquez sur **Enregistrer**. Le domaine est ajouté au filtre.

Pour supprimer un domaine d'e-mail du filtre, sélectionnez le dans le tableau Atispoofing et cliquez sur le bouton **⊖ Supprimer** en haut du tableau.

Antimalware

Le module Antimalware protège les serveurs de messagerie Exchange contre tous les types de malwares (virus, chevaux de Troie, spywares, rootkits, adwares etc.) en détectant les éléments infectés ou suspects et en tentant de les désinfecter ou d'isoler les infections, en fonction des actions spécifiées.

L'analyse antimalware a lieu à deux niveaux :

- **Niveau du transport**

- **Base Exchange**

Analyse au niveau du transport

Bitdefender Endpoint Security Tools s'intègre aux agents de transport de messagerie pour analyser l'ensemble du trafic de messagerie.

L'analyse au niveau du transport est activée par défaut. Bitdefender Endpoint Security Tools filtre le trafic de messagerie et, si nécessaire, informe les utilisateurs des actions appliquées par l'ajout d'un texte dans le corps de l'e-mail.

Utilisez la case **Filtrage Antimalware** pour désactiver ou réactiver cette fonctionnalité.

Pour configurer le texte de notification, cliquez sur le lien **Paramètres**. Voici les options proposées :

- **Ajouter un pied de page aux e-mails analysés.** Cochez cette case pour ajouter une phrase en bas des e-mails analysés. Pour modifier le texte par défaut, saisissez votre message dans la zone de texte ci-dessous.
- **Texte de remplacement.** Pour les e-mails dont des pièces jointes ont été supprimées ou placées en quarantaine, un fichier de notification peut être joint. Pour modifier les textes de notification par défaut, saisissez votre message dans les zones de texte correspondantes.

Le filtrage antimalware repose sur des règles. Chaque e-mail atteignant le serveur de messagerie est comparé aux règles de filtrage antimalware, par ordre de priorité, jusqu'à ce qu'il corresponde à une règle. L'e-mail est ensuite traité en fonction des options spécifiées par cette règle.

Gérer les règles de filtrage

Vous pouvez afficher toutes les règles existantes listées dans le tableau avec des informations sur leur priorité, état et portée. Les règles sont classées par ordre de priorité, la première ayant la plus élevée.

Toute politique antimalware a une règle par défaut qui devient active lorsque le filtrage antimalware est activé. Ce que vous devez savoir sur la règle par défaut :

- Vous ne pouvez pas copier, désactiver ni supprimer cette règle.
- Vous pouvez modifier uniquement les paramètres d'analyse et les actions.
- La priorité par défaut de la règle est toujours la plus faible.

Création de règles

Vous pouvez créer des règles de filtrage de deux manières :

- Commencez à partir des paramètres par défaut, en suivant ces étapes :

1. Cliquez sur le bouton **+ Ajouter** en haut du tableau pour ouvrir la fenêtre de configuration.
 2. Configurez les paramètres de la règle. Pour des informations concernant les options, consultez les [Options de la règle](#).
 3. Cliquez sur **Enregistrer**. La règle apparaît en premier dans le tableau.
- Utilisez le clone d'une règle personnalisée comme modèle, en procédant comme suit :
 1. Sélectionnez la règle souhaitée dans le tableau.
 2. Cliquez sur le bouton **+ Cloner** en haut du tableau pour ouvrir la fenêtre de configuration.
 3. Adaptez les options de la règle en fonction de vos besoins.
 4. Cliquez sur **Enregistrer**. La règle apparaît en premier dans le tableau.

Modifier des règles

Pour modifier une règle :

1. Cliquez sur le nom de la règle pour ouvrir la fenêtre de configuration.
2. Saisissez les nouvelles valeurs des options que vous souhaitez modifier.
3. Cliquez sur **Enregistrer**. Les modifications prennent effet après l'enregistrement de la politique.

Configuration de la priorité de la règle

Pour modifier la priorité d'une règle :

1. Sélectionnez la règle à déplacer.
2. Utilisez les boutons **↑ Haut** ou **↓ Bas** en haut du tableau pour faire augmenter ou diminuer la priorité de la règle.

Supprimer des règles

Vous pouvez supprimer une ou plusieurs règles personnalisées à la fois. Vous devez simplement :

1. Cochez la case des règles à supprimer.
2. Cliquez sur le bouton **- Supprimer** en haut du tableau. Lorsqu'une règle est supprimée, vous ne pouvez pas la récupérer.

Options de la règle

Voici les options proposées :

- **Général**. Vous devez déterminer un nom pour la règle dans cette section afin de pouvoir l'enregistrer. Cochez la case **Actif** si vous souhaitez que la règle s'applique après l'enregistrement de la politique.
- **Portée de la règle**. La règle peut s'appliquer uniquement à un sous-ensemble d'e-mails, si vous configurez les options de portée cumulatives suivantes :

- **Appliquer à (direction).** Sélectionnez la direction du trafic de messagerie à laquelle s'applique la règle.
- **Expéditeurs.** Vous pouvez décider d'appliquer la règle à tous les expéditeurs ou uniquement à certains. Pour limiter les expéditeurs, cliquez sur le bouton **Spécifique** et sélectionnez les groupes souhaités dans le tableau de gauche. Affichez les groupes sélectionnés dans le tableau à droite.
- **Destinataires.** Vous pouvez décider d'appliquer la règle à tous les destinataires ou uniquement à certains. Pour limiter les destinataires, cliquez sur le bouton **Spécifique** et sélectionnez les groupes souhaités dans le tableau de gauche. Vous pouvez afficher les groupes sélectionnés dans le tableau à droite.

La règle s'applique si l'un des destinataires correspond à votre sélection. Si vous souhaitez appliquer la règle uniquement si tous les destinataires se trouvent dans les groupes sélectionnés, sélectionnez **Détecter tous les destinataires**.



Note

Les adresses figurant dans les champs **Cc** et **Bcc** sont également prises en compte en tant que destinataires.



Important

Les règles basées sur les groupes d'utilisateurs s'appliquent uniquement aux rôles Transport Hub et Boîte aux lettres.

- **Options.** Configurez les options d'analyse pour les e-mails correspondant à la règle :
 - **Types de fichiers analysés.** Utilisez cette option pour spécifier quels types de fichiers vous souhaitez analyser. Vous pouvez choisir d'analyser tous les fichiers (quelle que soit leur extension), uniquement les fichiers d'applications, ou certaines extensions de fichiers que vous considérez dangereuses. L'analyse de tous les fichiers fournit la meilleure protection, alors que l'analyse des applications uniquement est recommandée pour une analyse plus rapide.



Note

Les fichiers d'applications sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers. Pour plus d'informations, reportez-vous à « [Types de fichiers d'applications](#) » (p. 529).

Si vous souhaitez uniquement analyser les fichiers avec certaines extensions, vous avez deux possibilités :

- **Extensions définies par l'utilisateur**, où vous devez indiquer uniquement les extensions à analyser.
- **Tous les fichiers, à l'exception d'extensions spécifiques**, où vous devez saisir uniquement les extensions à ne pas analyser.
- **Taille maximale du corps des e-mails/des pièces jointes (Mo)**. Cochez cette case et saisissez une valeur dans le champ correspondant pour définir la taille maximale acceptée d'un fichier joint ou du corps des e-mails à analyser.
- **Profondeur maximale des archives (niveaux)**. Cochez la case et sélectionnez la profondeur maximale des archives dans le champ correspondant. Plus le niveau de profondeur est faible, meilleures sont les performances et plus le degré de protection est faible.
- **Rechercher des applications potentiellement indésirables (PUA)**. Cochez cette case pour rechercher les applications potentiellement malveillantes ou indésirables telles que les adwares, qui peuvent s'installer sur les systèmes sans le consentement des utilisateurs, modifier le comportement de différents logiciels et faire diminuer les performances du système.
- **Actions**. Vous pouvez spécifier les différentes actions que l'agent de sécurité pour exécuter sur les fichiers, selon le type de détection.

Le type de détection sépare les fichiers en trois catégories :

- **Fichier(s) infecté(s)**. Bitdefender détecte les fichiers considérés comme infectés par le biais de divers mécanismes avancés, notamment les technologies basées sur l'intelligence artificielle, l'apprentissage machine et les signatures de logiciels malveillants.
- **Fichiers suspects**. Ces fichiers sont considérés comme étant suspicieux par l'analyse heuristique et les autres technologies Bitdefender. Ils offrent un taux de détection élevé, mais les utilisateurs doivent tenir compte de la probabilité de faux résultats positifs (fichiers propres détectés comme étant suspicieux), dans certains cas.
- **Fichiers non analysables**. Ces fichiers ne peuvent pas être analysés. Les fichiers non analysables incluent mais ne se limitent pas aux fichiers protégés par des mots de passe, chiffrés ou compressés.

Pour chaque type de détection, vous avez une action par défaut ou principale et une action alternative en cas d'échec de l'action principale. Bien que ce ne soit pas recommandé, vous pouvez changer ces actions à partir des menus correspondants. Sélectionnez l'action à appliquer :

- **Désinfecter.** Supprime le code malveillant des fichiers infectés et reconstruit le fichier d'origine. Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Nous vous recommandons de toujours la conserver comme première action à appliquer aux fichiers infectés. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible.
- **Rejeter/Supprimer l'e-mail.** Sur les serveurs avec le rôle Transport Edge, l'e-mail détecté est rejeté avec un code d'erreur SMTP 550. Dans tous les autres cas, l'e-mail est supprimé sans avertissement. Nous vous recommandons d'éviter d'utiliser cette action.
- **Supprimer le fichier.** Supprime les pièces jointes présentant des problèmes sans aucun avertissement. Nous vous recommandons d'éviter d'utiliser cette action.
- **Remplacer le fichier.** Supprime les fichiers présentant des problèmes et insère un fichier texte qui informe l'utilisateur des actions appliquées.
- **Placer le fichier en quarantaine.** Place les fichiers détectés dans le dossier de la quarantaine et insère un fichier texte qui informe l'utilisateur des actions appliquées. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Vous pouvez gérer les fichiers de la quarantaine à partir de la page **Quarantaine**.




Note

Veillez noter que 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.

- **Ignorer** Aucune action ne sera appliquée aux fichiers détectés. Ces fichiers apparaîtront uniquement dans le journal d'analyse. Les tâches d'analyse sont configurées par défaut pour ignorer les fichiers suspects. Vous pouvez modifier l'action par défaut afin de placer des fichiers suspects en quarantaine.
- Par défaut, lorsqu'un e-mail correspond à la portée d'une règle, il est traité exclusivement en fonction de cette règle, sans être comparé à toute autre règle restante. Si vous souhaitez continuer à effectuer une vérification par rapport aux autres règles, décochez la case **Si les conditions de la règle sont remplies, arrêter de traiter d'autres règles**.

Exclusions

Si vous souhaitez qu'un certain trafic de messagerie soit ignoré par toute règle de filtrage, vous pouvez définir des exclusions de l'analyse. Pour créer une exclusion :

1. Étendez la section **Exceptions aux règles antimalwares**.
2. Cliquez sur le bouton  **Ajouter** de la barre d'outils de cette section, qui ouvre la fenêtre de configuration.
3. Configurez les paramètres d'exclusion. Pour des informations sur les options, consultez les [Options de la règle](#).
4. Cliquez sur **Enregistrer**.

Analyse de la banque d'informations Exchange

La Protection Exchange utilise les services Web Exchange (EWS) de Microsoft pour autoriser l'analyse des bases de données des dossiers publics et des boîtes aux lettres Exchange. Vous pouvez configurer le module antimalware afin qu'il exécute des tâches d'analyse à la demande régulièrement sur les bases de données cibles, en fonction de la planification que vous spécifiez.



Note

- L'analyse à la demande n'est disponible que sur les serveurs Exchange sur lesquels est installé le rôle Boîte aux lettres.
- Veuillez noter que l'analyse à la demande fait augmenter la consommation de ressources et, en fonction des options d'analyse et du nombre d'objets à analyser, peut être très longue.

L'analyse à la demande nécessite un compte administrateur Exchange (compte de service) pour agir au nom des utilisateurs Exchange afin de récupérer les objets à analyser dans les boîtes aux lettres des utilisateurs et les dossiers publics. Nous vous recommandons de créer un compte réservé à cette fin.

Le compte administrateur Exchange doit remplir les conditions suivantes :

- Être un membre du groupe Gestion de l'organisation (Exchange 2016, 2013 et 2010)
- Être un membre du groupe Administrateurs d'organisation Exchange (Exchange 2007)
- Avoir une boîte aux lettres associée.

Activer l'analyse à la demande

1. Dans la section **Tâches d'analyse**, cliquez sur le lien **Ajouter des identifiants**.
2. Indiquez le nom d'utilisateur et le mot de passe du compte de service.

3. Si l'e-mail est différent du nom d'utilisateur, vous avez besoin d'indiquer également l'adresse e-mail du compte de service.
4. Saisissez l'URL des Services Web Exchange (EWS), indispensable lorsque la découverte automatique d'Exchange ne fonctionne pas.


Note

- Le nom d'utilisateur doit inclure le nom de domaine, comme dans `utilisateur@domaine` ou `domaine\utilisateur`.
- N'oubliez pas de mettre à jour les identifiants dans Control Center, dès qu'ils ont changé.


Gestion des tâches d'analyse

Le tableau des tâches d'analyse fournit toutes les tâches planifiées et fournit des informations sur leurs cibles et périodicité.

Pour créer des tâches pour l'analyse de la banque d'informations Exchange :

1. Dans la section **Tâches d'analyse**, cliquez sur le bouton  **Ajouter** en haut du tableau pour ouvrir la fenêtre de configuration.
2. Configurez les paramètres de la tâche, comme décrit dans la section suivante.
3. Cliquez sur **Enregistrer**. La tâche est ajoutée à la liste et devient effective une fois la politique enregistrée.

Vous pouvez modifier une tâche à tout moment en cliquant sur le nom de la tâche.

Pour retirer des tâches de la liste, sélectionnez-les et cliquez sur le bouton  **Supprimer** en haut du tableau.

Paramètres de la tâche d'analyse

Les tâches ont un ensemble de paramètres qui sont décrits ci-après :

- **Général**. Indiquez un nom explicite pour la tâche.

Note

Vous pouvez voir le nom de la tâche dans la timeline de Bitdefender Endpoint Security Tools.

- **Planificateur**. Utilisez les options de planification pour configurer la planification de l'analyse. Vous pouvez configurer l'analyse pour une exécution régulière, à partir d'une date et d'une heure spécifiées. Pour les bases de données importantes, la tâche d'analyse peut être longue et avoir un impact sur les

performances du serveur. Vous pouvez dans ces cas configurer la tâche afin qu'elle s'arrête après une période spécifiée.

- **Cible.** Sélectionnez les conteneurs et objets à analyser. Vous pouvez choisir d'analyser les boîtes aux lettres, les dossiers publics ou les deux. En plus des e-mails, vous pouvez choisir d'analyser d'autres objets tels que les **Contacts**, **Tâches**, **Rendez-vous** et **Éléments de publication**. Vous pouvez en outre définir les restrictions suivantes au contenu à analyser :
 - Uniquement les messages non lus
 - Uniquement les éléments avec des pièces jointes
 - Uniquement les nouveaux éléments, reçus pendant une période donnée

Vous pouvez par exemple choisir d'analyser uniquement les e-mails de boîtes aux lettres d'utilisateurs, reçus au cours des 7 derniers jours.

Cochez la case **Exclusions**, si vous souhaitez définir des exceptions à l'analyse. Pour créer une exception, utilisez les champs de l'en-tête du tableau comme suit :

1. Sélectionnez le type de référentiel dans le menu.
2. En fonction du type de référentiel, spécifiez l'objet à exclure :

Type de référentiel	Format de l'objet
Boîte de messagerie	Adresse e-mail
Dossier public	Chemin d'accès du dossier, depuis la racine
Base de données	L'identité de la base de données



Note

Pour obtenir l'identité de la base de données, utilisez la commande shell Exchange :

```
Get-MailboxDatabase | fl name,identity
```

Vous ne pouvez saisir qu'un élément à la fois. Si vous avez plusieurs éléments du même type, vous devez définir autant de règles que le nombre d'éléments.

3. Cliquez sur le bouton **+ Ajouter** en haut du tableau pour enregistrer l'exception et l'ajouter à la liste.

Pour retirer une règle d'exception de la liste, cliquez sur le bouton **- Supprimer** correspondant.

- **Options.** Configurez les options d'analyse pour les e-mails correspondant à la règle :
 - **Types de fichiers analysés.** Utilisez cette option pour spécifier quels types de fichiers vous souhaitez analyser. Vous pouvez choisir d'analyser tous les fichiers (quelle que soit leur extension), uniquement les fichiers d'applications, ou certaines extensions de fichiers que vous considérez dangereuses. L'analyse de tous les fichiers fournit la meilleure protection, alors que l'analyse des applications uniquement est recommandée pour une analyse plus rapide.



Note

Les fichiers d'applications sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers. Pour plus d'informations, reportez-vous à « [Types de fichiers d'applications](#) » (p. 529).

Si vous souhaitez uniquement analyser les fichiers avec certaines extensions, vous avez deux possibilités :

- **Extensions définies par l'utilisateur**, où vous devez indiquer uniquement les extensions à analyser.
- **Tous les fichiers, à l'exception d'extensions spécifiques**, où vous devez saisir uniquement les extensions à ne pas analyser.
- **Taille maximale du corps des e-mails/des pièces jointes (Mo).** Cochez cette case et saisissez une valeur dans le champ correspondant pour définir la taille maximale acceptée d'un fichier joint ou du corps des e-mails à analyser.
- **Profondeur maximale des archives (niveaux).** Cochez la case et sélectionnez la profondeur maximale des archives dans le champ correspondant. Plus le niveau de profondeur est faible, meilleures sont les performances et plus le degré de protection est faible.
- **Rechercher des applications potentiellement indésirables (PUA).** Cochez cette case pour rechercher les applications potentiellement malveillantes ou indésirables telles que les adwares, qui peuvent s'installer sur les systèmes sans le consentement des utilisateurs, modifier le comportement de différents logiciels et faire diminuer les performances du système.
- **Actions.** Vous pouvez spécifier les différentes actions que l'agent de sécurité pour exécuter sur les fichiers, selon le type de détection.

Le type de détection sépare les fichiers en trois catégories :

- **Fichier(s) infecté(s).** Bitdefender détecte les fichiers considérés comme infectés par le biais de divers mécanismes avancés, notamment les

technologies basées sur l'intelligence artificielle, l'apprentissage machine et les signatures de logiciels malveillants.

- **Fichiers suspects.** Ces fichiers sont considérés comme étant suspicieux par l'analyse heuristique et les autres technologies Bitdefender. Ils offrent un taux de détection élevé, mais les utilisateurs doivent tenir compte de la probabilité de faux résultats positifs (fichiers propres détectés comme étant suspicieux), dans certains cas.
- **Fichiers non analysables.** Ces fichiers ne peuvent pas être analysés. Les fichiers non analysables incluent mais ne se limitent pas aux fichiers protégés par des mots de passe, chiffrés ou compressés.

Pour chaque type de détection, vous avez une action par défaut ou principale et une action alternative en cas d'échec de l'action principale. Bien que ce ne soit pas recommandé, vous pouvez changer ces actions à partir des menus correspondants. Sélectionnez l'action à appliquer :

- **Désinfecter.** Supprime le code malveillant des fichiers infectés et reconstruit le fichier d'origine. Pour certains types de malware, la désinfection n'est pas possible, car le fichier détecté est entièrement malveillant. Nous vous recommandons de toujours la conserver comme première action à appliquer aux fichiers infectés. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible.
- **Rejeter/Supprimer l'e-mail.** L'e-mail est supprimé sans avertissement. Nous vous recommandons d'éviter d'utiliser cette action.
- **Supprimer le fichier.** Supprime les pièces jointes présentant des problèmes sans aucun avertissement. Nous vous recommandons d'éviter d'utiliser cette action.
- **Remplacer le fichier.** Supprime les fichiers présentant des problèmes et insère un fichier texte qui informe l'utilisateur des actions appliquées.
- **Placer le fichier en quarantaine.** Place les fichiers détectés dans le dossier de la quarantaine et insère un fichier texte qui informe l'utilisateur des actions appliquées. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui élimine le risque d'une infection. Vous pouvez gérer les fichiers de la quarantaine à partir de la page **Quarantaine**.



Note

Veillez noter que 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 et de la taille des e-mails qu'elle contient.

- **Ignorer** Aucune action ne sera appliquée aux fichiers détectés. Ces fichiers apparaîtront uniquement dans le journal d'analyse. Les tâches d'analyse sont configurées par défaut pour ignorer les fichiers suspects. Vous pouvez modifier l'action par défaut afin de placer des fichiers suspects en quarantaine.
- Par défaut, lorsqu'un e-mail correspond à la portée d'une règle, il est traité exclusivement en fonction de cette règle, sans être comparé à toute autre règle restante. Si vous souhaitez continuer à effectuer une vérification par rapport aux autres règles, décochez la case **Si les conditions de la règle sont remplies, arrêter de traiter d'autres règles**.

Antispam

Le module Antispam fournit une protection à plusieurs niveaux contre le spam et le phishing à l'aide d'une combinaison de différents filtres et moteurs afin de déterminer si des e-mails sont ou non du spam.



Note

- Le filtrage antispam est disponible pour :
 - Exchange Server 2016/2013 avec le rôle de Transport Edge ou le rôle Boîte aux lettres
 - Exchange Server 2010/2007 avec le rôle de transport Edge ou le rôle de transport Hub
- Si vous avez à la fois les rôles Edge et Hub dans votre organisation Exchange, nous vous recommandons d'activer le filtrage antispam sur le serveur avec le rôle de transport Edge.

Le filtrage antispam est automatiquement activé pour les e-mails entrants. Utilisez la case **Filtrage antispam** pour désactiver ou réactiver cette fonctionnalité.

Filtres antispam

Un e-mail est comparé aux règles de filtrage antispam des groupes d'expéditeurs et de destinataires, par ordre de priorité, jusqu'à ce qu'une concordance soit établie avec une règle. L'e-mail est ensuite traité en fonction des options de la règle et des actions sont appliquées au spam détecté.

Certains filtres antispam sont configurables et vous pouvez choisir de les utiliser ou non. Voici la liste des filtres en option :

- **Filtre de caractères.** De nombreux e-mails de spam sont rédigés en cyrillique ou avec des caractères asiatiques. Le filtre de caractères détecte ce type d'e-mails et les signale comme étant du SPAM.
- **Contenu signalé comme étant à caractère sexuel.** Le spam contenant du matériel sexuel doit contenir l'avertissement « SEXUALLY-EXPLICIT » dans son objet. Ce filtre détecte les e-mails signalés comme étant à CARACTÈRE SEXUEL (« SEXUALLY-EXPLICIT ») dans l'objet et les signale comme étant du spam.
- **Filtre des URL.** La plupart des e-mails de spam comportent des liens vers des pages Web. Ces pages contiennent habituellement davantage de publicité et permettent de faire des achats. Elles sont parfois également utilisées pour du phishing.

Bitdefender maintient une base de données de ce type de liens. Le filtre des URL recherche toutes les URL d'un message dans sa base de données. En cas de concordance, l'e-mail est signalé comme étant du spam.

- **Realtime Blackhole List (RBL).** C'est un filtre qui permet de comparer le serveur de messagerie de l'expéditeur à des serveurs RBL tiers. Le filtre utilise le protocole DNSBL et les serveurs RBL pour filtrer le spam en fonction de la réputation des serveurs de messagerie en tant qu'expéditeurs de spam.

L'adresse du serveur de messagerie est extraite de l'en-tête de l'e-mail et sa validité est vérifiée. Si l'adresse appartient à une classe privée (10.0.0.0, 172.16.0.0 à 172.31.0.0 ou 192.168.0.0 à 192.168.255.0), elle est ignorée.

Une vérification DNS est effectuée sur le domaine `d.c.b.a.rbl.exemple.com`, où `d.c.b.a` est l'adresse IP inversée du serveur et `rbl.exemple.com` est le serveur RBL. Si le DNS répond que le domaine est valide, cela signifie que l'IP se trouve dans la liste du serveur RBL, et un score serveur entre 0 et 100 lui est attribué. Ce score compris entre 0 et 100 représente le niveau de confiance que vous avez attribué au serveur.

Une requête est effectuée pour chaque serveur RBL de la liste et le score renvoyé par chacun d'entre eux est ajouté au score intermédiaire. Lorsque le score a atteint 100, plus aucune requête n'est effectuée.

Si le score du filtre RBL est de 100, ou supérieur, l'e-mail est considéré comme étant du spam et l'action spécifiée est appliquée. Sinon, un score de spam est calculé à partir du score du filtre RBL et ajouté au score de spam global de l'e-mail.

- **Filtre heuristique.** Développé par Bitdefender, le nouveau filtre heuristique détecte les nouveaux spams et des spams inconnus. Le filtre est automatiquement formé sur de grands volumes d'e-mails de spam dans les Laboratoires Antispam de Bitdefender. Lors de cette formation, il apprend à distinguer les e-mails de spam et ceux qui sont légitimes et à reconnaître les nouveaux messages de spam en percevant leurs similarités, souvent très subtiles, avec les e-mails déjà observés. Ce filtre est conçu pour améliorer la détection basée sur les signatures tout en conservant un nombre très faible de faux positifs.
- **Bitdefender Cloud Query.** Bitdefender dispose d'une base de données constamment actualisée, dans le cloud, des "empreintes" des e-mails de spam. Une requête contenant l'empreinte de l'e-mail est envoyée aux serveurs cloud afin de vérifier à la volée si l'e-mail est du spam. Même si l'empreinte ne figure pas dans la base de données, elle est comparée à d'autres requêtes récentes et, si certaines conditions sont remplies, l'e-mail est signalé comme étant du spam.

Gérer les règles antispam

Vous pouvez afficher toutes les règles existantes listées dans le tableau avec des informations sur leur priorité, état et portée. Les règles sont classées par ordre de priorité, la première ayant la plus élevée.

Toute politique antispam a une règle par défaut qui devient active lorsque le module est activé. Ce que vous devez savoir sur la règle par défaut :

- Vous ne pouvez pas copier, désactiver ni supprimer cette règle.
- Vous pouvez modifier uniquement les paramètres d'analyse et les actions.
- La priorité par défaut de la règle est toujours la plus faible.

Création de règles

Pour créer une règle :

1. Cliquez sur le bouton **+** **Ajouter** en haut du tableau pour ouvrir la fenêtre de configuration.
2. Configurez les paramètres de la règle. Pour des informations concernant les options, reportez-vous à « [Options de la règle](#) » (p. 377).
3. Cliquez sur **Enregistrer**. La règle apparaît en premier dans le tableau.

Modifier des règles

Pour modifier une règle :

1. Cliquez sur le nom de la règle pour ouvrir la fenêtre de configuration.
2. Saisissez les nouvelles valeurs des options que vous souhaitez modifier.

3. Cliquez sur **Enregistrer**. Si la règle est active, les modifications prennent effet après l'enregistrement de la politique.

Configuration de la priorité de la règle

Pour changer la priorité d'une règle, sélectionnez la règle de votre choix et utilisez les flèches **Haut** et **Bas** en haut du tableau. Vous ne pouvez déplacer qu'une règle à la fois.

Supprimer des règles

Si vous ne souhaitez plus utiliser une règle, sélectionnez-la et cliquez sur le bouton **Supprimer** en haut du tableau.

Options de la règle

Voici les options proposées :

- **Général**. Vous devez déterminer un nom pour la règle dans cette section afin de pouvoir l'enregistrer. Cochez la case **Actif** si vous souhaitez que la règle s'applique après l'enregistrement de la politique.
- **Portée de la règle**. La règle peut s'appliquer uniquement à un sous-ensemble d'e-mails, si vous configurez les options de portée cumulatives suivantes :
 - **Appliquer à (direction)**. Sélectionnez la direction du trafic de messagerie à laquelle s'applique la règle.
 - **Expéditeurs**. Vous pouvez décider d'appliquer la règle à tous les expéditeurs ou uniquement à certains. Pour limiter les expéditeurs, cliquez sur le bouton **Spécifique** et sélectionnez les groupes souhaités dans le tableau de gauche. Affichez les groupes sélectionnés dans le tableau à droite.
 - **Destinataires**. Vous pouvez décider d'appliquer la règle à tous les destinataires ou uniquement à certains. Pour limiter les destinataires, cliquez sur le bouton **Spécifique** et sélectionnez les groupes souhaités dans le tableau de gauche. Vous pouvez afficher les groupes sélectionnés dans le tableau à droite.

La règle s'applique si l'un des destinataires correspond à votre sélection. Si vous souhaitez appliquer la règle uniquement si tous les destinataires se trouvent dans les groupes sélectionnés, sélectionnez **Détecter tous les destinataires**.



Note

Les adresses figurant dans les champs **Cc** et **Bcc** sont également prises en compte en tant que destinataires.



Important

Les règles basées sur les groupes d'utilisateurs s'appliquent uniquement aux rôles Transport Hub et Boîte aux lettres.

- **Configuration.** Cliquez sur le niveau de sécurité qui correspond le mieux à vos besoins (**Agressif**, **Normal** ou **Tolérant**). Utilisez la description à droite de l'échelle pour faire votre choix.

Vous pouvez également activer plusieurs filtres. Pour des informations détaillées concernant ces filtres, référez-vous à « [Filtres antispam](#) » (p. 374).



Important

Le filtre RBL nécessite une configuration supplémentaire. Vous pouvez configurer le filtre après avoir créé ou modifié la règle. Pour plus d'informations, reportez-vous à « [Configurer le filtre RBL](#) » (p. 379)

Pour les connexions authentifiées, vous pouvez choisir de contourner ou non l'analyse antispam.

- **Actions.** Vous pouvez appliquer plusieurs actions aux e-mails détectés. Chaque action dispose également de plusieurs options possibles ou actions secondaires. Voici leur description :

Principales actions :

- **Remettre les e-mails.** Les e-mails de spam parviennent dans les boîtes aux lettres des destinataires.
- **Placer les e-mails en quarantaine** Les e-mails sont chiffrés et enregistrés dans le dossier de quarantaine du Serveur Exchange, sans être remis aux destinataires. Vous pouvez gérer les e-mails de la quarantaine sur la page **Quarantaine**.
- **Rediriger les e-mails vers.** les e-mails ne sont pas délivrés aux destinataires d'origine mais dans la boîte aux lettres spécifiée dans le champ correspondant.
- **Rejeter/Supprimer l'e-mail.** Sur les serveurs avec le rôle Transport Edge, l'e-mail détecté est rejeté avec un code d'erreur SMTP 550. Dans tous les autres cas, l'e-mail est supprimé sans avertissement. Nous vous recommandons d'éviter d'utiliser cette action.

Actions secondaires :

- **Intégrer à Exchange SCL.** Ajoute un en-tête aux e-mails de spam, permettant à Exchange Server ou à Microsoft Outlook d'appliquer une

action en fonction du mécanisme SCL (Spam confidence level ou seuil de probabilité de courrier indésirable).

- **Ajouter une étiquette à l'objet de l'e-mail.** Vous pouvez ajouter une étiquette à l'objet de l'e-mail pour aider les utilisateurs à filtrer les e-mails détectés dans le client de messagerie.
- **Ajouter un en-tête aux e-mails.** Un en-tête est ajouté aux e-mails détectés comme étant du spam. Vous pouvez modifier le nom de l'en-tête et sa valeur en saisissant les valeurs souhaitées dans les champs correspondants. Vous pouvez ensuite utiliser cet en-tête d'e-mail pour créer d'autres filtres.
- **Enregistrer l'e-mail sur le disque.** Une copie de l'e-mail de spam est enregistré en tant que fichier dans le dossier spécifié. Indiquez le chemin d'accès absolu du dossier dans le champ correspondant.



Note

Cette option supporte uniquement les e-mails au format MIME.

- **Archiver dans un compte.** Une copie de l'e-mail détecté est délivrée à l'adresse e-mail spécifiée. Cette action ajoute l'adresse e-mail spécifiée à la liste Bcc d'e-mails.
- Par défaut, lorsqu'un e-mail correspond à la portée d'une règle, il est traité exclusivement en fonction de cette règle, sans être comparé à toute autre règle restante. Si vous souhaitez continuer à effectuer une vérification par rapport aux autres règles, décochez la case **Si les conditions de la règle sont remplies, arrêter de traiter d'autres règles.**

Configurer le filtre RBL

Si vous souhaitez utiliser [le filtre RBL](#), vous devez fournir une liste de serveurs RBL.

Pour configurer le filtre :

1. Cliquez sur le lien **Paramètres** sur la page **Antispam** pour ouvrir la fenêtre de configuration.
2. Indiquez l'adresse IP du serveur DNS à interroger et le délai de réponse dans les champs correspondants. Si aucune adresse de serveur DNS n'est configurée, ou si le serveur DNS n'est pas disponible, le filtre RBL utilise les serveurs DNS du système.
3. Pour chaque serveur RBL :
 - a. Indiquez le nom d'hôte du serveur ou l'adresse IP et le niveau de confiance que vous avez attribué au serveur, dans les champs de l'en-tête du tableau.

- b. Cliquez sur le bouton **+Ajouter** en haut du tableau.
4. Cliquez sur **Enregistrer**.

Configurer la liste blanche des expéditeurs

Pour les expéditeurs d'e-mails connus, vous pouvez éviter la consommation inutile de ressources du serveur en les incluant dans des listes d'expéditeurs de confiance ou non fiables. Ainsi, le serveur de messagerie acceptera ou rejettera toujours les e-mails provenant de ces expéditeurs. Si, par exemple, vous communiquez souvent par e-mail avec un partenaire commercial et souhaitez vous assurer que vous recevrez tous ses e-mails, vous pouvez ajouter ce partenaire à la liste blanche.

Pour créer une liste blanche d'expéditeurs de confiance :

1. Cliquez sur le lien **Liste blanche** pour ouvrir la fenêtre de configuration.
2. Cochez la case **Liste blanche d'expéditeurs**.
3. Indiquez les adresses e-mail dans le champ correspondant. Lors de la modification de la liste, vous pouvez également utiliser des caractères génériques pour définir un domaine e-mail entier ou un modèle pour les adresses e-mails :
 - Astérisque (*), remplace zéro, un caractère ou plus
 - Le point d'interrogation (?) remplace n'importe quel caractère.Par exemple, si vous saisissez * . gov, tous les e-mails venant du domaine . gov seront acceptés.

4. Cliquez sur **Enregistrer**.

Note

Pour mettre en liste noire des expéditeurs de spam connus, utilisez l'option **Liste noire de connexion** dans la section **Protection Exchange > Général > Configuration**.

Contrôle de contenu

Utilisez le Contrôle de contenu pour améliorer la protection des messageries en filtrant tout le trafic de messagerie non conforme aux politiques de votre société (contenu potentiellement sensible ou indésirable).

Pour un contrôle global du contenu des e-mails ce module comprend deux options de filtrage des e-mails :

- [Filtrage du contenu](#)
- [Filtrage des pièces jointes](#)

 **Note**

Le Filtrage du contenu et le Filtrage des pièces jointes sont disponibles pour :

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

Gérer les règles de filtrage

Les filtres du Contrôle de contenu reposent sur des règles. Vous pouvez définir plusieurs règles pour différents utilisateurs et groupes d'utilisateurs. Chaque e-mail atteignant le serveur de messagerie est comparé aux règles de filtrage, par ordre de priorité, jusqu'à ce qu'une concordance avec une règle soit établie. L'e-mail est ensuite traité en fonction des options spécifiées par cette règle.

Les règles de filtrage de contenu précèdent les règles de filtrage de pièces jointes.

Les règles de filtrage du contenu et des pièces jointes figurent dans les tableaux correspondants par ordre de priorité, la première règle ayant la plus élevée. Les informations suivantes sont indiquées pour chaque règle :

- Priorité
- Nom
- Direction du trafic
- Groupes d'expéditeurs et de destinataires

Création de règles

Vous pouvez créer des règles de filtrage de deux manières :

- Commencez à partir des paramètres par défaut, en suivant ces étapes :
 1. Cliquez sur le bouton **+ Ajouter** en haut du tableau pour ouvrir la fenêtre de configuration.
 2. Configurez les paramètres de la règle. Pour des informations sur les options spécifiques de filtrage des pièces jointes et du contenu, référez-vous à :
 - [Options de la règle de filtrage du contenu](#)
 - [Options de la règle de filtrage des pièces jointes](#).
 3. Cliquez sur **Enregistrer**. La règle apparaît en premier dans le tableau.
- Utilisez le clone d'une règle personnalisée comme modèle, en procédant comme suit :
 1. Sélectionnez la règle souhaitée dans le tableau.
 2. Cliquez sur le bouton **🔄 Cloner** en haut du tableau pour ouvrir la fenêtre de configuration.

3. Adaptez les options de la règle en fonction de vos besoins.
4. Cliquez sur **Enregistrer**. La règle apparaît en premier dans le tableau.

Modifier des règles

Pour modifier une règle :

1. Cliquez sur le nom de la règle pour ouvrir la fenêtre de configuration.
2. Saisissez les nouvelles valeurs des options que vous souhaitez modifier.
3. Cliquez sur **Enregistrer**. Les modifications prennent effet après l'enregistrement de la politique.


Configuration de la priorité de la règle

Pour modifier la priorité d'une règle :

1. Sélectionnez la règle à déplacer.
2. Utilisez les boutons  **Haut** ou  **Bas** en haut du tableau pour faire augmenter ou diminuer la priorité de la règle.

Supprimer des règles

Vous pouvez supprimer une ou plusieurs règles personnalisées. Vous devez simplement :

1. Sélectionnez les règles à supprimer.
2. Cliquez sur le bouton  **Supprimer** en haut du tableau. Lorsqu'une règle est supprimée, vous ne pouvez pas la récupérer.

Filtrage du contenu

Le Filtrage du contenu vous aide à filtrer le trafic de messagerie à partir des chaînes de caractères que vous avez définies. Ces chaînes sont comparées à l'objet de l'e-mail et au texte du corps de l'e-mail. Le Filtrage du contenu vous permet d'atteindre les objectifs suivants :

- Empêcher que les e-mails indésirables n'atteignent les boîtes aux lettres des serveurs Exchange.
- Bloquer l'envoi d'e-mails contenant des données confidentielles.
- Archiver les e-mails remplissant certaines conditions dans un autre compte de messagerie ou sur le disque. Vous pouvez par exemple enregistrer les e-mails envoyés à l'adresse e-mail du support de votre entreprise dans un dossier ou sur le disque local.

