

Bitdefender® ENTERPRISE

**BITDEFENDER
SECURITY FOR
ENDPOINTS
(CONSOLE DANS LE
CLOUD)**

Guide de l'administrateur >>

Bitdefender Security for Endpoints (Console dans le Cloud)

Guide de l'administrateur

Date de publication 2014.04.16

Copyright© 2014 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. L'inclusion de courtes citations dans des tests n'est possible qu'avec la mention de la source. Le contenu ne peut en aucun cas être modifié.

Avertissement. Ce produit et sa documentation sont protégés par copyright. Les informations de 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

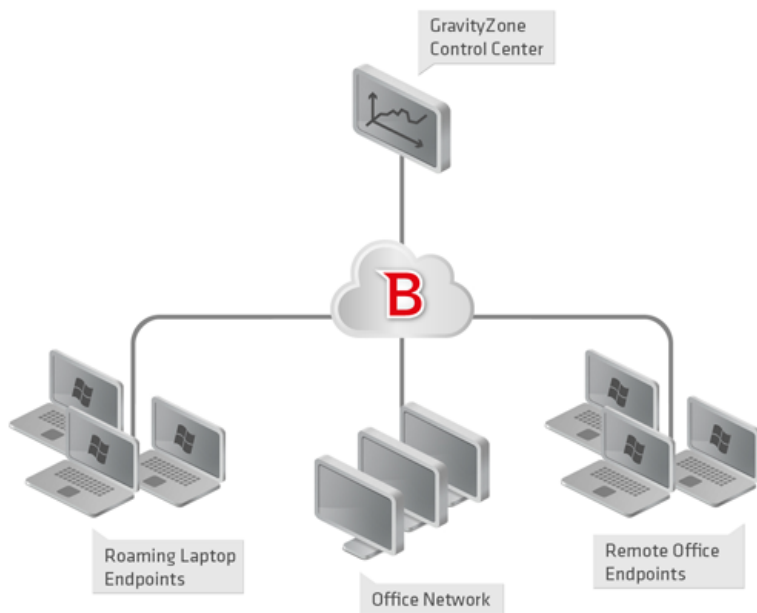
1. À propos de Security for Endpoints (Console dans le Cloud)	1
2. Pour démarrer	3
2.1. Connexion au Control Center	3
2.2. Le Control Center en un coup d'œil	4
2.2.1. Présentation du Control Center	4
2.2.2. Données du tableau	5
2.2.3. Barres d'outils d'actions	6
2.2.4. Menu contextuel	7
2.3. Gérer votre compte	7
2.4. Changer de mot de passe de connexion	8
3. Gestion des licences	9
3.1. Activer une licence	9
3.2. Vérification des détails de la licence actuelle	10
4. Gestion des comptes utilisateurs	11
4.1. Rôles Utilisateur	12
4.2. Droits de l'utilisateur	13
4.3. Créer des comptes utilisateurs	13
4.4. Modification des comptes	14
4.5. Supprimer des comptes	15
4.6. Réinitialiser les mots de passe de connexion	15
5. Installation de Security for Endpoints	16
5.1. Configuration requise	17
5.1.1. Systèmes d'exploitation pris en charge	17
5.1.2. Matériel	18
5.1.3. Navigateurs pris en charge	18
5.2. Préparation de l'Installation	19
5.3. Installation locale	19
5.3.1. Création de packages d'installation d'Endpoint Security	20
5.3.2. Téléchargement de packages d'installation	22
5.3.3. Exécution de packages d'installation	23
5.4. Installation à distance	23
5.4.1. Configuration requise à l'installation d'Endpoint Security à distance	24
5.4.2. Exécution des tâches d'installation d'Endpoint Security à distance	24
5.5. Fonctionnement de Network Discovery	27
5.5.1. Plus d'informations sur le service Explorateur d'ordinateurs de Microsoft	28
5.5.2. Configuration requise pour la découverte du réseau	29
6. Gestion des ordinateurs	31
6.1. Vérifier l'état de l'ordinateur	32
6.1.1. Ordinateurs administrés, non administrés et supprimés	32

6.1.2. Ordinateurs en ligne et hors connexion	33
6.1.3. Ordinateurs avec des problèmes de sécurité	34
6.2. Organiser les ordinateurs dans des groupes	34
6.3. Afficher des informations sur un ordinateur	36
6.4. Trier, filtrer et rechercher des ordinateurs	38
6.4.1. Trier des ordinateurs	38
6.4.2. Filtrer des ordinateurs	38
6.4.3. Recherche d'ordinateurs	41
6.5. Exécuter des tâches sur des ordinateurs	41
6.5.1. Analyse	42
6.5.2. Installer Client	49
6.5.3. Modifier le programme d'installation	52
6.5.4. Désinstaller Client	53
6.5.5. Mettre à jour le client	53
6.5.6. Redémarrer votre ordinateur.	54
6.5.7. Découverte du réseau	54
6.6. Créer des rapports rapides	55
6.7. Affecter des politiques	55
6.8. Supprimer des ordinateurs de l'inventaire du réseau	56
6.8.1. Exclure des ordinateurs de l'inventaire du réseau	56
6.8.2. Supprimer définitivement des ordinateurs	57
6.9. Packages d'installation	58
6.9.1. Créer des packages d'installation	58
6.9.2. Téléchargement de packages d'installation	61
6.10. Afficher et gérer des tâches	62
6.10.1. Vérifier l'état d'une tâche	62
6.10.2. Afficher les rapports sur les tâches	64
6.10.3. Relancer des tâches	64
6.10.4. Supprimer des tâches	65
6.11. Admin. des authentifications	65
6.11.1. Ajouter des identifiants dans l'Administrateur des authentifications	66
6.11.2. Supprimer les identifiants de l'Administrateur des authentifications	66
7. Politiques de sécurité	67
7.1. Administration des politiques	68
7.1.1. Création de politiques	68
7.1.2. Modification des paramètres de la politique	69
7.1.3. Renommer des politiques	69
7.1.4. Suppression de politiques	70
7.1.5. Affecter des politiques à des objets du réseau	70
7.2. Politiques de l'ordinateur	72
7.2.1. Général	72
7.2.2. Antimalware	80
7.2.3. Pare-feu	96
7.2.4. Contrôle de contenu	105
8. Tableau de bord de supervision	116
8.1. Actualiser les données du portlet	117
8.2. Modification des paramètres d'un portlet	117
8.3. Ajouter un nouveau portlet	117