Activer le filtrage du contenu

Si vous souhaitez utiliser le filtrage du contenu, cochez la case **Filtrage du contenu**.

Pour créer et gérer des règles de filtrage du contenu, référez-vous à « [Gérer les règles de filtrage](#) » (p. 381).

Options de la règle

- **Général.** Vous devez déterminer un nom pour la règle dans cette section afin de pouvoir l'enregistrer. Cochez la case **Actif** si vous souhaitez que la règle s'applique après l'enregistrement de la politique.
- **Portée de la règle.** La règle peut s'appliquer uniquement à un sous-ensemble d'e-mails, si vous configurez les options de portée cumulatives suivantes :
 - **Appliquer à (direction).** Sélectionnez la direction du trafic de messagerie à laquelle s'applique la règle.
 - **Expéditeurs.** Vous pouvez décider d'appliquer la règle à tous les expéditeurs ou uniquement à certains. Pour limiter les expéditeurs, cliquez sur le bouton **Spécifique** et sélectionnez les groupes souhaités dans le tableau de gauche. Affichez les groupes sélectionnés dans le tableau à droite.
 - **Destinataires.** Vous pouvez décider d'appliquer la règle à tous les destinataires ou uniquement à certains. Pour limiter les destinataires, cliquez sur le bouton **Spécifique** et sélectionnez les groupes souhaités dans le tableau de gauche. Vous pouvez afficher les groupes sélectionnés dans le tableau à droite.

La règle s'applique si l'un des destinataires correspond à votre sélection. Si vous souhaitez appliquer la règle uniquement si tous les destinataires se trouvent dans les groupes sélectionnés, sélectionnez **Détecter tous les destinataires**.



Note

Les adresses figurant dans les champs **Cc** et **Bcc** sont également prises en compte en tant que destinataires.



Important

Les règles basées sur les groupes d'utilisateurs s'appliquent uniquement aux rôles Transport Hub et Boîte aux lettres.

- **Configuration.** Configurez les expressions à rechercher dans les e-mails comme indiqué ici :
 1. Sélectionnez la partie de l'e-mail à vérifier :
 - L'objet de l'e-mail, en cochant la case **Filtrer par sujet**. Tous les e-mails dont l'objet contient l'une des expressions saisies dans le tableau correspondant sont filtrés.

- Le contenu du corps, en cochant la case **Filtrer par contenu du corps**. Tous les e-mails ayant dans leur corps l'une des expressions définies sont filtrés.
- À la fois l'objet et le contenu du corps des e-mails, en cochant les deux cases. Tous les e-mails dont l'objet correspond à une règle du premier tableau ET dont le corps contient une expression du second tableau sont filtrés. Par exemple :

Le premier tableau contient les expressions : `newsletter` et `hebdomadaire`. Le second tableau contient les expressions : `shopping`, `prix` et `offre`.

Un e-mail ayant pour objet « **newsletter** mensuelle de votre bijouterie préférée » et dont le corps de l'e-mail contient la phrase « Nous avons le plaisir de vous présenter notre nouvelle **offre** de montres sensationnelles à des **prix** irrésistibles. » correspondra à la règle et sera filtré. Si le sujet est « Des nouvelles de votre bijouterie », l'e-mail n'est pas filtré.

2. Créez les listes de conditions à l'aide des champs des en-têtes du tableau. Pour chaque condition, procédez comme suit :
 - a. Sélectionnez le type d'expression utilisé dans les recherches. Vous pouvez choisir de saisir l'expression exacte ou de créer des modèles de texte en utilisant des expressions habituelles.



Note

La syntaxe des expressions habituelles respecte le langage ECMAScript.

- b. Indiquez la chaîne à rechercher dans le champ **Expression**.

Par exemple :

- i. L'expression `5[1-5]\d{2}([\s\~]? \d{4}){3}` correspond aux cartes bancaires commençant entre 51 et 55, comptant 16 chiffres dans des groupes de 4, lesquels peuvent être séparés par un espace ou un trait d'union. Dans ce cas, tout e-mail contenant le numéro de carte bancaire présenté sous l'un des formats suivants : `5257-4938-3957-3948`, `5257 4938 3957 3948` ou `5257493839573948`, sera filtré.
- ii. cette expression détecte les e-mails contenant les mots `loto`, `mega` et `millions`, dans cet ordre exact :

```
(lottery)((.\|n|\r)*)(cash)((.\|n|\r)*)(prize)
```

Pour détecter les e-mails qui contiennent chacun de ces trois mots quel que soit leur ordre, ajoutez trois expressions régulières avec un ordre de mots différent.

- iii. Cette expression détecte les e-mails qui contiennent trois ou plus d'occurrences du mot gagnant :

```
(prize)((.\|n|\r)*)(prize)((.\|n|\r)*)(prize)
```

- c. Si vous souhaitez distinguer les majuscules des minuscules dans les comparaisons de textes, cochez la case **Respecter la casse**. Par exemple, lorsque cette case est cochée, `Newsletter` est différent de `newsletter`.
- d. Si vous ne souhaitez pas que l'expression puisse se trouver entre d'autres mots, cochez la case **Mots entiers**. Par exemple, lorsque cette case est cochée, l'expression `Anne's salary` est considérée comme différente de l'expression `MariAnne's salary`.
- e. Cliquez sur le bouton **+ Ajouter** dans l'en-tête de la colonne **Action** pour ajouter la condition à la liste.
- **Actions**. Vous pouvez appliquer plusieurs actions aux e-mails. Chaque action dispose également de plusieurs options possibles ou actions secondaires. Voici leur description :

Principales actions :

- **Remettre les e-mails**. Les e-mails détectés parviennent dans les boîtes aux lettres des destinataires.
- **Quarantaine**. L'e-mail est chiffré et enregistré dans le dossier de quarantaine du Serveur Exchange, sans être remis aux destinataires. Vous pouvez gérer les e-mails de la quarantaine sur la page **Quarantaine**.
- **Rediriger vers**. Les e-mails ne sont pas délivrés aux destinataires d'origine mais dans la boîte aux lettres que vous avez spécifiée dans le champ correspondant.
- **Rejeter/Supprimer l'e-mail**. Sur les serveurs avec le rôle Transport Edge, l'e-mail détecté est rejeté avec un code d'erreur SMTP 550. Dans tous les autres cas, l'e-mail est supprimé sans avertissement. Nous vous recommandons d'éviter d'utiliser cette action.

Actions secondaires :

- **Ajouter une étiquette à l'objet de l'e-mail.** Vous pouvez ajouter une étiquette à l'objet de l'e-mail détecté pour aider les utilisateurs à filtrer les e-mails dans le client de messagerie.
- **Ajouter un en-tête aux e-mails.** Vous pouvez ajouter un nom et une valeur aux en-têtes des e-mails détectés, en saisissant les valeurs souhaitées dans les champs correspondants.
- **Enregistrer l'e-mail sur le disque.** Une copie de l'e-mail détecté est enregistré en tant que fichier dans le dossier spécifié sur le Serveur Exchange. Si le dossier n'existe pas, il sera créé. Vous devez indiquer le chemin d'accès absolu du dossier dans le champ correspondant.



Note

Cette option supporte uniquement les e-mails au format MIME.

- **Archiver dans un compte.** Une copie de l'e-mail détecté est délivrée à l'adresse e-mail spécifiée. Cette action ajoute l'adresse e-mail spécifiée à la liste Bcc d'e-mails.
- Par défaut, lorsqu'un e-mail correspond aux conditions d'une règle, il n'est plus comparé aux autres règles. Si vous souhaitez continuer à traiter des règles, décochez la case **Si les conditions de la règle sont remplies, arrêter de traiter d'autres règles.**

Exclusions

Si vous souhaitez que les e-mails de certains expéditeurs ou destinataires soient délivrés quelle que soit la règle de filtrage du contenu, vous pouvez définir des exclusions de filtrage.

Pour créer une exclusion :

1. Cliquez sur le lien **Exclusions** à côté de la case **Filtrage du contenu**. Cette action ouvre la fenêtre de configuration.
2. Indiquez les adresses e-mail des expéditeurs et/ou destinataires de confiance dans les champs correspondants. Tout e-mail provenant d'un expéditeur de confiance ou destiné à un destinataire de confiance échappe au filtrage. Lors de la modification de la liste, vous pouvez également utiliser des caractères génériques pour définir un domaine e-mail entier ou un modèle pour les adresses e-mails :
 - Astérisque (*), remplace zéro, un caractère ou plus
 - Le point d'interrogation (?) remplace n'importe quel caractère.

- Par exemple, si vous saisissez * .gov, tous les e-mails venant du domaine .gov seront acceptés.
3. Pour les e-mails avec plusieurs destinataires, vous pouvez cocher la case **Exclure les e-mails du filtrage uniquement si tous les destinataires sont de confiance** pour appliquer l'exclusion uniquement si tous les destinataires des e-mails se trouvent dans la liste des destinataires de confiance.
 4. Cliquez sur **Enregistrer**.

Pièces jointes

Le module Pièces jointes fournit des fonctionnalités de filtrage des pièces jointes d'e-mail. Il peut détecter des pièces jointes avec certains modèles de noms ou d'un certain type. Le module Pièces jointes vous permet de :

- Bloquez les pièces jointes présentant un danger potentiel telles que les fichiers .vbs ou .exe, ou les e-mails les contenant.
- Bloquez les pièces jointes ayant des noms choquants ou les e-mails les contenant.

Activer le filtrage des pièces jointes

Si vous souhaitez utiliser le filtrage des pièces jointes, cochez la case **Pièces jointes**. Pour créer et gérer des règles de filtrage de pièces jointes, référez-vous à « [Gérer les règles de filtrage](#) » (p. 381).

Options de la règle

- **Général**. Vous devez déterminer un nom pour la règle dans cette section afin de pouvoir l'enregistrer. Cochez la case **Actif** si vous souhaitez que la règle s'applique après l'enregistrement de la politique.
- **Portée de la règle**. La règle peut s'appliquer uniquement à un sous-ensemble d'e-mails, si vous configurez les options de portée cumulatives suivantes :
 - **Appliquer à (direction)**. Sélectionnez la direction du trafic de messagerie à laquelle s'applique la règle.
 - **Expéditeurs**. Vous pouvez décider d'appliquer la règle à tous les expéditeurs ou uniquement à certains. Pour limiter les expéditeurs, cliquez sur le bouton **Spécifique** et sélectionnez les groupes souhaités dans le tableau de gauche. Affichez les groupes sélectionnés dans le tableau à droite.
 - **Destinataires**. Vous pouvez décider d'appliquer la règle à tous les destinataires ou uniquement à certains. Pour limiter les destinataires, cliquez sur le bouton **Spécifique** et sélectionnez les groupes souhaités dans le

tableau de gauche. Vous pouvez afficher les groupes sélectionnés dans le tableau à droite.

La règle s'applique si l'un des destinataires correspond à votre sélection. Si vous souhaitez appliquer la règle uniquement si tous les destinataires se trouvent dans les groupes sélectionnés, sélectionnez **Détecter tous les destinataires**.



Note

Les adresses figurant dans les champs **Cc** et **Bcc** sont également prises en compte en tant que destinataires.



Important

Les règles basées sur les groupes d'utilisateurs s'appliquent uniquement aux rôles Transport Hub et Boîte aux lettres.

- **Configuration.** Spécifiez les fichiers qui sont autorisés ou refusés dans les pièces jointes des e-mails.

Vous pouvez filtrer les pièces jointes des e-mails par type de fichier ou par nom de fichier.

Pour filtrer les pièces jointes par type de fichier, procédez comme suit :

1. Cochez la case **Détecter par type de contenu**.
2. Sélectionnez l'option de détection qui répond le mieux à vos besoins :
 - **Uniquement les catégories suivantes**, lorsque vous avez une liste limitée de catégories de types de fichiers interdits.
 - **Toutes les catégories à l'exception des suivantes**, lorsque vous avez une liste limitée de catégories de types de fichiers autorisés.
3. Sélectionnez les catégories de types de fichiers qui vous intéressent dans la liste disponible. Pour des détails sur les extensions de chaque catégorie, référez-vous à « [Types de fichiers du filtrage des pièces jointes](#) » (p. 530).

Si vous êtes intéressé par certains types de fichiers uniquement, cochez la case **Extensions personnalisées** et saisissez la liste d'extensions dans le champ correspondant.

4. Cochez la case **Activer la détection du véritable type** pour vérifier les en-têtes de fichiers et identifier correctement le type de fichier des pièces jointes lors de la recherche d'extensions interdites. Cela signifie qu'une extension ne peut pas simplement être renommée pour échapper aux politiques de filtrage des pièces jointes.

**Note**

La détection du véritable type peut consommer beaucoup de ressources.

Pour filtrer les pièces jointes en fonction de leur nom, cochez la case **Détecter par nom de fichier** et saisissez les noms de fichier que vous souhaitez filtrer, dans le champ correspondant. Lorsque vous modifiez la liste, vous pouvez également utiliser les caractères génériques suivants pour définir des schémas :

- Astérisque (*), remplace zéro, un caractère ou plus
- Le point d'interrogation (?) remplace n'importe quel caractère.

Par exemple, si vous saisissez `base de données.*`, tous les fichiers nommés `base de données`, quelle que soit leur extension, seront détectés.

**Note**

Si vous activez à la fois les détections des noms de fichiers et du type du contenu (sans la détection du véritable type), le fichier doit remplir les conditions des deux types de détection. Vous avez par exemple sélectionné la catégorie **Multimédia** et saisi le nom de fichier `test.pdf`. Dans ce cas, tout e-mail passe la règle car le fichier PDF n'est pas un fichier multimédia.

Sélectionnez la case **Analyser l'intérieur des archives** pour empêcher les fichiers bloqués d'être cachés dans des archives apparemment inoffensives et ainsi contourner la règle de filtrage.

L'analyse est récursive à l'intérieur des archives et se fait par défaut jusqu'au quatrième niveau de l'archive. Vous pouvez optimiser l'analyse comme décrit ci-dessous :

1. Sélectionnez la case **Maximum profondeur archive (niveaux)**.
2. Choisissez une valeur différente dans le menu correspondant. Pour les meilleures performances, choisissez la valeur la plus faible, pour la protection maximale, choisissez la valeur la plus élevée.

**Note**

Si vous avez sélectionné l'analyse d'archives, **Analyser l'intérieur des archives** est désactivé et toutes les archives sont analysées.

- **Actions.** Vous pouvez appliquer plusieurs actions aux pièces jointes détectées ou aux e-mails les contenant. Chaque action dispose également de plusieurs options possibles ou actions secondaires. Voici leur description :

Principales actions :

- **Remplacer le fichier.** Supprime les fichiers détectés et insère un fichier texte qui informe l'utilisateur des actions appliquées.

Pour configurer le texte de notification :

1. Cliquez sur le lien **Configuration** à côté de la case **Pièces jointes**.
2. Indiquez le texte de notification dans le champ correspondant.
3. Cliquez sur **Enregistrer**.

- **Supprimer le fichier.** Supprime les fichiers détectés sans avertissement. Nous vous recommandons d'éviter d'utiliser cette action.
- **Rejeter/Supprimer l'e-mail.** Sur les serveurs avec le rôle Transport Edge, l'e-mail détecté est rejeté avec un code d'erreur SMTP 550. Dans tous les autres cas, l'e-mail est supprimé sans avertissement. Nous vous recommandons d'éviter d'utiliser cette action.
- **Placer les e-mails en quarantaine** Les e-mails sont chiffrés et enregistrés dans le dossier de quarantaine du Serveur Exchange, sans être remis aux destinataires. Vous pouvez gérer les e-mails de la quarantaine sur la page **Quarantaine**.
- **Rediriger le courrier vers.** L'e-mail n'est pas délivré aux destinataires d'origine mais à l'adresse e-mail que vous indiquez dans le champ correspondant.
- **Remettre les e-mails.** Ne filtre pas les e-mails.

Actions secondaires :

- **Ajouter une étiquette à l'objet de l'e-mail.** Vous pouvez ajouter une étiquette à l'objet de l'e-mail détecté pour aider les utilisateurs à filtrer les e-mails dans le client de messagerie.
- **Ajouter un en-tête aux e-mails.** Vous pouvez ajouter un nom et une valeur aux en-têtes des e-mails détectés, en saisissant les valeurs souhaitées dans les champs correspondants.
- **Enregistrer l'e-mail sur le disque.** Une copie de l'e-mail détecté est enregistré en tant que fichier dans le dossier spécifié sur le Serveur Exchange. Si le dossier n'existe pas, il sera créé. Vous devez indiquer le chemin d'accès absolu du dossier dans le champ correspondant.

**Note**

Cette option supporte uniquement les e-mails au format MIME.

- **Archiver dans un compte.** Une copie de l'e-mail détecté est délivrée à l'adresse e-mail spécifiée. Cette action ajoute l'adresse e-mail spécifiée à la liste Bcc d'e-mails.
- Par défaut, lorsqu'un e-mail correspond à la portée d'une règle, il est traité exclusivement en fonction de cette règle, sans être comparé à toute autre règle restante. Si vous souhaitez continuer à effectuer une vérification par rapport aux autres règles, décochez la case **Si les conditions de la règle sont remplies, arrêter de traiter d'autres règles.**

Exclusions

Si vous souhaitez que les e-mails de certains expéditeurs ou destinataires soient délivrés quelle que soit la règle de filtrage des pièces jointes, vous pouvez définir des exclusions de filtrage.

Pour créer une exclusion :

1. Cliquez sur le lien **Exclusions** à côté de la case **Pièces jointes**. Cette action ouvre la fenêtre de configuration.
2. Indiquez les adresses e-mail des expéditeurs et/ou destinataires de confiance dans les champs correspondants. Tout e-mail provenant d'un expéditeur de confiance ou destiné à un destinataire de confiance échappe au filtrage. Lors de la modification de la liste, vous pouvez également utiliser des caractères génériques pour définir un domaine e-mail entier ou un modèle pour les adresses e-mails :
 - Astérisque (*), remplace zéro, un caractère ou plus
 - Le point d'interrogation (?) remplace n'importe quel caractère.

Par exemple, si vous saisissez * . gov, tous les e-mails venant du domaine . gov seront acceptés.

3. Pour les e-mails avec plusieurs destinataires, vous pouvez cocher la case **Exclure les e-mails du filtrage uniquement si tous les destinataires sont de confiance** pour appliquer l'exclusion uniquement si tous les destinataires des e-mails se trouvent dans la liste des destinataires de confiance.
4. Cliquez sur **Enregistrer**.

7.2.12. Chiffrement de disque

Note

Ce module est disponible pour :

- Windows pour postes de travail
- Windows pour serveurs
- macOS

Le module de chiffrement gère tout le chiffrement du disque sur les endpoints en exploitant BitLocker sur Windows et FileVault et l'utilitaire de ligne de commande diskutil sur macOS, respectivement.

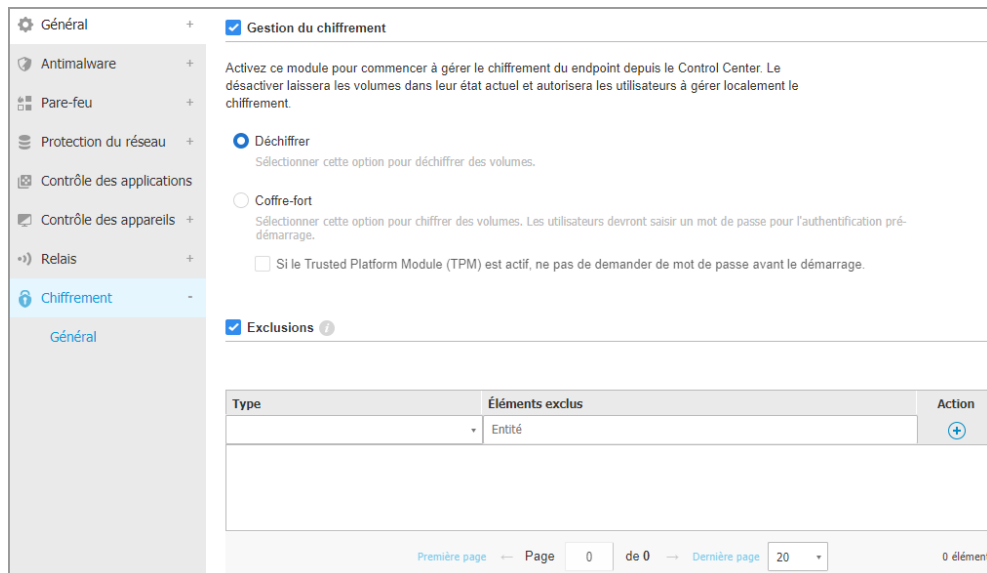
Grâce à cette approche, GravityZone est en mesure d'offrir de sérieux avantages :

- Données sécurisées en cas de perte ou de vol d'appareils.
- Une protection étendue pour les plateformes informatiques les plus populaires dans le monde, grâce à l'application de normes de chiffrement recommandées avec le soutien total de Microsoft et d'Apple.
- Impact minime sur les performances des endpoints, grâce aux outils de chiffrement natifs.

Le module de chiffrement fonctionne avec les solutions suivantes :

- BitLocker version 1.2 et ultérieures, sur les endpoints Windows équipés d'une puce TPM (Trusted Platform Module), pour les volumes d'amorçage et de non-amorçage.
- BitLocker version 1.2 et ultérieures, sur les endpoints Windows non équipés d'une puce TPM (Trusted Platform Module), pour les volumes d'amorçage et de non-amorçage.
- FileVault sur les endpoints macOS, pour les volumes d'amorçage.
- diskutil sur les endpoints macOS, pour les volumes de non-amorçage.

Pour la liste des systèmes d'exploitation pris en charge par le module de chiffrement, veuillez vous référer au Guide d'installation de GravityZone.



Général +

Gestion du chiffrement

Antimalware +

Pare-feu +

Protection du réseau +

Contrôle des applications

Contrôle des appareils +

Relais +

Chiffrement -

Général

Activez ce module pour commencer à gérer le chiffrement de l'endpoint depuis le Control Center. Le désactiver laissera les volumes dans leur état actuel et autorisera les utilisateurs à gérer localement le chiffrement.

Déchiffrer
Sélectionner cette option pour déchiffrer des volumes.

Coffre-fort
Sélectionner cette option pour chiffrer des volumes. Les utilisateurs devront saisir un mot de passe pour l'authentification pré-démarrage.

Si le Trusted Platform Module (TPM) est actif, ne pas de demander de mot de passe avant le démarrage.

Exclusions ⓘ

Type	Éléments exclus	Action
	Entité	+

Première page — Page 0 de 0 — Dernière page 20 0 élément

La page Chiffrement

Pour commencer à gérer le chiffrement des endpoints à partir de la Control Center, cochez la case **Gestion du chiffrement**. Tant que ce paramètre sera activé, les utilisateurs des endpoints ne pourront pas gérer localement le chiffrement et toutes leurs actions seront annulées ou inversées. Si vous désactivez ce paramètre, les volumes des endpoints resteront dans leur état actuel (chiffré ou non chiffré) et les utilisateurs pourront gérer le chiffrement sur leurs machines.

Trois options sont disponibles pour gérer les processus de chiffrement et de déchiffrement :

- **Déchiffrer** – déchiffre les volumes et les maintient déchiffrés lorsque la politique est activée sur les endpoints.
- **Chiffrer** – chiffre les volumes et les maintient chiffrés lorsque la politique est activée sur les endpoints.

Dans l'option Chiffrement, vous pouvez cocher la case **Si la puce TPM (Trusted Platform Module) est active, ne pas demander de mot de passe pour le chiffrement**. Ce paramètre permet le chiffrement des endpoints Windows équipés d'une puce TPM sans que les utilisateurs aient à fournir de mot de passe pour

le chiffrement. Pour plus d'informations reportez-vous à « [Chiffrer des volumes](#) » (p. 394).

● Exclusions

GravityZone prend en charge la méthode AES (Advanced Encryption Standard) avec des clés de 128 et 256 bits sur Windows et macOS. L'algorithme de chiffrement réellement utilisé dépend de la configuration de chaque système d'exploitation.

Note

GravityZone détecte et gère des volumes chiffrés manuellement avec BitLocker, FileVault et diskutil. Pour commencer à gérer ces volumes, l'agent de sécurité va inviter les utilisateurs des endpoints à modifier leurs clés de récupération. Dans le cas où d'autres solutions de chiffrement seraient utilisées, les volumes doivent être déchiffrés avant l'application d'une politique GravityZone.

Chiffrer des volumes

Pour chiffrer des volumes :

1. Sélectionnez la case **Gestion du chiffrement**.
2. Sélectionnez l'option **Chiffrer**.

Le processus de chiffrement commence à l'activation de la politique sur les endpoints, avec certaines différences entre Windows et Mac.

Sous Windows

Par défaut, l'agent de sécurité invitera les utilisateurs à configurer un mot de passe pour commencer le chiffrement. Si la machine est équipée d'une puce TPM fonctionnelle, l'agent de sécurité invitera les utilisateurs à configurer un numéro d'identification personnel (PIN) pour commencer le chiffrement. Les utilisateurs doivent saisir le mot de passe ou le code PIN configuré à ce stade chaque fois que l'endpoint démarre, dans un écran d'authentification avant démarrage.

Note

L'agent de sécurité vous permet de configurer les exigences de complexité du code PIN et les privilèges utilisateurs nécessaires pour modifier leur code PIN via les paramètres de la politique de groupe (GPO) de Bitlocker.

Pour commencer le chiffrement sans demander de mot de passe aux utilisateurs des endpoints, cochez la case **Si une puce TPM (Trusted Platform Module) est active, ne pas demander de mot de passe avant démarrage**. Ce paramètre est

compatible avec les endpoints Windows équipés d'une puce TPM et d'une interface UEFI.

Lorsque la case **Si une puce TPM (Trusted Platform Module) est active, ne pas demander de mot de passe avant démarrage** est cochée :

- Sur un endpoint non chiffré :
 - Le chiffrement se poursuit sans avoir à saisir un mot de passe.
 - L'écran d'authentification prédémarrage n'apparaît pas à l'allumage de la machine.
- Sur un endpoint chiffré avec mot de passe :
 - Le mot de passe est supprimé.
 - Le volume n'est pas chiffré.
- Sur un endpoint chiffré ou non, non équipé d'une puce TPM ou équipé d'une puce TPM non détectée ou ne fonctionnant pas :
 - Il est demandé à l'utilisateur de saisir un mot de passe pour commencer le chiffrement.
 - L'écran d'authentification prédémarrage apparaît à l'allumage de la machine.

Lorsque la case **Si une puce TPM (Trusted Platform Module) est active, ne pas demander de mot de passe avant démarrage** n'est pas cochée :

- L'utilisateur doit saisir un mot de passe pour commencer le chiffrement.
- Le volume n'est pas chiffré.

Sous Mac

Pour commencer le chiffrement sur les volumes d'amorçage, l'agent de sécurité invitera les utilisateurs à saisir leur identifiants système. Seuls les utilisateurs disposant d'un compte local avec les privilèges administrateur peuvent activer le chiffrement.

Pour commencer le chiffrement sur des volumes de non-amorçage, l'agent de sécurité invitera les utilisateurs à configurer un mot de passe de chiffrement. Ce mot de passe sera requis pour déverrouiller le volume de non-amorçage chaque fois que l'ordinateur démarrera. Si l'ordinateur possède plusieurs volumes de non-amorçage, les utilisateurs doivent configurer un mot de passe de chiffrement pour chacun d'entre eux.

Déchiffrer des volumes

Pour déchiffrer des volumes sur les endpoints :

1. Sélectionnez la case **Gestion du chiffrement**.

2. Sélectionnez l'option **Déchiffrer**.

Le processus de déchiffrement commence à l'activation de la politique sur les endpoints, avec certaines différences entre Windows et Mac.

Sous Windows

Les volumes sont déchiffrés sans interaction avec les utilisateurs.


Sous Mac


Pour les volumes d'amorçage, les utilisateurs doivent saisir leurs identifiants système. Pour les volumes de non-amorçage, les utilisateurs doivent saisir le mot de passe configuré lors du processus de chiffrement.

Les utilisateurs d'endpoints qui oublieraient leurs mots de passe de chiffrement auront besoin de clés de récupération pour déverrouiller leurs machines. Pour de plus amples informations relatives aux clés de récupérations, veuillez vous référer à « » (p. 106).

Exclure des partitions

Vous pouvez créer une liste d'exclusions du chiffrement en ajoutant des lettres de lecteurs spécifiques, des label ou nom de partition et le GUID de la partition. Créer une règle pour que des partitions ne soient pas chiffrées.

1. Cochez la case **Exclusions**.
2. Cliquez sur **Type** et sélectionnez un type de lecteur dans le menu déroulant.
3. Saisissez une valeur de lecteur dans le champ **Éléments exclus** en respectant les conditions suivantes :
 - Pour une **lettre de lecteur**, saisissez D :, ou la lettre de votre lecteur suivie d'un deux-points.
 - Pour un **label/nom**, vous pouvez saisir le label de votre choix, comme Travail.
 - Pour le **GUID** d'une partition, saisissez la valeur comme suit :
`\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\.`
4. Cliquez sur **Ajouter**  pour ajouter une exclusion à la liste.

Pour supprimer une exclusion, choisissez un élément et cliquez sur **Supprimer** .

7.2.13. NSX

Dans cette rubrique, vous pouvez établir la politique à utiliser comme profil de sécurité dans NSX. Pour ce faire :

1. Cochez la case **NSX** pour configurer sa visibilité également dans vSphere Web Client.
2. Saisissez le nom sous lequel vous pourrez identifier la politique dans NSX. Ce nom peut être différent du nom de la politique dans GravityZone Control Center. Dans vSphere il apparaîtra avec le préfixe `Bitdefender_`. Faites attention lors du choix de ce nom car il sera en lecture seule une fois que la politique est enregistrée.

7.2.14. Protection de stockage



Note

Storage Protection est disponible pour les périphériques de stockage en réseau (NAS) et les solutions de partage de fichiers conformes au protocole ICAP (Internet Content Adaptation Protocol).

Dans cette section, vous pouvez configurer les Security Server en tant que service d'analyse pour les NAS et les solutions de partage de fichiers compatibles avec le protocole ICAP, telles que Nutanix Files et Citrix ShareFile.

Les Security Server peuvent analyser n'importe quels fichiers, y compris des archives, lorsque les périphériques de stockage le leur demandent. En fonction des réglages choisis, les Security Server prennent des mesures appropriées concernant les fichiers infectés, telles que la désinfection ou le refus d'accès.

Les paramètres sont organisés dans les sections suivantes :

- [ICAP](#)
- [Exclusions](#)

ICAP

Vous pouvez configurer les options suivantes pour les Security Server :

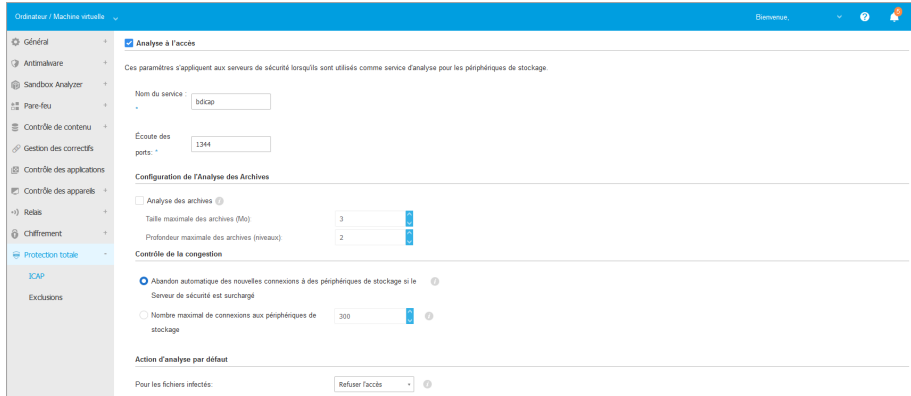
- Cochez la case **Analyse à l'accès** pour activer le module de Protection du stockage. Les réglages requis pour la communication entre les Security Server et les périphériques de stockage sont prédéfinis de la manière suivante :

- Nom du service : bdicap.
- Port d'écoute : 1344.
- Dans **Paramètres de l'analyse des archives**, cochez la case **Analyser les archives** pour permettre l'analyse des archives. Configurez la taille maximale et la profondeur maximale des archives à analyser.

**Note**

Lorsque vous réglez la taille maximale des archives sur 0 (zéro), le Security Server analyse les archives quelle que soit leur taille.

- Dans **Contrôle de la congestion**, choisissez la méthode de gestion des connexions sur les périphériques de stockage à privilégier en cas de surcharge du Security Server :
 - **Abandon automatique des nouvelles connexions sur les périphériques de stockage si le Security Server est surchargé.** Lorsqu'un Security Server aura atteint le nombre maximal de connexions, le périphérique de stockage redirigera le surplus vers un second Security Server.
 - **Nombre maximal de connexions aux périphériques de stockage.** La valeur par défaut est établie à 300 connexions.
- Dans **Analyser les actions**, les options suivantes sont disponibles :
 - **Refuser l'accès** - le Security Server refuse l'accès à des fichiers infectés.
 - **Désinfecter** - le Security Server supprime le code malveillant des fichiers infectés.



Politiques - Protection du stockage - ICAP

Exclusions

Si vous souhaitez que des objets spécifiques soient exclus de l'analyse, cochez la case **Exclusions**.


Vous pouvez définir des exclusions :

- Par hachage - vous identifiez le fichier exclu par hachage SHA-256.
- Par caractère de remplacement - vous identifiez le fichier exclu par chemin d'accès.

Configuration des exceptions

Pour ajouter une exclusion :

1. Sélectionnez le type d'exclusion dans le menu.
2. En fonction du type d'exclusion, spécifiez l'objet à exclure comme suit :
 - **Hachage** - saisissez les hachages SHA-256, séparés par une virgule.
 - **Caractère de remplacement** - spécifiez un nom de chemin d'accès absolu ou relatif en utilisant des caractères de remplacement. Le symbole astérisque (*) correspond à n'importe quel fichier au sein d'un répertoire. Un point d'interrogation (?) correspond à un caractère unique.
3. Ajouter une description pour l'exclusion.
4. Cliquez sur le bouton **Ajouter**. La nouvelle exclusion sera ajoutée à la liste.

Pour retirer une règle de la liste, cliquez sur le bouton  **Supprimer** correspondant.

Importer et exporter les Exclusions

Si vous avez l'intention de réutiliser les exclusions dans d'autres politiques, vous pouvez choisir de les exporter et de les importer.

Pour exporter des exclusions :

1. Cliquez sur **Exporter** dans le coin supérieur du tableau des exclusions.
2. Enregistrez le fichier CSV sur votre ordinateur. En fonction des paramètres de votre navigateur, le fichier peut être téléchargé automatiquement, ou on vous demandera de l'enregistrer vers un emplacement de téléchargement par défaut.

Chaque ligne dans le fichier CSV correspond à une exclusion unique, avec les champs dans l'ordre suivant :

```
<exclusion type>, <object to be excluded>, <description>
```

Voici les valeurs disponibles pour les champs CSV :

Type d'exclusion :

- 1, pour un hachage SHA-256
- 2, pour un caractère de remplacement

Objet à exclure :

Une valeur de hachage ou un nom de chemin d'accès

Description

Un texte pour aider à identifier l'exclusion.

Exemple d'exclusions dans le fichier CSV :

```
2,*/file.txt,text  
2,*/image.jpg,image  
1,e4b0c44298fc1c19afb4c8996fb9227ae41e4649b934ca991b7852b855,hash
```

Pour importer des exclusions :

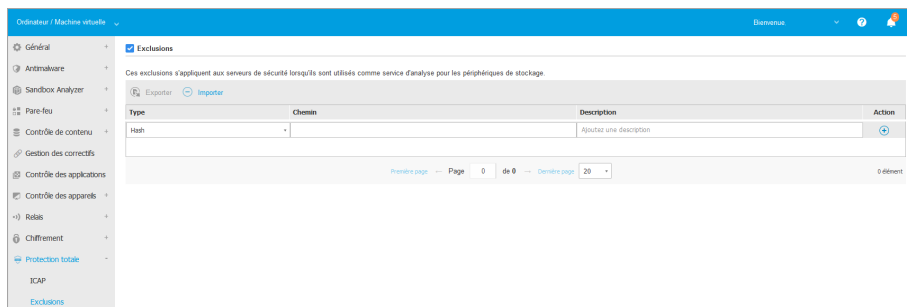
1. Cliquez sur **Importer**. La fenêtre **Importer Exclusions de politique** s'ouvre.
2. Cliquez sur **Ajouter** et sélectionnez le fichier CSV.

3. Cliquez sur **Enregistrer**. Le tableau est rempli avec les exclusions valides. Si le fichier CSV contient des exclusions invalides, un message d'avertissement vous informe des numéros de ligne correspondants.

Modifier Les Exclusions

Pour modifier une exclusion :

1. Cliquez sur le nom de l'exclusion dans la colonne **Chemin d'accès** ou dans la description.
2. Modifiez l'exclusion.
3. Appuyez sur **Entrée** lorsque vous avez terminé.



Politiques - Protection du stockage - ICAP

7.3. Politiques des appareils mobiles

Les paramètres de la politique peuvent être configurés lors de sa création. Vous pouvez ensuite les modifier selon vos besoins à tout moment.

Pour configurer les paramètres d'une politique :

1. Allez sur la page **Politiques**.
2. Sélectionnez **Appareils mobiles** dans le [sélecteur de vues](#).
3. Cliquez sur le nom de la politique. Cela ouvrira la page des paramètres de la politique.
4. Configurez les paramètres de la politique selon vos besoins. Les paramètres sont regroupés dans les catégories suivantes :
 - [Généraux](#)

- Détails
- Gestion de l'appareil
 - Sécurité
 - Mot de passe
 - Profils

Vous pouvez sélectionner la catégorie des paramètres à l'aide du menu dans la partie gauche de la page.

5. Cliquez sur **Enregistrer** pour enregistrer les modifications et les appliquer aux appareils mobiles cibles. Pour quitter la page de la politique sans enregistrer les modifications, cliquez sur **Annuler**.

7.3.1. Généraux

La catégorie **Général** contient des informations descriptives concernant la politique sélectionnée.

Détails

La page Détails présente des informations générales sur la politique :

- Nom de la politique
- L'utilisateur qui a créé la politique
- La date et l'heure auxquelles la politique a été créée
- La date et l'heure de la dernière modification de la politique

Vous pouvez renommer la politique en indiquant le nouveau nom dans le champ correspondant. Les politiques doivent porter des noms explicites afin que vous, ou un autre administrateur, puissiez les identifier rapidement.



Note

Par défaut, seul l'utilisateur qui a créé la politique peut la modifier. Pour changer cela, le propriétaire de la politique doit cocher l'option **Autoriser d'autres utilisateurs à modifier cette politique** à partir de la page **Détails** de la politique.

7.3.2. Gestion de l'appareil

Les paramètres d'administration de l'appareil permettent de définir les options de sécurité des appareils mobiles, le verrouillage de l'écran par mot de passe ainsi que plusieurs profils pour chaque politique d'appareil mobile.

Les paramètres sont organisés dans les sections suivantes :

- Sécurité
- Mot de passe
- Profils

Sécurité

Cette section vous permet de configurer différents paramètres de sécurité pour les appareils mobiles, y compris des analyses antimalwares pour les appareils Android, l'administration d'appareils rootés ou jailbreakés ou l'action à appliquer aux appareils non conformes.



Important

L'analyse est effectuée dans le cloud et l'appareil mobile doit donc avoir un accès à Internet.

The screenshot shows the 'Sécurité Android' settings page. On the left, a navigation menu includes 'Général', 'Gestion de l'appareil', 'Sécurité', 'Mot de passe', and 'Profils'. The main content area is titled 'Sécurité Android' and contains the following options:

- Analyser les applications à l'installation
- Analyser la mémoire (montage)
- Requérir le cryptage de l'appareil
- Protection de débogage USB
- Sécurité Web
 - Bloquer les pages web de phishing
 - Bloquer les pages web contenant des malwares ou des exploits
 - Bloquer les pages web utilisées dans des arnaques ou des fraudes
 - Signaler à l'utilisateur les pages web non fiables

Below these are sections for 'Changements d'OS' and 'Conformité':

- Autoriser l'administration d'appareils rootés ou jailbreakés
- Action par défaut quand un appareil d'entreprise n'est pas conforme: Ignorer
- Action par défaut quand un appareil personnel n'est pas conforme: Ignorer

Politiques des appareils mobiles - Paramètres de sécurité

Sécurité Android

- Sélectionnez **Analyser les applications à l'installation** si vous souhaitez effectuer une analyse lorsque de nouvelles applications sont installées sur les appareils mobiles gérés.
- Sélectionnez **Analyser la mémoire (montage)** si vous souhaitez effectuer une analyse de chaque support de stockage lorsque celui-ci est monté.

Avertissement

Si des malwares sont détectés, l'utilisateur est invité à les supprimer. Si l'utilisateur ne supprime pas les malwares détectés dans l'heure qui suit leur détection, l'appareil mobile est déclaré non conforme et l'action de non conformité sélectionnée s'applique automatiquement (Ignorer, Refuser l'accès, Verrouiller, Supprimer ou Dissocier).

- Sélectionnez **Requérir le cryptage de l'appareil** pour demander à l'utilisateur d'activer la fonctionnalité de cryptage disponible dans le système d'exploitation Android. Le cryptage protège les données présentes sur les appareils Android y compris les comptes, les paramètres, les applications téléchargées, les fichiers multimédias ou autres, contre l'accès non autorisé. Les données cryptées sont accessibles à partir d'appareils externes uniquement si l'on indique le mot de passe de déverrouillage.

Important

- Le cryptage de l'appareil est disponible pour Android 3.0 ou une version supérieure. Tous les modèles d'appareils ne permettent pas le cryptage. Consultez la fenêtre **Détails des appareils mobiles** pour des informations sur le support du cryptage.
- Le cryptage peut avoir un impact sur les performances de l'appareil.

Avertissement

- Le cryptage de l'appareil est définitif et la seule façon de revenir à l'état non crypté est d'effacer les données de l'appareil.
- Il est recommandé aux utilisateurs de sauvegarder leurs données avant d'activer le cryptage de l'appareil.
- Les utilisateurs ne doivent pas interrompre le processus de cryptage car ils perdraient l'ensemble ou une partie de leurs données.

Si vous activez cette option, GravityZone Mobile Client indique un problème permanent informant l'utilisateur de la nécessité d'activer le cryptage. L'utilisateur doit cliquer sur le bouton **Résoudre** pour poursuivre vers le cryptage et lancer le processus. Si le cryptage n'est pas activé dans les sept jours suivant la notification, l'appareil devient non conforme.

Pour activer le cryptage sur un appareil Android :

- La batterie doit être chargée à plus de 80%.

- L'appareil doit être branché jusqu'à la fin du cryptage.
- L'utilisateur doit définir un mot de passe de déverrouillage respectant les exigences de complexité.

Note

- Les appareils Android utilisent le même mot de passe pour déverrouiller l'écran et le contenu crypté.
- Le cryptage requiert un mot de passe, PIN ou une identification par reconnaissance faciale pour déverrouiller l'appareil en désactivant les autres paramètres de verrouillage de l'écran.

Le processus de cryptage peut nécessiter une heure ou plus, pendant laquelle l'appareil peut redémarrer plusieurs fois.

Vous pouvez consulter l'état du cryptage de la mémoire de chaque appareil mobile dans la fenêtre **Détails des appareils mobiles**.

- Les appareils Android en mode debugging peuvent être connectés à un PC grâce à un câble USB, ce qui permet un contrôle avancé sur les applications et le système d'exploitation. Dans ce cas, la sécurité des appareils mobiles peut être soumise à risque. Activée par défaut, l'option **Protection mode debugging USB** empêche l'utilisation des appareils en mode debugging USB. Si l'utilisateur active le mode debugging USB, l'appareil devient automatiquement non-conforme et l'action de non-conformité est prise en compte. Dans le cas où l'action de non-conformité est **Ignorer**, l'utilisateur est prévenu du risque lié à ce réglage.

Néanmoins, vous pouvez désactiver cette option pour les appareils mobiles fonctionnant en mode debugging USB (comme les appareils dédiés au développement ou aux tests d'applications).

- Sélectionnez **Sécurité Web** pour activer les fonctionnalités de sécurité Web sur les appareils Android.

La Sécurité Web analyse dans le cloud toutes les URL visitées puis renvoie un état de sécurité à GravityZone Mobile Client. L'état de sécurité de l'URL peut être : saine, fraude, malware, phishing ou non fiable.

GravityZone Mobile Client peut appliquer une action spécifique en fonction de l'état de sécurité de l'URL :

- **Bloquer les pages web de phishing.** Lorsque l'utilisateur essaie d'accéder à un site web de phishing, GravityZone Mobile Client bloque l'URL correspondante et affiche à la place une page d'avertissement.
- **Bloquer les pages web contenant des malwares ou des exploits.** Lorsque l'utilisateur essaie d'accéder à un site web diffusant des malwares ou des exploits web, GravityZone Mobile Client bloque l'URL correspondante et affiche à la place une page d'avertissement.
- **Bloquer les pages web utilisées dans des arnaques ou des fraudes.** Étend la protection à d'autres types d'arnaques que le phishing (par exemple, aux faux tiers de confiance, aux fausses œuvres de charité, aux menaces sur les réseaux sociaux etc.). Lorsque l'utilisateur essaie d'accéder à une page web frauduleuse, GravityZone Mobile Client bloque l'URL correspondante et affiche à la place une page d'avertissement.
- **Signaler à l'utilisateur les pages web non fiables.** Lorsque l'utilisateur accède à un site web qui a été piraté auparavant à des fins de phishing ou récemment promu via du spam ou des e-mails de phishing, un message pop-up d'avertissement s'affiche, sans bloquer la page web.



Important

Les fonctionnalités de Sécurité Web fonctionnent uniquement jusqu'à Android 5, et seulement avec Chrome et avec le navigateur Android intégré.

Changements d'OS

Considérés comme un risque de sécurité pour les réseaux d'entreprise, les appareils rootés ou jailbreakés sont automatiquement déclarés non conformes.

- Sélectionnez **Autoriser l'administration d'appareils rootés ou jailbreakés** si vous souhaitez administrer des appareils rootés ou jailbreakés à partir du Control Center. Veuillez noter que ces appareils étant par défaut non conformes, l'**action de non-conformité** sélectionnée leur est automatiquement appliquée dès qu'ils sont détectés. Ainsi, pour pouvoir leur appliquer les paramètres de sécurité de la politique ou pour y exécuter des tâches, vous devez régler l'action de non-conformité sur Ignorer.
- Si vous décochez la case **Autoriser l'administration d'appareils rootés ou jailbreakés**, vous pouvez dissocier automatiquement les appareils rootés ou jailbreakés à partir du réseau de GravityZone. Dans ce cas, l'application GravityZone Mobile Client affiche un message indiquant que l'appareil est rooté

/ jailbreaké. L'utilisateur peut cliquer sur le bouton OK, qui redirige vers l'écran d'enregistrement. Dès que l'appareil n'est plus rooté/jailbreaké ou lorsque la politique est réglée pour autoriser l'administration des appareils rootés/jailbreakés, il peut être enregistré de nouveau (avec le même jeton pour les appareils Android / avec un nouveau jeton pour les appareils iOS).

Conformité

Vous pouvez configurer des actions spécifiques à appliquer automatiquement aux appareils détectés comme étant non conformes en fonction du type d'appareil (appartenant à l'entreprise ou personnel).



Note

Lorsque vous ajoutez un nouvel appareil dans Control Center, l'on vous demande de spécifier le type d'appareil dont il s'agit (appartenant à l'entreprise ou personnel). Cela permettra à GravityZone de gérer séparément les appareils personnels et ceux de l'entreprise.

- [Critères de non-conformité](#)
- [Actions de non-conformité](#)

Critères de non-conformité

Un appareil est déclaré non conforme dans les situations suivantes :

- **Appareils Android**
 - L'appareil est rooté.
 - GravityZone Mobile Client n'est pas l'Administrateur de l'Appareil.
 - Des malwares ne sont pas supprimés une heure après leur détection.
 - Politique non respectée :
 - L'utilisateur ne définit pas le mot de passe de verrouillage de l'écran dans les 24 heures qui suivent la première notification.
 - L'utilisateur ne change pas le mot de passe de verrouillage de l'écran au moment spécifié.
 - L'utilisateur n'active pas le cryptage de l'appareil dans les sept jours suivant la première notification.
 - Le mode débogage USB est activé sur l'appareil lorsque l'option de la politique Protection de débogage USB est activée.

- **appareils iOS**

- L'appareil est jailbreaké.
- GravityZone Mobile Client est désinstallé de l'appareil mobile.
- Politique non respectée :
 - L'utilisateur ne définit pas le mot de passe de verrouillage de l'écran dans les 24 heures qui suivent la première notification.
 - L'utilisateur ne change pas le mot de passe de verrouillage de l'écran au moment spécifié.

Action par défaut quand l'appareil n'est pas conforme

Lorsqu'un appareil est déclaré non conforme, l'utilisateur est invité à corriger le problème de non-conformité. L'utilisateur doit appliquer les modifications requises dans le délai spécifié, sinon, l'action sélectionnée pour les appareils non conformes sera appliquée (Ignorer, Refuser l'accès, Verrouiller, Supprimer ou Dissocier).

Vous pouvez changer l'action pour les appareils non conformes dans la politique à tout moment. La nouvelle action est appliquée aux appareils non conformes une fois que la politique est enregistrée.

Sélectionnez dans le menu correspondant à chaque type d'appareil l'action à appliquer lorsqu'un appareil est déclaré non conforme :

- **Ignorer.** Informe uniquement l'utilisateur que l'appareil n'est pas conforme à la politique d'utilisation des appareils mobiles.
- **Refuser l'accès.** Bloque l'accès de l'appareil aux réseaux de l'entreprise en supprimant les paramètres Wifi et VPN, tout en conservant tous les autres paramètres définis dans la politique. Les paramètres bloqués sont restaurés dès que l'appareil devient conforme.



Important

Lorsque l'Administrateur de l'appareil est désactivé pour GravityZone Mobile Client, l'appareil correspondant devient non conforme et on lui applique automatiquement l'action **Refuser l'accès**.

- **Verrouiller.** Verrouille immédiatement l'écran de l'appareil.
 - Sur Android, l'écran est verrouillé avec un mot de passe généré par GravityZone uniquement si aucune autre protection par verrouillage n'est

configurée sur l'appareil. Cela ne passera pas outre une option de verrouillage d'écran déjà configurée telle que Schéma, PIN, Mot de passe, Empreinte digitale ou Smart Lock.

- Sous iOS, si l'appareil a un mot de passe de verrouillage de l'écran, il est demandé pour le déverrouillage.
- **Supprimer.** Restaure les paramètres d'usine de l'appareil mobile, en effaçant définitivement toutes les données de l'utilisateur.



Note

L'option Supprimer ne supprime actuellement pas les données des appareils montés (cartes SD).

- **Dissocier.** L'appareil est immédiatement supprimé du réseau.



Note

Pour réenregistrer un appareil mobile auquel l'action Dissocier a été appliquée, vous devez ajouter de nouveau l'appareil dans le Control Center. L'appareil doit alors être réenregistré avec le nouveau jeton d'activation. Avant de réenregistrer l'appareil, vérifiez que les conditions qui conduisent l'appareil à être non lié ne sont plus présentes ou modifiez les paramètres de la politique afin de permettre la gestion de l'appareil.

Mot de passe

Cette section vous permet de choisir d'activer la fonction de verrouillage de l'écran par mot de passe disponible dans le système d'exploitation des appareils mobiles.

The screenshot shows the 'Verrouillage de l'écran par mot de passe' (Screen lock by password) configuration page. On the left, a sidebar lists menu items: 'Général', 'Gestion de l'appareil', 'Sécurité', 'Mot de passe', and 'Profil'. The 'Mot de passe' option is selected. The main content area shows a checked box for 'Verrouillage de l'écran par mot de passe' and a 'Configuration' link. Below this, there are four radio button options: 'Agressif', 'Normal', 'Tolérant', and 'Personnalisé'. The 'Normal' option is selected. To the right of these options, the text reads: 'Normal – Niveau de sécurité moyen du mot de passe' and 'Mot de passe d'au moins 8 caractères (dont au moins 2 complexes) et un délai de verrouillage court (3 minutes). Les mots de passe expirent tous les 3 mois et il n'est pas possible de réutiliser les 4 précédents.'

Politiques des appareils mobiles - Paramètres de la protection par mot de passe

Une fois cette fonctionnalité activée, une notification à l'écran demande à l'utilisateur de définir un mot de passe de verrouillage de l'écran. L'utilisateur doit saisir un mot de passe respectant les critères de mot de passe définis dans la

politique. Une fois que le mot de passe a été défini par l'utilisateur, toutes les notifications concernant ce problème sont effacées. Un message demandant de saisir le mot de passe s'affiche à chaque tentative de déverrouillage de l'écran.

Note

Si l'utilisateur ne définit pas un mot de passe lorsqu'il y est invité, l'appareil peut être utilisé sans mot de passe de verrouillage de l'écran jusqu'à 24 heures après la première notification. Pendant ce temps, un message demandant à l'utilisateur de saisir un mot de passe de verrouillage de l'écran apparaît toutes les 15 minutes à l'écran.

Avertissement

Si l'utilisateur ne définit pas un mot de passe dans les 24 heures qui suivent la première notification, l'appareil mobile devient non conforme et [l'action sélectionnée pour les appareils non conformes](#) est appliquée.

Pour configurer les paramètres du mot de passe de verrouillage de l'écran :

1. Cochez la case **Verrouillage de l'écran par mot de passe**.
2. Cliquez sur le niveau de sécurité du mot de passe qui correspond le mieux à vos besoins (Agressif, Normal ou Tolérant). Utilisez la description à droite de l'échelle pour faire votre choix.
3. Pour une configuration de pointe, sélectionnez le niveau de protection **Personnalisé** puis cliquez sur le lien **Configuration**.

Paramètres du mot de passe

Configuration

Type:

Requérir une valeur alphanumérique

Longueur minimale

Nombre minimal de caractères complexes

Période d'expiration (mois)

Restriction liée à l'historique (mots de passe précédents)

Nombre maximal d'échecs

Verrouillage automatique après (mn)

Politiques des appareils mobiles - Paramètres avancés de la protection par mot de passe



Note

Pour voir les conditions de configuration requises du mot de passe d'un niveau de sécurité prédéfini, sélectionnez ce niveau et cliquez sur le lien **Configuration**. Si vous modifiez une option, le niveau de sécurité du mot de passe deviendra automatiquement **Personnalisé**.

Options personnalisées.

- **Type.** Vous pouvez exiger que le mot de passe soit simple ou complexe. Les critères de complexité des mots de passe sont définis dans les systèmes d'exploitation des appareils mobiles.
 - Sur les appareils Android, les mots de passe complexes doivent contenir au moins une lettre, un chiffre et un caractère spécial.



Note

Les mots de passe complexes sont supportés sous Android 3.0 ou version supérieure.

- Sur les appareils iOS, les mots de passe complexes n'autorisent pas l'utilisation de caractères séquentiels ou répétés (tels que abcdef, 12345 ou aaaaa, 11111).

En fonction de l'option sélectionnée, lorsque l'utilisateur définit le mot de passe de verrouillage de l'écran, le système d'exploitation vérifie et demande à l'utilisateur d'intervenir si les critères requis ne sont pas remplis.

- **Requérir une valeur alphanumérique.** Requérir que le mot de passe contienne à la fois des lettres et des chiffres.
- **Longueur minimale.** Requérir que le mot de passe contienne un nombre minimal de caractères, que vous indiquez dans le champ correspondant.
- **Nombre minimal de caractères complexes.** Requérir que le mot de passe contienne un nombre minimal de caractères non alphanumériques (tels que @, # ou \$), que vous spécifiez dans le champ correspondant.
- **Période d'expiration (mois).** Forcer l'utilisateur à changer le mot de passe de verrouillage de l'écran à un intervalle spécifié (en mois). Par exemple, si vous saisissez 3, l'utilisateur sera invité à changer le mot de passe de verrouillage de l'écran tous les trois mois.

**Note**

Sous Android, cette fonctionnalité est proposée dans la version 3.0 ou supérieure.

- **Restriction liée à l'historique (mots de passe précédents).** Sélectionnez ou saisissez une valeur dans le champ correspondant pour indiquer le nombre d'anciens mots de passe ne pouvant pas être réutilisés. Par exemple, si vous indiquez le chiffre 4, l'utilisateur ne peut pas réutiliser l'un des quatre derniers mots de passe utilisés.

**Note**

Sous Android, cette fonctionnalité est proposée dans la version 3.0 ou supérieure.

- **Nombre maximal d'échecs.** Spécifiez combien de fois l'utilisateur est autorisé à saisir un mot de passe incorrect.

**Note**

Sur les appareils iOS, lorsque ce nombre est supérieur à 6 : après six tentatives ayant échoué, un délai est imposé avant que l'utilisateur puisse saisir de nouveau le mot de passe. Le délai augmente avec chaque tentative ayant échoué.



Avertissement

Si l'utilisateur dépasse le nombre maximal de tentatives autorisées pour déverrouiller l'écran, les données de l'appareil seront supprimées (toutes les données et les configurations seront effacées).

- **Verrouillage automatique après (mn).** Définissez la période d'inactivité (en minutes) après laquelle l'appareil est automatiquement verrouillé.



Note

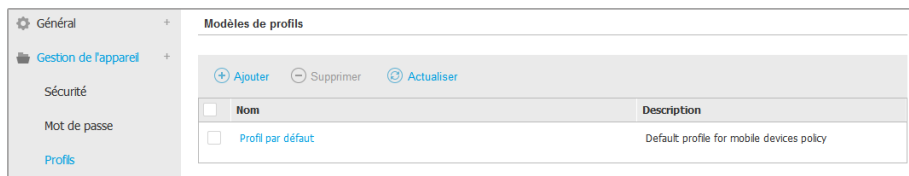
Les appareils iOS ont une liste prédéfinie de durées avant le verrouillage automatique et ne permettent pas de saisir des valeurs personnalisées. Lorsqu'on affecte une politique avec une durée avant le verrouillage automatique incompatible, l'appareil applique la valeur précédente la plus proche de la liste. Par exemple, si la durée avant le verrouillage automatique définie dans la politique est de trois minutes, l'appareil sera automatiquement verrouillé après deux minutes d'inactivité.

Lorsque vous modifierez la politique, si vous choisissez un niveau de sécurité plus élevé pour le mot de passe de verrouillage de l'écran, les utilisateurs seront invités à modifier leur mot de passe en fonction des nouveaux critères.

Si vous décochez l'option **Verrouillage de l'écran par mot de passe**, les utilisateurs retrouveront un accès complet aux paramètres de verrouillage de l'écran sur leur appareil mobile. Le mot de passe existant demeure actif jusqu'à ce que l'utilisateur décide de le changer ou de le supprimer.

Profils

Cette section vous permet de créer, de modifier et de supprimer des profils d'utilisation pour les appareils mobiles. Les profils d'utilisation vous aident à envoyer les paramètres Wifi et VPN et à appliquer le contrôle de l'accès à Internet sur les appareils mobiles gérés.



Politiques d'appareils mobiles - Modèles de profil

Vous pouvez configurer un ou plusieurs profils mais seul un peut être actif à la fois sur un appareil.

- Si vous ne configurez qu'un profil, ce profil s'applique automatiquement à tous les appareils auxquels la politique est affectée.
- Si vous configurez plusieurs profils, le premier de la liste s'applique automatiquement à tous les appareils auxquels la politique est affectée.

Les utilisateurs d'appareils mobiles peuvent voir les profils affectés et les paramètres configurés pour chaque profil dans l'application GravityZone Mobile Client. Les utilisateurs ne peuvent pas modifier les paramètres d'un profil mais peuvent passer d'un profil à l'autre si plusieurs profils sont disponibles.



Note

Passer d'un profil à l'autre nécessite une connexion à Internet.

Pour créer un nouveau profil :

1. Cliquez sur le bouton **+** **Ajouter** à droite du tableau. La page de configuration du profil s'affiche.
2. Configurez les paramètres du profil selon vos besoins. Pour plus d'informations, reportez-vous à :
 - [« Détails » \(p. 414\)](#)
 - [« Réseaux » \(p. 415\)](#)
 - [« Accès à Internet » \(p. 418\)](#)
3. Cliquez sur **Enregistrer**. Le nouveau profil est ajouté à la liste.

Pour supprimer un ou plusieurs profils, cochez la/les case(s) correspondante(s) et cliquez sur le bouton **-** **Supprimer** à droite du tableau.

Pour modifier un profil, cliquez sur son nom, modifiez les paramètres selon vos besoins et cliquez sur **Enregistrer**.

Détails

La page **Détails** contient des informations générales sur le profil :

- **Nom.** Saisissez le nom du profil souhaité. Les profils devraient porter des noms explicites afin que vous ou un autre administrateur puissiez les identifier rapidement.

- **Description.** Indiquez une description détaillée du profil. Cette option peut aider les administrateurs à identifier facilement un profil parmi plusieurs autres.

Réseaux

Cette section vous permet de spécifier les paramètres d'un ou plusieurs réseaux Wifi et VPN. Les paramètres VPN sont disponibles uniquement pour les appareils iOS.

The screenshot shows the 'Réseaux' (Networks) section of the mobile device policy configuration. It is divided into two main sections: 'Wi-Fi' and 'VPN pour iOS'. Each section has a header with action buttons: '+ Ajouter' (Add), '- Supprimer' (Remove), 'Actualiser' (Refresh), 'Haut' (Up), and 'Bas' (Down). Below each header is a table with columns for 'Priorité' (Priority), 'Nom' (Name), and 'Cryptage' (Encryption). The tables are currently empty.

Politiques des appareils mobiles - Paramètres de connexion aux réseaux du profil



Important

Avant de définir les connexions Wifi et VPN, vérifiez que vous disposez de toutes les informations nécessaires (mots de passe, paramètres du proxy, etc.).

Les appareils mobiles affectés au profil correspondant se connecteront automatiquement au réseau défini, lorsque celui-ci sera à portée. Vous pouvez définir la priorité lorsque plusieurs réseaux sont créés, en tenant compte du fait que seul un réseau peut être utilisé à la fois. Lorsque le premier réseau n'est pas disponible, l'appareil mobile se connecte au deuxième, et ainsi de suite.

Pour définir la priorité des réseaux :

1. Cochez la case du réseau souhaité.
2. Utilisez les boutons de priorité à droite du tableau :
 - Cliquez sur **la flèche vers le haut** pour faire monter le réseau sélectionné.
 - Cliquez sur **la flèche vers le bas** pour le faire descendre.

● Wi-Fi

Vous pouvez ajouter autant de réseaux Wifi que nécessaire. Pour ajouter un réseau Wifi :

1. Dans la section **Wifi**, cliquez sur le bouton **+ Ajouter** à droite du tableau. Une fenêtre de configuration s'affiche.
2. L'onglet **Général** vous permet de configurer les détails de la connexion Wifi :
 - **Nom (SSID)**. Saisissez le nom du nouveau réseau Wifi.
 - **Sécurité**. Sélectionnez l'option correspondant au niveau de sécurité du réseau Wifi :
 - **Aucune**. Sélectionnez cette option lorsque la connexion Wifi est publique (aucun identifiant n'est requis).
 - **WEP**. Sélectionnez cette option pour définir une connexion WEP (Wireless Encryption Protocol). Saisissez le mot de passe requis pour ce type de connexion dans le champ correspondant ci-dessous.
 - **WPA/WPA2 Personnel**. Sélectionnez cette option si le réseau Wifi est sécurisé à l'aide de WPA (Wi-Fi Protected Access). Saisissez le mot de passe requis pour ce type de connexion dans le champ correspondant ci-dessous.
3. L'onglet **TCP/IP** vous permet de configurer les paramètres TCP/IP de la connexion Wifi. Chaque connexion Wifi peut utiliser IPv4, IPv6 ou les deux.
 - **Configurer IPv4**. Si vous souhaitez utiliser la méthode IPv4, sélectionnez la méthode d'attribution d'IP dans le menu correspondant :
 - DHCP** : si l'adresse IP est attribuée automatiquement par un serveur DHCP. Si besoin, indiquez l'ID du client DHCP dans le champ suivant.
 - Désactivé** : sélectionnez cette option si vous ne souhaitez pas utiliser le protocole IPv4.
 - **Configurer IPv6**. Si vous souhaitez utiliser la méthode IPv6, sélectionnez la méthode d'attribution d'IP dans le menu correspondant :
 - DHCP** : si l'adresse IP est attribuée automatiquement par un serveur DHCP.
 - Désactivé** : sélectionnez cette option si vous ne souhaitez pas utiliser le protocole IPv6.
 - **Serveurs DNS**. Saisissez l'adresse d'au moins un serveur DNS du réseau.

4. Sous l'onglet **Proxy**, configurez les paramètres du proxy de la connexion Wifi. Sélectionnez la méthode de configuration du proxy souhaitée dans le menu **Type** :
 - **Désactivé**. Sélectionnez cette option si le réseau Wifi n'a pas de paramètres de proxy.
 - **Manuel**. Sélectionnez cette option pour spécifier manuellement les paramètres du proxy. Saisissez le nom d'hôte du serveur proxy et le port sur lequel il écoute les connexions. Si le serveur proxy requiert une authentification, cochez la case **Authentification** et indiquez le nom d'utilisateur et le mot de passe dans les champs suivants.
 - **Automatique**. Sélectionnez cette option pour récupérer les paramètres de proxy à partir d'un fichier de Configuration Automatique de Proxy (PAC) publié dans le réseau local. Indiquez l'adresse du fichier PAC dans le champ **URL**.
5. Cliquez sur **Enregistrer**. La nouvelle connexion Wifi est ajoutée à la liste.

● VPN pour iOS

Vous pouvez ajouter autant de VPN que nécessaire. Pour ajouter un VPN :

1. Dans la section **VPN pour iOS**, cliquez sur le bouton **+ Ajouter** à droite du tableau. Une fenêtre de configuration s'affiche.
2. Définissez les paramètres VPN dans la fenêtre **Connexion VPN** :

Général:


- **Nom**. Saisissez le nom de la connexion VPN.
- **Cryptage**. Le protocole d'authentification disponible pour ce type de connexion est **IPSec**, qui requiert l'authentification de l'utilisateur par mot de passe et l'authentification de la machine par secret partagé.
- **Serveur**. Saisissez l'adresse du serveur VPN.
- **Utilisateur**. Saisissez le nom d'utilisateur VPN.
- **Mot de passe**. Saisissez le mot de passe VPN.
- **Nom du groupe**. Saisissez le nom du groupe.
- **Clé secrète**. Saisissez la clé prépartagée.

Proxy :

Cette section vous permet de configurer les paramètres proxy de la connexion VPN. Sélectionnez la méthode de configuration du proxy souhaitée dans le menu **Type** :

- **Désactivé**. Sélectionnez cette option si la connexion VPN n'a pas de paramètres de proxy.
- **Manuel**. Cette option vous permet de spécifier manuellement les paramètres du proxy :
 - **Serveur** : saisissez le nom d'hôte du proxy.
 - **Port** : saisissez le numéro de port du proxy.
 - Si le serveur proxy requiert une authentification, cochez la case **Authentification** et indiquez le nom d'utilisateur et le mot de passe dans les champs suivants.
- **Automatique**. Sélectionnez cette option pour récupérer les paramètres de proxy à partir d'un fichier de Configuration Automatique de Proxy (PAC) publié dans le réseau local. Indiquez l'adresse du fichier PAC dans le champ **URL**.

3. Cliquez sur **Enregistrer**. La nouvelle connexion VPN sera ajoutée à la liste.

Pour supprimer un ou plusieurs réseaux, cochez la/les case(s) correspondante(s) et cliquez sur le bouton  **Supprimer** à droite du tableau.

Pour modifier un réseau, cliquez sur son nom, modifiez les paramètres selon vos besoins et cliquez sur **Enregistrer**.

Accès à Internet

Cette section vous permet de configurer le contrôle de l'accès à Internet pour les appareils Android et iOS.



Politiques des appareils mobiles - Paramètres d'accès Web du profil

- **Contrôle de l'Accès à Internet pour Android.** Activez cette option pour filtrer l'accès Web pour Chrome et pour le navigateur Android intégré. Vous pouvez définir des restrictions horaires sur l'accès à Internet et également autoriser ou bloquer expressément l'accès à certaines pages Web. Les pages Web bloquées par le Contrôle de l'accès à Internet ne s'affichent pas dans le navigateur. Une page Web est affichée par défaut et informe l'utilisateur que la page Web demandée a été bloquée par Contrôle de l'accès à Internet.



Important

Le Contrôle de l'accès Web pour Android fonctionne uniquement jusqu'à Android 5, et seulement avec Chrome et avec le navigateur Android intégré.

Vous avez trois options de configuration :

- Sélectionnez **Autoriser** pour toujours accorder l'accès à Internet.
- Sélectionnez **Bloquer** pour toujours refuser l'accès à Internet.
- Sélectionnez **Planifier** afin d'activer des restrictions horaires pour l'accès à Internet à partir d'un planning détaillé.

Si vous choisissez d'autoriser ou de bloquer l'accès à Internet, vous pouvez définir des exceptions à ces actions pour l'ensemble des catégories web ou uniquement pour certaines adresses web. Cliquez sur **Configuration** pour configurer votre planification de l'accès à Internet et les exceptions comme suit :

Planificateur

Pour limiter l'accès à Internet à certaines heures de la journée sur une base hebdomadaire :

1. Sélectionnez dans la grille les intervalles pendant lesquels vous souhaitez bloquer l'accès à Internet.

Vous pouvez cliquer sur des cellules individuelles pour choisir des heures ou cliquer et faire glisser la souris sur plusieurs cellules pour bloquer de plus longues périodes. Cliquez de nouveau dans la cellule pour annuler la sélection.

	Dimanche	Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi
0	Red	White	White	White	White	White	Red
6	Red	White	White	White	White	White	Red
12	Red	White	White	White	White	White	Red
18	Red	White	White	White	White	White	Red
24	Red	White	White	White	White	White	Red

Politiques des appareils mobiles - Planificateur de l'accès à Internet

Pour effectuer une nouvelle sélection, cliquez sur **Tout autoriser** ou **Tout bloquer**, en fonction du type de restriction que vous souhaitez mettre en place.

2. Cliquez sur **Enregistrer**.

Règles Internet

Vous pouvez également définir des règles Web pour bloquer ou autoriser expressément certaines adresses Internet, écrasant ainsi les paramètres

existants du Contrôle de l'accès à Internet. Les utilisateurs pourront ainsi accéder à une page web spécifique même lorsque la navigation sur Internet est bloquée par le Contrôle de l'accès à Internet.

Pour créer une règle Internet :

1. Sélectionnez **Utiliser des exceptions** pour activer les exceptions web.
2. Saisissez l'adresse que vous souhaitez autoriser ou bloquer dans le champ **Adresse Web**.
3. Sélectionnez **Autoriser** ou **Bloquer** dans le menu **Permission**.
4. Cliquez sur le bouton **+ Ajouter** à droite du tableau pour ajouter l'adresse à la liste d'exceptions.
5. Cliquez sur **Enregistrer**.

Pour éditer une règle Internet :

1. Cliquez sur l'adresse web que vous souhaitez éditer.
2. Modifiez l'URL existante.
3. Cliquez sur **Enregistrer**.

Pour supprimer une règle Internet :

1. Placez le curseur sur l'adresse Web que vous souhaitez supprimer.
2. Cliquez sur le bouton **⊗ Supprimer**.
3. Cliquez sur **Enregistrer**.

Utilisez les caractères génériques pour spécifier des schémas d'adresses Internet :

- L'astérisque (*) remplace zéro caractère ou plus.
- Le point d'interrogation (?) remplace exactement un caractère. Vous pouvez utiliser plusieurs points d'interrogation pour définir toute combinaison d'un nombre spécifique de caractères. Par exemple, ??? remplace toute combinaison de 3 caractères précisément.

Dans le tableau suivant, vous trouverez des exemples de syntaxe pour les adresses Internet spécifiques.

Syntaxe	Applicabilité
<code>www.exemple*</code>	<p>Chaque site web ou page web commençant par <code>www.exemple</code> (sans tenir compte de l'extension de domaine).</p> <p>La règle ne s'appliquera pas aux sous-domaines du site web spécifié, tel que <code>sousdomaine.exemple.com</code>.</p>
<code>*exemple.com</code>	Tout site Internet se terminant par <code>exemple.com</code> , y compris les pages et sous-domaines de celui-ci.
<code>*chaîne*</code>	Tout site Internet ou page web dont l'adresse contient la chaîne spécifiée.
<code>*.com</code>	Chaque site Internet ayant l'extension de domaine <code>.com</code> , y compris les pages et sous-domaines de celui-ci. Utilisez cette syntaxe pour exclure de l'analyse des domaines entiers de premier niveau.
<code>www.exemple?.com</code>	Toutes les adresses web commençant par <code>www.exemple?.com</code> , où le ? peut être remplacé avec n'importe quel caractère unique. Ces sites Web pourraient inclure : <code>www.exemple1.com</code> ou <code>www.exempleA.com</code> .

- **Contrôle de l'Accès à Internet pour iOS.** Activez cette option pour gérer de façon centralisée les paramètres du navigateur iOS intégré (Safari). Les utilisateurs d'appareils mobiles ne pourront plus modifier les paramètres correspondants sur leurs appareils.
 - **Autoriser l'utilisation de Safari.** Cette option vous aide à contrôler l'utilisation du navigateur Safari sur les appareils mobiles. Désactiver cette option supprime le raccourci Safari de l'interface d'iOS, empêchant ainsi les utilisateurs d'accéder à Internet via Safari.
 - **Activer la saisie automatique.** Désactivez cette option si vous souhaitez éviter que le navigateur stocke des données saisies dans le formulaire, susceptibles de contenir des informations sensibles.

- **Forcer le signalement de sites frauduleux.** Sélectionnez cette option pour garantir que les utilisateurs seront avertis lorsqu'ils accèderont à des pages Web frauduleuses.
- **Activer Javascript.** Désactivez cette option si vous souhaitez que Safari ignore Javascript sur les sites Web.
- **Bloquer les pop-up.** Sélectionnez cette option pour empêcher que des fenêtres pop-up ne s'ouvrent automatiquement.
- **Accepter les cookies.** Safari autorise les cookies par défaut. Désactivez cette option si vous souhaitez empêcher que des sites Web ne stockent des informations sur la navigation.

**Important**

Web Access Control for iOS n'est pas compatible avec iOS 13.

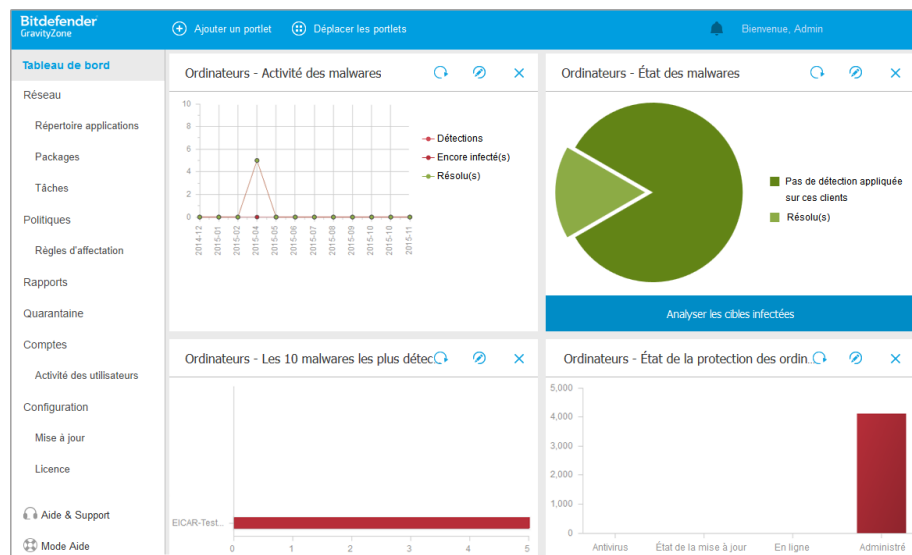
8. TABLEAU DE BORD DE SUPERVISION

Une bonne analyse de la sécurité de votre réseau nécessite l'accessibilité à vos données et leur corrélation. En centralisant les informations de sécurité, vous pouvez surveiller les politiques de sécurité de votre entreprise, garantir sa conformité, identifier rapidement les problèmes, analyser les menaces et les vulnérabilités.

8.1. Tableau de bord

Le tableau de bord de Control Center est un écran personnalisable fournissant un aperçu rapide de la sécurité de tous les endpoints protégés et de l'état du réseau.