8.4. Suppression d'un portlet	118
8.5. Réorganiser les portlets	118
9. Utilisation des rapports	119
9.1. Types de rapports disponibles	119
9.2. Création de rapports	122
9.3. Afficher et gérer des rapports planifiés	123
9.3.1. Afficher les rapports	124
9.3.2. Modifier les rapports planifiés	125
9.3.3. Supprimer les rapports planifiés	126
9.4. Enregistrer des rapports	126
9.4.1. Exportation de rapports	126
9.4.2. Télécharger des Rapports	127
9.5. Envoyer des rapports par e-mail	127
9.6. Impression des rapports	128
10. Quarantaine	129
10.1. Navigation et Recherche	130
10.2. Restaurer les fichiers en quarantaine	130
10.3. Suppression automatique des fichiers en quarantaine	131
10.4. Supprimer les fichiers en quarantaine	131
11. Journal d'activité de l'utilisateur	133
12. Notifications	135
12.1. Types de notifications	135
12.2. Afficher les notifications	136
12.3. Supprimer des notifications	137
12.4. Configurer les paramètres de notification	137
13. Obtenir de l'aide	139
13.1. Centre de support de Bitdefender	139
13.2. Demande d'aide	140
13.3. Utiliser l'Outil de Support	140
13.4. Contacts	142
13.4.1. Adresses Web	142
13.4.2. Bureaux de Bitdefender	142
A. Annexes	145
A.1. Liste des types de fichier d'Application	145
A.2. Utilisation des variables du système	145
Glossaire	147

1. À propos de Security for Endpoints (Console dans le Cloud)

Security for Endpoints (Console dans le Cloud) est un service de protection antimalware développé par Bitdefender pour les ordinateurs avec systèmes d'exploitation Microsoft Windows et Macintosh. Il utilise un modèle de déploiement multiple centralisé en mode SaaS, adapté aux entreprises, tout en bénéficiant des technologies de protection antivirus éprouvées et développées par Bitdefender pour le marché des particuliers.



L'architecture de Security for Endpoints (Console dans le Cloud)

La console d'administration est hébergée sur le cloud public de Bitdefender. Les abonnés ont accès à une console d'administration Web nommée **Control Center**. Depuis cette interface, les administrateurs peuvent installer et administrer à distance la protection antimalware sur tous leurs ordinateurs Windows et Macintosh tels que : les serveurs et postes de travail du réseau interne, les ordinateurs portables ou les postes de bureaux distants.

Une application locale nommée **Endpoint Security** est installée sur chaque ordinateur protégé. Les utilisateurs locaux ont une visibilité limitée et un accès en lecture seule aux paramètres de sécurité, qui sont administrés de façon centrale par l'administrateur depuis le Control Center; alors que les analyses, les mises à jour et les modifications de configuration sont généralement effectuées en tâche de fond.

2. Pour démarrer

Les fonctionnalités de Security for Endpoints (Console dans le Cloud) 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.

2.1. 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+
- Résolution d'écran recommandée : 1024x768 ou supérieure

Pour se connecter à la Control Center :

1. Ouvrez votre navigateur web.
2. Rendez-vous à l'adresse suivante : <https://gravityzone.bitdefender.com>
3. Indiquez l'adresse e-mail et le mot de passe de votre compte.
4. Cliquez sur **Connexion**.

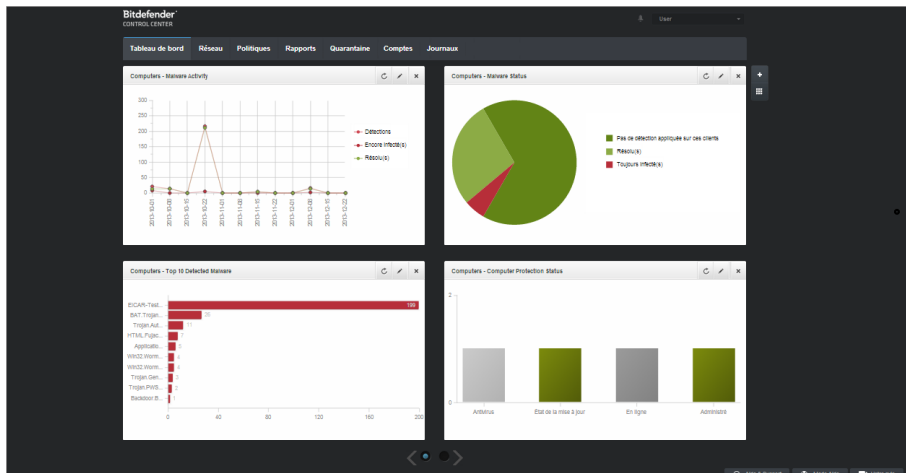


Note

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.