Les portlets du tableau de bord affichent différentes informations de sécurité, en temps réel, sous la forme de graphiques faciles à lire, vous permettant d'identifier rapidement tout problème susceptible de requérir votre attention.



Le tableau de bord

Voici ce que vous avez besoin de savoir au sujet des portlets du tableau de bord :

- Le Control Center dispose de plusieurs portlets prédéfinis sur le tableau de bord.

- Chaque portlet du tableau de bord comprend un rapport détaillé en arrière-plan, accessible d'un simple clic sur le graphique.
- Il existe plusieurs types de portlets comprenant différentes informations sur la protection des endpoints tels que l'état de la mise à jour, l'état des malwares, l'activité du pare-feu.




Note


Par défaut, les portlets récupèrent les données pour la journée en cours et, à la différence des rapports, ne peuvent être réglés pour des intervalles de plus d'un mois.

- Les informations affichées via les portlets se réfèrent aux endpoints sous votre compte uniquement. Vous pouvez personnaliser les préférences et la cible de chaque portlet en utilisant la commande **Modifier le portlet**.
- Cliquez sur les entrées de la légende du graphique, lorsque cela est possible, pour masquer ou afficher la variable correspondante sur le graphique.
- Les portlets s'affichent en groupes de quatre. Utilisez la barre de défilement verticale ou les flèches haut et bas pour parcourir les groupes de portlets.
- Pour plusieurs types de rapports, vous avez la possibilité d'exécuter instantanément les tâches spécifiques sur les endpoints cibles, sans avoir à vous rendre sur la page **Réseau** pour exécuter la tâche (par exemple, analyser les endpoints infectés ou mettre à jour les endpoints). Utilisez le bouton en bas du portlet pour **appliquer l'action disponible**.

Le tableau de bord est facile à configurer en fonction des préférences personnelles. Vous pouvez **éditer** des paramètres de portlet, **ajouter** des portlets, **supprimer** ou **réorganiser** des portlets existants.


8.1.1. Actualiser les données du portlet

Pour que le portlet affiche des informations à jour, cliquez sur le bouton  **Actualiser** sur sa barre de titre.

Pour mettre à jour les informations de tous les portlets en même temps, cliquez sur le bouton  **Actualiser les portlets** situé en haut du tableau de bord.

8.1.2. Modification des paramètres d'un portlet


Certains portlets fournissent des informations sur l'état, alors que d'autres affichent des rapports sur les événements de sécurité au cours de la dernière période. Vous

pouvez consulter et configurer la période de reporting d'un portlet en cliquant sur l'icône  **Modifier le portlet** dans la barre de titre.

8.1.3. Ajouter un nouveau portlet

Vous pouvez ajouter des portlets pour obtenir les informations dont vous avez besoin.


Pour ajouter un nouveau portlet :

1. Allez sur la page **Tableau de bord**.
2. Cliquez sur le bouton  **Ajouter un portlet** en haut de la console. La fenêtre de configuration s'affiche.
3. Sous l'onglet **Détails**, configurez les informations du portlet :
 - Type d'endpoint (**Ordinateurs**, **Machines virtuelles** ou **Appareils mobiles**)
 - Le type de rapport en arrière-plan
 - Un nom de portlet explicite
 - L'intervalle avant que les événements soient signalés

Pour plus d'informations sur les types de rapports disponibles, référez-vous à « [Types de rapport](#) : » (p. 427).

4. Sous l'onglet **Cibles**, sélectionnez les objets et les groupes du réseau à inclure.
5. Cliquez sur **Enregistrer**.

8.1.4. Suppression d'un portlet

Vous pouvez facilement supprimer tout portlet en cliquant sur l'icône  **Supprimer** dans la barre de titre. Une fois que vous avez supprimé un portlet, vous ne pouvez plus le récupérer. Vous pouvez cependant créer un autre portlet avec exactement les mêmes paramètres.

8.1.5. Réorganiser les portlets

Vous pouvez réorganiser les portlets du tableau de bord en fonction de vos besoins. Pour réorganiser les portlets :

1. Allez sur la page **Tableau de bord**.
2. Glissez-déposez chaque portlet à l'emplacement de votre choix. Tous les autres portlets entre la nouvelle et l'ancienne positions sont déplacés pour préserver leur ordre.



Note

Vous pouvez déplacer les portlets uniquement dans les positions déjà occupées.

9. UTILISATION DES RAPPORTS

Le Control Center vous permet de créer et d'afficher des rapports centralisés sur l'état de sécurité des éléments administrés du réseau. Les rapports peuvent être utilisés à des fins diverses :

- Surveiller et garantir le respect des politiques de sécurité de l'organisation.
- Vérifier et évaluer l'état de sécurité du réseau.
- Identifier les problèmes de sécurité, les menaces et les vulnérabilités du réseau.
- Surveillance des incidents de sécurité.
- Fournir à la direction des données faciles à interpréter sur la sécurité du réseau.

Plusieurs types de rapports différents sont disponibles afin que vous puissiez obtenir facilement les informations dont vous avez besoin. Celles-ci sont présentées sous la forme de graphiques et de tableaux interactifs faciles à consulter, qui vous permettent de vérifier rapidement l'état de la sécurité du réseau et d'identifier les problèmes.

Les rapports peuvent regrouper l'ensemble des données du réseau ou uniquement de certains groupes. Ainsi, dans un rapport unique, vous pouvez trouver :

- Des informations statistiques sur tous les groupes ou éléments du réseau administrés.
- Des informations détaillées sur chaque élément du réseau administré.
- La liste des ordinateurs répondant à certains critères (par exemple, ceux dont la protection antimalware est désactivée.)

Certains rapports vous permettent également de corriger rapidement les problèmes détectés dans votre réseau. Vous pouvez par exemple facilement mettre à jour tous les objets cibles du réseau directement dans le rapport, sans avoir à vous rendre sur la page **Réseau** pour exécuter une tâche de mise à jour.

Tous les rapports planifiés sont disponibles dans le Control Center mais vous pouvez les enregistrer sur votre ordinateur ou les envoyer par e-mail.

Les formats PDF (Portable Document Format) et CSV (comma-separated values) sont disponibles.

9.1. Types de rapport :

Différents types de rapports sont disponibles pour chaque type d'endpoint :

- [Rapports Ordinateur et Machine virtuelle](#)
- [Rapports Exchange](#)

- [Rapports Appareil Mobile](#)

9.1.1. Rapports Ordinateur et Machine virtuelle

Voici les types de rapports disponibles pour les machines physiques et virtuelles :

Activité Antiphishing

Vous informe de l'activité du module Antiphishing de Bitdefender Endpoint Security Tools. Vous pouvez voir le nombre de sites Web de phishing bloqués sur les endpoints sélectionnés et l'utilisateur qui était connecté au moment de la dernière détection. En cliquant sur les liens de la colonne **Sites Web Bloqués**, vous pouvez également afficher les URL de sites Web, combien de fois elles ont été bloquées et quand a eu lieu le dernier blocage.

Applications bloquées

Vous informe de l'activité des modules suivants : Antimalware, Pare-feu, Contrôle de contenu, Contrôle des applications, Anti-exploit avancé, ATC/IDS et HVI. Vous pouvez voir le nombre d'applications bloqués sur les endpoints sélectionnés et l'utilisateur qui était connecté au moment de la dernière détection.

Cliquez sur le nombre associé à une cible pour voir des informations supplémentaires sur les applications bloquées, le nombre d'événements ayant eu lieu et la date et l'heure auxquelles a eu lieu le dernier blocage.

Dans ce rapport, vous pouvez rapidement demander aux modules de protection de laisser les applications sélectionnées s'exécuter sur l'endpoint cible :

- Cliquez sur le bouton **Ajouter une exception** pour définir des exceptions dans les modules suivants : Antimalware, ATC, Contrôle de contenu, Pare-feu et HVI. Une fenêtre de confirmation va apparaître, vous informant de la nouvelle règle qui va modifier la politique existante pour cet endpoint spécifique.
- Cliquez sur le bouton **Ajouter une règle** pour définir une règle pour une application ou un processus dans le Contrôle des applications. Dans la fenêtre de configuration, appliquez la règle à une politique existante. Un message vous informera de la nouvelle règle qui modifiera la politique affectée à cet endpoint spécifique. Le rapport affiche également le nombre de tentatives d'accès et indique si le module s'est exécuté en Mode test ou en Mode production.

Sites Web bloqués

Vous informe de l'activité du module Contrôle Web de Bitdefender Endpoint Security Tools. Pour chaque cible, vous pouvez voir le nombre de sites Web bloqués. En cliquant sur ce nombre, vous pouvez afficher des informations supplémentaires telles que :

- L'URL et la catégorie du site Web
- Le nombre de tentatives d'accès par site Web
- Date et heure de la dernière tentative, ainsi que l'utilisateur qui était connecté au moment de la détection.
- Motif de blocage, qui comprend l'accès programmé, la détection de malwares, le filtrage par catégorie et la liste noire.

Protection des données

Vous informe de l'activité du module Données de Bitdefender Endpoint Security Tools. Vous pouvez voir le nombre d'e-mails et de sites Web bloqués sur les endpoints sélectionnés, ainsi que l'utilisateur qui était connecté au moment de la dernière détection.

Activité du Contrôle des appareils

Vous informe au sujet des événements ayant eu lieu lors de l'accès aux endpoints via les appareils surveillés. Pour chaque endpoint cible, vous pouvez afficher le nombre d'événements de lecture seule et d'accès autorisés/bloqués. Si des événements ont eu lieu, des informations supplémentaires sont disponibles, en cliquant sur les numéros correspondants. Les informations concernent :

- L'utilisateur connecté sur la machine
- Le type et l'identifiant de l'appareil
- Le fournisseur de l'appareil et l'ID du produit
- La date et l'heure de l'événement.

État du chiffrement du endpoint

Vous fournit des données relatives à l'état du chiffrement sur les endpoints. Un diagramme circulaire affiche le nombre de machines respectivement conformes et non conformes aux paramètres de la politique de chiffrement.

En-dessous du diagramme, un tableau fournit d'autres informations :

- Nom de l'endpoint.

- Nom de domaine complet au format FQDN.
- IP de la machine.
- Système d'exploitation .
- Conformité politique appareil:
 - **Conforme** – lorsque les volumes sont tous chiffrés ou déchiffrés, conformément à la politique.
 - **Non conforme** – lorsque l'état des volumes n'est pas conforme à la politique attribuée (par exemple, seul l'un des deux volumes est chiffré, ou bien un processus de chiffrement est en cours sur le volume en question).
- Politique de l'appareil (**Chiffrer** ou **Déchiffrer**).
- Cliquez sur les chiffres de la colonne Synthèse des volumes afin de visualiser les informations relatives aux volumes de chaque endpoint : Identifiant, nom, état de chiffrement (**Chiffré** ou **Non chiffré**), problématiques, type (**Amorçage** ou **Non amorçage**), taille, identifiant de la clé de récupération.

État des modules de l'Endpoint

Fournit un aperçu de la couverture des modules de protection sur les cibles sélectionnées. Dans les détails du rapport, pour chaque endpoint cible, vous pouvez voir quels modules sont actifs, désactivés ou non installés, ainsi que le moteur d'analyse utilisé. Cliquer sur le nom du endpoint fera apparaître la fenêtre **Informations** avec des détails concernant l'endpoint et les couches de protection installées.

En cliquant sur le bouton **Reconfigurer le client**, vous lancerez une tâche de modification des paramètres initiaux d'un ou plusieurs endpoints sélectionnés. Pour plus d'informations, consultez la section [Reconfigurer le client](#).

État de la protection des endpoints

Vous fournit différentes informations d'état au sujet des endpoints de votre réseau sélectionnés.

- État de la protection antimalware
- État de la mise à jour de Bitdefender Endpoint Security Tools
- État de l'activité du réseau (en ligne/hors ligne)
- État de l'administration

Vous pouvez appliquer les filtres par aspect et par état de la sécurité afin de trouver les informations que vous recherchez.

Activité du pare-feu

Vous informe de l'activité du module Pare-feu de Bitdefender Endpoint Security Tools. Vous pouvez voir le nombre de tentatives de trafic et d'analyses de port bloqués sur les endpoints sélectionnés, ainsi que l'utilisateur qui était connecté au moment de la dernière détection.

Activité HyperDetect

Vous informe de l'activité du module HyperDetect de Bitdefender Endpoint Security Tools.

Le graphique en haut à droite de la page des rapports vous indique la fréquence des tentatives d'attaques sur la période de temps définie, ainsi que leur répartition par types d'attaques. Le fait de déplacer la souris sur les légendes des rubriques mettra en évidence le type d'attaque correspondant dans le graphique. Le fait de cliquer sur la rubrique fera apparaître ou masquera la ligne respective dans le graphique. Cliquez sur n'importe quel élément d'une ligne afin de filtrer les données de votre tableau, conformément au type sélectionné. Par exemple, si vous cliquez sur un élément de la ligne orange, le tableau n'affichera que les exploits.

Les informations figurant sur la partie inférieure du rapport vous permettent d'identifier les failles dans votre réseau et de savoir si elles ont été traitées. Elles font référence :

- L'emplacement du fichier malveillant, ou l'URL détectée, en cas de fichiers infectés. Pour les attaques sans fichier, le nom de l'exécutable utilisé pour l'attaque est indiqué, avec un lien vers une fenêtre d'information qui affiche la raison de la détection et la ligne de commande malveillante.
- Le endpoint sur lequel la détection a été faite
- Au module de protection qui a détecté la menace. HyperDetect agissant en tant que couche supplémentaire pour les modules antimalware et de contrôle de contenu, le rapport donnera des informations sur l'un de ces deux modules, en fonction du type de détection.
- Le type d'attaque (attaque ciblée, grayware, exploits, ransomware, fichiers suspects et trafic réseau)
- L'état de la menace

- Le niveau de protection du module auquel la menace a été détectée (Permissif, Normal, Agressif)
- Le nombre de fois où la menace a été détectée
- La détection la plus récente
- Identification en tant qu'attaque sans fichier (oui ou non) pour filtrer rapidement les détections d'attaques sans fichier.

**Note**

Un même fichier peut être utilisé dans plusieurs types d'attaques. Ainsi, GravityZone signale cela pour chaque type d'attaque subie.

À partir de ce rapport, vous pourrez rapidement résoudre les problèmes de faux résultats positifs, en ajoutant des exceptions dans les politiques de sécurité attribuées. Pour ce faire :

1. Dans la tableau, sélectionnez autant de rubriques que nécessaire.

**Note**

Les détections des attaques sans fichiers ne peuvent être ajoutées à la liste des exceptions, car l'exécutable détecté n'est pas un malware en soi, mais il peut être une menace en cas d'utilisation d'une ligne de commande malveillante.

2. Cliquez sur le bouton **Ajouter une exception** en haut à droite du tableau.
3. Dans la fenêtre de configuration, sélectionnez les politiques auxquelles l'exception doit être ajoutée, puis cliquez sur **Ajouter**.

Par défaut, les informations relatives à chaque exception ajoutée sont envoyées à Bitdefender Labs, pour participer à l'amélioration des capacités de détection des produits Bitdefender. Vous pouvez contrôler cette action à l'aide de la case **Envoyer un rapport à Bitdefender pour une meilleure analyse**.

Si la menace a été détectée par le module antimalware, l'exception s'appliquera aussi bien aux modes d'analyse à l'accès qu'à la demande.

**Note**

Vous pouvez retrouver ces exceptions dans les sections suivantes des politiques sélectionnées : **Antimalware et Paramètres** pour les fichiers, et **Contrôle de contenu et Trafic** pour les URL.

État des malwares

Vous aide à découvrir combien et quels endpoints sélectionnés ont été affectés par des malwares pendant une période spécifique et comment les menaces ont été gérées. Vous pouvez également voir l'utilisateur qui était connecté au moment de la dernière détection.

Les endpoints sont regroupés en fonction des critères suivants :

- Endpoints sans détection (aucun malware n'a été détecté pendant la période spécifiée)
- Endpoints avec des malwares résolus (tous les fichiers détectés ont bien été désinfectés ou placés dans la [quarantaine](#))
- Endpoints avec des malwares non résolus (certains des fichiers détectés dont l'accès a été refusé)

Pour chaque endpoint, vous pouvez cliquer sur les liens des colonnes de résultat de la désinfection pour afficher la liste des menaces et chemins d'accès aux fichiers affectés.

Dans ce rapport, vous pouvez rapidement réaliser une Analyse complète sur les cibles non résolues, en cliquant sur le bouton **Analyser les cibles infectées** de la barre d'action située au-dessus du tableau.

Incidents du réseau

Vous informe de l'activité du module Network Attack Defense. Un graphique présente le nombre de tentatives d'attaques détectées sur une période donnée. Les détails du rapport comprennent :

- Nom de l'endpoint, adresse IP et FQDN
- Utilisateur
- Nom de détection
- Technique Attack
- Nombre d'essais
- IP de l'attaquant
- IP et port ciblés
- Quand l'attaque a été pour la dernière fois bloquée

En cliquant sur le bouton **Ajouter des exceptions** pour une détection sélectionnée, une entrée est automatiquement créée dans les **Exclusions globales** de la section **Protection du réseau**.

État des patchs du réseau

Contrôlez le statut de mise à jour du logiciel installé sur votre réseau. Le rapport présente les informations suivantes :

- Machine cible (nom, IP et système d'exploitation de l'endpoint).
- Patchs de sécurité (patchs installés, patchs dont l'installation a échoué, patchs manquants : de sécurité ou non).
- État et date de dernière modification des endpoints contrôlés.

État de la protection du réseau

Fournit des informations détaillées sur l'état de sécurité global des endpoints cibles. Vous pouvez par exemple consulter des informations sur :

- Nom, adresse IP et FQDN
- État :
 - **Problèmes** - des vulnérabilités ont été repérées dans la protection de l'endpoint (l'agent de sécurité n'est pas à jour, des menaces ont été détectées, etc.)
 - **Pas de problème** - l'endpoint est protégé, il n'y a aucun motif d'inquiétude.
 - **Inconnu** - l'endpoint était hors ligne au moment de la génération du rapport.
 - **Non administré** - l'agent de sécurité n'est pas encore installé sur l'endpoint.
- Couches de protection disponibles
- Endpoints administrés et non administrés (l'agent de sécurité est installé ou non)
- Le type et l'état de la licence (des colonnes supplémentaires sur la licence sont masquées par défaut)
- État d'infection (l'endpoint est « propre » ou non)
- L'état des mises à jour du produit et des contenus de sécurité
- L'état des correctifs de sécurité du logiciel (correctifs manquants, de sécurité ou non)

Pour les endpoints non administrés, les autres colonnes contiendront l'état **Non administré**.

Analyse à la demande

Fournit des informations concernant les analyses à la demande exécutées sur les cibles sélectionnées. Un graphique affiche les statistiques des analyses réussies et de celles qui ont échoué. Le tableau sous le graphique fournit des détails concernant le type d'analyse, leur occurrence, et la dernière analyse réalisée avec succès pour chaque endpoint.

Respect de la politique

Fournit des informations concernant les politiques de sécurité appliquées aux cibles sélectionnées. Un graphique affiche l'état de la politique. Dans le tableau sous le graphique, vous pouvez voir la politique appliquée à chaque endpoint et le type de politique, ainsi que la date et l'utilisateur qui l'a assignée.

Échecs d'envoi vers Sandbox Analyzer

Affiche l'ensemble des tentatives d'envois d'éléments manquées, depuis les endpoints vers Sandbox Analyzer, sur une période de temps définie. L'échec de l'envoi survient après plusieurs tentatives manquées.

Le graphique indique la variation des échecs d'envoi au cours de la période sélectionnée, tandis que le tableau détaillé vous permet de visualiser les fichiers qui n'ont pas pu être envoyés vers Sandbox Analyzer, la machine depuis laquelle les éléments ont été envoyés, l'heure et la date de chaque tentative, le code d'erreur renvoyé, la description de chaque tentative manquée et le nom de la société.

Résultats Sandbox Analyzer (obsolète)

Vous fournit des informations détaillées relatives aux fichiers présents sur les endpoints ciblés, qui ont été analysés dans le sandbox sur une période de temps définie. Un graphique linéaire indique le nombre de fichiers propres ou dangereux analysés, tandis que le tableau affiche des données détaillées pour chaque cas.

Vous pouvez générer un rapport des Résultats de Sandbox Analyzer pour l'ensemble des fichiers analysés ou uniquement pour ceux qui ont été détectés comme malveillants.

Vous pouvez afficher :

- Verdict de l'analyse, indiquant si le fichier est propre, dangereux ou inconnu (**Menace détectée** / **Aucune menace détectée** / **Non supporté**). Cette colonne n'apparaît que lorsque vous sélectionnez le rapport qui affiche l'ensemble des objets analysés.

Pour visualiser la liste complète des types de fichiers et extensions pris en charge par Sandbox Analyzer, veuillez vous référer à « [Types et extensions de fichier pris en charge pour l'envoi manuel](#) » (p. 533).

- Types de menaces, parmi lesquelles les adware, rootkits, fichiers à télécharger, exploit, modificateurs de fichiers hosts, outils malveillants, voleurs de mots de passe, ransomware, spams ou chevaux de Troie.
- Date et heure de la détection, que vous pouvez filtrer en fonction de la période de signalement.
- Nom d'hôte et IP de l'endpoint où le fichier a été détecté.
- Noms des fichiers, s'ils sont soumis individuellement, ou nombre de fichiers analysés en cas de lot. Cliquez sur le nom de fichier ou lien du lot, afin de visualiser les détails et les actions appliquées.
- État des actions de réparation pour les fichiers soumis (**Partielle, Échec, Signalée uniquement, Réussie**).
- Nom de l'entreprise .
- De plus amples informations relatives aux propriétés du fichier analysé sont disponibles en cliquant sur le bouton ⓘ **En savoir plus** dans la colonne **Résultat d'analyse**. Ici, vous pouvez visualiser les informations de sécurité et les rapports détaillés relatifs au comportement type.

Sandbox Analyzer enregistre les événements comportementaux suivants :

- Écriture / suppression / déplacement / duplication / remplacement de fichiers sur le système et sur des disques amovibles.
- Exécution de fichiers récemment créés.
- Modifications dans le système de fichiers.
- Modifications au niveau des applications exécutées à l'intérieur de la machine virtuelle.
- Modifications au niveau de la barre des tâches Windows et du menu Démarrer.
- Création/interruption/injection de processus.
- Écriture/suppression des clés de registre.
- Création d'objets mutex.
- Création / démarrage / arrêt / modification / requête / suppression de services.
- Modifications des paramètres de sécurité du navigateur.
- Modification des paramètres d'affichage Windows Explorer.
- Ajout de fichiers à la liste d'exception du pare-feu.
- Modifications des paramètres du réseau.
- Activation de l'exécution lors du démarrage du système.

- Connexion à un hôte distant.
- Accès à certains domaines.
- Transfert de données vers et à partir de certains domaines.
- Accès à des URL, IP et ports via divers protocoles de communication.
- Vérification des indicateurs de l'environnement virtuel.
- Vérification des indicateurs des outils de surveillance.
- Création de captures d'écran.
- Crochetage SSDT, IDT, IRP.
- Déchargement de mémoire pour les processus suspects.
- Appels de fonction Windows API.
- Se montrer inactif pendant un certain temps, afin de retarder l'exécution.
- Créer des fichiers dont les actions seront exécutées à intervalles réguliers.

Dans la fenêtre des **Résultats d'analyse**, cliquez sur le bouton **Télécharger** afin de sauvegarder sur votre ordinateur le contenu de la synthèse comportementale, dans les formats suivants : XML, HTML, JSON, PDF.

Ce rapport sera encore proposé pendant un certain temps. Nous vous recommandons plutôt d'utiliser les fiches d'envoi pour obtenir les informations nécessaires sur les échantillons analysés. Les fiches d'envoi sont disponibles dans la section **Sandbox Analyzer**, accessible depuis le menu principal de la Control Center.

Audit de sécurité

Fournit des informations, sur les événements de sécurité qui se sont produits sur une cible sélectionnée. Les informations réfèrent aux événements suivants :

- Détection des malwares
- Application bloquée
- Port d'analyse bloqué
- Trafic bloqué
- Site Web bloqué
- Bloquer l'appareil
- E-mail bloqué
- Processus bloqué
- Événements HVI
- Événements Anti-exploit avancée
- Événements Network Attack Defense
- Détection des ransomwares

État du Security Server

Vous aide à évaluer l'état des Security Server cibles. Vous pouvez identifier les problèmes que chaque Security Server peut rencontrer, à l'aide de différents indicateurs d'état tels que :

- **État** : présente l'état global du Security Server.
- **État des machines** : indique quelles appliances Security Server sont arrêtées.
- **État de l'AV** : précise si le module Antimalware est activé ou désactivé.
- **État de mise à jour** : indique si les appliances Security Server sont mises à jour ou si les mises à jour ont été désactivées.
- **État de chargement** : indique le niveau de chargement de l'analyse d'un Security Server comme indiqué ci-dessous :
 - **En sous-charge**, lorsque moins de 5% de sa capacité d'analyse est utilisée.
 - **Normal**, lorsque le chargement de l'analyse est équilibré.
 - **En surcharge**, lorsque le chargement de l'analyse dépasse 90% de sa capacité. Dans ce cas, vérifiez les politiques de sécurité. Si tous les Security Server alloués dans une politique sont surchargés, vous devez ajouter un autre Security Server à la liste. Sinon, vérifiez la connexion réseau entre les clients et les Security Server n'ayant pas de problèmes de charge.
- **MV protégées HVI** : vous informe des machines virtuelles qui sont contrôlées et protégées par le module.
- **état HVI** : indique si le module HVI est activé ou désactivé. HVI est activé si Security Server et le package de complément sont tous deux installés sur l'hôte.
- **Périphériques de stockage connectés** : indique le nombre de périphériques de stockage conformes au protocole ICAP connectés au Security Server. En cliquant sur le nombre, vous afficherez la liste des périphériques de stockage, avec des informations propres à chacun : nom, adresse IP, type, date et heure de la dernière connexion.
- **Statut de l'analyse du stockage** : indique si le service Security for Storage est activé ou désactivé.

Vous pouvez également voir combien d'agents sont connectés au Security Server. Plus loin, cliquer sur le nombre de clients connectés affichera la liste des endpoints. Ces endpoints peuvent être vulnérables si le Security Server a des problèmes.

Les 10 malwares les plus détectés

Vous indique les 10 principaux malwares détectés au cours d'une période donnée sur les endpoints sélectionnés.



Note

Le tableau détails indique tous les endpoints ayant été infectés par les 10 malwares les plus souvent détectés.

Les 10 endpoints les plus infectés

Vous indique les 10 endpoints les plus infectés en fonction du nombre total de détections sur une période donnée pour les endpoints sélectionnés.



Note

Le tableau détails indique tous les malwares détectés sur les 10 endpoints les plus infectés.

État de la mise à jour

Vous montre l'état de la mise à jour de l'agent de sécurité ou du Security Server installé sur les cibles sélectionnées. L'état des mises à jour concerne les versions du produit et du contenu de sécurité.

Les filtres vous permettent de connaître facilement les clients ayant été ou non mis à jour au cours des 24 dernières heures.

Dans ce rapport, vous pouvez rapidement mettre à jour les agents vers la dernière version. Pour cela, cliquez sur le bouton **Mettre à jour** de la barre d'action située au-dessus du tableau.

État de la mise à niveau

Vous indique les agents de sécurité installés sur les cibles sélectionnées et si une solution plus récente est disponible.

Pour les endpoints sur lesquels d'anciens agents de sécurité sont installés, vous pouvez installer rapidement le dernier agent de sécurité pris en charge en cliquant sur le bouton **Mettre à niveau**.

**Note**

Ce rapport est disponible uniquement lorsqu'une mise à niveau de la solution GravityZone a été effectuée.

État de la protection du réseau de machines virtuelles

Vous informe de la portée de la protection Bitdefender dans votre environnement virtualisé. Pour chacune des machines sélectionnées, vous pouvez voir quel composant résout les problèmes de sécurité :

- Security Server, pour les déploiements sans agent dans les environnement VMware NSX et VShield, et pour HVI
- Un agent de sécurité, dans toute autre situation

Activité HVI

Vous informe de toutes les attaques que les modules HVI ont détectées sur les machines sélectionnées dans un certain laps de temps.

Le rapport contient également des informations sur la date et l'heure du dernier incident détecté qui impliquait des processus surveillés, le statut final de l'action prise contre l'attaque, l'utilisateur avec lequel le processus a été exécuté et la machine cible.

Selon l'action effectuée, le même processus peut être rapporté plusieurs fois. Par exemple, si un processus a été arrêté une fois et qu'une fois l'accès a été refusé, vous verrez deux entrées dans le tableau de rapport.

Pour chaque processus, lorsque vous cliquez sur la dernière date de détection, un journal séparé contenant tous les incidents détectés depuis que le processus a commencé s'affichera. Le journal révèle des informations importantes, telles que le type d'incident et sa description, la source et la cible de l'attaque et les actions effectuées pour corriger le problème.

Dans ce rapport, vous pouvez rapidement commander au module de protection d'ignorer certains événements que vous considérez comme légitimes. Pour cela, cliquez sur le bouton **Ajouter une exception** de la barre d'action située au-dessus du tableau.

**Note**

Le module HVI pour votre solution GravityZone est disponible via une clé de licence distincte.

État de l'injection d'outils tiers HVI

Vous donne des informations détaillées sur chaque injection exécutée sur les endpoints sélectionnés. Ces informations comprennent :

- Le nom de l'endpoint.
- Le nom de l'outil injecté.
- L'adresse IP de l'endpoint.
- Le système d'exploitation invité.
- Le déclencheur. Il peut s'agit d'une violation de mémoire, d'une tâche à la demande ou d'une exécution planifiée.
- Le nombre d'exécutions réussies. En cliquant sur le numéro, une fenêtre s'ouvre avec l'emplacement des journaux et l'horodatage de chaque exécution d'outil. Cliquez sur l'icône située devant le chemin pour le copier dans le presse-papier.
- Le nombre d'exécutions ratées. En cliquant sur le numéro, une fenêtre s'ouvre sur laquelle vous pouvez voir la raison de l'échec et l'horodatage.
- Dernière injection réussie.

Les injections sont regroupées par endpoints cibles. Vous pouvez filtrer le rapport pour ne voir que les données relatives à un outil particulier en utilisant les options de filtrage de l'en-tête du tableau.

Activité du ransomware

Vous informe sur les attaques de ransomware détectées par GravityZone sur les endpoints que vous administrez et vous fournit les outils nécessaires pour récupérer les fichiers impactés par ces attaques.

Le rapport est disponible sous la forme d'une page distincte de Control Center, accessible depuis le menu principal de GravityZone.

La page **Activité de ransomware** est composée d'une grille qui liste les éléments suivants pour chaque attaque de ransomware :

- Le nom, l'adresse IP et le FQDN de l'endpoint sur lequel est survenue l'attaque
- L'entreprise à laquelle le poste de travail appartient.
- Le nom de l'utilisateur connecté au moment de l'attaque
- Le type d'attaque, soit local ou à distance

- Le processus utilisé par le ransomware pour les attaques locales, ou l'adresse IP depuis laquelle l'attaque a été initiée pour les attaques à distance
- La date et l'heure de la dernière détection
- Le nombre de fichiers chiffrés avant que l'attaque ne soit bloquée
- L'état des actions de restauration pour tous les fichiers de l'endpoint ciblé

Certains détails sont cachés par défaut. Cliquez sur le bouton **Afficher/Masquer les colonnes** en haut à droite de la page pour configurer les informations que vous voulez voir dans la grille. Si votre grille compte de nombreuses entrées, vous pouvez choisir de masquer les filtres en utilisant le bouton **Afficher/Masquer les filtres** situé en haut à droite de la page.

D'autres informations peuvent être consultées en cliquant sur le numéro des fichiers. Vous pouvez voir le chemin complet du fichier d'origine et du fichier restauré, et le statut de la restauration de tous les fichiers impliqués dans l'attaque de ransomware sélectionnée.



Important

Les copies de sauvegarde sont disponibles au maximum pendant une période de 30 jours. Veuillez prendre note de la date et de l'heure à partir desquelles les fichiers ne pourront plus être restaurés.

Pour restaurer les fichiers impactés par un ransomware :

1. Sélectionnez l'attaque désirée sur la grille.
2. Cliquez sur le bouton **Restaurer les fichiers**. Une fenêtre de confirmation apparaît.

Une tâche de récupération est créée. Vous pouvez en consulter l'état depuis la page **Tâches**, comme n'importe quelle autre tâche de GravityZone.

Si des détections résultent de processus légitimes, suivez les instructions suivantes :

1. Sélectionnez les enregistrements désirés sur la grille.
2. Cliquez sur le bouton **Ajouter une exception**.
3. Dans cette nouvelle fenêtre, sélectionnez la politique à laquelle l'exception doit s'appliquer.
4. Cliquez sur **Ajouter**.

appliquera toutes les exceptions possibles : sur le dossier, sur le processus et sur l'adresse IP.

Vous pouvez les consulter et les modifier dans la section **Antimalware > Paramètres > Exceptions personnalisées** de la politique.



Note

Activités de ransomware conserve les événements des deux dernières années.

9.1.2. Rapports Serveur Exchange

Ce sont les types de rapports disponibles pour les serveurs Exchange :

Exchange - Contenu et pièces jointes bloqués

Vous fournit des informations sur les e-mails ou les pièces jointes que le Contrôle de Contenu a supprimés des serveurs sélectionnés pendant une période donnée. Ces informations comprennent :

- L'adresse e-mail de l'expéditeur et des destinataires.
Lorsque l'e-mail a plusieurs destinataires, au lieu des adresses e-mail, le rapport indique le nombre de destinataires avec un lien vers une fenêtre contenant la liste des adresses e-mail.
- Sujet de l'e-mail.
- Type de détection, indiquant quel filtre du Contrôle de Contenu a détecté la menace.
- L'action appliquée à la détection.
- Le serveur sur lequel la menace a été détectée.

Exchange - Pièces jointes bloquées et non-analysables

Vous fournit les informations à propos des e-mails contenant des pièces jointes non analysables (compressées, protégées par mot de passe, etc.) bloquées sur les serveurs e-mails Exchange sélectionnés pendant une période de temps définie. Les informations se réfèrent à :

- L'adresse e-mail de l'expéditeur et des destinataires.
Lorsque l'e-mail est envoyé à plusieurs destinataires, au lieu des adresses e-mail, le rapport indique le nombre de destinataires avec un lien vers une fenêtre contenant la liste des adresses e-mail.
- Sujet de l'e-mail.

- Les actions effectuées pour supprimer les pièces jointes non analysables :
 - **E-mail supprimé**, indique que la totalité de l'e-mail a été supprimée.
 - **Pièces jointes supprimées**, nom générique pour toutes les actions qui suppriment les pièces jointes de l'e-mail, comme la suppression des pièces jointes, le déplacement en quarantaine ou le remplacement par une notice.
- En cliquant sur le lien dans la colonne **Action**, vous pouvez voir des détails sur chaque pièce jointe bloquée et l'action prise correspondante.
- Date et l'heure de la détection.
 - Le serveur sur lequel l'e-mail a été détecté.

Exchange - Activité d'analyse des e-mails

Présente des statistiques sur les actions prises par le module Protection Exchange pendant une période donnée.

Les actions sont regroupées par type de détection (malware, spam, pièce jointe interdite et contenu interdit) et par serveur.

Les statistiques se réfèrent aux états d'e-mails suivants :

- **Quarantaine**. Ces e-mails ont été placés dans le dossier Quarantaine.
- **Supprimé/Rejeté**. Ces e-mails ont été supprimés ou rejetés par le serveur.
- **Redirigé**. Ces e-mails ont été redirigés vers l'adresse de messagerie indiquée dans la politique.
- **Nettoyés et délivrés**. Les menaces de ces e-mails ont été supprimées et les messages ont franchi les filtres.

Un e-mail est considéré comme nettoyé quand toutes ses pièces jointes détectées ont été désinfectées, placées en quarantaine, supprimées ou remplacées par du texte.

- **Modifiés et délivrés**. Les informations d'analyse ont été ajoutées aux en-têtes d'e-mail et les e-mails ont franchi les filtres.
- **Délivrés sans aucune autre action**. Ces e-mails ont été ignorés par la Protection Exchange et ont franchi les filtres.

Exchange - Activité des malwares

Vous fournit des informations sur les e-mails avec des malwares, détectés sur les serveurs de messagerie Exchange sélectionnés pendant une période donnée.

Les informations se réfèrent à :

- L'adresse e-mail de l'expéditeur et des destinataires.

Lorsque l'e-mail est envoyé à plusieurs destinataires, au lieu des adresses e-mail, le rapport indique le nombre de destinataires avec un lien vers une fenêtre contenant la liste des adresses e-mail.

- Sujet de l'e-mail.
- État de l'e-mail après l'analyse antimalware.

En cliquant sur l'état du lien, vous pouvez afficher des informations sur les malwares détectés et sur l'action appliquée.

- Date et l'heure de la détection.
- Le serveur sur lequel la menace a été détectée.

Exchange - Les 10 malwares les plus détectés

Vous indique les 10 malwares les plus détectés dans les pièces jointes d'e-mail. Vous pouvez générer deux affichages contenant différentes statistiques. Un affichage indique le nombre de détections par destinataires affectés et un autre par expéditeurs.

Par exemple, GravityZone a détecté un e-mail avec une pièce jointe infectée envoyé à cinq destinataires.

- Dans l'affichage des expéditeurs :
 - Le rapport présente cinq détections.
 - Les détails du rapport indiquent uniquement les destinataires, pas les expéditeurs.
- Dans l'affichage des destinataires :
 - Le rapport présente une détection.
 - Les détails du rapport indiquent uniquement l'expéditeur, pas les destinataires.

En plus du nom de l'expéditeur/des destinataires et du malware, le rapport vous fournit les informations suivantes :

- Le type de malware (virus, spyware, PUA, etc.)

- Le serveur sur lequel la menace a été détectée.
- Les mesures prises par le module Antimalware.
- La date et l'heure de la dernière détection.

Exchange - Les 10 principaux destinataires de malwares

Vous indique les 10 principaux destinataires d'e-mails les plus ciblés par des malwares sur une période donnée.

Les détails du rapport vous indiquent la liste complète de malwares ayant affecté ces destinataires, ainsi que les actions appliquées.

Exchange - Les 10 principaux destinataires de spam

Vous indique les 10 principaux destinataires d'e-mails en fonction du nombre d'e-mails de spam ou de phishing détectés sur une période donnée. Ce rapport fournit également des informations sur les actions appliquées aux e-mails respectifs.

9.1.3. Rapports Appareils Mobiles



Note

La protection contre les malwares et les rapports associés sont uniquement disponibles pour les appareils Android.

Voici la liste des types de rapports disponibles pour les appareils mobiles :

État des malwares

Vous aide à découvrir combien et quels appareils mobiles cibles ont été affectés par des malwares pendant une période spécifique et comment les menaces ont été gérées. Les appareils mobiles sont regroupés en fonction des critères suivants :

- Les appareils mobiles sans détection (aucun malware n'a été détecté pendant la période spécifiée)
- Les appareils mobiles avec des malwares résolus (tous les fichiers détectés ont été supprimés)
- Les appareils mobiles avec des malwares (certains des fichiers détectés n'ont pas été supprimés)

Les 10 appareils les plus infectés

Vous indique les 10 appareils mobiles les plus infectés pendant une période donnée parmi les appareils mobiles cibles.

**Note**

Le tableau détails indique tous les malwares détectés sur les 10 appareils mobiles les plus infectés.

Les 10 malwares les plus détectés

Vous indique les 10 principaux malwares détectés au cours d'une période donnée sur les appareils mobiles cibles.

**Note**

Le tableau détails indique tous les appareils mobiles ayant été infectés par les 10 malwares les plus souvent détectés.

Conformité de l'appareil

Vous informe de l'état de conformité des appareils mobiles cibles. Vous pouvez voir le nom de l'appareil, son état, système d'exploitation et la raison de la non-conformité.

Pour plus d'informations sur les exigences de conformité, veuillez consulter « [Critères de non-conformité](#) » (p. 407).

Synchronisation de l'appareil

Vous informe de l'état de la synchronisation des appareils mobiles cibles. Vous pouvez afficher le nom de l'appareil, l'utilisateur auquel il est affecté ainsi que l'état de la synchronisation, le système d'exploitation et quand l'appareil a été vu en ligne pour la dernière fois.

Pour plus d'informations, reportez-vous à « [Consulter l'état des appareils mobiles](#) » (p. 176).

Sites Web bloqués

Vous indique le nombre de tentatives d'accès des appareils cibles à des sites web bloqués par les règles **Accès Web** au cours d'une période donnée.

Pour chaque appareil avec des détections, cliquez sur le nombre figurant dans la colonne **Sites Web Bloqués** pour afficher des informations détaillées sur chaque page web bloquée telles que :

- URL
- Le composant de la politique ayant effectué l'action
- Nombre de tentatives bloquées
- La dernière fois que le site web a été bloqué

Pour plus d'informations sur les paramètres de la politique d'accès à Internet, reportez-vous à « [Profils](#) » (p. 413).

Activités de la Sécurité Web

Vous informe du nombre de tentatives d'accès des appareils mobiles cibles à des sites web avec des menaces de sécurité (phishing, fraude, malwares ou sites web non fiables) au cours d'une période donnée. Pour chaque appareil avec des détections, cliquez sur le nombre figurant dans la colonne Sites Web Bloqués pour afficher des informations détaillées sur chaque page web bloquée telles que :

- URL
- Le type de menace (phishing, malware, fraude, non fiable)
- Nombre de tentatives bloquées
- La dernière fois que le site web a été bloqué

Sécurité Web est le composant de la politique qui détecte et bloque les sites web ayant des problèmes de sécurité. Pour plus d'informations sur les paramètres de la politique de sécurité web, reportez-vous à « [Sécurité](#) » (p. 403).

9.2. Création de rapports

Vous pouvez créer deux catégories de rapports :

- **Les rapports instantanés.** Les rapports instantanés s'affichent automatiquement une fois que vous les avez générés.
- **Rapports planifiés.** Les rapports planifiés peuvent être configurés pour s'exécuter régulièrement, à une date et une heure spécifiées. Une liste de tous les rapports planifiés apparaît sur la page **Rapports**.



Important

Les rapports instantanés sont supprimés automatiquement lorsque vous fermez la page du rapport. Les rapports planifiés sont enregistrés et affichés sur la page **Rapports**.

Pour créer un rapport :

1. Allez sur la page **Rapports**.
2. Sélectionnez le type d'objets du réseau dans le [sélecteur d'affichage](#).

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

Créer un rapport

Détails

Type:

Nom: *

Configuration

Maintenant

Planifié

Fréquence des rapports :

Afficher: Tous les endpoints

Uniquement les endpoints avec des sites web bloqués

Distribution: Envoyer par e-mail à

Sélectionner la Cible

Ordinateur / Machine virtuelle

Groupes sélectionnés

Générer Annuler

Options du rapport Ordinateurs et Machines virtuelles

4. Sélectionnez le type de rapport souhaité dans le menu. Pour plus d'informations, reportez-vous à « [Types de rapport](#) : » (p. 427)
5. Indiquez un nom explicite pour le rapport. Lorsque vous choisissez un nom, prenez en compte le type et la cible du rapport, et, éventuellement, les options du rapport.
6. Configurez la périodicité des rapports :
 - Sélectionnez **Maintenant** afin de créer un rapport.
 - Sélectionnez **Planifier** afin de configurer les rapports qui seront automatiquement générés, aux intervalles souhaités:
 - Par heure, à un intervalle horaire spécifique.

- Tous les jours. Dans ce cas, vous pouvez aussi établir l'heure du début (heure et minutes).
 - Par semaine, à un jour précis de la semaine et à l'heure choisie (heure et minutes).
 - Par mois, à n'importe quel jour du mois et à l'heure choisie (heure et minutes).
7. Pour la plupart des types de rapport, vous devez spécifier l'intervalle de temps sur lequel les données se réfèrent. Le rapport affichera uniquement des données sur la période sélectionnée.
8. Plusieurs types de rapports fournissent des options de filtrage pour vous aider à trouver facilement les informations qui vous intéressent. Utilisez les options de filtrage sous le menu **Voir** pour obtenir uniquement les informations souhaitées.
- Par exemple, pour un rapport sur l'**État de la mise à jour**, vous pouvez choisir la liste des objets du réseau qui n'ont pas été mis à jour, ou de ceux qui nécessitent d'être redémarrés afin de terminer la mise à jour.
9. **Livraison.** Pour recevoir un rapport planifié par e-mail, cochez la case correspondante. Entrez l'adresse e-mail souhaitée dans le champs ci-dessous. Par défaut, l'e-mail contient une archive avec tous les rapports (PDF et CSV). Utilisez les cases à cocher dans la rubrique **Joindre des fichiers** pour personnaliser quels fichiers envoyer par e-mail.
10. **Sélectionner la cible.** Dérouler vers le bas afin de configurer le rapport. Sélectionnez un ou plusieurs groupes d'endpoints que vous souhaitez inclure dans le rapport.
11. En fonction de la périodicité sélectionnée, cliquez sur **Générer** pour créer un rapport instantané ou sur **Enregistrer** pour créer un rapport planifié.
- Le rapport instantané s'affichera immédiatement après avoir cliqué sur **Générer**. Le temps nécessaire à la création des rapports peut varier en fonction du nombre d'objets du réseau administrés. Veuillez patienter le temps que le rapport demandé soit créé.
 - Le rapport planifié apparaîtra dans la liste sur la page **Rapports**. Une fois une instance de rapport générée, vous pouvez la consulter en cliquant sur le lien correspondant dans la colonne **Afficher le rapport** sur la page **Rapports**.

9.3. Afficher et gérer des rapports planifiés

Pour afficher et gérer les rapports planifiés, allez sur la page **Rapports**.

Nom du rapport	Type	Périodicité	Afficher le rapport
<input type="checkbox"/> Rapport sur l'état des malwares	État des malwares	Tous les jours	23 Jul 2015 - 00:00

La page Rapports

Tous les rapports planifiés apparaissent dans le tableau avec des informations utiles les concernant :


- Le nom et le type de rapport
- Récurrence des rapports
- La dernière instance générée.


Note

Les rapports planifiés sont disponibles uniquement pour l'utilisateur les ayant créés.

Pour trier les rapports en fonction d'une colonne, cliquez simplement sur l'en-tête de cette colonne. Cliquez de nouveau sur l'en-tête de colonne pour modifier l'ordre de tri.

Pour trouver facilement ce que vous recherchez, utilisez les zones de recherche ou les options de filtrage sous les en-têtes de colonne.

Pour effacer une zone de recherche, placez le curseur dessus et cliquez sur l'icône  **Supprimer**.

Pour afficher les informations les plus récentes, cliquez sur le bouton  **Actualiser** en haut du tableau.

9.3.1. Afficher les rapports

Pour afficher un rapport :

1. Allez sur la page **Rapports**.

2. Classez les rapports par nom, type ou périodicité pour trouver facilement le rapport que vous recherchez.
3. Cliquez sur le lien correspondant dans la colonne **Afficher le rapport** pour afficher le rapport. L'instance du rapport la plus récente s'affichera.

Pour afficher toutes les instances d'un rapport, consultez « [Enregistrer des rapports](#) » (p. 455)

Tous les rapports comportent une section Résumé (la partie supérieure de la page du rapport) et une section Détails (la partie inférieure de la page du rapport).

- La section résumé vous fournit des données statistiques (graphiques) sur tous les objets du réseau cibles ainsi que des informations générales sur le rapport telles que la période couverte par le rapport (le cas échéant), la cible du rapport, etc.
- La section détails vous fournit des informations sur chaque élément du réseau cible.

Note

- Pour configurer les informations affichées par le graphique, cliquez sur les entrées de la légende pour faire apparaître ou masquer les données sélectionnées.
- Cliquez sur la zone du graphique qui vous intéresse (partie du graphique circulaire, barre) pour faire apparaître les informations correspondantes dans le tableau.

9.3.2. Modifier les rapports planifiés

Note

Lorsqu'un rapport planifié est modifié, toutes les mises à jour sont appliquées à partir de la prochaine génération du rapport. Les rapports générés auparavant ne seront pas affectés par la modification.

Pour modifier les paramètres d'un rapport planifié :

1. Allez sur la page **Rapports**.
2. Cliquez sur le nom du rapport.
3. Modifiez les paramètres du rapport selon vos besoins. Vous pouvez modifier les options suivantes :
 - **Nom du rapport** Choisissez un nom de rapport explicite afin de l'identifier facilement. Lorsque vous choisissez un nom, prenez en compte le type et


la cible du rapport, et, éventuellement, les options du rapport. Les rapports générés par un rapport planifié portent son nom.

- **Récurrence des rapports (planifier).** Vous pouvez planifier les rapports afin qu'ils soient automatiquement générés toutes les heures (par intervalle), tous les jours (à un horaire précis), toutes les semaines (à un jour et un horaire défini) ou tous les mois (un jour et un horaire précis du mois). En fonction de la planification sélectionnée, le rapport contiendra uniquement des données de la veille, de la semaine ou du mois précédent.
 - **Réglages**
 - Vous pouvez planifier les rapports afin qu'ils soient automatiquement générés toutes les heures (par intervalle), tous les jours (à un horaire précis), toutes les semaines (à un jour et un horaire défini) ou tous les mois (un jour et un horaire précis du mois). En fonction de la planification sélectionnée, le rapport contiendra uniquement des données de la veille, de la semaine ou du mois précédent.
 - Le rapport comprendra uniquement des données sur l'intervalle de temps sélectionné. Vous pouvez modifier l'intervalle dès la nouvelle génération du rapport.
 - La plupart des rapports fournissent des options de filtrage pour vous aider à trouver facilement les informations qui vous intéressent. Lorsque vous affichez le rapport dans la console, toutes les informations seront disponibles, quelles que soient les options sélectionnées. Si vous téléchargez ou envoyez le rapport par e-mail, seul le résumé du rapport et les informations sélectionnées figureront dans le fichier PDF. Les données du rapport seront uniquement disponibles au format CSV.
 - Vous pouvez également choisir de recevoir le rapport par e-mail.
 - **Sélectionner la Cible.** L'option sélectionnée indique le type de cible du rapport actuel (les groupes ou les éléments individuels du réseau). Cliquez sur le lien correspondant pour afficher la cible du rapport actuel. Pour la changer, sélectionnez les groupes ou les éléments du réseau à inclure dans le rapport.
4. Cliquez sur **Enregistrer** pour appliquer les modifications.

9.3.3. Supprimer les rapports planifiés

Lorsqu'un rapport planifié n'est plus nécessaire, il vaut mieux le supprimer. Supprimer un rapport planifié effacera toutes les instances qu'il a générées automatiquement jusqu'à présent.

Pour supprimer un rapport planifié :

1. Allez sur la page **Rapports**.
2. Sélectionnez le rapport que vous souhaitez supprimer.
3. Cliquez sur le bouton  **Supprimer** en haut du tableau.

9.4. Prendre des actions basées sur un rapport

Alors que la plupart des rapports mettent uniquement en évidence les problèmes de votre réseau, certains d'entre eux vous proposent plusieurs options pour corriger les problèmes détectés d'un simple clic sur un bouton.

Pour corriger les problèmes affichés dans le rapport, cliquez sur le bouton approprié dans la barre d'outils d'actions située au-dessus du tableau de données.

Note

Vous avez besoin des droits **Gérer les réseaux** pour effectuer ces actions.

Voici les options disponibles pour chaque rapport :

Applications bloquées

- **Ajouter une Exception.** Ajoute une exclusion à la politique pour empêcher les modules de protection de bloquer de nouveau l'application.
- **Ajouter une règle.** Définit une règle pour une application ou un processus du Contrôle des applications.

Activité HVI

- **Ajouter une Exception.** Ajoute une exclusion à la politique pour empêcher les modules de protection de faire de nouveau état de l'incident.

État des malwares

- **Analyser les cibles infectées.** Exécute une tâche d'Analyse Complète préconfigurée sur les cibles apparaissant encore comme étant infectées.

État de la mise à jour

- **Mise à jour.** Met à jour les clients cibles vers les dernières versions disponibles.

État de la mise à niveau

- **Mettre à niveau.** Remplace les anciens clients d'endpoints par la dernière génération de produits disponibles.

9.5. Enregistrer des rapports

Par défaut, les rapports planifiés sont automatiquement enregistrés dans le Control Center.

Si vous avez besoin que des rapports soient disponibles plus longtemps, vous pouvez les enregistrer sur votre ordinateur. Le résumé du rapport sera disponible au format PDF, alors que les données du rapport seront uniquement disponibles au format CSV.

Il y a deux façons d'enregistrer les rapports :

- [Exporter](#)
- [Télécharger](#)

9.5.1. Exportation de rapports

Pour exporter le rapport sur votre ordinateur :


1. Choisissez un format et cliquez sur **Exporter en CSV** ou **Exporter en PDF**.
2. En fonction des paramètres de votre navigateur, le fichier peut être téléchargé automatiquement sur un emplacement par défaut, ou une fenêtre de téléchargement apparaîtra et vous devrez spécifier le dossier de destination.

9.5.2. Télécharger des Rapports

L'archive d'un rapport contient à la fois le résumé et les détails du rapport.

Pour télécharger l'archive d'un rapport :

1. Allez sur la page **Rapports**.
2. Sélectionnez le rapport que vous souhaitez enregistrer.

3. Cliquez sur le bouton  **Télécharger** et sélectionnez **Dernière instance** pour télécharger la dernière instance du rapport générée ou **Archive complète** pour télécharger une archive contenant toutes les instances.

En fonction des paramètres de votre navigateur, le fichier peut être téléchargé automatiquement sur un emplacement par défaut, ou une fenêtre de téléchargement apparaîtra et vous devrez spécifier le dossier de destination.

9.6. Envoyer des rapports par e-mail

Vous pouvez envoyer des rapports par e-mail à l'aide des options suivantes :

1. Pour envoyer par e-mail le rapport que vous êtes en train de consulter, cliquez sur le bouton **E-mail**. Le rapport sera envoyé à l'adresse e-mail associée à votre compte.
2. Pour configurer l'envoi des rapports planifiés souhaités par e-mail :
 - a. Allez sur la page **Rapports**.
 - b. Cliquez sur le nom du rapport souhaité.
 - c. Sous **Paramètres > Livraison**, sélectionnez **Envoyer par e-mail à**.
 - d. Indiquez l'adresse e-mail souhaitée dans le champ ci-dessous. Vous pouvez ajouter autant d'adresses e-mail que vous le souhaitez.
 - e. Cliquez sur **Enregistrer**.



Note

Seuls le résumé et le graphique du rapport seront inclus dans le fichier PDF envoyé par e-mail. Les détails du rapport seront disponibles dans le fichier CSV.

Les rapports sont envoyés par e-mail en archives .zip.

9.7. Impression des rapports

Le Control Center ne prend pas en charge actuellement la fonctionnalité du bouton imprimer. Pour imprimer un rapport, vous devez d'abord l'enregistrer sur votre ordinateur.

9.8. Créateur de rapports

Dans Control Center, vous pouvez créer et gérer des requêtes pour obtenir des rapports détaillés qui vous permettent de comprendre tout événement ou changement survenu dans votre réseau, à tout moment.

Les requêtes vous offrent la possibilité d'enquêter sur un problème de sécurité en utilisant différents critères, tout en gardant les informations concises et bien ordonnées. Avec les filtres, vous pouvez regrouper les paramètres selon certains critères et sélectionner les données pertinentes pour vous.

A partir d'un rapport basé sur les requêtes vous pouvez trouver des détails tels que l'heure à laquelle l'incident a eu lieu, le nombre d'endpoints touchés, quels utilisateurs étaient connectés au moment de l'incident, quelles politiques ont été appliquées, le statut d'agent de sécurité, les mesures prises, sur un seul endpoint ou sur un groupe d'endpoints.

Tous les rapports basés sur des requêtes sont disponibles dans Control Center, mais vous pouvez les enregistrer sur votre ordinateur ou les envoyer par e-mail. Les formats PDF (Portable Document Format) et CSV (comma-separated values) sont disponibles.

Avec les demandes, vous pouvez profiter des multiples avantages par rapport aux rapports GravityZone standards :

- Des données très volumineuses pour créer des rapports convaincants.
- Rapports flexibles car les événements ne sont pas agrégés.
- Haut niveau de personnalisation. Même si les rapports standards GravityZone vous offrent la possibilité d'opter entre plusieurs options prédéfinies, avec les requêtes il n'y a pas de limite dans le choix de vos filtres de données.
- La corrélation des événements, avec n'importe quelle information accompagnée des données de l'état agent et appareil.
- Effort de développement minimum, puisque vous pouvez créer, enregistrer et réutiliser tout type de rapport.
- Des rapports complets qui, contrairement à des rapports standards, ont des résumés et des détails intégrés dans le même document PDF.
- Les requêtes peuvent récupérer des informations sur les deux dernières années.

Pour utiliser les requêtes, vous devez installer le rôle Créateur de rapports avec votre appliance virtuelle GravityZone. Pour plus de détails concernant l'installation du Créateur de rapports, veuillez vous référer au Guide d'installation GravityZone.

9.8.1. Types de requête

GravityZone inclut les types de requête suivants :

- [État de l'endpoint](#)
- [Événements endpoint](#)
- [Événements Exchange](#)

État de l'endpoint

Cette requête fournit des informations sur l'état de la sécurité des endpoints ciblés sélectionnés, pour une date spécifique. De cette façon, vous savez si l'agent de sécurité et les contenus de sécurité sont mis à jour ou non, ou désactivés. En outre, vous pouvez voir si les endpoints sont infectés ou propres, quelle infrastructure est utilisée et quels modules sont allumés/éteints ou non installés.

Cette requête comprend des détails relatifs aux endpoints ciblés, tels que :

- Type de machine (physique, virtuelle or Security Server)
- Infrastructure du réseau à laquelle l'endpoint appartient (Active Directory, Nutanix Prism, VMWare ou Citrix Xen)
- Données agent de sécurité (type, état, configuration du moteur d'analyse, état sécurité)
- État des modules de protection
- Rôles endpoint (Relais, Protection Exchange)

Événements endpoint

Cette requête vous permet d'afficher des détails sur les événements de sécurité qui se sont produits sur les endpoints ciblés, pour une date ou une période spécifique. Cela inclut des informations liées à :

- La machine cible sur laquelle l'événement a eu lieu (nom, type, IP, OS, infrastructure du réseau)
- Type, état et configuration de l'agent de sécurité installé
- État des modules de protection et des rôles installés sur l'agent de sécurité

- Nom de politique et assignation
- Utilisateur connecté pendant l'événement
- Événements, qui peut se référer à des sites bloqués, des applications bloquées, des détections de malwares ou à l'activité de l'appareil

Événements Exchange

Il vous aide à trouver les incidents se produisant sur les serveurs Microsoft Exchange sélectionnés, à une date précise ou pour une certaine période de temps. Il prend en considération des données sur :

- La direction du trafic de messagerie
- Les événements de sécurité (tels que la détection de malwares ou de pièces jointes)
- Les mesures prises pour chaque situation (désinfecter, supprimer, remplacer ou placer un fichier en quarantaine, supprimer ou rejeter un e-mail)

9.8.2. Gestion des requêtes

Vous pouvez créer et gérer des requêtes et des rapports basés sur les requêtes sur la page **Rapports > Requêtes**.

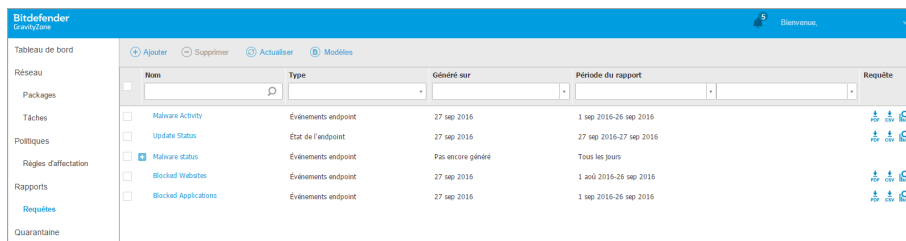


Tableau de bord	Ajouter	Supprimer	Actualiser	Modèles		
Réseau	Nom	Type	Généré sur	Période du rapport	Requête	
⊞ Packages	<input type="checkbox"/> Malware Activity	Événements endpoint	27 sep 2016	1 sep 2016-26 sep 2016		⚙️ ⏏️ 🔍
Tâches	<input type="checkbox"/> Update Status	État de l'endpoint	27 sep 2016	27 sep 2016-27 sep 2016		⚙️ ⏏️ 🔍
Politiques	<input checked="" type="checkbox"/> Malware status	Événements endpoint	Pas encore généré	Tous les jours		⚙️ ⏏️ 🔍
Règles d'affectation	<input type="checkbox"/> Blocked Websites	Événements endpoint	27 sep 2016	1 août 2016-26 sep 2016		⚙️ ⏏️ 🔍
Rapports	<input type="checkbox"/> Blocked Applications	Événements endpoint	27 sep 2016	1 sep 2016-26 sep 2016		⚙️ ⏏️ 🔍
Requêtes						
Quarantaine						

La page Requêtes

Les requêtes sont des interrogations de base de données complexes, utilisant un grand nombre de filtres, ce qui peut prendre plusieurs minutes à configurer et à créer. Devoir remplir un formulaire de requête à chaque fois que vous voulez un nouveau rapport, semblable à des rapports existants, peut devenir frustrant. GravityZone vous aide à créer facilement des requêtes grâce à des modèles, qui sont remplies automatiquement dans le formulaire de requête, vous laissant moins de personnalisation à gérer.

Utilisation des templates

Vous pouvez ajouter, cloner et rechercher rapidement des modèles spécifiques dans la fenêtre du **Gestionnaire de modèles**.

Gestionnaire de modèles

+ Ajouter Cloner

Rechercher

Presets

- Malware Activity
- Update Status
- Malware status
- Blocked Websites
- Blocked Applications

Custom Templates

Détails

Nom du modèle : * Malware Activity

Type de requête:

- État de l'endpoint
- Événements endpoint
- Événements Exchange

Envoyer par e-mail à

Récurrent

Faire requête sur:

- Date spécifique
- Période

À :

Chart Settings

Type: None

Utiliser des données de : * Type d'événement

Supprimer le modèle Enregistrer

Pour afficher les modèles de requête disponibles :

1. Allez sur la page **Rapports > Requêtes**.
2. Cliquez sur le bouton **Modèles** en haut du tableau. La fenêtre **Gestionnaire de modèles** va s'afficher. Tous les modèles sont affichés dans le volet de gauche, tandis que dans le volet de droite, vous pouvez afficher les paramètres du modèle sélectionné.

Pour trouver rapidement un modèle, entrez le nom dans le champ **Recherche**, sur le côté supérieur du volet de gauche. Vous pouvez voir les résultats de la recherche pendant que vous tapez. Pour effacer le champ **Rechercher** cliquez sur l'icône **X Supprimer** à sa droite.

Voici les deux catégories de modèles disponibles :

- **Préconfigurés.** Ce sont des modèles prédéfinis présents par défaut dans GravityZone.
- **Modèles personnalisés.** Ce sont les modèles que vous créez selon vos besoins.

Préconfigurations

GravityZone contient cinq préconfigurations :

- **Activité des Malwares,** vous fournit des informations globales sur les malwares détectés pendant une certaine période sur les endpoints sélectionnés.

Le rapport contient le nom de la cible de la machine, l'IP, l'état de l'infection (infecté ou propre), le nom du malware, les mesures prises contre la menace (ignorée, présente, supprimée, bloquée, mise en quarantaine, nettoyée ou restaurée), le type de fichier, le chemin d'accès du fichier et l'utilisateur connecté en ce moment.

- **État de mise à jour,** montre l'état de mise à jour de l'agent de sécurité installé sur les cibles sélectionnées. Le rapport contient le nom de la cible de la machine, l'IP, l'état de mise à jour du produit (mis à jour, obsolète, désactivé), l'état de mise à jour de la signature (mise à jour, obsolète, désactivée), le type d'agent de sécurité, la version du produit et la version de la signature.

- **État du malware** vous aide à découvrir combien et quels endpoints sélectionnés ont été affectés par des malwares pendant une période spécifique et comment les menaces ont été gérées.

Le rapport contient le nom de la cible de la machine, l'IP, l'état de l'infection (infecté ou propre), le nom des malwares, l'action de la menace (ignoré, présent, supprimé, bloqué, mis en quarantaine, nettoyé ou restauré) .

- **Sites web bloqués,** vous informant de l'activité du module de contrôle web de l'agent de sécurité.

Le rapport contient le nom de la machine cible, l'IP, le type de menace (phishing, fraude ou non fiable), le nom de la règle, la catégorie de site Web et l'URL bloquée.

- **Applications bloquées** vous aide à voir quelles applications ont été bloquées sur une certaine période de temps.

Le rapport fournit des informations sur le nom de la machine cible, l'IP, le nom de l'application bloquée, son chemin d'accès et comment la menace a été contenue : avec ATC, IDS ou Contrôle application.

Modèles personnalisés

Si vous avez besoin d'un autre modèle que les presets fournis par GravityZone, vous pouvez créer des modèles de requêtes personnalisés. Vous pouvez sauvegarder autant de modèles que vous le souhaitez.

Pour créer un modèle personnalisé :

1. Allez sur la page **Rapports > Requêtes**.
2. Cliquez sur le bouton **Modèles** en haut du tableau. La fenêtre de configuration **Gestionnaire de modèles** va s'afficher.
3. Cliquez sur le bouton **Ajouter** dans l'angle supérieur gauche de la fenêtre. Un formulaire de requête sera affiché dans le volet latéral droit.
4. Remplissez le formulaire de requête avec les informations requises. Pour plus de détails pour remplir un formulaire de requête, reportez-vous à « [Création de requêtes](#) » (p. 463).
5. Cliquez sur **Enregistrer**. Le modèle nouvellement créé sera affiché dans le volet de gauche, sous **Modèles personnalisés**.

Alternativement, vous pouvez créer un modèle personnalisé en utilisant une pré-configuration.

1. Allez sur la page **Rapports > Requêtes**.
2. Cliquez sur le bouton **Modèles** en haut du tableau. La fenêtre de configuration **Gestionnaire de modèles** va s'afficher.
3. Sélectionnez une pré-configuration dans le panneau de gauche. Les réglages correspondants seront affichés dans le panneau latéral de droite.
4. Cliquez sur **Clone** dans le coin supérieur gauche pour créer une copie de la pré-configuration.
5. Modifier tous les paramètres que vous souhaitez dans le formulaire de requête. Pour plus de détails pour remplir un formulaire de requête, reportez-vous à « [Création de requêtes](#) » (p. 463).
6. Cliquez sur **Enregistrer**. Le modèle nouvellement créé sera affiché dans le volet de gauche, sous **Modèles personnalisés**.

En outre, lors de la création d'une nouvelle requête, vous pouvez l'enregistrer comme modèle. Pour plus d'informations, reportez-vous à « [Création de requêtes](#) » (p. 463).

Pour supprimer un modèle personnalisé :

1. Allez sur la page **Rapports > Requêtes**.

2. Cliquez sur le bouton **Modèles** en haut du tableau. La fenêtre de configuration **Gestionnaire de modèles** va s'afficher.
3. Dans la rubrique **Modèles personnalisés**, cliquez sur le modèle que vous souhaitez supprimer. Les réglages de modèle seront affichés dans le panneau latéral de droite.
4. Cliquez sur **Supprimer modèle** en bas de la fenêtre puis confirmez votre action en cliquant sur **Oui**.

Création de requêtes

Pour créer une nouvelle requête :

1. Allez sur la page **Rapports > Requêtes**.
2. Cliquez sur le bouton **Ajouter** en haut du tableau. Une fenêtre de configuration s'affiche.
3. Cochez la case **Utiliser modèle** si vous souhaitez utiliser un modèle par défaut ou déjà créé.
4. Dans la rubrique **Détails**, saisissez un nom clair pour la demande. Lorsque vous choisissez un nom, pensez au type de la requête, aux cibles et aux autres paramètres.
5. Sélectionnez le type de requête. Pour plus d'informations, reportez-vous à [« Types de requête » \(p. 458\)](#)
6. Cochez la case **Envoyer par e-mail à** pour envoyer les résultats de requête à certains destinataires. Dans le champ correspondant, ajoutez autant d'adresses e-mail que vous le souhaitez.
7. Dans la rubrique **Récurrence**, sélectionnez :
 - a. **Date spécifique** pour un jour en particulier.
 - b. **Période** pour un intervalle de temps étendu.
 - c. Cochez la case **Récurrente** si vous souhaitez que la requête soit générée à des intervalles spécifiques que vous pouvez configurer dans la zone **Période de rapports**.
8. Configurez les paramètres du graphique.
 - a. Dans le menu **Type**, sélectionnez le graphique avec lequel vous souhaitez illustrer la requête, ou choisissez de l'omettre avec **Aucun**. Selon le type de

requête et la période du rapport, vous pouvez utiliser un diagramme circulaire, un histogramme, ou un graphique avec des lignes.

- b. Dans le champ **Prendre valeurs à partir de** sélectionnez les catégories de données que vous souhaitez utiliser pour votre requête. Chaque type de requête fournit des informations spécifiques liées aux endpoints, agents de sécurité et événements de sécurité. Pour des informations concernant les types de données, reportez-vous à « [Types de requête](#) » (p. 458).
9. Dans la rubrique **Paramètres tableau** sélectionnez les colonnes que vous souhaitez voir dans le rapport. Les données que vous pouvez sélectionner dépendent du type de requête, et peuvent se référer au type d'endpoint et à l'OS, au statut d'agent de sécurité et des événements, aux modules, aux politiques et aux événements de sécurité. Toutes les colonnes sélectionnées sont affichées dans le tableau **Colonnes**. Utiliser glisser-et-déposer pour en changer l'ordre.



Note

Veillez garder à l'esprit l'espace disponible lors de la création de la disposition du tableau. Utilisez un maximum de 10 colonnes pour une bonne visualisation du tableau au format PDF.

10. Dans la rubrique **Filtres**, sélectionnez les données que vous souhaitez présentes dans le rapport en utilisant les critères de filtrage :
 - a. Dans le menu **Type de filtre**, choisissez un filtre puis cliquez sur **+ Ajouter filtre**.
 - b. Dans le tableau ci-dessous, cliquez sur **Valeur** pour spécifier une ou plusieurs options de filtres.

Par exemple, le filtre **OS hôte** nécessite de spécifier le nom de l'OS, comme Windows ou Linux, tandis que le filtre **Module contrôle de l'appareil** permet de sélectionner dans une liste déroulante les endpoints où le module est désactivé.
 - c. Cliquez sur le bouton **- Supprimer** pour éliminer un filtre.
11. **Sélectionner les cibles**. Dérouler vers le bas afin de configurer les cibles du rapport. Sélectionnez un ou plusieurs groupes d'endpoints que vous souhaitez inclure dans le rapport. Avec le sélecteur d'affichage, assurez-vous d'avoir bien vérifié les cibles correctes dans tous les affichages réseaux.

12. Cochez la case **Enregistrer comme modèle** pour utiliser ces paramètres dans d'autres requêtes. Dans ce cas, saisissez un nom clair pour le modèle.
13. Cliquez sur **Générer** pour créer la requête. Une fois que la requête est enregistrée, vous recevrez un message dans la zone des **Notifications**.

Suppression des requêtes

Pour supprimer une requête :

1. Allez sur la page **Rapports > Requêtes**.
2. Sélectionnez le rapport que vous souhaitez supprimer.
3. Cliquez sur le bouton  **Supprimer** en haut du tableau.

Note

Supprimer une requête va également supprimer tous les rapports générés.

9.8.3. Afficher et gérer des rapports


Tous les rapports basés sur des requêtes s'affichent sur la page **Rapports > Requêtes**.

Note

Les rapports sont disponibles uniquement pour l'utilisateur les ayant créés.

Afficher les rapports

Pour voir un rapport basé sur une requête :


1. Allez sur la page **Rapports > Requêtes**.
2. Trier les rapports par nom, type, date de génération ou période de déclaration pour trouver facilement ce que vous recherchez. Par défaut, les rapports sont rangés par date de dernière instance générée.
3. Cliquez sur n'importe quel nom pour voir les informations de la requête dans une nouvelle fenêtre. Les détails ne peuvent pas être modifiés.
4. Cliquez sur le bouton plus devant le nom de la requête pour développer la liste d'instances d'un rapport et sur le bouton moins pour la fermer.
5. Cliquez sur l'icône  **Voir rapport** pour afficher la plus récente instance d'un rapport. Les instances plus anciennes ne sont disponibles que dans les formats PDF et CSV.

Tous les rapports comportent une section résumé dans la partie supérieure de la page du rapport et une section détails dans la partie inférieure de la page du rapport.

La rubrique sommaire vous fournit des données statistiques (diagrammes circulaires, diagrammes à barres ou des graphiques linéaires) pour tous les endpoints cibles, des informations générales sur la requête, comme la récurrence, la période du rapport, le type de requête et les filtres utilisés.

Pour configurer les informations affichées par le graphique, cliquez sur les entrées de la légende pour faire apparaître ou masquer les données sélectionnées. Cliquez également sur la zone qui vous intéresse dans le graphique pour afficher les données liées dans le tableau.

La section détails vous fournit des informations sur chaque endpoint cible. Pour trouver rapidement les données que vous cherchez, cliquez sur les zones de recherche ou les options de filtrage sous les en-têtes de colonne.

Cliquez sur le bouton  **Colonnes** pour personnaliser chaque colonne du tableau.


Enregistrer des rapports

Par défaut, tous les rapports sont automatiquement enregistrés dans le Control Center. Vous pouvez également les exporter vers votre ordinateur, à la fois en format PDF et CSV.

Vous pouvez sauvegarder les rapports sur votre ordinateur :

- A partir de la page rapports.
- A partir du tableau **Demandes**.

Pour sauvegarder un rapport pendant que vous êtes sur sa page :

1. Cliquez sur le bouton  **Exporter** dans le coin en bas à gauche.
2. Sélectionnez le format désiré du rapport :
 - a. Portable Document Format (PDF) ou
 - b. Valeurs séparées par des virgules (CSV)
3. En fonction des paramètres de votre navigateur, le fichier peut être téléchargé automatiquement sur un emplacement par défaut, ou une fenêtre de téléchargement apparaîtra et vous devrez spécifier le dossier de destination.

Pour exporter un rapport alors que vous êtes sur la page **Rapport > Requêtes** :


1. Allez sur la page **Rapports > Requêtes**.
2. Cliquez sur les boutons  **PDF** ou  **CSV** correspondant à chaque rapport.

3. En fonction des paramètres de votre navigateur, le fichier peut être téléchargé automatiquement sur un emplacement par défaut, ou une fenêtre de téléchargement apparaîtra et vous devrez spécifier le dossier de destination.

Tous les rapports exportés au format PDF ont le résumé et les détails dans le même document, sur des pages en portrait A4 ou Paysage. Les détails sont limités à 100 lignes par document PDF.

Envoyer des rapports par e-mail

Vous avez deux options pour envoyer des rapports par e-mail :

1. Dans la page du rapport que vous consultez, cliquez sur le bouton  **Email** dans l'angle inférieur gauche de la page. Le rapport sera envoyé à l'adresse e-mail associée à votre compte.
2. Lors de la création d'une nouvelle requête, cochez la case **Envoyer par e-mail** à et saisissez les adresses e-mail que vous souhaitez dans le champ correspondant.

Impression des rapports

Le Control Center ne prend pas en charge actuellement la fonctionnalité du bouton imprimer. Pour imprimer un rapport basé sur une requête, vous devez d'abord l'enregistrer sur votre ordinateur.

10. MISE EN QUARANTAINE

La quarantaine est un dossier chiffré qui contient des fichiers potentiellement malveillants tels que des fichiers suspectés d'être des malwares, d'être infectés par des malwares ou d'autres fichiers indésirables. Quand un virus ou une autre forme de malware est en quarantaine, il ne peut faire aucun dégât car il ne peut ni être exécuté, ni être lu.

GravityZone place les fichiers en quarantaine en fonction des politiques affectées aux endpoints. Par défaut, les fichiers qui ne peuvent pas être désinfectés sont placés en quarantaine.

La quarantaine est enregistrée en local sur chaque endpoint, à l'exception de VMware vCenter Server intégré à vShield Endpoint et à NSX, où elle est enregistrée sur le Security Server.



Important

La quarantaine n'est pas disponible pour les appareils mobiles.

10.1. Explorer la Quarantaine

La page **Quarantaine** fournit des informations détaillées sur les fichiers en quarantaine de tous les endpoints que vous gérez.