2.2. 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 de la zone supérieure pour naviguer à travers la console. Les fonctionnalités disponibles dépendent du type d'utilisateur accédant à la console.



Le tableau de bord

2.2.1. 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.

En fonction de leur rôle, les administrateurs de Security for Endpoints (Console dans le Cloud) peuvent accéder aux sections suivantes à partir de la barre de menus :

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.

Quarantaine

Administrer à distance les fichiers en quarantaine.

Comptes

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




Note

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

Journaux

Vérifier le journal d'activité de l'utilisateur.

En outre, dans l'angle supérieur droit de la console, l'icône  **Notifications** offre un accès facile aux messages de notification ainsi qu'à la page **Notifications**.

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

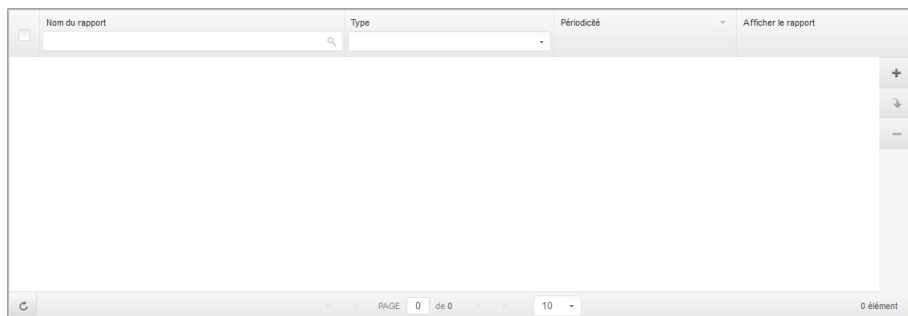
- **Mon Compte.** Cliquez sur cette option pour gérer les détails et les préférences de votre compte utilisateur.
- **Mon Entreprise.** Cliquez sur cette option pour gérer les détails et les préférences de votre entreprise.
- **Admin. des authentifications.** Cliquez sur cette option pour ajouter et gérer les informations d'authentification requises pour les tâches d'installation à distance.
- **Déconnexion.** Cliquez sur cette option pour vous déconnecter de votre compte.

Vous trouverez les liens suivants dans l'angle inférieur droit de la console :

- **Aide et Support.** Cliquez sur ce bouton pour obtenir des informations sur l'aide et le support.
- **Mode Aide.** Cliquez sur ce bouton pour activer une fonctionnalité d'aide fournissant des info-bulles extensibles sur les éléments de Control Center. Vous trouverez facilement des informations utiles au sujet des fonctionnalités de Control Center.
- **Votre avis.** Cliquez sur ce bouton pour faire apparaître un formulaire vous permettant de modifier et d'envoyer vos messages concernant votre avis au sujet de l'utilisation de Security for Endpoints (Console dans le Cloud).

2.2.2. Données du tableau

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



La page Rapports - Tableau Rapports

Naviguer entre les pages

Les tableaux de plus de 10 entrées comportent plusieurs pages. Par défaut, seules 10 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

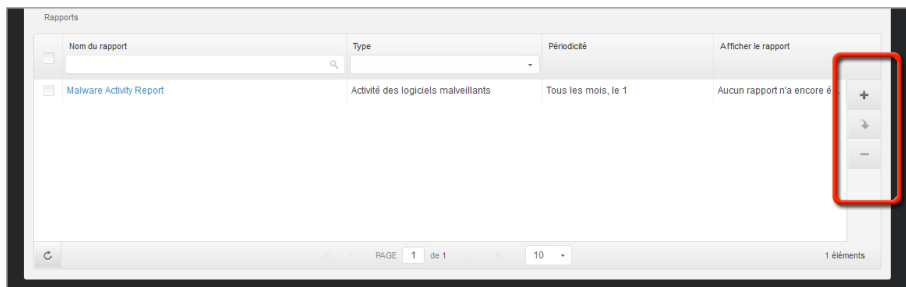
Pour que la console affiche des informations à jour, cliquez sur le bouton  **Actualiser** dans l'angle inférieur gauche du tableau.

2.2.3. 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 généralement placé sur la partie droite du

tableau. Par exemple, la barre d'outils d'actions de la section **Rapports** vous permet d'effectuer les actions suivantes :

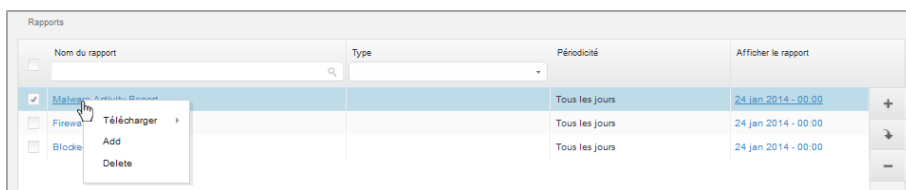
- Créer un nouveau rapport.
- Télécharger les rapports générés par un rapport planifié.
- Supprimer un rapport planifié.



La page Rapports - Barre d'outil d'actions

2.2.4. 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 du Control Center que vous utilisez en ce moment et sélectionnez la commande dont vous avez besoin dans la liste disponible.

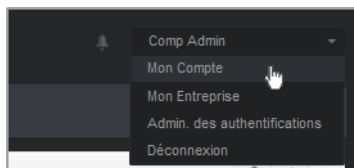


La page Rapports - Menu contextuel

2.3. Gérer votre compte

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

1. Pointez 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.
 - **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.
 - **Mot de passe**. 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 du compte. La console affichera des 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. Cliquez sur **Enregistrer** pour enregistrer les modifications.