Ordinateur	IP	Fichier	Nom de la menace	Mis en quarantaine	État de l'action
------------	----	---------	------------------	--------------------	------------------

La page Quarantaine

La page Quarantaine comprend deux affichages :

- **Ordinateurs et Machines virtuelles**, pour les fichiers détectés directement dans le système de fichiers des endpoints.


- **Serveurs Exchange**, pour les e-mails et les fichiers joints à des e-mails, détectés sur les serveurs de messagerie Exchange.

Le sélecteur d'affichage en haut de la page permet de passer d'un affichage à un autre.

Des informations sur les fichiers en quarantaine sont affichées dans un tableau. En fonction du nombre d'endpoints gérés et du niveau d'infection, le tableau Quarantaine peut comporter un grand nombre d'entrées. Le tableau peut comprendre plusieurs pages (par défaut, seules 20 entrées par page sont affichées).

Pour parcourir les pages, utilisez les boutons de navigation en bas du tableau. Pour modifier le nombre d'entrées affichées sur une page, sélectionnez une option dans le menu à côté des boutons de déplacement.

Pour une meilleure visibilité des données qui vous intéressent, vous pouvez utiliser les zones de recherche des en-têtes de colonnes pour filtrer les données affichées. Vous pouvez, par exemple, rechercher une menace spécifique détectée dans le réseau ou un élément spécifique du réseau. Vous pouvez également cliquer sur les en-têtes de colonne pour trier les données en fonction d'une colonne spécifique.

Pour afficher les informations les plus récentes, cliquez sur le bouton  **Actualiser** en haut du tableau. Cela peut être nécessaire lorsque vous passez du temps sur la page.

10.2. Quarantaine Ordinateurs et Machines virtuelles

Par défaut, les fichiers de la quarantaine sont automatiquement envoyés aux laboratoires de Bitdefender afin d'être analysés par les spécialistes en malwares de Bitdefender. Si la présence de malwares est confirmée, une signature est publiée afin de permettre de les supprimer. De plus, les fichiers en quarantaine sont analysés après chaque mise à jour des signatures de malwares. Les fichiers nettoyés sont automatiquement remis à leur emplacement d'origine. Ces fonctionnalités concernent toutes les politiques de sécurité de la page **Politiques** et vous pouvez choisir de les conserver ou de les désactiver. Pour plus d'informations, reportez-vous à « [Mise en quarantaine](#) » (p. 291).

10.2.1. Afficher les informations sur la quarantaine

Le tableau Quarantaine vous fournit les informations suivantes :

- Le nom de l'endpoint sur lequel la menace a été détectée.
- L'IP de l'endpoint sur lequel la menace a été détectée.

- Chemin vers le fichier infecté ou suspect sur l'endpoint où il a été détecté.
- Nom donné à la menace malware par les chercheurs de sécurité de Bitdefender.
- La date et l'heure de la mise en quarantaine du fichier.
- L'état de l'action requise à appliquer au fichier en quarantaine.

10.2.2. Gérer les fichiers en quarantaine

Le comportement de la quarantaine est différent pour chaque environnement :

- **Security for Endpoints** stocke les fichiers en quarantaine sur chaque ordinateur administré. Le Control Center vous permet de supprimer ou de restaurer des fichiers en quarantaine.
- **Security for Virtualized Environments (Multiplateforme)** stocke les fichiers en quarantaine sur chaque machine virtuelle administrée. Le Control Center vous permet de supprimer ou de restaurer des fichiers en quarantaine.
- **Security for Virtualized Environments (intégré à VMware vShield Endpoint ou NSX)** stocke les fichiers en quarantaine sur l'appliance Security Server. Le Control Center vous permet de supprimer des fichiers en quarantaine ou de les télécharger à l'emplacement de votre choix.


Restaurer les fichiers en quarantaine

Vous pouvez parfois avoir besoin de restaurer des fichiers en quarantaine, à leur emplacement d'origine ou à un autre emplacement. Par exemple, vous avez la possibilité de récupérer d'importants fichiers contenus dans une archive infectée placée en quarantaine.

Note

Restaurer les fichiers en quarantaine est possible uniquement dans les environnements protégés par Security for Endpoints et Security for Virtualized Environments (Multiplateforme).

Pour restaurer un ou plusieurs fichiers en quarantaine :

1. Allez sur la page **Quarantaine**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le sélecteur d'affichage situé en haut de la page.
3. Cochez les cases correspondant aux fichiers en quarantaine que vous souhaitez restaurer.
4. Cliquez sur le bouton  **Restaurer** en haut du tableau.

5. Choisissez l'emplacement où vous souhaitez que les fichiers sélectionnés soient restaurés (soit l'emplacement d'origine soit un emplacement personnalisé sur l'ordinateur cible).

Si vous choisissez de restaurer un fichier à un emplacement personnalisé, vous devez indiquer le chemin d'accès absolu dans le champ correspondant.

6. Sélectionnez **Ajouter automatiquement une exclusion dans la politique** pour exclure les fichiers à restaurer des futures analyses. L'exclusion s'applique à toutes les politiques affectant les fichiers sélectionnés, à l'exception de la politique par défaut qui ne peut pas être modifiée.
7. Cliquez sur **Enregistrer** pour demander une restauration du fichier. Vous pouvez remarquer l'état en attente dans la colonne **Action**.
8. L'action requise est envoyée aux endpoints cibles immédiatement ou dès qu'ils sont connectés de nouveau.

Vous pouvez afficher des informations relatives à l'état de l'action sur la page **Tâches**. Une fois un fichier restauré, l'entrée correspondante disparaîtra du tableau Quarantaine.

Télécharger les fichiers en quarantaine

Dans les environnements virtualisés VMware intégrés à vShield Endpoint ou NSX, la quarantaine est enregistrée sur le Security Server. Si vous souhaitez examiner ou récupérer des données de fichiers en quarantaine, vous devez les télécharger à partir de Security Server à l'aide de Control Center. Les fichiers en quarantaine sont téléchargés en tant qu'archive ZIP protégée par mot de passe, chiffrée, pour empêcher l'infection accidentelle de malwares.

Pour ouvrir l'archive et extraire son contenu, vous devez utiliser l'outil de quarantaine, une application Bitdefender autonome qui ne requiert pas d'installation.

L'outil de quarantaine est disponible pour les systèmes d'exploitation suivants :

- Windows 7 ou supérieur
- La plupart des distributions Linux 32 bits avec une interface graphique utilisateur (GUI).

Note

Veuillez noter que l'outil de quarantaine n'a pas d'interface en ligne de commande.

Avertissement


Soyez prudents lorsque vous extrayez les fichiers en quarantaine car ils peuvent infecter votre système. Nous vous recommandons d'extraire et d'analyser les fichiers

en quarantaine sur un système de test ou isolé, fonctionnant de préférence sous Linux. Les infections de malwares sont plus faciles à contenir sous Linux.

Pour télécharger les fichiers en quarantaine sur votre ordinateur :

1. Allez sur la page **Quarantaine**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le sélecteur d'affichage situé en haut de la page.
3. Filtrez les données du tableau en indiquant le nom d'hôte ou l'adresse IP de Security Server dans le champ correspondant de l'en-tête du tableau.

Si la quarantaine est volumineuse, pour afficher les fichiers qui vous intéressent, vous pouvez avoir besoin d'appliquer des filtres supplémentaires ou d'augmenter le nombre de fichiers affichés par page.

4. Cochez les cases correspondant aux fichiers que vous souhaitez télécharger.
5. Cliquez sur le bouton  **Télécharger** en haut du tableau. En fonction des paramètres de votre navigateur, l'on vous demandera d'enregistrer les fichiers sur un dossier de votre choix, ou les fichiers seront téléchargés à l'emplacement de téléchargement par défaut.

Pour accéder aux fichiers restaurés :

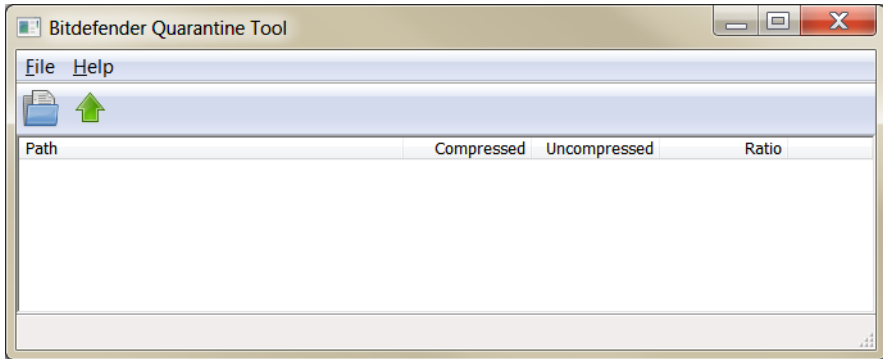
1. Téléchargez l'outil de quarantaine adapté à votre système d'exploitation à partir de la page **Aide & Support** ou à partir des adresses suivantes :
 - [Outil de quarantaine pour Windows](#)
 - [Outil de quarantaine pour Linux](#)



Note

L'outil de quarantaine pour Linux est archivé dans un fichier `tar`.


2. Exécutez le fichier exécutable de l'outil de quarantaine.



Outil de quarantaine

3. Dans le menu **Fichier**, cliquez sur **Ouvrir** (CTRL+O) ou cliquez sur le bouton  **Ouvrir** pour charger l'archive dans l'outil.

Les fichiers sont organisés en fonction de la machine virtuelle sur laquelle ils ont été détectés et de façon à préserver leur chemin d'origine.

4. Avant d'extraire les fichiers archivés, si l'analyse antimalware à l'accès est activée sur le système, veillez à la désactiver ou à configurer une exclusion d'analyse pour l'emplacement où vous extrairez les fichiers. Sinon, votre programme antimalware détectera et appliquera une action aux fichiers extraits.
5. Sélectionnez les fichiers que vous souhaitez extraire.
6. Dans le menu **Fichier**, cliquez sur **Extraire** (CTRL+E) ou cliquez sur le bouton  **Extraire**.
7. Sélectionnez le dossier de destination. Les fichiers sont extraits à l'emplacement sélectionné, tout en préservant la structure de dossiers d'origine.

Suppression automatique des fichiers en quarantaine

Par défaut, les fichiers placés en quarantaine depuis plus de 30 jours sont automatiquement supprimés. Ce paramètre peut être modifié en éditant la politique affectée aux endpoints administrés.

Pour modifier l'intervalle de suppression automatique des fichiers en quarantaine :

1. Allez sur la page **Politiques**.
2. Trouvez la politique affectée aux endpoints sur lesquels vous souhaitez modifier le paramètre et cliquez sur son nom.


3. Rendez-vous sur la page **Antimalware > Configuration**.
4. Dans la section **Quarantaine**, sélectionnez le nombre de jours après lequel les fichiers sont supprimés.
5. Cliquez sur **Enregistrer** pour appliquer les modifications.

Suppression manuelle des fichiers en quarantaine

Si vous souhaitez supprimer des fichiers de la quarantaine manuellement, nous vous recommandons de vérifier que les fichiers que vous souhaitez supprimer ne sont pas nécessaires.

Un fichier peut être un malware en lui-même. Si vos recherches aboutissent à cette situation, vous pouvez rechercher cette menace dans la quarantaine et la supprimer.

Pour supprimer un ou plusieurs fichiers en quarantaine :

1. Allez sur la page **Quarantaine**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le sélecteur d'affichage situé en haut de la page.
3. Cochez les cases correspondant aux fichiers en quarantaine que vous souhaitez supprimer.
4. Cliquez sur le bouton  **Supprimer** en haut du tableau. Vous devrez confirmer votre action en cliquant sur **Oui**.

Vous pouvez remarquer l'état en attente dans la colonne **Action**.

L'action requise est envoyée immédiatement aux éléments du réseau cibles ou dès qu'ils sont connectés de nouveau. Une fois un fichier supprimé, l'entrée correspondante disparaîtra du tableau Quarantaine.

Vider la Quarantaine

Pour supprimer tous les objets en quarantaine :

1. Allez sur la page **Quarantaine**.
2. Sélectionnez **Ordinateur / Machine virtuelle** dans le sélecteur d'affichage.
3. Cliquez sur le bouton **Vider la quarantaine**.

Vous devrez confirmer votre action en cliquant sur **Oui**.

Toutes les entrées du tableau de Quarantaine ont été effacées. L'action requise est envoyée immédiatement aux éléments du réseau cibles ou dès qu'ils sont connectés de nouveau.

10.3. Quarantaine Serveurs Exchange

La quarantaine Exchange contient des e-mails et pièces jointes. Le module Antimalware met en quarantaine les pièces jointes d'e-mails alors que l'Antispam et le Filtrage du Contenu et des pièces jointes mettent en quarantaine les e-mails entiers.



Note

Veillez noter que 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.

10.3.1. Afficher les informations sur la quarantaine

La page **Quarantaine** propose des informations détaillées sur les objets en quarantaine de tous les Serveurs Exchange de votre entreprise. Ces informations sont disponibles dans le tableau Quarantaine et dans la fenêtre des détails de chaque objet.

Le tableau Quarantaine vous fournit les informations suivantes :

- **Sujet.** Le sujet de l'e-mail en quarantaine.
- **Expéditeur.** L'adresse e-mail de l'expéditeur telle qu'elle apparaît dans le champ de l'en-tête de l'e-mail **De**.
- **Destinataires.** La liste de destinataires tels qu'ils apparaissent dans les champs des en-têtes d'e-mail **À** et **Cc**.
- **Destinataires réels.** La liste des adresses e-mail des utilisateurs individuels auxquels les e-mails devaient être délivrés avant d'être placés en quarantaine.
- **État.** État de l'objet après analyse. L'état montre si un e-mail est marqué comme spam ou contient du contenu indésirable ou si une pièce jointe est infectée par un malware, suspectée d'être infectée, indésirable ou non analysable.
- **Nom du code malveillant.** Nom donné à la menace malware par les chercheurs de sécurité de Bitdefender.
- **Nom du serveur.** Le nom d'hôte du serveur sur lequel la menace a été détectée.
- **Mis en quarantaine.** Date et heure auxquelles l'objet a été placé en quarantaine.
- **État de l'action.** L'état de l'action appliquée à l'objet en quarantaine. Vous pouvez ainsi voir rapidement si une action est encore en attente ou si elle a échoué.

 **Note**

- Les colonnes **Destinataires réels**, **Nom du code malveillant** et **Nom du serveur** sont masquées dans l'affichage par défaut.
- Lorsque plusieurs pièces jointes du même e-mail sont placées en quarantaine, le tableau Quarantaine présente une entrée séparée pour chaque pièce jointe.

Pour personnaliser les informations sur la quarantaine apparaissant dans le tableau :

1. Cliquez sur le bouton **III Colonnes** à droite de l'en-tête du tableau.
2. Sélectionnez les colonnes que vous souhaitez afficher.

Pour revenir à l'affichage des colonnes par défaut, cliquez sur le bouton **Réinitialiser**.

Vous pouvez obtenir davantage d'informations en cliquant sur le lien **Sujet** correspondant à chaque objet. La fenêtre **Détails de l'objet** apparaît, qui vous indique les informations suivantes :

- **Objet en quarantaine.** Le type d'objet en quarantaine : e-mail ou pièce jointe.
- **Mis en quarantaine.** Date et heure auxquelles l'objet a été placé en quarantaine.
- **État.** État de l'objet après analyse. L'état montre si un e-mail est marqué comme spam ou contient du contenu indésirable ou si une pièce jointe est infectée par un malware, suspectée d'être infectée, indésirable ou non analysable.
- **Nom de la pièce jointe.** Le nom de fichier de la pièce jointe détectée par les modules Antimalware ou Pièces jointes.
- **Nom du code malveillant.** Nom donné à la menace malware par les chercheurs de sécurité de Bitdefender. Cette information est disponible uniquement si l'objet était infecté.
- **Point de détection.** Un objet est détecté au niveau du transport, ou dans une boîte aux lettres ou un dossier public de la banque d'informations Exchange.
- **Règle vérifiée.** La règle de la politique à laquelle la menace correspond.
- **Serveur.** Le nom d'hôte du serveur sur lequel la menace a été détectée.
- **IP de l'expéditeur** :. Adresse IP de l'expéditeur.
- **Expéditeur.** L'adresse e-mail de l'expéditeur telle qu'elle apparaît dans le champ de l'en-tête de l'e-mail **De**.

- **Destinataires.** La liste de destinataires tels qu'ils apparaissent dans les champs des en-têtes d'e-mail **À** et **Cc**.
- **Destinataires réels.** La liste des adresses e-mail des utilisateurs individuels auxquels les e-mails devaient être délivrés avant d'être placés en quarantaine.
- **Sujet.** Le sujet de l'e-mail en quarantaine.

**Note**

Les points de suspension à la fin du texte indiquent qu'il manque une partie du texte. Dans ce cas, placez la souris sur le texte pour l'afficher dans une info-bulle.

10.3.2. Objets en quarantaine

Les e-mails et les fichiers mis en quarantaine par le module de protection Exchange sont stockés localement sur le serveur comme fichiers chiffrés. En utilisant le Control Center, vous avez l'option de restaurer les e-mails mis en quarantaine, ainsi que de supprimer ou de sauvegarder n'importe quel fichier ou e-mail mis en quarantaine.

Restaurer les e-mails en quarantaine

Si vous décidez qu'un e-mail en quarantaine ne constitue pas une menace, vous pouvez le retirer de la quarantaine. En utilisant les services Web Exchange, la protection Exchange envoie les e-mails mis en quarantaine à leurs destinataires en tant que pièce jointe à un e-mail de notification de Bitdefender.

**Note**

Vous ne pouvez restaurer que les e-mails. Pour récupérer une pièce jointe placée en quarantaine, vous devez l'enregistrer dans un dossier local sur le serveur Exchange.

Pour restaurer un ou plusieurs e-mails :

1. Allez sur la page **Quarantaine**.
2. Sélectionnez **Exchange** dans le sélecteur d'affichage situé en haut de la page.
3. Cochez les cases correspondant aux e-mails que vous souhaitez restaurer.
4. Cliquez sur le bouton **Restaurer** en haut du tableau. La fenêtre **Restaurer identifiants** va apparaître.

5. Sélectionnez les identifiants d'un utilisateur Exchange autorisé à envoyer les e-mails à restaurer. Si les identifiants que vous comptez utiliser sont nouveaux, vous devez les ajouter dans le Manager d'identifiants au préalable.


Pour ajouter les identifiants requis :

- a. Saisissez les informations nécessaires dans les champs correspondants à partir de l'en-tête du tableau :
 - Le nom d'utilisateur et le mot de passe de l'utilisateur Exchange.



Note

Le nom d'utilisateur doit inclure le nom de domaine, comme dans `utilisateur@domaine` ou `domaine\utilisateur`.

- L'adresse e-mail de l'utilisateur Exchange, nécessaire seulement lorsque l'adresse e-mail est différente du nom d'utilisateur.
 - URL des Services Web Exchange (EWS), indispensable lorsque la découverte automatique d'Exchange ne fonctionne pas. C'est généralement le cas avec les serveurs Edge Transport dans un DMZ.
- b. Cliquez sur le bouton  **Ajouter** à droite du tableau. Le nouveau jeu d'authentifiants est ajouté au tableau.
6. Cliquez sur le bouton **Restaurer**. Une message de confirmation s'affichera.

L'action requise est immédiatement envoyée aux serveurs cibles. Une fois qu'un e-mail a été restauré, il est également supprimé de la quarantaine, ce qui fait que l'entrée correspondante va disparaître du tableau de Quarantaine.

Vous pouvez vérifier le statut de l'action de restauration dans les endroits suivants :


- La colonne **Statut action** du tableau de Quarantaine.
- La page **Tâches > réseau**.

Enregistrer les fichiers en quarantaine

Si vous souhaitez examiner ou récupérer des données dans des fichiers mis en quarantaine, vous pouvez sauvegarder les fichiers dans un dossier local dans l'Exchange Server. Bitdefender Endpoint Security Tools déchiffre les fichiers et les sauvegarde dans l'emplacement spécifié.

Pour enregistrer un ou plusieurs fichiers en quarantaine :

1. Allez sur la page **Quarantaine**.

2. Sélectionnez **Exchange** dans le sélecteur d'affichage situé en haut de la page.
3. Filtrez les données du tableau pour afficher tous les fichiers que vous souhaitez enregistrer, en saisissant les termes recherchés dans les champs d'en-tête de colonne.
4. Cochez les cases correspondant aux fichiers en quarantaine que vous souhaitez restaurer.
5. Cliquez sur le bouton  **Enregistrer** en haut du tableau.
6. Indiquez le chemin vers le dossier de destination sur le Serveur Exchange. Si le dossier n'existe pas sur le serveur, il sera créé.



Important

Vous devez exclure ce dossier de l'analyse au niveau du système de fichiers, sinon les fichiers seront déplacés vers la Quarantaine Ordinateurs et Machines virtuelles. Pour plus d'informations, reportez-vous à « [Exclusions](#) » (p. 294).

7. Cliquez sur **Enregistrer**. Une message de confirmation s'affichera.
Vous pouvez remarquer l'état en attente dans la colonne **État de l'action**. Vous pouvez également afficher l'état de l'action sur la page **Réseau > Tâches**.

Suppression automatique des fichiers en quarantaine


Par défaut, les fichiers placés en quarantaine depuis plus de 30 jours sont automatiquement supprimés. Vous pouvez changer ce paramètre en modifiant la politique affectée au Serveur Exchange administré.

Pour modifier l'intervalle de suppression automatique des fichiers en quarantaine :

1. Allez sur la page **Politiques**.
2. Cliquez sur le nom de la politique affectée au Serveur Exchange qui vous intéresse.
3. Allez sur la page **Protection Exchange > Général**.
4. Dans la section **Configuration**, sélectionnez le nombre de jours après lequel les fichiers sont supprimés.
5. Cliquez sur **Enregistrer** pour appliquer les modifications.

Suppression manuelle des fichiers en quarantaine

Pour supprimer un ou plusieurs objets en quarantaine :

1. Allez sur la page **Quarantaine**.
2. Sélectionnez **Exchange** dans le sélecteur d'affichage.
3. Cochez les cases correspondant aux fichiers que vous souhaitez supprimer.
4. Cliquez sur le bouton  **Supprimer** en haut du tableau. Vous devrez confirmer votre action en cliquant sur **Oui**.

Vous pouvez remarquer l'état en attente dans la colonne **État de l'action**.

L'action requise est immédiatement envoyée aux serveurs cibles. Une fois un fichier supprimé, l'entrée correspondante disparaîtra du tableau Quarantaine.

Vider la Quarantaine

Pour supprimer tous les objets en quarantaine :

1. Allez sur la page **Quarantaine**.
2. Sélectionnez **Échanger** dans le sélecteur d'affichage.
3. Cliquez sur le bouton **Vider la quarantaine**.

Vous devrez confirmer votre action en cliquant sur **Oui**.

Toutes les entrées du tableau de Quarantaine ont été effacées. L'action requise est immédiatement lancée sur les objets du réseau cible.

11. UTILISER SANDBOX ANALYZER

La page **Sandbox Analyzer** comporte une interface unifiée pour visualiser, filtrer et rechercher les **envois automatiques** et **manuels** dans l'environnement Sandbox. La page **Sandbox Analyzer** est divisée en deux zones :

The screenshot shows the Bitdefender GravityZone Sandbox Analyzer interface. On the left is a navigation sidebar with categories like 'Réseau', 'Inventaire des applications', 'Paquets', 'Tâches', 'Politiques', 'Règles d'affectation', 'Rapports', 'Quarantaine', 'Comptes', 'Activité des utilisateurs', 'État du système', 'Sandbox Analyzer', 'Envoi manuel', 'Infrastructure', 'Configuration', 'Mise à jour', and 'Licence'. The main area is titled 'Sandbox Analyzer' and includes a search bar and a 'Rechercher' button. Below the search bar are several filter tabs: 'Résultat de l'analyse', 'Score de sécurité', 'Date de soumission', 'État de l'envoi', 'Environnement', and 'Techniques ATT&CK'. The 'Score de sécurité' tab is selected, showing a scale from 0 (Faible) to 100 (Élevé) with a red bar indicating a score of 5. Below the filters, there are two rows of analysis results for 'TestSample.exe' files, each with a score of 5 and a 'Fichiers et processus Impliqué: 44' or '42'. The interface is divided into two zones by a red line, with '1.' marking the filter section and '2.' marking the results list.

La page Sandbox Analyzer

1. La **zone de filtrage** vous permet de rechercher et de filtrer les envois selon divers critères : nom, somme de contrôle, date, résultats de l'analyse, état, environnement de détonation et techniques MITRE ATT&CK.
2. La **zone des fiches d'envoi** regroupe tous les envois et donne des informations détaillées sur chacun d'eux.

Depuis la page Sandbox Analyzer vous pouvez faire les choses suivantes :


- **Filtrer les fiches d'envoi**
- **Voir la liste des envois et les informations détaillées de l'analyse**
- **Envoyer de nouveau les échantillons en analyse depuis la fiche d'envoi**
- **Supprimer les fiches d'envoi**
- **Procéder à des envois manuels**

11.1. Filtrage des fiches d'envoi

Voici ce que vous pouvez faire depuis la zone filtres :

- Filtrer les envois selon plusieurs critères. La page se chargera automatiquement que les fiches d'événement de sécurité correspondant aux critères de recherche.
- Pour réinitialiser les filtres, cliquez sur le bouton **Supprimer les filtres**.
- Pour masquer la zone des filtres, cliquez sur le bouton **Masquer les filtres**. Vous pourrez de nouveau afficher les options masquées en cliquant sur **Afficher les filtres**.

Vous pouvez filtrer les envois à Sandbox Analyzer selon les critères suivants :

- **Nom et somme de contrôle (MD5) de l'échantillon**. Saisissez dans le champ de recherche tout ou partie du nom ou du hash de l'échantillon que vous cherchez puis appuyer sur **Rechercher**, à droite du champ.
- **Date**. Pour filtrer par date :
 1. Cliquez sur l'icône calendrier  pour définir l'intervalle sur lequel doit porter la recherche.
 2. Pour définir l'intervalle . Cliquez sur les boutons **Du** et **Au** en haut du calendrier pour sélectionner les dates délimitant l'intervalle. Vous pouvez également sélectionner une période prédéterminée à droite de la liste des options, en rapport à la date actuelle (par exemple, les 30 derniers jours).
Vous pouvez également indiquer l'heure et les minutes pour chaque date de l'intervalle, en utilisant les options situées sous le calendrier.
 3. Cliquez sur **OK** pour appliquer le filtre.
- **Résultat de l'analyse**. Sélectionnez au moins une des options suivantes :
 - **Sain** – L'échantillon est sûr.
 - **Infecté** – L'échantillon est dangereux.
 - **Non pris en charge** – L'échantillon est dans un format que Sandbox Analyzer n'a pas pu traiter. Pour visualiser la liste complète des types de fichiers et extensions pris en charge par Sandbox Analyzer, rendez-vous à la section « [Types et extensions de fichier pris en charge pour l'envoi manuel](#) » (p. 533).
- **Sévérité**. La valeur indique la dangerosité d'un échantillon sur une échelle de 0 à 100. Plus le score est élevé, plus l'échantillon est dangereux. Ce score

s'applique à tous les échantillons envoyés, y compris ceux des catégories **Sain** et **Non pris en charge**.

- **Type d'envoi.** Sélectionnez au moins une des options suivantes :
 - **Manuel.** Sandbox Analyzer a reçu l'échantillon via l'option **Envoi manuel**.
 - **Capteur de l'endpoint.** Bitdefender Endpoint Security Tools a envoyé l'échantillon Sandbox Analyzer conformément aux paramètres de la politique.
 - **Capteur de trafic du réseau.** Le capteur réseau a envoyé l'échantillon à une instance de Sandbox Analyzer conformément aux paramètres de la politique.
 - **Quarantaine centralisée.** GravityZone] a envoyé l'échantillon à une instance locale de Sandbox Analyzer conformément aux paramètres de la politique.
 - **API.** L'échantillon a été envoyé à une instance locale de Sandbox Analyzer par le biais de l'API.
 - **Capteur ICAP Security Server** a envoyé l'échantillon à une instance locale de Sandbox Analyzer après analyse d'un serveur ICAP.
- **État de l'envoi .** Cochez une ou plusieurs des cases suivantes.
 - **Achévé** – Sandbox Analyzer a fourni le résultat de l'analyse.
 - **En attente d'analyse** – Sandbox Analyzer est en train de traiter l'échantillon.
 - **Échec** – Sandbox Analyzer n'a pas pu traiter l' échantillon.
- **Environnement.** Ici sont listées les machines virtuelles disponibles pour la détonation, y compris l'instance Sandbox Analyzer hébergée par Bitdefender. Cochez une ou plusieurs cases pour voir quels échantillons ont été détonés dans certains environnements.
- **Techniques d'ATT&CK.** Cette option de filtrage intègre la base de connaissances MITRE's ATT&CK, si applicable. Les valeurs des techniques ATT&CK changent de manière dynamique en fonction des événements de sécurité.
Cliquez sur **À propos** pour ouvrir la matrice ATT&CK dans un nouvel onglet.

11.2. Afficher les détails d'une analyse

La page **Sandbox Analyzer** affiche les fiches d'envoi par date, de la plus récente à la plus ancienne. Les fiches d'envoi comprennent les données suivantes :

- Résultat de l'analyse
- Nom de l'échantillon

- Type d'envoi
- Sévérité
- Fichiers et processus impliqués
- Environnement de détonation
- Somme de contrôle (MD5)
- Techniques d'ATT&CK
- État de l'envoi lorsqu'aucun résultat n'est disponible

Chaque fiche contient également un lien vers un rapport d'analyse détaillée au format HTML, s'il existe. Pour ouvrir un rapport, cliquez sur le bouton **Voir** à droite de la fiche.

Le rapport HTML fournit des informations complètes organisées sur plusieurs niveaux, avec des textes descriptifs, des graphiques et des captures d'écran qui illustrent le comportement de l'échantillon dans l'environnement de détonation. Voici ce que vous pouvez apprendre grâce au rapport HTML de Sandbox Analyzer :

- Les données générales sur l'échantillon analysé comme : le nom et la classification du malware, les détails de l'envoi (nom, type et taille du fichier, somme de contrôle, heure de l'envoi et durée de l'analyse).
- Les résultats de l'analyse comportementale, qui comprend tous les événements de sécurité capturés pendant la détonation, organisés en sections. Voici la liste des événements de sécurité pouvant être détectés :
 - Écriture / suppression / déplacement / duplication / remplacement de fichiers sur le système et sur des disques amovibles.
 - Exécution de fichiers récemment créés.
 - Modifications dans le système de fichiers.
 - Modifications au niveau des applications exécutées à l'intérieur de la machine virtuelle.
 - Modifications au niveau de la barre des tâches Windows et du menu Démarrer.
 - Création/interruption/injection de processus.
 - Écriture/suppression des clés de registre.
 - Création d'objets mutex.
 - Création / démarrage / arrêt / modification / requête / suppression de services.
 - Modifications des paramètres de sécurité du navigateur.
 - Modification des paramètres d'affichage Windows Explorer.
 - Ajout de fichiers à la liste d'exception du pare-feu.

- Modifications des paramètres du réseau.
- Activation de l'exécution lors du démarrage du système.
- Connexion à un hôte distant.
- Accès à certains domaines.
- Transfert de données vers et à partir de certains domaines.
- Accès à des URL, IP et ports via divers protocoles de communication.
- Vérification des indicateurs de l'environnement virtuel.
- Vérification des indicateurs des outils de surveillance.
- Création de captures d'écran.
- Crochetage SSDT, IDT, IRP.
- Déchargement de mémoire pour les processus suspects.
- Appels de fonction Windows API.
- Se montrer inactif pendant un certain temps, afin de retarder l'exécution.
- Créer des fichiers dont les actions seront exécutées à intervalles réguliers.



Important

Les rapports HTML ne sont disponibles qu'en anglais, quelle que soit la langue que vous utilisez sur la Control Center GravityZone.

11.3. Renvoyer un échantillon

Dans la zone des fiches d'envoi, vous pouvez soumettre des échantillons déjà détonés à une instance de Sandbox Analyzer sans avoir à les charger de nouveau. Vous pouvez faire cela pour les échantillons déjà envoyés à l'instance locale de Sandbox Analyzer par n'importe quel capteur ou méthode, manuellement, automatiquement ou via l'API.

Pour envoyer de nouveau un échantillon :

1. Cliquez sur **Envoyer de nouveau en analyse** sur la fiche d'envoi.
2. Sur la fenêtre de configuration, conservez les réglages de l'envoi précédent ou modifiez-les comme suit :
 - a. Sous **Gestion de l'image**, sélectionnez l'image de machine virtuelle que vous voulez utiliser pour la détonation.
 - b. Dans **Configurations de la détonation**, configurez les paramètres suivants :
 - i. **Limite de temps pour la détonation d'un échantillon (minutes)**. Définissez une durée maximale pour l'analyse de chaque échantillon. Par défaut, cette durée est de 4 minutes mais il arrive que l'analyse prenne plus de

temps. À la fin du temps imparti, Sandbox Analyzer interrompt l'analyse et génère un rapport se fondant sur les données rassemblées jusqu'alors. Si elle n'est pas complète, l'analyse peut donner des résultats inexacts.

- ii. **Nombre de tentatives autorisées.** En cas d'erreur inattendue, Sandbox Analyzer tente de détoner un l'échantillon comme configuré jusqu'à terminer l'analyse. La valeur par défaut est 2. Cela signifie qu'en cas d'erreur, Sandbox Analyzer essaiera deux fois de traiter l'échantillon.
- iii. **Pré-filtrage** Sélectionnez cette option pour exclure les échantillons déjà analysés.
- iv. **Accès à Internet pendant la détonation.** L'analyse de certains échantillons nécessite un accès à Internet. Pour optimiser les résultats, nous vous recommandons d'activer cette option.

- c. Dans **Profil de détonation**, ajustez le niveau de complexité de l'analyse comportementale, qui affecte les performances de Sandbox Analyzer. Par exemple, avec un niveau **Élevé**, Sandbox Analyzer réalisera une analyse plus poussée sur moins d'échantillons que ce qu'il traiterait au niveau **Moyen** ou **Faible**.

3. Cliquez sur **Envoyer de nouveau**.

Une fois l'objet renvoyé, la page **Sandbox Analyzer** affiche une nouvelle fiche et la rétention des données pour cet échantillon est prolongée selon les paramètres.



Note

L'option **Envoyer de nouveau en analyse** est disponible pour les échantillons qui sont toujours présents dans le datastore de Sandbox Analyzer. Veillez à ce que la rétention des données soit configurée sur la page [Sandbox Analyzer > Sandbox Manager](#) des paramètres de la politique.

11.4. Supprimer les fiches d'envoi

Pour supprimer les fiches d'envoi dont vous n'avez plus besoin :

1. Accédez à la fiche d'envoi que vous voulez supprimer.
2. Cliquez sur **Supprimer l'entrée** à droite de la fiche.
3. Cliquez sur **Oui** pour confirmer l'action.



Note

En procédant comme cela, vous supprimez uniquement la fiche d'envoi concernée. Les informations concernant cet envoi restent disponibles dans le rapport **Résultats Sandbox Analyzer (obsolète)**. Toutefois, ce rapport ne sera bientôt plus disponible.

11.5. Envoi manuel

Depuis **Sandbox Analyzer > Envoi manuel**, vous pouvez envoyer des échantillons d'éléments douteux à Sandbox Analyzer, pour déterminer si ce sont des menaces ou des fichiers inoffensifs. Vous pouvez également accéder à la page **Envoi manuel** en cliquant sur le bouton **Soumettre un échantillon** en haut à droite de la zone de filtrage de la page Sandbox Analyzer.



Note

L'envoi manuel vers Sandbox Analyzer est compatible avec tous les navigateurs requis par Control Center, sauf Internet Explorer 9. Pour envoyer des éléments à Sandbox Analyzer, connectez-vous à Control Center en utilisant tout autre navigateur compatible mentionné dans « [Connexion au Control Center](#) » (p. 20).

Tableau de bord Réseau Inventaire des applications Packages Tâches Politiques Règles d'affectation Rapports Quarantaine Comptes Activité des utilisateurs État du système Sandbox Analyzer Envoi manuel Infrastructure Configuration Mise à jour Licence	Téléchargement Paramètres généraux
	Echantillons
	<input checked="" type="radio"/> Fichiers
	<input type="text"/> <input type="button" value="Parcourir"/>
	Fournir un mot de passe pour les archives chiffrées :
	<input type="text"/>
	<small>Vous ne pouvez ajouter qu'un mot de passe à la fois. Si vous envoyez plusieurs archives chiffrées, Sandbox Analyzer utilisera le même mot de passe pour toutes les archives.</small>
	<input type="radio"/> URL
	<input type="text"/>
	Paramètres de détonation
<input type="checkbox"/> Utiliser Sandbox Analyzer dans le cloud	
Sandbox Analyzer en local: <input type="text" value="bitdefender-sba-tpf3 (10.10.10.10)"/>	
Image: <input type="text" value="win10_x64_rs6_geb8"/>	
Arguments de ligne de commande: <input type="text"/>	
<input checked="" type="checkbox"/> Détoner les échantillons individuellement	

Sandbox Analyzer > Envoi manuel

Pour envoyer des échantillons à Sandbox Analyzer :

1. Sur la page **Téléchargement**, sous **Échantillons**, sélectionnez le type d'objet :
 - a. **Fichiers**. Cliquez sur **Parcourir** pour sélectionner les éléments que vous voulez envoyer pour une analyse comportementale. En cas d'archives protégées par mot de passe, vous pouvez définir un mot de passe par session de téléchargement dans un champ dédié. Lors du processus d'analyse, Sandbox Analyzer applique le mot de passe spécifié à toutes les archives envoyées.
 - b. **URL**. Saisissez dans ce champ l'URL que vous voulez analyser. Vous ne pouvez envoyer qu'une seule URL par session.
2. Dans **Paramètres de détonation**, configurez les paramètres de l'analyse pour la session en cours :
 - L'instance Sandbox Analyzer que vous voulez utiliser. Vous pouvez sélectionner soit l'instance cloud ou une instance Sandbox Analyzer installée en local.
En choisissant d'utiliser une instance locale de Sandbox Analyzer, vous pouvez sélectionner de multiples machines virtuelles auxquelles vous pouvez envoyer l'échantillon en simultané.
 - **Arguments de ligne de commande**. Ajoutez autant d'arguments de ligne de commande que vous le voulez, séparés par des espaces, pour modifier le fonctionnement de certains programmes, par exemple les exécutables. Ces arguments s'appliquent à tous les échantillons envoyés en analyse.
 - **Détoner les échantillons individuellement**. Cochez cette case pour que les fichiers d'un lot soient analysés un par un
3. Dans **Profil de détonation**, ajustez le niveau de complexité de l'analyse comportementale, qui affecte les performances de Sandbox Analyzer. Par exemple, avec un niveau **Élevé**, Sandbox Analyzer réalisera une analyse plus poussée sur moins d'échantillons que ce qu'il traiterait au niveau **Moyen** ou **Faible**.
4. Sur la page **Paramètres généraux**, vous pouvez sélectionner des options qui s'appliquent à tous les envois manuels, quelle que soit la session :
 - a. **Limite de temps pour la détonation d'un échantillon (minutes)**. Définissez une durée maximale pour l'analyse de chaque échantillon. Par défaut, cette durée est de 4 minutes mais il arrive que l'analyse prenne plus de temps. À

la fin du temps imparti, Sandbox Analyzer interrompt l'analyse et génère un rapport se fondant sur les données rassemblées jusqu'alors. Si elle n'est pas complète, l'analyse peut donner des résultats inexacts.

- b. **Nombre de tentatives autorisées.** En cas d'erreur inattendue, Sandbox Analyzer tente de détoner un l'échantillon comme configuré jusqu'à terminer l'analyse. La valeur par défaut est 2. Cela signifie qu'en cas d'erreur, Sandbox Analyzer essaiera deux fois de traiter l'échantillon.
 - c. **Pré-filtrage** Sélectionnez cette option pour exclure les échantillons déjà analysés.
 - d. **Accès à Internet pendant la détonation.** L'analyse de certains échantillons nécessite un accès à Internet. Pour optimiser les résultats, nous vous recommandons d'activer cette option.
 - e. Cliquez sur **Enregistrer** pour conserver les modifications.
5. Retournez à la page **Téléchargement**.
6. Cliquez sur **Valider**. Une barre indique la progression de l'envoi.

Après l'envoi, la page **Sandbox Analyzer** comprend une nouvelle fiche. Lorsque l'analyse est terminée, la fiche indique le verdict et les détails correspondants.



Note

Pour envoyer manuellement des échantillons à Sandbox Analyzer, vous devez disposer des droits **Gérer les réseaux**.

11.6. Gestion de l'infrastructure Sandbox Analyzer

Dans la section **Sandbox Analyzer > Infrastructure**, vous pouvez prendre les mesures suivantes en ce qui concerne l'instance de Sandbox Analyzer installée en local :

- [Consultez l'état de l'instance Sandbox Analyzer](#)
- [Configurer les détonations simultanées](#)
- [Vérifier l'état des images de machines virtuelles](#)
- [Configurer et gérer les images de machines virtuelles.](#)

11.6.1. Consulter l'état de Sandbox Analyzer

Après avoir déployé et configuré l'appliance virtuelle Sandbox Analyzer sur l'hyperviseur ESXi, vous pouvez obtenir des informations sur l'instance locale de Sandbox Analyzer depuis la page **État**.

Tableau de bord		État Gestion d'image				
Réseau		Actualiser				
Inventaire des applications		Instance de Sandbox Analyzer				
Packages		Échantillons détonés	Espace disque utili...	État	Détonations simultanées maximales	Détonations simultanées configurées
Tâches						
Politiques		bitdefender-aba-4508 ()	30	65%	Le 11 nov à 15:42 ... 21	0
Règles d'affectation		bitdefender-aba-4h5e ()	N/D	0%	Non installé 21	0
Rapports		bitdefender-aba-3pf3 ()	N/D	51%	En ligne 21	2
Quarantaine		bitdefender-aba-qfcs ()	N/D	51%	En ligne 21	2
Comptes						
Activité des utilisateurs						
État du système						
Sandbox Analyzer						
Envoi manuel						
Infrastructure						

Sandbox Analyzer > Infrastructure > État

Le tableau vous fournit les informations détaillées suivantes :

- **Nom de l'instance Sandbox Analyzer.** Chaque nom correspond à une instance de Sandbox Analyzer installée sur un hyperviseur ESXi. Vous pouvez installer Sandbox Analyzer sur de multiples hyperviseurs ESXi.
- **Échantillons détonés.** La valeur indique la quantité d'échantillons analysés par l'instance Sandbox Analyzer depuis la première activation de sa licence.
- **Espace disque utilisé.** Le pourcentage indique le volume d'espace disque utilisé par Sandbox Analyzer sur le datastore.
- **état.** Dans cette colonne, vous pouvez voir si l'instance Sandbox Analyzer est en ligne, hors ligne, non installée, en cours d'installation ou si l'installation a échoué.
- **Détonations simultanées maximales.** La valeur représente le nombre maximal de machines virtuelles que Sandbox Analyzer peut créer pour détoner des échantillons. À un instant T, une machine virtuelle peut réaliser une détonation. La quantité de machines virtuelles est déterminée par les ressources matérielles disponibles sur ESXi.

- **Détonations simultanées configurées.** Quantité réelle de machines virtuelles créées selon la licence disponible.
- **Utiliser un proxy.** Cliquez sur le bouton On/Off pour activer ou désactiver la communication entre GravityZone Control Center et les instances de Sandbox Analyzer via un serveur proxy. Pour configurer un proxy, rendez-vous dans **Configuration > Proxy** depuis le menu principal de Control Center. Si aucun proxy n'est configuré, Control Center ne tient pas compte de cette option.

Pour plus d'informations sur la configuration d'un proxy, référez-vous à **Installer la protection > Installation et configuration de GravityZone > Configurer les paramètres de Control Center > Proxy** du Guide d'installation de GravityZone.



Note

Control Center n'utilise ce proxy que pour communiquer avec les instances de Sandbox Analyzer On-Premises. Pour communiquer avec l'instance cloud de Sandbox Analyzer, Control Center utilise le serveur proxy configuré sur la page Sandbox Analyzer des paramètres de la politique.

Ce proxy est également différent de celui configuré sur la page **Général > Paramètres** des paramètres de la politique, qui assure la communication entre les endpoints et les composants de GravityZone.

Vous pouvez effectuer des recherches et filtrer les colonnes selon les noms d'instances Sandbox Analyzer ou leur statut. Utilisez le bouton situé en haut à droite du tableau pour actualiser la page et afficher et masquer les filtres et colonnes.

11.6.2. Configurer les détonations simultanées

Sur la page **État**, vous pouvez configurer les détonations simultanées, soit le nombre de machines virtuelles pouvant simultanément exécuter et détoner des échantillons sur une instance Sandbox Analyzer. La quantité de détonations simultanées dépend des ressources matérielles et de la distribution des sièges de licence sur plusieurs instances de Sandbox Analyzer.

Pour configurer les détonations simultanées :

1. Cliquez sur le numéro ou sur l'icône **Modifier** dans la colonne **Détonations simultanées configurées**.
2. Sur cette nouvelle fenêtre, indiquez dans le champ correspondant la quantité de détonations simultanées que vous voulez autoriser pour l'instance Sandbox Analyzer.

3. Cliquez sur **Enregistrer**.

11.6.3. Vérifier l'état des images VM

Sandbox Analyzer utilise des images de machine virtuelle comme environnements de détonation pour réaliser l'analyse comportementale des échantillons envoyés. Vous pouvez vérifier l'état des machines virtuelles sur la page **Gestion de l'image**.

Tableau de bord		État Gestion d'image			
Réseau		Actualiser			
Inventaire des applications					
Packages					
Tâches					
Politiques					
Règles d'affectation					
Rapports					
Quarantaine					
Comptes					
Activité des utilisateurs					
État du système					
Sandbox Analyzer					
Envoi manuel					
Infrastructure					
bitdefender-sba-e508 ()					
	__wr10_x64_r1_14393_87tg	os	04 novembre 2019, 16:41:44	● Prêt	Définir par défaut Supprim
	__wr10_x64_r5_17763_v5_v499	os	04 novembre 2019, 16:53:51	● Prêt	Définir par défaut Supprim
	__wr10_x64_r5_17763_v13_u97v	os	04 novembre 2019, 16:42:24	● Prêt	Définir par défaut Supprim
	__wr10_x64_r6_Bn23	os	04 novembre 2019, 17:03:22	● Prêt	Définir par défaut Supprimer
	__wr10_r4_x64_1sta	os	04 novembre 2019, 17:02:08	● Prêt	Définir par défaut Supprim
	__wr10_x64_r5_17763_v0_4694	os	04 novembre 2019, 17:01:32	● Prêt	Définir par défaut Supprim
	__wr10_x64_r5_17763_v12_d1o	os	04 novembre 2019, 17:00:57	● Prêt	Définir par défaut Supprim
	__wr10_x64_r5_17763_v0_83r6	os	04 novembre 2019, 17:00:13	● Prêt	Définir par défaut Supprim
	__wr10_x64_r5_17763_v11_38fp	os	04 novembre 2019, 16:59:21	● Prêt	Définir par défaut Supprim

Sandbox Analyzer > Infrastructure > Gestion de l'image

Le tableau vous fournit les informations détaillées suivantes :

- **Nom** des images de machines virtuelles disponibles, comme indiqué dans la console de l'appliance Sandbox Analyzer. Plusieurs images de machine virtuelle sont regroupées dans la même instance de Sandbox Analyzer.
- **Système d'exploitation**, comme indiqué dans la console de l'appliance Sandbox Analyzer.
- La date de l'ajout de l'image de machine virtuelle.
- **état**. Cette colonne indique si une image de machine virtuelle est nouvelle et peut être préparée pour procéder à la détonation, est prête pour procéder à une détonation ou si le processus de préparation a échoué.
- **Actions**. Cette colonne indique les actions disponibles pour les images de machines virtuelles, en fonction de leur état : générer des images pour détonation, les configurer comme environnement de détonation par défaut, ou les supprimer.

11.6.4. Configurer et gérer les images VM

Générer les machines virtuelles de détonation

Pour détoner des échantillons en utilisant l'instance Sandbox Analyzer locale, vous devez générer des machines virtuelles dédiées. La page **Gestion de l'image** vous permet de créer des machines virtuelles de détonation, si tant est que vous avez ajouté des images VM sur la console de l'appliance Sandbox Analyzer.



Note

Pour découvrir comment ajouter des images VM dans la console de l'appliance Sandbox Analyzer, consultez le chapitre **Installer Sandbox Analyzer Virtual Appliance** du Guide d'installation de GravityZone.

Pour créer des machines virtuelles de détonation, dans la colonne **Actions**, cliquez sur l'option **Créer une image** pour les images VM dont l'état est : **Nouvelle – Doit être créée**. La génération d'une machine virtuelle prend habituellement entre 15 et 30 minutes en fonction de sa taille. Une fois le processus de génération terminé, l'état des machines virtuelles devient **Prête**.

Configurer la machine virtuelle par défaut

Une instance de Sandbox Analyzer peut avoir de multiples images installées et configurées en tant que machines virtuelles de détonation. Dans le cas d'envois automatiques, Sandbox Analyzer utilise la première image VM créée pour détoner les échantillons.

Vous pouvez modifier ce comportement en configurant une image VM par défaut. Pour cela, cliquez sur l'option **Définir par défaut** de l'image VM à privilégier.

Supprimer des machines virtuelles

Pour supprimer une image de machine virtuelle de la page **Gestion de l'image**, cliquez sur **Supprimer** dans la colonne **Actions**. Sur la fenêtre de configuration, cliquez sur **Supprimer l'image**.

12. JOURNAL D'ACTIVITÉ DE L'UTILISATEUR

La Control Center enregistre toutes les opérations et actions effectuées par les utilisateurs. La liste des activités utilisateurs comprend les événements suivants, en fonction de votre niveau d'autorisation administrative :

- Connexion et déconnexion
- Créer, éditer, renommer et supprimer des rapports
- Ajouter et supprimer des portlets du tableau de bord
- Créer, éditer et supprimer des identifiants
- Créer, modifier, télécharger et supprimer des packages réseau
- Créer des tâches réseau
- Commencer, arrêter, annuler et stopper le processus de résolution des problèmes sur les machines affectées
- Créer, éditer, renommer et supprimer des comptes d'utilisateur
- Supprimer ou déplacer des endpoints entre des groupes
- Créer, déplacer, renommer et supprimer des groupes
- Supprimer et restaurer des fichiers en quarantaine
- Créer, éditer et supprimer des comptes d'utilisateur
- Créer, modifier et supprimer des règles de permission d'accès.
- Créer, éditer, renommer, affecter et supprimer des politiques
- Modification des paramètres d'authentification pour les comptes GravityZone.
- Créer, éditer, synchroniser et supprimer des intégrations à Amazon EC2.
- Créer, modifier, synchroniser et supprimer des intégrations Microsoft Azure.
- Mettre à jour l'appliance GravityZone.

Pour consulter les enregistrements de l'activité de l'utilisateur, allez sur la page **Comptes >Activité de l'utilisateur** et sélectionnez ce que vous souhaitez afficher dans le [sélecteur d'affichage](#).

<ul style="list-style-type: none"> Tableau de bord Réseau Packages Tâches Politiques Rapports Quarantaine Comptes <li style="background-color: #e0e0e0;">Activité des utilisateurs Configuration Mise à jour Licence 	Utilisateur <input type="text"/>	Action <input type="text"/>	Cible <input type="text"/>	Rechercher															
	Rôle <input type="text"/>	Zone <input type="text"/>	Créé <input type="text"/>																
	<table border="1"> <thead> <tr> <th>Utilisateur</th> <th>Rôle</th> <th>Action</th> <th>Zone</th> <th>Cible</th> <th>Créé</th> </tr> </thead> <tbody> <tr> <td colspan="7" style="text-align: center;"> Première page ← Page 0 de 0 → Dernière page 20 </td> </tr> </tbody> </table>							Utilisateur	Rôle	Action	Zone	Cible	Créé	Première page ← Page 0 de 0 → Dernière page 20					
Utilisateur	Rôle	Action	Zone	Cible	Créé														
Première page ← Page 0 de 0 → Dernière page 20																			

La page d'activité de l'utilisateur

Pour afficher les événements enregistrés qui vous intéressent, vous devez définir une recherche. Complétez les champs disponibles avec les critères de recherche et cliquez sur le bouton **Rechercher**. Tous les enregistrements correspondant à vos critères apparaîtront dans le tableau.

Les colonnes du tableau vous donnent les informations utiles sur les événements de la liste suivante :

- Le nom d'utilisateur de la personne ayant effectué l'action.
- Le rôle utilisateur.
- L'action ayant causée l'événement.
- Le type d'élément infecté par l'action.
- L'élément spécifique infecté.
- L'heure à laquelle l'événement s'est produit.

Pour trier les événements en fonction d'une colonne, cliquez simplement sur l'en-tête de cette colonne. Cliquez de nouveau sur l'en-tête de colonne pour inverser l'ordre de tri.

Pour afficher des informations détaillées sur un événement, sélectionnez-le et consultez la section sous le tableau.

13. UTILISATION DES OUTILS

13.1. Injection d'outils personnalisés avec HVI

Bitdefender HVI vous évite d'avoir à dépanner les problèmes, collecter les données forensiques ou exécuter des tâches de maintenance régulière sur votre environnement Citrix en vous permettant d'injecter des outils tiers à la volée dans les systèmes d'exploitation invités. Ces opérations sont réalisées via l'API Direct inspect (pas de connexion TCP/IP nécessaire) et sans déranger les utilisateurs finaux. À cette fin, les outils doivent pouvoir fonctionner de manière silencieuse.

GravityZone vous donne 3 Go d'espace pour conserver vos outils en sécurité et les injecter dans les systèmes d'exploitation invités.

Pour envoyer des kits d'outils dans GravityZone :

1. Téléchargez la dernière version du kit d'outils sur votre ordinateur.
2. Archivez le kit au format ZIP.
3. Rendez-vous dans la Control Center GravityZone et cliquez sur le menu **Outils** situé en bas à gauche de la page. La page du **Centre de gestion des outils** apparaît.
4. Cliquez sur le bouton Envoyer adapté au système d'exploitation de destination dans la partie supérieure du tableau : **Envoyer un outil Windows** ou **Envoyer un outil Linux**.
5. Si les outils sont pour Windows, vous devez également choisir l'architecture de l'ordinateur dans le menu déroulant.
6. Localisez le fichier ZIP, sélectionnez-le et cliquez sur **Ouvrir**.

Il est possible que vous ayez à attendre quelques minutes pour envoyer des fichiers volumineux. Une fois terminé, l'outil est ajouté au tableau et la barre de progression située au-dessus du tableau rafraichit les informations sur l'espace disponible pour d'autres envois.

En plus du nom de l'outil, le tableau présente des informations utiles, telles que :

- Le système d'exploitation et la plateforme sur lesquels l'outil est exécuté.
- Une brève description de l'outil. Vous pouvez éditer ce fichier quand vous le souhaitez.
- Le nom de l'utilisateur qui a envoyé l'outil.

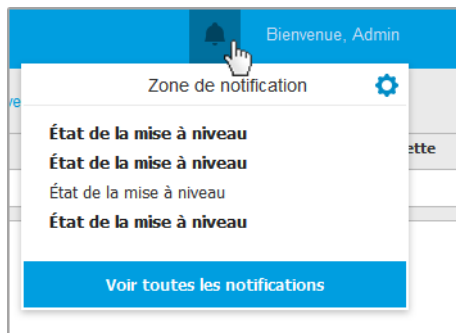
- État de l'envoi. Consultez ce champ pour vérifier que l'envoi a été réalisé avec succès.
- Date et heure de l'envoi.

Vous pouvez ensuite planifier via des politiques quand injecter les outils, ou vous pouvez les injecter n'importe quand en exécutant des tâches depuis la page **Réseau**.


Lorsque vous n'utiliserez plus les outils, sélectionnez-les et cliquez sur le bouton **Supprimer** situé en haut du tableau. Cliquez sur **Oui** pour confirmer.

14. NOTIFICATIONS

En fonction des événements susceptibles de se produire dans votre réseau, le Control Center affichera plusieurs notifications pour vous informer de l'état de sécurité de votre environnement. Les notifications s'afficheront dans la **Zone de notification**, située en haut à droite de Control Center.



Zone de notification

Lorsque de nouveaux événements sont détectés dans le réseau, l'icône  dans le coin supérieur droit de Control Center indiquera le nombre d'événements venant d'être détectés. Cliquer sur l'icône affiche la Zone de notification qui contient la liste des événements détectés.

14.1. Types de notifications

Voici la liste des types de notification disponibles :

Épidémie de malwares

Cette notification est envoyée aux utilisateurs qui ont, au moins, 5% de l'ensemble de leurs éléments administrés, infectés par le même malware.

Vous pouvez configurer le seuil de déclenchement antimalware selon vos besoins dans la fenêtre **Paramètres**. Pour plus d'informations, reportez-vous à « [Configurer les paramètres de notification](#) » (p. 508).

Cette notification ne prend pas en compte les menaces détectées par HyperDetect.

Disponibilité du format Syslog : JSON, CEF

Expiration de licence

Cette notification est envoyée 30, 7 et 1 jour avant l'expiration de la licence.

Vous devez avoir les droits de **Gestion de l'entreprise** pour voir cette notification.

Disponibilité du format Syslog : JSON, CEF

Limite d'utilisation de la licence atteinte

Cette notification est envoyée lorsque toutes les licences disponibles ont été utilisées.

Disponibilité du format Syslog : JSON, CEF

Limite de la licence sur le point d'être atteinte

Cette notification est envoyée lorsque 90% des licences disponibles ont été utilisées.

Vous devez avoir les droits de **Gestion de l'entreprise** pour voir cette notification.

Disponibilité du format Syslog : JSON, CEF

Limite d'utilisation de la licence Exchange atteinte

Cette notification est déclenchée à chaque fois que le nombre de boîtes aux lettres protégées de vos serveurs Exchange atteint la limite spécifiée sur votre clé de licence.

Vous devez avoir les droits de **Gestion de l'entreprise** pour voir cette notification.

Disponibilité du format Syslog : JSON, CEF

Identifiants utilisateur Exchange non valides

Cette notification est envoyée lorsqu'une tâche d'analyse à la demande n'a pas pu démarrer sur le serveur Exchange cible en raison d'identifiants utilisateur Exchange non valides.

Disponibilité du format Syslog : JSON, CEF

État de la mise à niveau

Cette notification est déclenchée toutes les semaines, si d'anciennes versions du produit sont détectées dans votre réseau.

Disponibilité du format Syslog : JSON, CEF

Mise à jour disponible

Cette notification vous informe de la disponibilité d'une nouvelle mise à jour de GravityZone d'un nouveau package ou d'un nouveau produit.

Disponibilité du format Syslog : JSON, CEF

Connexion Internet

Cette notification est envoyée lorsque des modifications de connectivité Internet sont détectées par les processus suivants :

- Validation de la licence
- Obtenir une demande de signature de certificat Apple
- Communication avec les appareils mobiles Apple et Android
- Accès à un compte MyBitdefender

Disponibilité du format Syslog : JSON, CEF

Connexion SMTP

Cette notification est envoyée à chaque fois que Bitdefender GravityZone détecte des modifications concernant la connectivité du serveur de messagerie.

Disponibilité du format Syslog : JSON, CEF

Utilisateurs de mobiles sans adresse email

Cette notification est envoyée après l'ajout d'appareils mobiles à plusieurs utilisateurs lorsqu'un ou plusieurs utilisateurs sélectionnés n'ont pas d'adresse e-mail de spécifiée pour leur compte. Cette notification est destinée à vous signaler que les utilisateurs pour lesquels aucune adresse e-mail n'a été spécifiée ne peuvent pas enregistrer les appareils mobiles qui leur sont attribués, puisque les détails de l'activation sont envoyés automatiquement par e-mail.

Pour des informations concernant l'ajout d'appareils mobiles à plusieurs utilisateurs, référez-vous au Guide d'installation de GravityZone.

Disponibilité du format Syslog : JSON, CEF

Sauvegarde de la base de données

Cette notification vous informe de l'état d'une sauvegarde de base de données planifiée, qu'elle ait ou non réussi. Si la sauvegarde de la base de données a échoué, le message de notification indiquera également la cause de cet échec.

Pour des informations sur la configuration des sauvegardes de bases de données GravityZone, référez-vous au Guide d'installation de GravityZone.

Disponibilité du format Syslog : JSON, CEF

Malware détecté sur Exchange

Cette notification vous signale la détection de malwares sur un serveur Exchange de votre réseau.

Disponibilité du format Syslog : JSON, CEF

Anti-exploît avancé

Cette notification vous avertit lorsque Advanced Anti- Exploit a détecté une tentative d'exploitation d'un exploit sur votre réseau.

Disponibilité du format Syslog : JSON, CEF

Événement de l'Antimalware

Cette notification vous signale la détection de malwares sur un endpoint de votre réseau. Cette notification est créée à chaque détection de malware pour fournir des informations détaillées sur l'endpoint affecté (nom, IP, agent installé), le type d'analyse, le malware détecté, la version de la signature, l'heure de détection et le type de moteur d'analyse.

Disponibilité du format Syslog : JSON, CEF

Intégration non synchronisée

Cette notification est envoyée lorsqu'une intégration à la plateforme virtuelle existante n'a pas pu se synchroniser avec GravityZone. Dans les paramètres de notification, vous pouvez sélectionner les intégrations pour lesquelles vous souhaitez être notifié(e) lorsqu'une erreur de synchronisation se produit. Davantage d'informations sur le statut de la synchronisation sont disponibles dans les détails de la notification.

Disponibilité du format Syslog : JSON, CEF

Événement de l'Antiphishing

Cette notification vous informe à chaque fois que l'agent de l'endpoint bloque l'accès à une page web de phishing connue. Cette notification fournit également des informations telles que le poste de travail ayant tenté d'accéder au site web dangereux (nom et IP), l'agent installé ou l'URL bloquée.

Disponibilité du format Syslog : JSON, CEF

Événement du Pare-Feu

Cette notification vous informe à chaque fois que le module pare-feu d'un agent installé a empêché une analyse de ports ou une application d'accéder au réseau, selon la politique appliquée.

Disponibilité du format Syslog : JSON, CEF

Événement de l'ATC/IDS

Cette notification est envoyée à chaque fois qu'une application potentiellement dangereuse est détectée et bloquée sur un endpoint de votre réseau. Vous y

trouvez des informations telles que le nom, le type et le chemin de l'application, ainsi que le chemin et l'identifiant du processus parent et la ligne de commande qui a initié le processus, le cas échéant.

Disponibilité du format Syslog : JSON, CEF

Événement du Contrôle Utilisateur

Cette notification est déclenchée à chaque fois que l'activité d'un utilisateur comme sa navigation sur Internet ou une application logicielle est bloquée par l'endpoint client en raison de la politique appliquée.

Disponibilité du format Syslog : JSON, CEF

Événement de la protection des données

Cette notification est envoyée à chaque fois que le trafic des données est bloqué sur un endpoint en raison des règles de protection des données.

Disponibilité du format Syslog : JSON, CEF

Événement des modules du produit

Cette notification est envoyée à chaque fois qu'un module de sécurité d'un agent installé est activé ou désactivé.

Disponibilité du format Syslog : JSON, CEF

Événement état Security Server

Ce type de notification fournit des informations sur les modifications d'état d'un certain Security Server installé dans votre réseau. Les modifications d'état de Security Server se réfèrent aux événements suivants : éteint / allumé, Mise à jour du produit, mise à jour des contenus de sécurité et redémarrage nécessaire

Disponibilité du format Syslog : JSON, CEF

Événement Security Server surchargé

Cette notification est envoyée lorsque la charge d'analyse de Security Server de votre réseau dépasse le seuil défini.

Disponibilité du format Syslog : JSON, CEF

Événement Enregistrement du produit

Cette notification vous informe lorsque l'état d'activation d'un agent installé dans votre réseau a changé.

Disponibilité du format Syslog : JSON, CEF

Vérification de l'authentification

Cette notification vous informe quand un autre compte GravityZone, à part le votre, a été utilisé pour se connecter à la Control Center, depuis un appareil inconnu.

Disponibilité du format Syslog : JSON, CEF

Connexion à partir d'un nouvel appareil

Cette notification vous informe que votre compte GravityZone a été utilisé pour se connecter à la Control Center à partir d'un appareil que vous n'aviez pas utilisé à cet effet auparavant. La notification est automatiquement configurée de façon à être visible à la fois dans Control Center et dans l'e-mail et vous ne pouvez que la voir.

Disponibilité du format Syslog : JSON, CEF

Expiration du certificat

Cette notification vous informe qu'une authentification de sécurité expire. Cette notification s'affiche 30, 7 et 1 jours avant la date d'expiration.

Disponibilité du format Syslog : JSON, CEF

Mise à jour GravityZone

La notification est envoyée lorsque la mise à jour GravityZone est terminée. Si elle a échoué, la mise à jour s'effectuera de nouveau dans 24h.

Disponibilité du format Syslog : JSON, CEF

État d'avancement de la tâche

Cette notification vous informe à chaque fois que l'état d'une tâche change ou lorsqu'une tâche se termine, en fonction de vos préférences.

Disponibilité du format Syslog : JSON, CEF

Serveur de mise à jour non à jour

Cette notification est envoyée lorsqu'un serveur de mise à jour de votre réseau a des contenus de sécurité non à jour.

Disponibilité du format Syslog : JSON, CEF

Événement incidents du réseau

Cette notification est envoyée à chaque fois que le module Network Attack Defense détecte une tentative d'attaque sur votre réseau. Cette notification vous informe également si la tentative d'attaque a été réalisée depuis l'extérieur du réseau ou depuis un endpoint compromis au sein du réseau. Sont également

présentées des données sur l'endpoint, la technique d'attaque, l'IP de l'attaquant et la mesure prise par Network Attack Defense.

Disponibilité du format Syslog : JSON, CEF

Rapport personnalisé généré

Cette notification vous informe lorsqu'un rapport basé sur une requête a été généré.

Disponibilité du format Syslog : n/a

Faible détectée dans la mémoire

Cette notification vous informe lorsque HVI détecte une attaque qui enfreint la mémoire des machines virtuelles protégées dans l'environnement Citrix Xen. La notification vous fournit des détails importants, tels que le nom et l'IP de la machine infectée, la description de l'incident, la source et la cible de l'attaque, ainsi que l'action effectuée pour supprimer la menace et l'heure de détection.

Des notifications sont créées pour les incidents suivants :

- Tentatives d'utiliser la zone mémoire différemment que ce que l'hyperviseur avait prévu, via les Extended Page Tables (EPT).
- Tentatives de processus d'injecter du code dans d'autres processus.
- Tentatives de modification des adresses des processus dans les tables de conversion.
- Tentatives de modification des Model Specific Registers (MSR).
- Tentatives de modification du contenu d'objets pilotes spécifiques ou de l'Interrupt Descriptor Table (IDT).
- Tentatives de chargement d'un Control Register (CR) spécifique avec une valeur non valide.
- Tentatives de chargement d'un Extended Control Register (XCR) spécifique avec une valeur non valide.
- Tentatives de modification des Global ou Interrupt Descriptor Tables.



Note

La fonctionnalité HVI pour votre solution GravityZone est disponible via une clé de licence distincte.

Disponibilité du format Syslog : JSON, CEF

Nouvelle application dans l'Inventaire des applications

Cette notification vous informe lorsque le Contrôle des applications détecte une nouvelle application installée sur des endpoints contrôlés.

Disponibilité du format Syslog : JSON, CEF

Application bloquée

Cette notification vous informe lorsque le Contrôle des applications a bloqué ou aurait bloqué un processus d'une application non autorisée, en fonction de la configuration du module (Mode production ou Mode test).

Disponibilité du format Syslog : JSON, CEF

Détection de Sandbox Analyzer

Cette notification vous prévient à chaque fois que Sandbox Analyzer détecte une nouvelle menace parmi les échantillons envoyés. Des données telles que le nom d'hôte ou l'IP de l'endpoint vous seront communiquées, ainsi que l'heure et la date de la détection, le type de menace, le chemin, le nom, la taille des fichiers et les actions de réparation appliquées sur chacun d'eux.



Note

Vous ne recevez pas de notifications lorsque les échantillons envoyés sont sains. Les informations relatives à tous les échantillons envoyés sont disponibles dans le rapport **Résultats de Sandbox Analyzer (obsolètes)** et dans la section **Sandbox Analyzer**, dans le menu principal de Control Center.

Disponibilité du format Syslog : JSON, CEF

Problème de patch manquant

Cette notification apparaît quand certains endpoints de votre réseau n'ont pas installé tous les patches disponibles.

GravityZone envoie automatiquement une notification contenant toutes les découvertes faites pendant les 24 h précédant la notification.

Vous pouvez voir quels sont les endpoints dans cette situation en cliquant sur le bouton **Afficher le rapport** de la notification.

Par défaut, ces notifications ne traitent que des patches liés à la sécurité, mais vous pouvez les configurer pour également vous tenir informé des patches non liés à la sécurité.

Disponibilité du format Syslog : JSON, CEF

Detection des ransomwares

Cette notification vous informe lorsque GravityZone a détecté une attaque de ransomware sur votre réseau. Des informations relatives à l'endpoint ciblé, à l'utilisateur qui y était connecté, à la source de l'attaque, au nombre de fichiers chiffrés et à la date et l'heure de l'attaque, apparaissent.

Lorsque vous recevez la notification, l'attaque est déjà bloquée.

Le lien présent dans la notification vous redirigera vers la page **Activité de ransomware**, où vous pourrez voir la liste des fichiers chiffrés et les restaurer si nécessaire.

Disponibilité du format Syslog : JSON, CEF

Antimalware pour les périphériques de stockage

Cette notification est envoyée lorsqu'un malware est détecté sur un périphérique de stockage conforme au protocole ICAP. Cette notification est créée pour chaque détection de malware et fournit des informations relatives au périphérique de stockage infecté (nom, adresse IP, type), au malware détecté et à l'heure de la détection.


Disponibilité du format Syslog : JSON, CEF

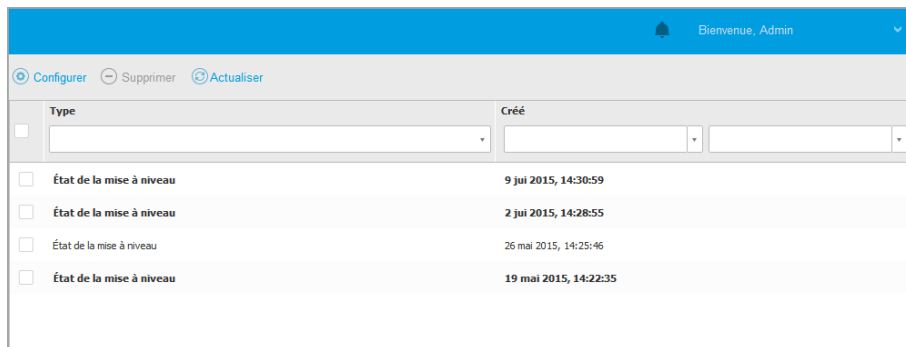
Appareils bloqués

Cette notification apparaît lorsqu'un appareil bloqué ou un appareil n'ayant que la permission lecture seule est connecté sur l'endpoint. Si le même appareil est connecté plusieurs fois au cours de la même heure, une seule notification apparaît pendant cette période. Si l'appareil se connecte de nouveau après une heure, une nouvelle notification apparaît.

Disponibilité du format Syslog : JSON, CEF

14.2. Afficher les notifications

Pour afficher les notifications, cliquez sur le bouton  **Notifications** puis cliquez sur **Voir toutes les notifications**. Un tableau contenant toutes les notifications s'affiche.



Type	Créé
<input type="checkbox"/> État de la mise à niveau	9 jui 2015, 14:30:59
<input type="checkbox"/> État de la mise à niveau	2 jui 2015, 14:28:55
<input type="checkbox"/> État de la mise à niveau	26 mai 2015, 14:25:46
<input type="checkbox"/> État de la mise à niveau	19 mai 2015, 14:22:35

La page Notifications

En fonction du nombre de notifications, le tableau peut comporter plusieurs pages (seules 20 entrées sont affichées par page, par défaut).

Pour parcourir les pages, utilisez les boutons de navigation en bas du tableau.

Pour modifier le nombre d'entrées affichées sur une page, sélectionnez une option dans le menu à côté des boutons de déplacement.

S'il y a trop d'entrées, vous pouvez utiliser les zones de recherche sous les en-têtes de colonne ou le menu du filtre en haut du tableau, afin de filtrer les données affichées.

- Pour filtrer les notifications, sélectionnez le type de notification que vous souhaitez afficher dans le menu **Type**. Vous pouvez également sélectionner l'intervalle au cours duquel la notification a été générée afin de réduire le nombre d'entrées du tableau, notamment s'il en existe un grand nombre.
- Pour afficher les détails de la notification, cliquez sur le nom de la notification dans le tableau. Une section **Détails** apparaît sous le tableau, où vous pouvez voir l'événement ayant généré la notification.

14.3. Supprimer des notifications

Pour supprimer des notifications :

1. Cliquez sur le bouton  **Notification** situé à droite de la barre de menu, puis cliquez sur **Voir toutes les notifications**. Un tableau contenant toutes les notifications s'affiche.
2. Sélectionnez les notifications que vous voulez supprimer.



3. Cliquez sur le bouton  **Supprimer** en haut du tableau.

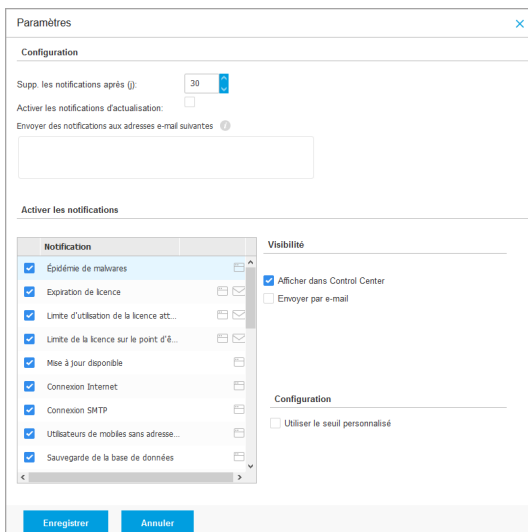
Vous pouvez également configurer la suppression automatique des notifications après un certain nombre de jours. Pour plus d'informations, reportez-vous à [« Configurer les paramètres de notification » \(p. 508\)](#).

14.4. Configurer les paramètres de notification

Le type de notifications à envoyer et les adresses e-mails auxquelles elles sont envoyées peuvent être configurés pour chaque utilisateur.

Pour configurer les paramètres de notification :

1. Cliquez sur le bouton  **Notification** situé à droite de la barre de menu, puis cliquez sur **Voir toutes les notifications**. Un tableau contenant toutes les notifications s'affiche.
2. Cliquez sur le bouton  **Configurer** en haut du tableau. La fenêtre **Paramètres de notification** apparaît.



Paramètres

Configuration

Supp. les notifications après (j): 30

Activer les notifications d'actualisation:

Envoyer des notifications aux adresses e-mail suivantes

Activer les notifications

Notification	Visibilité
<input checked="" type="checkbox"/> Epidémie de malwares	<input checked="" type="checkbox"/> Afficher dans Control Center
<input checked="" type="checkbox"/> Expiration de licence	<input type="checkbox"/> Envoyer par e-mail
<input checked="" type="checkbox"/> Limite d'utilisation de la licence att...	
<input checked="" type="checkbox"/> Limite de la licence sur le point d'é...	
<input checked="" type="checkbox"/> Mise à jour disponible	
<input checked="" type="checkbox"/> Connexion Internet	
<input checked="" type="checkbox"/> Connexion SMTP	
<input checked="" type="checkbox"/> Utilisateurs de mobiles sans adresse...	
<input checked="" type="checkbox"/> Sauvegarde de la base de données	

Configuration

Utiliser le seul personnalisé

Enregistrer Annuler

Paramètres


**Note**

Vous pouvez également accéder à la fenêtre **Paramètres de notification** directement à partir de l'icône  **Configurer** dans l'angle supérieur droit de la fenêtre **Zone de notification**.