Note

Vous ne pouvez pas supprimer votre propre compte.

2.4. Changer de mot de passe de connexion

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

- 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. Pointez 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 enregistrer les modifications.

3. Gestion des licences

Le service de sécurité fourni par Security for Endpoints (Console dans le Cloud) requiert une clé de licence valide.

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

Vous pouvez vous abonner au service de deux façons :

- S'abonner via un revendeur Bitdefender. Nos revendeurs vous fourniront toutes les informations dont vous avez besoin et vous aideront à choisir le meilleur plan d'abonnement pour vous. Certains revendeurs proposent des services à valeur ajoutée, tels que le support premium, et d'autres fournissent un service entièrement géré.

Pour trouver un revendeur Bitdefender dans votre pays :

1. Allez à <http://www.bitdefender.fr/partenaires/trouver-un-partenaire.html>.
 2. Allez dans **Trouver un partenaire**.
 3. Les informations de contact des partenaires 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 revendeur Bitdefender dans votre pays, n'hésitez pas à nous contacter par e-mail à l'adresse bitdefender@editions-profil.eu. Veuillez rédiger votre e-mail en anglais pour optimiser le traitement de votre demande.
- S'abonner sur le [site web Bitdefender](#).

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

3.1. Activer une licence

Lorsque vous achetez un abonnement payant pour la première fois, une clé de licence est générée pour vous. L'abonnement à Security for Endpoints (Console dans le Cloud) est activé avec cette clé de licence.



Avertissement

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

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

1. Connectez-vous au Control Center à l'aide de votre compte client.
2. Pointez sur votre compte utilisateur dans l'angle supérieur droit de la console et sélectionnez **Mon Entreprise**.
3. Consultez des informations sur la licence actuelle dans la section **Licence**.
4. Saisissez votre clé de licence dans le champ **Licence**.
5. Cliquez sur le bouton **Vérifier** et attendez que le Control Center récupère des informations sur la clé de licence saisie.
6. Cliquez sur **Enregistrer**.

3.2. Vérification des détails de la licence actuelle

Pour vérifier l'état de votre abonnement :

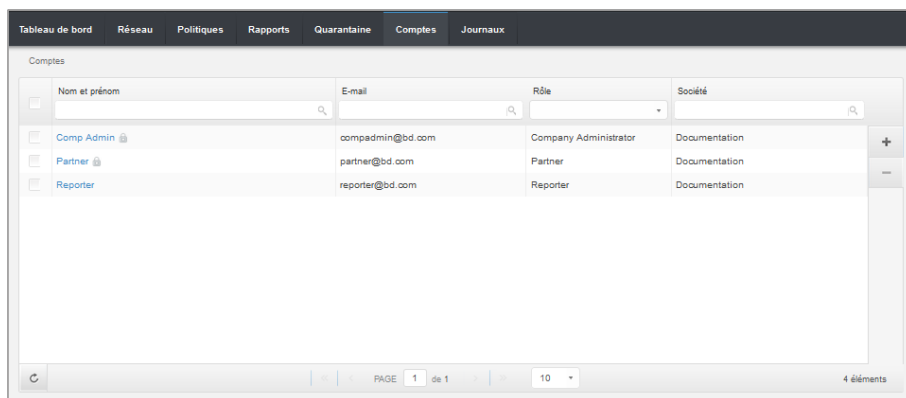
1. Connectez-vous au Control Center avec votre e-mail et le mot de passe que vous avez reçu par e-mail.
2. Pointez sur votre compte utilisateur dans l'angle supérieur droit de la console et sélectionnez **Mon Entreprise**.
3. Consultez des informations sur la licence actuelle dans la section **Licence**.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

4. Gestion des comptes utilisateurs

Le service Security for Endpoints peut être configuré et géré à partir du Control Center à l'aide du compte reçu après l'inscription au service.

Voici ce que vous avez besoin de savoir sur les comptes utilisateur de Security for Endpoints (Console dans le Cloud) :

- Pour autoriser d'autres employés de la société à accéder au Control Center, vous pouvez créer des comptes utilisateur internes. 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 Security for Endpoints (Console dans le Cloud) ou à certaines parties du réseau auquel il appartient.
- 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 que votre compte, ou moins.
- Vous pouvez créer et administrer des comptes utilisateurs sur la page **Comptes**.



	Nom et prénom	E-mail	Rôle	Société	
<input type="checkbox"/>					
<input type="checkbox"/>	Comp Admin	compadmin@bd.com	Company Administrator	Documentation	+
<input type="checkbox"/>	Partner	partner@bd.com	Partner	Documentation	
<input type="checkbox"/>	Reporter	reporter@bd.com	Reporter	Documentation	-

PAGE 1 de 1 | 10 | 4 éléments

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 (partenaire / administrateur de la société / administrateur / rapporteur / personnalisé).

4.1. 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 l'entreprise** - Adapté aux responsables des entreprises clientes ayant acheté une licence Security for Endpoints (Console dans le Cloud) à un partenaire. L'administrateur de l'entreprise gère: la licence, le profil de l'entreprise ainsi que l'ensemble du déploiement de Security for Endpoints (Console dans le Cloud) permettant un contrôle de haut niveau de l'ensemble des paramètres de sécurité (sauf en cas d'écrasement par le partenaire, administrant le compte, dans le cas d'un fournisseur de services de sécurité). Les administrateurs de la société peuvent partager ou déléguer leurs responsabilités opérationnelles aux comptes utilisateurs administrateurs et rapporteurs secondaires.
2. **Administrateur** - Plusieurs comptes avec un rôle Administrateur peuvent être créés pour une société, avec des privilèges d'administration sur le déploiement de Security for Endpoints dans l'ensemble de la société ou sur un groupe spécifique d'ordinateurs, y compris l'administration des utilisateurs. Les administrateurs sont responsables de la gestion active des paramètres de sécurité du réseau.
3. **Rapporteurs** - Les comptes rapporteurs sont des comptes en lecture seule internes. Ils permettent uniquement d'accéder aux rapports et aux journaux. Ces comptes peuvent être alloués au 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. 13).

Rôle du Compte	Comptes Enfants Autorisés	Droits de l'utilisateur
Administrateur de la société	Administrateurs de la société, Administrateurs, Rapporteurs	Gérer l'entreprise Gérer les utilisateurs Gérer les réseaux Gérer les rapports
Administrateur	Administrateurs, Rapporteurs	Gérer les utilisateurs Gérer les réseaux Gérer les rapports
Rapporteur	-	Gérer les rapports

4.2. Droits de l'utilisateur

Vous pouvez affecter les droits utilisateurs suivants aux comptes utilisateurs de Security for Endpoints (Console dans le Cloud) :

- **Gérer les utilisateurs.** Créer, modifier ou supprimer des comptes utilisateurs
- **Gérer la société.** Les utilisateurs peuvent gérer leur propre clé de licence Security for Endpoints (Console dans le Cloud) 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 administrateurs.
- **Gérer les rapports.** Créer, éditer, supprimer des rapports et gérer le tableau de bord.

4.3. Créer des comptes utilisateurs

Avant de créer un compte utilisateur, vérifiez que vous disposez de l'adresse e-mail requise. Cette adresse est indispensable à la création du compte utilisateur Security for Endpoints (Console dans le Cloud). Les utilisateurs recevront leurs informations de connexion à Security for Endpoints (Console dans le Cloud) à l'adresse e-mail indiquée. Les utilisateurs auront également besoin de l'adresse e-mail pour se connecter à Security for Endpoints (Console dans le Cloud).

Pour créer un compte utilisateur:

1. Allez sur la page **Comptes**.
2. Cliquez sur le bouton **+ Ajouter** à droite du tableau. Une fenêtre de configuration s'affiche.

3. Sous la section **Détails**, saisissez les détails du compte.

- **E-mail.** Indiquez l'adresse e-mail de l'utilisateur. Les informations de connexion seront envoyées à cette adresse immédiatement après la création du compte.



Note

L'adresse e-mail doit être unique. Vous ne pouvez pas créer d'autre compte utilisateur avec la même adresse e-mail.

- **Prénom et Nom.** Indiquez le nom complet du propriétaire du compte.

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 des 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. 12).
- **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. 13).
- **Sélectionner les cibles.** Faites défiler vers le bas la fenêtre de configuration pour afficher la section des cibles. Sélectionnez les groupes du réseau auxquels l'utilisateur aura accès. Vous pouvez limiter l'accès de l'utilisateur à certaines zones du réseau.

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



Note

Le mot de passe de chaque compte utilisateur est automatiquement généré une fois le compte créé et envoyé à l'adresse e-mail de l'utilisateur avec les autres détails du compte. Vous pouvez changer le mot de passe une fois que le compte a été créé. Cliquez sur le nom du compte sur la page **Comptes** pour modifier son mot de passe. Lorsque le mot de passe a été modifié, l'utilisateur en est immédiatement informé par e-mail. Les utilisateurs peuvent changer leur mot de passe de connexion à partir du Control Center, en accédant à la page **Mon Compte**.

4.4. Modification des comptes

Modifiez les comptes pour actualiser leurs données ou modifier leurs paramètres.

Pour modifier un compte utilisateur :

1. Connectez-vous au Control Center.
2. Allez sur la page **Comptes**.
3. Cliquez sur le nom de l'utilisateur.
4. Modifier les détails et les paramètres des comptes selon vos besoins.
5. Cliquez sur **Enregistrer** pour enregistrer 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 que votre propre compte, ou moins.

4.5. Supprimer des comptes

Supprimer les comptes quand ils ne sont plus utiles. Si le propriétaire du compte, par exemple, a quitté l'entreprise.

Pour supprimer un compte :

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

4.6. 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 au 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 enregistrer les modifications. Le propriétaire du compte recevra un e-mail avec le nouveau mot de passe.

5. Installation de Security for Endpoints

Security for Endpoints est destiné aux ordinateurs de bureau et aux portables fonctionnant sous les systèmes d'exploitation Windows et Mac OS X et aux serveurs Windows. Pour protéger vos ordinateurs physiques avec Security for Endpoints, vous devez installer Endpoint Security (le logiciel client) sur chacun d'entre eux. Endpoint Security gère la protection sur l'ordinateur local. Il communique également avec Control Center pour recevoir les commandes de l'administrateur et envoyer les résultats de ses actions.

Vous pouvez installer Endpoint Security avec l'un des rôles suivants (disponibles dans l'assistant d'installation) :

1. **Poste de travail**, lorsque l'ordinateur correspondant est un poste standard du réseau.
2. **Endpoint Security Relay**, lorsque l'ordinateur correspondant est utilisé par d'autres postes de travail du réseau pour communiquer avec Control Center. Le rôle Endpoint Security Relay installe Endpoint Security avec un serveur de mise à jour qui peut être utilisé pour mettre à jour tous les autres clients du réseau. Les postes de travail du même réseau peuvent être configurés via une politique pour communiquer avec Control Center via un ou plusieurs ordinateurs avec le rôle Endpoint Security Relay. Ainsi, lorsqu'un Endpoint Security Relay n'est pas disponible, le suivant est pris en compte pour assurer la communication de l'ordinateur avec Control Center.