3. La section **Configuration** vous permet de définir les paramètres suivants :
 - Suppression automatique des notifications après un certain laps de temps. Configurez le nombre que vous souhaitez entre 0 et 365 dans le champs **Supprimer les notifications après (jours) (days)**.
 - Cochez la case **Activer l'actualisation des notifications** si vous souhaitez que la zone de notifications se mette à jour automatiquement toutes les 60 secondes.
 - De plus, vous pouvez envoyer les notifications par e-mail aux destinataires spécifiques. Saisissez les adresses e-mail dans le champ prévu à cet effet, en appuyant sur la touche **Entrée** après chaque adresse.
4. La section **Activer la notification** vous permet de choisir le type de notifications que vous souhaitez recevoir de la part de GravityZone. Vous pouvez également configurer la visibilité et les options d'envoi séparément pour chaque type de notification.

Sélectionnez le type de notification de votre choix dans la liste. Pour plus d'informations, reportez-vous à « [Types de notifications](#) » (p. 498). Lorsqu'un type de notification est sélectionné, vous pouvez configurer ses options spécifiques (le cas échéant) à droite :

Visibilité

- **Afficher dans la Control Center** spécifie que ce type d'événement est affiché dans la Control Center, à l'aide du bouton  **Notifications**.
- **Log to server** spécifie que ce type d'événement est également envoyé au fichier `syslog` lorsque celui-ci est configuré.

Pour savoir comment configurer les serveurs syslog, référez-vous au guide d'installation de GravityZone.

- **Envoyer par e-mail** spécifie que ce type d'événement est également envoyé à certaines adresses e-mails. Dans ce cas, vous devez indiquer les adresses

e-mail dans le champ correspondant, en appuyant sur **Entrée** après chaque adresse.

Configuration

- **Seuil de détection personnalisé** - permet de définir un seuil pour les événements ayant eu lieu, à partir duquel la notification sélectionnée est envoyée.

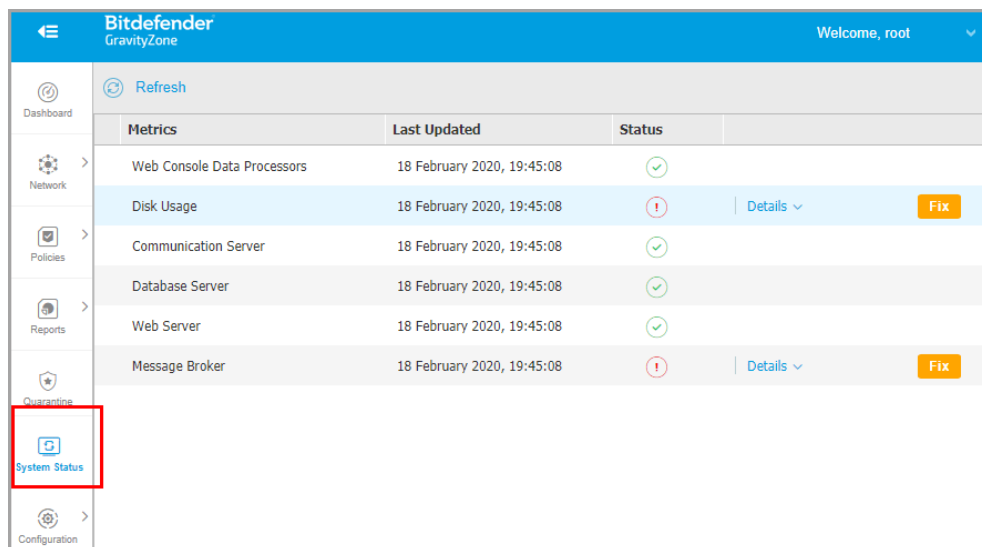
Par exemple, la notification **Épidémie de malwares** est envoyée par défaut aux utilisateurs dont au moins 5% de l'ensemble de leurs éléments administrés sont infectés par le même malware. Pour modifier la sensibilité de la détection antimalware, activez l'option **Seuil de détection personnalisé**, puis indiquez la valeur que vous souhaitez dans le champs **Seuil de déclenchement antimalware**.

- Pour la notification **Sauvegarde de la base de donnée**, vous pouvez choisir d'être averti uniquement lorsqu'une sauvegarde de base de données a échoué. Ne cochez pas cette case si vous souhaitez être informé de tous les événements concernant la sauvegarde d'une base de données.
- Pour l'événement **État du Security Server**, vous pouvez sélectionner les événements Security Server qui déclencheront ce type de notification :
 - **Dépassé** - vous informe à chaque fois qu'un Security Server de votre réseau est obsolète.
 - **Éteint** - vous informe à chaque fois qu'un Security Server de votre réseau a été éteint.
 - **Redémarrage nécessaire** - vous informe à chaque fois qu'un Security Server de votre réseau nécessite un redémarrage.
- Pour l'**État de la tâche**, vous pouvez sélectionner le type d'état qui déclenchera ce type de notification :
 - **Tout état** - informe à chaque fois qu'une tâche envoyée à partir de Control Center est effectuée avec tout état.
 - **Les échecs uniquement** - informe à chaque fois qu'une tâche envoyée à partir de Control Center a échoué.

5. Cliquez sur **Enregistrer**.

15. ÉTAT DU SYSTÈME

La page **État du système** affiche les informations sur l'état du déploiement de GravityZone, vous permettant de facilement détecter tout problème. La page comporte des métriques des systèmes, leur état et leur dernière mise à jour, le tout présenté sur une grille.






Bitdefender GravityZone		Welcome, root	
Refresh			
	Metrics	Last Updated	Status
Network	Web Console Data Processors	18 February 2020, 19:45:08	OK
	Disk Usage	18 February 2020, 19:45:08	Attention Details
Policies	Communication Server	18 February 2020, 19:45:08	OK
	Database Server	18 February 2020, 19:45:08	OK
Reports	Web Server	18 February 2020, 19:45:08	OK
Quarantine	Message Broker	18 February 2020, 19:45:08	Attention Details
Configuration			

Page d'état du système

La colonne **Métrique** affiche tous les indicateurs surveillés par GravityZone Control Center. Pour en apprendre plus sur chaque métrique et sur les messages d'état, voir « [Processeurs de données](#) » (p. 535).

La colonne **Dernière mise à jour** affiche la date et l'heure du dernier contrôle d'état des métriques.

La colonne **État** affiche l'état de chaque métrique :  **OK** ou  **Attention**. L'**État** d'une métrique est mis à jour toutes les 15 minutes ou à chaque fois que vous cliquez sur le bouton  **Actualiser**.

15.1. État OK

L'état OK indique que les métriques se comportent normalement. Aucune autre information n'est affichée dans cette case.

15.2. État Attention

L'état Attention indique que la métrique n'est pas exécutée avec des paramètres normaux.

En ce cas, vous devez poursuivre l'examen pour découvrir ce qu'il s'est passé et corriger les problèmes :

1. Cliquez sur le bouton **Détails** pour afficher les informations complémentaires relatives à la métrique en cours d'examen.

Refresh			
Metrics	Last Updated	Status	
Database Server	09 October 2019, 08:47:08		Details ^
Appliance	Details		
10.17.44.111	The service is inactive since Wed 2019-10-09 08:46:52 UTC; 13s ago		

Détails sur la métrique

- Dans **Appliance**, vous pouvez trouver l'adresse IP des machines affectées.
 - Dans **Détails** vous pouvez voir les informations spécifiques à chaque métrique.
2. Cliquez sur **Corriger** pour modifier la métrique et GravityZone s'occupera du reste.

Database Server		Details ^	Fix
Appliance	Details		
10.17.43.29	The service is inactive since Mon 2020-02-17 16:09:29 UTC; 5min ago		

Détails sur la métrique

L'état de la métrique redeviendra OK une fois celle-ci corrigée.

**Note**

Pour tout autre problème de métrique, contactez l'[équipe de support pour entreprises](#).

15.3. Métriques

La page **System Status** contient des détails sur les métriques suivantes :

- [Processeurs de données de la console web](#)
- [Espace disque utilisé](#)
- [Serveur de communication](#)
- [Serveur de base de données](#)
- [Serveur web](#)
- [Courtier de messages](#)

Processeurs de données de la console web

Cette métrique surveille l'état des processeurs de données utilisés pour compiler les données affichées par Control Center.

Message d'état Attention	Détails
Processeur en échec sur cette appliance : <quantité de processeurs de données> .	Un ou plusieurs processeurs sont arrêtés.
L'appliance virtuelle est injoignable	L'appliance virtuelle utilisant les services de la console web est arrêtée.

Pour obtenir une liste complète des processeurs utilisés par Control Center, voir [« Processeurs de données »](#) (p. 535).

Espace disque utilisé

Cette métrique surveille le volume d'espace disque utilisé sur chaque appliance virtuelle, la quantité d'espace disponible, ainsi que l'espace total sur le disque. Si un disque est utilisé à plus de 80 %, la métrique affiche l'état **Attention**.

Message d'état Attention	Détails
Espace utilisé sur le disque (nom du disque)	Un ou plusieurs disques sont utilisés à plus de 80 % de leur capacité maximale.
L'apppliance virtuelle est injoignable	L'apppliance virtuelle examinée est éteinte.

Serveur de communication

Cette métrique surveille le lien entre les agents de sécurité installés sur vos endpoints et le serveur de base de données.

Message d'état Attention	Détails
Ce service est inactif depuis <horodatage>	Le service s'est arrêté.

Serveur de base de données

Cette métrique surveille l'état de la base de données GravityZone.

Message d'état Attention	Détails
Ce service est inactif depuis <horodatage>	Le service s'est arrêté sur une des appliances.
L'apppliance virtuelle est injoignable	L'apppliance virtuelle utilisant le serveur de base de données est arrêtée.

Serveur web

Cette métrique surveille l'état du serveur web qui héberge GravityZone Control Center.

Message d'état Attention	Détails
Ce service est inactif depuis <horodatage>	Le serveur s'est arrêté sur une des appliances.
L'apppliance virtuelle est injoignable	L'apppliance virtuelle utilisant ce serveur est arrêtée.

Courtier de messages

Cette métrique surveille l'état du service de courtier de message sur les appliances ayant les rôles de Console web et de Communication.

Message d'état Attention	Détails
Le service de courtier de messages de ces appliances est injoignable	Le service s'est arrêté sur une des appliances.
Échec de la connexion réseau entre les appliances :	La connexion entre deux appliances a été interrompue.
L'appliance virtuelle est injoignable	L'appliance virtuelle utilisant ce service est arrêtée.

16. 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.

16.1. 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.

16.2. 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.

16.3. 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.

16.3.1. 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](#)
Pour tout problème lorsque BEST est installé sur l'ordinateur.
- [Problème d'installation](#)
Si BEST n'est pas encore installé sur l'ordinateur et que l'installation échoue.

Méthode en ligne de commande

La ligne de commande permet de collecter des fichiers directement depuis l'ordinateur affecté. Cette méthode est à privilégier dans les cas où vous ne pouvez pas accéder au Centre de contrôle GravityZone ou lorsque l'ordinateur ne communique pas avec la console.

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.

Pour envoyer les fichiers journaux à l'équipe de support Bitdefender dédiée aux entreprises, accédez au dossier C:\Windows\Temp ou à l'emplacement choisi et sélectionnez le fichier d'archive nommé ST_[nomordinateur]_[datedujour]. Joignez l'archive à votre ticket de support pour que la procédure de dépannage puisse se poursuivre.

Problème d'installation

1. Pour télécharger l'Outil Support BEST, cliquez [ici](#).
2. Exécuter le fichier en tant qu'administrateur. Une fenêtre s'ouvre.
3. Choisissez l'emplacement où enregistrer l'archive des fichiers journaux.

Pendant la collecte des fichiers une barre de progression s'affichera sur l'écran. Une fois le processus achevé, le nom de l'archive et son emplacement apparaissent à l'écran.

Pour envoyer les fichiers journaux à l'équipe de support Bitdefender dédiée aux entreprises, accédez à l'emplacement choisi et sélectionnez le fichier d'archive nommé ST_[nomordinateur]_[datedujour]. Joignez l'archive à votre ticket de support pour que la procédure de dépannage puisse se poursuivre.

16.3.2. 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

16.3.3. 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.

16.4. Contact

Une communication efficace est la clé d'une relation réussie. Au cours des 18 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.

16.4.1. 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>

16.4.2. 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.

16.4.3. 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.com

Site 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.fr

Site 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.es

Site 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) 2304 99 93 004

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

Orhideea Towers
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; z1?; zoo

A.2. États et types d'objets du réseau

A.2.1. Types d'objets du réseau

Chaque type d'objet disponible sur la page **Réseau** est représenté par une icône spécifique.

Vous trouverez dans le tableau ci-après l'icône et la description de tous les types d'objets disponibles.

Icône	Type
	Groupe de réseau
	Ordinateur
	Ordinateur relais
	Ordinateur Serveur Exchange
	Ordinateur Serveur Exchange Relais
	Machine virtuelle
	Machine virtuelle relais
	Image principale
	Machine virtuelle Serveur Exchange
	Machine virtuelle Serveur Exchange Relais
	Machine virtuelle avec vShield
	Machine virtuelle relais avec vShield
	Inventaire Nutanix
	Nutanix Prism
	Cluster Nutanix
	Inventaire VMware
	VMware vCenter
	Datacenter VMware

Icône	Type
	Pool de ressources VMware
	Cluster VMware
	Inventaire Citrix
	XenServer
	Pool Xen
	Inventaire Amazon EC2
	Intégration à Amazon EC2
	Région Amazon EC2 / Microsoft Azure
	Zone de disponibilité d'Amazon EC2 / de Microsoft Azure
	Inventaire Microsoft Azure
	Intégration Microsoft Azure
	Security Server
	Security Server avec vShield
	Hôte sans Security Server
	Hôte avec Security Server
	VMware vApp
	Utilisateur d'appareil mobile
	Appareil mobile









A.2.2. États des objets du réseau

Chaque objet du réseau peut avoir différents états, concernant l'état d'administration, les problèmes de sécurité, la connectivité, etc. Vous trouverez dans le tableau suivant toutes les icônes d'état existantes ainsi que leur description.



Note

Le tableau ci-dessous contient quelques exemples d'état génériques. Les mêmes états peuvent s'appliquer, seuls ou combinés, à tous les types d'objets du réseau tels que les groupes du réseau, les ordinateurs, etc.

Icône	État
	Hôte sans serveur de sécurité, Déconnecté
	Machine virtuelle, Hors connexion, Non administrée
	Machine virtuelle, En ligne, Non administrée
	Machine virtuelle, En ligne, Administrée
	Machine virtuelle, En ligne, Administrée, Avec des problèmes
	Machine virtuelle, redémarrage en attente
	Machine virtuelle, Suspendue
	Machine virtuelle, Supprimée

A.3. Types de fichiers d'applications

Les moteurs d'analyse antimalware incluent dans les solutions de sécurité Bitdefender peuvent être configurés pour limiter l'analyse aux fichiers d'applications (ou de programmes). Les fichiers d'applications sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers.

Cette catégorie comprend des fichiers avec les extensions suivantes :

386; a6p; ac; accda; accddb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; iso; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; ps1; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk;

ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

A.4. Types de fichiers du filtrage des pièces jointes

Le module Contrôle de Contenu fourni par Security for Exchange peut filtrer des pièces jointes d'e-mail en fonction du type de fichier. Les types de fichier disponibles dans Control Center incluent les extensions suivantes :

Fichiers exécutables

386; acm; ax; com; cpl; dll; drv; exe; flt; fon; lrc; ocx; scr; sys; vxd; x32

Images

bmp; cal; dcx; drw; ds4; eps; gif; gx2; ico; img; jfif; jpe; jpeg; jpg; pat; pcx; pgm; png; psd; psp; rgb; sdr; sh3; shw; sym; tif; tiff; wpg

Multimédia

3g2; 3gg; asf; au; avi; mid; mmf; mov; mp3; mpeg; mpg; ogg; qt; ra; ram; rm; swf; wav; wpl

Archives

7z; ain; arc; arj; bz; bz2; cab; cpio; cru; crush; gz; hap; img; jar; lha; lzh; pak; ppz; rar; rpm; sit; snp; tar; tar.z; tb2; tbz2; tgz; ufa; z; zip; zoo

Feuilles de calcul

fm3; ods; wk1; wk3; wks; xls; xlsx

Présentations

odp; pps; ppt; pptx

Documents

doc; docx; dtd; htm; html; odt; pcx; pdf; qxd; rtf; wks; wpf; ws; ws2; xml

A.5. Variables du système

Certains paramètres disponibles dans la console requièrent de spécifier le chemin sur les ordinateurs cibles. Il est recommandé d'utiliser les variables du système

(le cas échéant) afin de s'assurer que le chemin soit valide sur tous les ordinateurs cibles.

Voici la liste des variables du système prédéfinies :

`%ALLUSERSPROFILE%`

Le dossier de profil All Users. Chemin typique :

`C:\Documents and Settings\All Users`

`%APPDATA%`

Le dossier Application Data de l'utilisateur connecté. Chemin typique :

`C:\Users\{username}\AppData\Roaming`

`%LOCALAPPDATA%`

Les fichiers temporaires d'applications. Chemin typique :

`C:\Users\{username}\AppData\Local`

`%PROGRAMFILES%`

Le dossier Program Files. Le chemin d'accès est généralement `C:\Program Files`.

`%PROGRAMFILES(X86)%`

Le dossier Program Files pour les applications 32 bits (sur les systèmes 64 bits). Chemin typique :

`C:\Program Files (x86)`

`%COMMONPROGRAMFILES%`

Le dossier Fichiers communs. Chemin typique :

`C:\Program Files\Common Files`

`%COMMONPROGRAMFILES(X86)%`

Le dossier Fichiers communs pour les applications 32 bits (sur les systèmes 64 bits). Chemin typique :

`C:\Program Files (x86)\Common Files`

`%WINDIR%`

Le répertoire Windows ou SYSROOT. Le chemin d'accès est généralement `C:\Windows`.

%USERPROFILE%

Le chemin vers le dossier du profil utilisateur. Chemin typique :

C:\Users\{username}

Sur macOS, le dossier de profil de l'utilisateur est le dossier Home. Utilisez \$HOME ou ~ lors de la configuration des exclusions.

A.6. Outils du Contrôle des applications

Pour définir les règles du Contrôle des applications sur la base du hash de l'exécutable ou de l'empreinte numérique du certificat, vous devez télécharger les outils suivants :

- **Empreinte digitale**, pour obtenir la valeur personnalisée du hash.
- **Empreinte numérique**, pour obtenir la valeur personnalisée de l'empreinte numérique du certificat.

Empreinte digitale

Cliquez [ici](#) pour télécharger l'exécutable d'empreinte digitale, ou rendez-vous sur <http://download.bitdefender.com/business/tools/ApplicationControl/>

Pour obtenir le hash de l'application :

1. Ouvrez la fenêtre **Invite de commandes**.
2. Naviguez jusqu'à l'emplacement de l'outil Empreinte digitale. Par exemple :

```
cd/users/fingerprint.exe
```

3. Pour afficher la valeur de hash d'une application, exécutez la commande suivante :

```
fingerprint <application_full_path>
```

4. Retournez sur Control Center et configurez la règle sur la base de la valeur que vous avez obtenue. Pour plus d'informations, reportez-vous à « [Contrôle des applications](#) » (p. 346).

Empreinte numérique

Cliquez [ici](#) pour télécharger l'exécutable d'empreinte numérique, ou rendez-vous sur <http://download.bitdefender.com/business/tools/ApplicationControl/>

Pour obtenir l'empreinte numérique du certificat :

1. Exécutez l'**Invite de commandes** en tant qu'administrateur.
2. Naviguez jusqu'à l'emplacement de l'outil Empreinte numérique. Par exemple :

```
cd/users/thumbprint.exe
```

3. Pour afficher l'empreinte numérique du certificat, exécutez la commande suivante :

```
thumbprint <application_full_path>
```

4. Retournez sur Control Center et configurez la règle sur la base de la valeur que vous avez obtenue. Pour plus d'informations, reportez-vous à « [Contrôle des applications](#) » (p. 346).

A.7. Objets de Sandbox Analyzer

A.7.1. Types et extensions de fichier pris en charge pour l'envoi manuel

Les extensions de fichier suivantes sont prises en charge et peuvent être détonées manuellement dans Sandbox Analyzer :

Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (exécutable), PDF, PEF (exécutable), PIF (exécutable), RTF, SCR, URL (binaire), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

Sandbox Analyzer est capable de détecter les types de fichiers mentionnés ci-dessus, mais aussi lorsqu'ils sont inclus dans les types de dossiers suivants : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, dossier

compressé LZMA, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.

A.7.2. Types de fichier pris en charge par le préfiltrage de contenu lors de l'envoi automatique

Le préfiltrage de contenu déterminera le type d'un fichier en combinant le contenu et l'extension de l'objet. Ainsi, un exécutable avec l'extension `.tmp` sera reconnu comme une application et, si il est détecté comme étant suspect, il sera envoyé à Sandbox Analyzer.

- Applications - fichiers au format PE32, notamment, mais sans s'y limiter, les extensions suivantes : `exe`, `dll`, `com`.
- Documents - fichiers au format document, notamment, mais sans s'y limiter, les extensions suivantes : `xlsx`, `xls`, `ppt`, `doc`, `docx`, `dot`, `chm`, `xlm`, `docm`, `dotm`, `potm`, `potx`, `ppam`, `ppax`, `pps`, `ppsm`, `pptx`, `sldm`, `sldx`, `xlam`, `xlm`, `xltm`, `rtf`, `pdf`.
- Scripts : `ps`, `wsf`, `ws`, `php`, `py`, `js`, `vb`, `vbs`, `pyc`, `pyo`, `wsc`, `wsh`, `pscl`, `jse`, `vbe`.
- Archives : `zip`, `jar`, `7z`, `bz`, `bz2`, `tgz`, `msi`, `rar`, `rev`, `z`, `arj`, `iso`, `lha`, `lhz`, `uu`, `uue`, `xxe`, `lzma`, `ace`, `r00`.
- E-mails (sauvegardés dans le système de fichiers) : `eml`, `tnef`.

A.7.3. Exclusions par défaut de l'envoi automatique

`asc`, `avi`, `bmp`, `gif`, `jpeg`, `jpg`, `mkv`, `mp4`, `pgp`, `png`, `txt`.

A.7.4. Applications recommandées pour les VM de détonation

Sandbox Analyzer On-Premises nécessite que certaines applications soient installées sur les machines virtuelles de détonation pour qu'elles puissent ouvrir les échantillons envoyés.

Applications	Types de fichiers
Suite Microsoft Office	<code>xls</code> , <code>xltm</code> , <code>xltx</code> , <code>ppt</code> , <code>doc</code> , <code>dotx</code> , <code>docm</code> , <code>potm</code> , <code>potx</code> , <code>ppam</code> , <code>ppax</code> , <code>pps</code> , <code>ppsm</code> , <code>ppsx</code>

Applications	Types de fichiers
Adobe Flash Player	swf
Adobe Acrobat Reader	pdf
Outils Windows par défaut	bat, cmd, ws, wsf, reg, exe, dll, lnk, com, chm, application, gadget, hta, cpl, msc, vbe, jse, wsc, wsh, psc1, scf, vb, vbs, pif
7zip WinZip WinRAR	7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue
Google Chrome Internet Explorer	html, url
Python	py, pyc, pyp
Mozilla Thunderbird Microsoft Outlook	eml

A.8. Processeurs de données

Nom	Détails
Transmetteur de requête au processeur	Transfère les demandes du processeur dans les environnements distribués
Intégrateur VMware Hypervision	Synchronise l'inventaire VMware et d'autres informations avec GravityZone
Intégrateur Citrix Hypervisor	Synchronise l'inventaire Xen et d'autres informations avec GravityZone
Intégrateur de virtualisation générique	Synchronise l'inventaire Nutanix, Amazon EC2 et Azure avec GravityZone
Intégrateur NTSA	Synchronise l'état de l'intégration Network Traffic Security Analytics (NTSA) et envoie les mises à jour de licence à l'appliance NTSA
Synchronisateur d'inventaire des ordinateurs Active Directory	Synchronise l'inventaire Active Directory de l'ordinateur avec GravityZone

Nom	Détails
Synchronisateur d'inventaire des groupes Active Directory	Synchronise l'inventaire des groupes Active Directory avec GravityZone
Synchronisateur d'importation des utilisateurs Active Directory	Synchronise les comptes utilisateurs Active Directory avec GravityZone (utilisé pour lier des comptes AD à des comptes GravityZone)
Synchronisateur d'inventaire des utilisateurs Active Directory	Synchronise l'inventaire des utilisateurs Active Directory avec GravityZone
Processeur d'e-mails	Met les e-mails en file d'attente pour envoi par GravityZone
Processeur des rapports	Traite les rapports et portlets
Système de déploiement de l'agent de sécurité Windows	Déploie l'agent de sécurité Bitdefender sur les appareils Windows
Système de déploiement du serveur de sécurité	Déploie les appliance virtuelle de sécurité
Gestionnaire des licences	Gère les licences des endpoints installés
Processeur des notifications push mobiles	Envoie des notifications push aux appareils mobiles protégés
Système de déploiement de l'agent de sécurité Linux et macOS	Déploie l'agent Bitdefender GravityZone Enterprise Security for Virtualized Environments (SVE) sur les appareils Linux et macOS
Kits d'endpoint et utilitaire de mise à jour de produit	Télécharge et diffuse les kits et mises à jour de produit d'endpoint Bitdefender
GravityZone Updater	Met automatiquement à jour GravityZone lorsqu'il est configuré. Met à jour la version des appliances virtuelles de GravityZone
Nettoyeur de package	Supprime les fichiers de package inutilisés
Processeur des problèmes de Sécurité	Traite les problèmes de sécurité pour les éléments de la section Réseau
Processeur de secours	Réalise des copies de sauvegarde de la base de données GravityZone
Processeur des notifications	Envoie des notifications aux utilisateurs

Nom	Détails
Processeur des événements système	Traite les événements de l'infrastructure (contrôle des applications, Sandbox Analyzer, Serenity, SVA) ou des intégrations (Exchange, Nutanix, NSX)
Système de déploiement du package complémentaire HVI	Traite l'installation, la mise à jour et la suppression du pack supplémentaire HVI pour les hôtes XEN
Processeur tâche de redémarrage HVI	Gère les tâches de redémarrage sur les hôtes HVI
Processeur de l'alimentation et de l'état de la connexion	Calcule l'état de l'alimentation et de la connectivité des ordinateurs et machines virtuelles
Processeur de nettoyage des machines hors ligne	Supprime les machines hors ligne du réseau
Exécuteur de tâches en arrière-plan	Gère et exécute les tâches et processus en tâche de fond

Glossaire

Archive

Une disquette, une bande, ou un répertoire qui contient des fichiers qui ont été sauvegardés.

Un fichier qui contient un ou plusieurs fichiers dans un format compressé.

Attaques ciblées

Les cyberattaques qui visent essentiellement des avantages financiers ou l'atteinte à une réputation. La cible peut être un individu, une société, un logiciel ou un système, minutieusement étudié avant que l'attaque ne survienne. Ces attaques s'étalent sur la durée et par étapes, via un ou plusieurs points d'infiltration. Ils passent presque inaperçus et sont détectés, généralement, lorsque le mal est déjà fait.

Bootkit

Un bootkit est un programme malveillant qui a la capacité d'infecter le master boot record (MBR), le volume boot record (VBR) ou le secteur de démarrage. Un bootkit reste actif même après un redémarrage.

Conflit de ressources d'analyse antimalware

Utilisation intensive des ressources système se produisant lorsque le logiciel antivirus analyse simultanément plusieurs machines virtuelles sur un seul hôte physique.

Cookie

Sur Internet, les cookies sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des cookies est encore en développement et l'intention est de cibler directement ce que vous avez dit être vos intérêts. C'est une arme à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent car vous voyez seulement les annonces vous intéressant. Mais cela implique également le "pistage" et le "suivi" des sites que vous consultez et de ce sur quoi vous cliquez. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple "numéro SKU" (le code barres se trouvant

au dos des produits). Bien que ce point de vue puisse paraître extrême, il est parfois justifié.

Downloader Windows

Il s'agit d'un nom générique donné à un programme ayant comme fonction principale de télécharger des contenus à fin malveillante ou indésirable.

Enregistreur de frappe

Application qui enregistre tout ce qui est tapé.

Les enregistreurs de frappe ne sont pas nécessairement malveillants. Ils peuvent être utilisés à des fins légitimes, comme pour surveiller les activités d'employés ou d'enfants. Ils sont toutefois de plus en plus utilisés par les cybercriminels à des fins malveillantes (par exemple, pour recueillir des informations confidentielles, telles que des identifiants de connexion ou des numéros d'assurance sociale).

Événements

Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme le manque de mémoire.

Exploits

Par exploit, on entend généralement toute méthode utilisée pour gagner un accès non autorisé à des ordinateurs ou une vulnérabilité dans la sécurité d'un système qui le rend susceptible d'être attaqué.

Extension de fichier

La partie d'un fichier, après le point final, qui indique le type de données stockées dans le fichier.

De nombreux systèmes d'exploitation utilisent des extensions de fichiers, par exemple Unix, VMS, MS-DOS. Elles comportent communément une à trois lettres (certains anciens OS n'en supportent pas plus de trois). Exemples: ".c" pour du code source en C, ".ps" pour PostScript, ".txt" pour du texte.

Fausse alerte

Se produit lorsqu'une analyse identifie un fichier comme infecté alors qu'il ne l'est pas.

Fichier journal (Log)

Fichier qui enregistre les actions ayant eu lieu. La Bitdefender maintient un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.

Fichiers suspects et trafic réseau

Les fichiers suspects sont ceux dont la réputation sème le doute. Ce classement repose sur de nombreux facteurs, parmi lesquels : l'existence d'une signature numérique, le nombre d'occurrences dans les réseaux informatiques, l'emballage utilisé, etc. Le trafic de réseau est considéré comme étant suspect, lorsqu'il s'écarte du modèle type. Par exemple, une source peu fiable, des demandes de connexion à des ports inhabituels, une hausse de l'utilisation de la bande passante, des horaires de connexion aléatoires, etc.

Grayware

Une classe d'applications logicielles entre les logiciels licites et les malware. Bien qu'ils ne soient pas aussi nuisibles que les malware qui affectent l'intégrité du système, leur comportement est tout de même dérangentant et provoque des situations non voulues, telles que le vol et l'usage non autorisé de données, et la publicité indésirable. Les applications grayware les plus communes sont les [spyware](#) et les [adware](#).

Heuristique

Méthode basée sur des règles permettant d'identifier de nouveaux virus. Cette méthode d'analyse ne s'appuie pas sur des définitions virales spécifiques. L'avantage de l'analyse heuristique est de pouvoir détecter les variantes d'un virus existant. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.

IP

Protocole Internet - Un protocole routable de la suite de protocoles TCP/IP chargé de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.

Ligne de commande

Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.

Malwares

« Malware » est un terme générique regroupant les logiciels conçus pour faire du tort ; il s'agit de la contraction de « malicious software » (logiciels malveillants) L'emploi de ce terme n'est pas encore universel, mais sa popularité pour désigner les virus, les chevaux de Troie, les vers et les codes mobiles malveillants progresse.

Mise à jour

Nouvelle version d'un logiciel ou d'un produit hardware, destinée à remplacer une version antérieure du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, et si ce n'est pas le cas, la mise à jour ne se fait pas.

Bitdefender a son propre module de mise à jour permettant à l'utilisateur de rechercher manuellement les mises à jour ou de les programmer automatiquement.

Navigateur

Raccourci pour navigateur internet, il s'agit d'un logiciel utilisé pour visualiser des pages Web.

Niveaux de protection

GravityZone vous protège grâce à une série de modules et de rôles, appelés couches de protection. On distingue la protection des endpoints, ou protection de base, et la protection assurée par différents modules complémentaires. La protection des endpoints englobe les modules suivants : Antimalware, Advanced Threat Control, Advanced Anti-Exploit, Firewall, Content Control, Device Control, Network Attack Defense, Power User et Relay. Notre solution inclut aussi des couches de protection supplémentaires comme Security for Exchange et Sandbox Analyzer.

Pour plus d'informations sur les couches de protection comprises dans votre solution GravityZone, consultez « [Couches de protection de GravityZone](#) » (p. 2).

Non-heuristique

Cette méthode d'analyse utilise les définitions spécifiques des virus. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut sembler être un virus et ne génère donc pas de fausses alertes.

Phishing

Action d'envoyer un e-mail à un utilisateur en prétendant être une entreprise connue dans le but d'obtenir frauduleusement des informations privées qui permettront d'utiliser l'identité du destinataire de l'e-mail. Cet e-mail oriente l'utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n'a pour objectif que de voler les informations de l'utilisateur.

Port

Une interface sur un ordinateur auquel vous pouvez connecter un appareil. Les ordinateurs comportent plusieurs sortes de ports. Il existe plusieurs ports internes permettant de connecter des lecteurs de disques, des écrans et des claviers. A l'extérieur, les ordinateurs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques.

Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.

Portes dérobées

Il s'agit d'une faille dans la sécurité d'un système délibérément laissée en place par des développeurs ou des personnes chargées de la maintenance. Les intentions ne sont pas toujours malveillantes ; quelques systèmes d'exploitation, par exemple, permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.

Publiciels

Les publiciels sont souvent associés à des applications gratuites mais exigeant leur acceptation par l'utilisateur. Ces publiciels étant généralement installés une fois que l'utilisateur en a accepté le principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux.

Cependant, les fenêtres publicitaires peuvent devenir contrariantes et, dans certains cas, nuire aux performances du système. De plus, les informations collectées peuvent mettre en péril la vie privée des utilisateurs qui n'ont pas totalement pris connaissance des termes de l'accord de licence.

Ransomwares

Un malware qui vous bloque sur votre ordinateur ou bloque l'accès à vos fichiers et applications. Le ransomware exigera que vous payez une certaine somme (paiement de rançon) en échange d'une clé de déchiffrement qui vous permet de retrouver l'accès à votre ordinateur ou à vos fichiers.

Rootkit

Un rootkit est un ensemble d'outils logiciels permettant un accès de niveau administrateur à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX et se réfère à des outils recompilés fournissant des droits administrateurs "intrusifs", permettant de cacher leur présence aux administrateurs système.

Le principal rôle des rootkits est de masquer des processus, des fichiers, des logins et des logs. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseau ou des périphériques, s'ils incluent les logiciels appropriés.

Les rootkits ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des rootkits. Cependant, ils sont principalement utilisés pour camoufler des codes malveillants ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des codes malveillants, les rootkits sont une menace importante contre l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, créer des portes dérobées sur le système, modifier des fichiers et des logs et passer inaperçus.

Scripts

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.

Secteur de boot :

Secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, du cluster, etc). Pour les disques de démarrage, le secteur d'amorçage contient aussi un programme qui charge le système d'exploitation.

Signature du malware

Les signatures de malwares sont des fragments de codes extraits à partir de malwares réels. Elles sont utilisées par les programmes antivirus pour rechercher certaines caractéristiques et détecter les malwares. Les signatures

sont également utilisées pour supprimer le code malveillant des fichiers infectés.

La base de données de signatures de malwares de Bitdefender rassemble des signatures de malwares mises à jour toutes les heures par les chercheurs de malwares de Bitdefender.

Spam

Messages électroniques ou messages de groupes de discussion indésirables. Souvent répertoriés comme des emails non sollicités.

Spywares

Tout type de logiciel récupérant les informations des utilisateurs via leur connexion Internet à leur insu, généralement à des fins publicitaires. Les logiciels espions sont généralement cachés dans des partagiels et logiciels gratuits pouvant être téléchargés sur Internet. Notons toutefois que la plupart des partagiels et logiciels gratuits ne contiennent pas de logiciels espions. Une fois installé, le logiciel espion surveille l'activité de l'utilisateur sur Internet et transmet discrètement ces informations à une tierce personne. Les spywares peuvent également récupérer des informations sur les adresses mail, les mots de passe ou même, les numéros de cartes bancaires.

Leur point commun avec les chevaux de Troie est le fait que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une des manières les plus classiques d'être victime de logiciels espions est de télécharger des logiciels de partage de fichiers (Peer to peer).

En plus des questions d'éthique et de respect de la vie privée, les logiciels espions volent les ressources de l'ordinateur de l'utilisateur en utilisant sa bande passante lors de l'envoi d'informations à leur base via la connexion Internet. En raison de cette utilisation de la mémoire et des ressources du système, les applications qui fonctionnent en tâche de fond peuvent aller jusqu'à entraîner des plantages ou provoquer une instabilité globale du système.

TCP/IP

Transmission Control Protocol/Internet Protocol - Ensemble de protocoles réseau utilisés largement sur Internet assurant la communication entre des réseaux interconnectés d'ordinateurs avec diverses architectures matérielles et divers systèmes d'exploitation. TCP/IP inclut des standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

Trojan (Cheval de Troie)

Programme destructeur qui prétend être une application normale. Contrairement aux virus, les chevaux de Troie ne se répliquent pas, mais ils peuvent être tout aussi destructeurs. Un des types de chevaux de Troie les plus insidieux est un logiciel qui prétend désinfecter votre PC mais qui au lieu de cela l'infecte.

Le terme provient de la fameuse histoire de l'Illiade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Troyens, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.

Ver

Programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure de sa propagation. Il ne peut pas se joindre à d'autres programmes.

Virus

Programme ou morceau de code chargé dans votre ordinateur à votre insu et qui fonctionne contre votre gré. La plupart des virus peuvent également se répliquer. Tous les virus informatiques sont créés par des personnes. Un virus simple peut se copier très rapidement et sans arrêt et est relativement facile à créer. Même un virus simple comme celui décrit est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est par exemple capable de se transmettre via un réseau et de déjouer les systèmes de sécurité.

Virus d'amorçage

Virus qui infecte le secteur d'amorçage d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus d'amorçage rendra le virus actif en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez le virus actif en mémoire.

Virus Macro

Type de virus codé sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent de puissants langages macro.

Ces applications vous permettent d'intégrer une macro dans un document, et de le faire s'exécuter chaque fois que le document est ouvert.

Virus polymorphique

Virus qui change de forme avec chaque fichier qu'il infecte. Ces virus n'ayant pas de forme unique bien définie, ils sont plus difficiles à identifier.

Voleur de mots de passe

Un voleur de mots de passe collecte des informations telles que les identifiants de compte et les mots de passe associés. Ces identifiants volés sont ensuite utilisés à des fins malveillantes, comme la prise de contrôle de compte.

Zone de notification

Introduite avec Windows 95, la zone de notification se situe dans la barre de tâches Windows (en général, à côté de l'horloge) et contient des icônes miniatures permettant d'accéder facilement aux fonctions système : télécopieur, imprimante, modem, volume, etc. Double-cliquez ou faites un clic-droit sur une icône pour afficher les options.