Avertissement

- Le premier ordinateur sur lequel vous installez la protection doit avoir le rôle Endpoint Security Relay, vous ne pourrez sinon pas déployer Endpoint Security sur les autres ordinateurs du réseau.
- L'ordinateur avec le rôle Endpoint Security Relay doit être allumé et en ligne pour que les clients communiquent avec Control Center.

Vous pouvez installer Endpoint Security sur les ordinateurs [en exécutant les packages d'installation en local](#) ou [en exécutant des tâches d'installation à distance](#) depuis Control Center.

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

Endpoint Security dispose d'une interface utilisateur minimale. Elle permet uniquement aux utilisateurs de consulter l'état de la protection et d'exécuter des tâches de sécurité de base (mises à jour et analyses) sans fournir d'accès aux paramètres.

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

Pour installer l'interface utilisateur dans une autre langue sur certains ordinateurs, vous pouvez créer un package d'installation et définir la langue de votre choix dans les options de configuration du package. Pour plus d'informations sur la création de packages d'installation, reportez-vous à « [Création de packages d'installation d'Endpoint Security](#) » (p. 20).

5.1. Configuration requise

5.1.1. Systèmes d'exploitation pris en charge

Security for Endpoints protège actuellement les systèmes d'exploitation suivants :

Systèmes d'exploitation des stations de travail :

- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista avec Service Pack 1
- Windows XP avec Service Pack 3
- Mac OS X Lion (10.7.x)
- Mac OS X Mountain Lion (10.8.x)
- Mac OS X Mavericks (10.9.x)

Systèmes d'exploitation tablettes et embarqués* :

- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7
- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP Embedded avec Service Pack 2
- Windows XP Tablet PC Edition

*Des modules spécifiques du système d'exploitation doivent être installés pour que Security for Endpoints fonctionne.

Systèmes d'exploitation serveurs :

- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Small Business Server (SBS) 2008
- Windows Server 2008 R2
- Windows Server 2008
- Windows Small Business Server (SBS) 2003

- Windows Server 2003 R2
- Windows Server 2003 avec le Service Pack 1
- Windows Home Server

5.1.2. Matériel

- Processeur compatible Intel® Pentium :

Systèmes d'exploitation des stations de travail

- 1 GHz ou plus pour Microsoft Windows XP SP3, Windows XP SP2 64 bits et Windows 7 Enterprise (32 et 64 bits)
- 2 GHz ou plus pour Microsoft Windows Vista SP1 ou version supérieure (32 et 64 bits), Microsoft Windows 7 (32 et 64 bits), Microsoft Windows 7 SP1 (32 et 64 bits), Windows 8
- 800 MHz ou plus pour Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded avec Service Pack 2, Microsoft Windows XP Tablet PC Edition

Systèmes d'exploitation serveurs

- Minimum : processeur simple cœur de 2,4 GHz
- Recommandé : processeur multicœur Intel Xeon 1,86 GHz ou plus

- **Mémoire RAM disponible :**

- Pour Windows : 512 Mo au minimum, 1 Go recommandé
- Pour Mac : 1 Go minimum

- **Espace disque :**

- 1.5 Go d'espace libre du disque dur



Note

Au moins 6 Go d'espace disque libre sont requis pour les entités avec le rôle Endpoint Security Relay puisqu'elles stockeront toutes les mises à jour et packages d'installation.

5.1.3. Navigateurs pris en charge

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

- Internet Explorer 8+
- Mozilla Firefox 8+
- Google Chrome 15+
- Safari 4+

5.2. Préparation de l'Installation

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

1. Vérifiez que les ordinateurs disposent de la [configuration système minimale requise](#). Pour certains ordinateurs, vous pouvez avoir besoin d'installer le dernier service pack du système d'exploitation disponible ou de libérer de l'espace disque. Établissez une liste d'ordinateurs ne correspondant pas aux critères nécessaires afin que vous puissiez les exclure de l'administration.
2. Désinstaller des ordinateurs (ne pas simplement désactiver) tout logiciel antimalware, pare-feu ou de sécurité Internet. Faire fonctionner simultanément Endpoint Security avec d'autres logiciels de sécurité installés sur l'ordinateur peut affecter leur fonctionnement et causer d'importants problèmes avec le système.

Beaucoup de programmes de sécurité avec lesquels Endpoint Security est incompatible seront automatiquement détectés et supprimés lors de l'installation. Pour en savoir plus et pour vérifier la liste des logiciels de sécurité détectés, merci de vous référer à [cet article](#).



Important

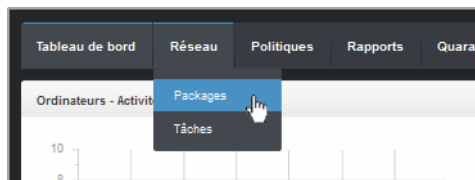
Ne vous occupez pas des fonctionnalités de sécurité Windows (Windows Defender, Pare-Feu Windows) puisqu'elles seront désactivées automatiquement avant le lancement de l'installation.

3. L'installation requiert des privilèges d'administration et un accès à Internet. Vérifiez que vous disposez des identifiants nécessaires de tous les ordinateurs.
4. Les ordinateurs doivent disposer d'une connectivité à Control Center.

5.3. Installation locale

Il est possible d'installer Endpoint Security sur un ordinateur en exécutant un package d'installation en local.

Vous pouvez créer et gérer des packages d'installation en fonction de vos besoins sur la page **Réseau > Packages**.



Le menu Réseau > Packages



Avertissement

- Le premier ordinateur sur lequel vous installez la protection doit avoir le rôle Endpoint Security Relay, vous ne pourrez sinon pas déployer Endpoint Security sur les autres ordinateurs du réseau.
- L'ordinateur avec le rôle Endpoint Security Relay doit être allumé et en ligne pour que les clients communiquent avec Control Center.

Une fois installé, l'ordinateur avec le rôle Endpoint Security Relay sera utilisé pour détecter d'autres ordinateurs du même réseau, à partir de la fonction Network Discovery. Pour plus d'informations sur la fonction Network Discovery, merci de vous référer à « [Fonctionnement de Network Discovery](#) » (p. 27).

Pour installer Endpoint Security en local sur un ordinateur, suivez les étapes suivantes :

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



Note

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

2. [Téléchargez le package d'installation](#) sur l'ordinateur.
3. [Exécutez le package d'installation](#) sur l'ordinateur.

5.3.1. Création de packages d'installation d'Endpoint Security

Pour créer un package d'installation d'Endpoint Security :

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

Nom	Type	Langue	Description	État
<input type="checkbox"/> Rly	Endpoint Security	English		Prêt à télécharger
<input type="checkbox"/> EPSr	Endpoint Security	English	company1	Prêt à télécharger

La page Packages

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

Endpoint Security

Options

Avancé

Détails

Nom: * EPS-FR

Description: Endpoint Security FR

Général

Role: Endpoint Security Relay

Société: Sélectionner une entreprise

Modules à installer :

Antimalware ⓘ

Pare-feu ⓘ

Contrôle de contenu

Configuration

Langue: Français

Analyser avant l'installation

Utiliser le chemin d'installation personnalisé

Mot de passe de désinstallation

Mot de passe: Cliquez ici pour changer le m

Confirmer: Veuillez saisir de nouveau le

Endpoint Security by Bitdefender désinstalle automatiquement les autres logiciels de sécurité.

Suivant > Annuler

Créer des packages Endpoint Security - Options

4. Indiquez un nom et une description explicites pour le package d'installation que vous souhaitez créer.
5. Sélectionnez le rôle de l'ordinateur cible :
 - **Poste de travail.** Sélectionnez cette option pour créer le package pour un poste de travail standard.
 - **Endpoint Security Relay.** Sélectionnez cette option pour créer le package pour un poste de travail avec le rôle Endpoint Security Relay. Endpoint Security Relay est un rôle spécial qui installe un serveur de mise à jour sur la machine cible avec Endpoint Security, lequel peut être utilisé pour mettre à jour tous les autres clients du réseau, faisant diminuer ainsi la consommation de bande passante entre les machines clientes et le Control Center.


6. Sélectionnez l'entreprise où le package d'installation sera utilisé.
7. Sélectionnez les modules de protection que vous voulez installer.
8. Dans le champ **Langue**, sélectionnez la langue souhaitée pour l'interface du client.
9. Sélectionnez **Analyser avant l'installation** si vous souhaitez vous assurer que les ordinateurs sont sains avant d'y installer Endpoint Security. Une analyse rapide dans le Cloud sera réalisée sur les ordinateurs correspondants avant de commencer l'installation.
10. Endpoint Security est installé dans le répertoire d'installation par défaut sur les ordinateurs sélectionnés. Sélectionnez **Utiliser le chemin d'installation personnalisé** si vous souhaitez installer Endpoint Security à un emplacement différent. Dans ce cas, saisissez le chemin souhaité dans le champ correspondant. Utilisez les conventions Windows lorsque vous saisissez le chemin (par exemple, D:\folder). Si le dossier spécifié n'existe pas, il sera créé lors de l'installation.
11. Vous pouvez, si vous le souhaitez, définir un mot de passe pour empêcher les utilisateurs de supprimer la protection. Sélectionnez **Mot de passe de désinstallation** et indiquez le mot de passe souhaité dans les champs correspondants.
12. Cliquez sur **Suivant**.
13. En fonction du rôle du package d'installation (Endpoint ou Endpoint Security Relay), sélectionnez l'entité auprès de laquelle les ordinateurs cibles se connecteront régulièrement pour mettre à jour le client :
 - **Cloud Bitdefender**, si vous souhaitez mettre à jour les clients directement à partir d'Internet.
 - **Endpoint Security Relay**, si vous souhaitez mettre à jour les clients via les postes de travail Endpoint Security Relay installés dans votre réseau. Dans ce cas, tous les postes de travail avec le rôle Endpoint Security Relay détectés dans votre réseau apparaîtront dans le tableau ci-dessous. Sélectionnez le Endpoint Security Relay que vous souhaitez utiliser pour les mises à jour clientes.
14. Cliquez sur **Enregistrer**.

Le nouveau package d'installation apparaîtra dans la liste de packages de l'entreprise cible.

5.3.2. Téléchargement de packages d'installation

Pour télécharger des packages d'installation d'Endpoint Security :

1. Identifiez-vous auprès de Control Center à partir de l'ordinateur sur lequel vous souhaitez installer la protection.
2. Accédez à la page **Réseau > Packages**.
3. Sélectionnez le package d'installation d'Endpoint Security que vous souhaitez télécharger.

4. Cliquez sur le bouton  **Télécharger** sur la partie droite du tableau et sélectionnez le type de programme d'installation que vous souhaitez utiliser. Deux types de fichiers d'installation sont disponibles :
 - **Programme de téléchargement** . Le downloader commence par télécharger le kit d'installation complet sur les serveurs cloud de Bitdefender avant de lancer l'installation. Il est peu volumineux et peut être exécuté à la fois sur les systèmes 32 et 64 bits (ce qui facilite sa distribution). Il requiert par contre une connexion active à Internet.
 - **Kit complet**. Le kit complet est à utiliser pour installer la protection sur les ordinateurs avec une connexion Internet lente ou sans connexion. Téléchargez ce fichier sur un ordinateur connecté à Internet puis transmettez-le à d'autres ordinateurs à l'aide de supports de stockage externes ou d'un partage réseau.



Note

Versions du kit complet disponibles :

- **OS Windows** : systèmes 32 et 64 bits
- **Mac OS X** : uniquement les systèmes 64 bits

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

5. Enregistrez le fichier sur l'ordinateur.

5.3.3. Exécution de packages d'installation

Pour que l'installation fonctionne, le package d'installation doit être exécuté à l'aide de privilèges administrateur ou sous un compte administrateur.

1. Connectez-vous et identifiez-vous sur le Control Center.
2. Téléchargez ou copiez le fichier d'installation sur l'ordinateur cible ou sur un partage réseau accessible à partir de cet ordinateur.
3. Exécutez le package d'installation.
4. Suivez les instructions à l'écran.

Une fois Endpoint Security installé, l'ordinateur apparaît comme étant administré dans Control Center (page **Réseau**) après quelques minutes.

5.4. Installation à distance

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

Security for Endpoints comprend un mécanisme de découverte du réseau automatique qui permet de détecter d'autres ordinateurs du même réseau. Les ordinateurs détectés sont affichés en tant qu'**ordinateurs non administrés** sur la page **Réseau**.

Pour plus d'informations sur la fonction Network Discovery, merci de vous référer à « [Fonctionnement de Network Discovery](#) » (p. 27).

5.4.1. Configuration requise à l'installation d'Endpoint Security à distance

Pour que l'installation à distance fonctionne :

- Chaque ordinateur cible doit avoir le partage administratif "admin\$" activé. Configurez chaque poste de travail cible afin qu'il utilise le partage de fichiers avancé.
- Désactivez temporairement le contrôle de compte utilisateur sur tous les ordinateurs exécutant les systèmes d'exploitation Windows qui disposent de cette fonction de sécurité (Windows Vista, Windows 7, Windows Server 2008, etc.). Si les ordinateurs sont dans un domaine, vous pouvez utiliser une politique de groupe pour désactiver le Contrôle de compte d'utilisateur à distance.
- Désactivez ou éteignez la protection pare-feu sur les ordinateurs. Si les ordinateurs sont dans un domaine, vous pouvez utiliser une politique de groupe pour désactiver le Pare-Feu Windows à distance.

5.4.2. Exécution des tâches d'installation d'Endpoint Security à distance

Pour exécuter une tâche d'installation à distance :


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

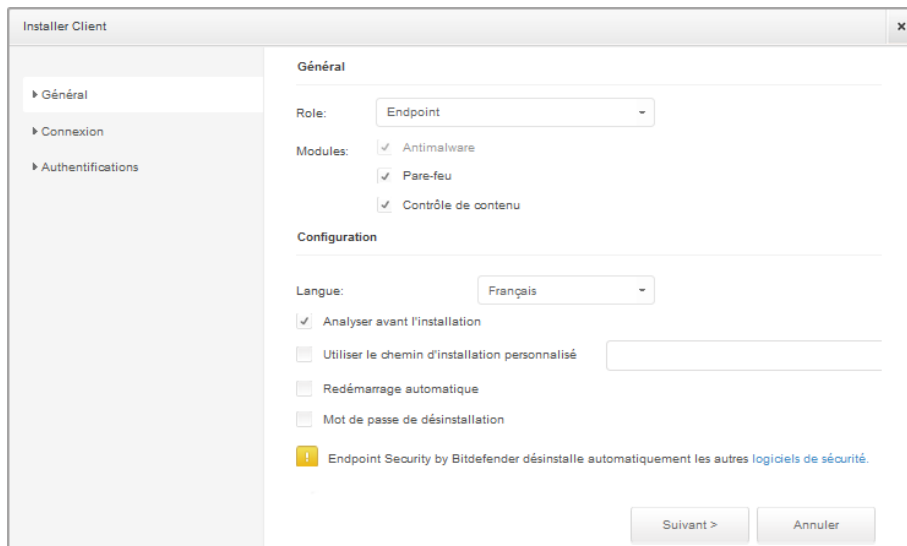


Note

Vous pouvez aussi appliquer des filtres pour afficher uniquement les ordinateurs non administrés. Cliquez sur le bouton **Filtres** et sélectionnez les options suivantes : **Non administré** dans la catégorie **Sécurité** et **Tous les éléments de manière récurrente** dans la catégorie **Profondeur**.

4. Sélectionnez les entités (ordinateurs ou groupes d'ordinateurs) sur lesquelles vous souhaitez installer la protection.

5. Cliquez sur le bouton  **Tâches** à droite du tableau et sélectionnez **Installer le client**. L'assistant **Installer le client** apparaît.



Installer Endpoint Security à partir du menu Tâches

6. Configurer les options d'installation :

- Sélectionnez le rôle que vous souhaitez que le client ait :
 - **Poste de travail**. Sélectionnez cette option si vous souhaitez installer le client sur un poste de travail standard.
 - **Endpoint Security Relay**. Sélectionnez cette option pour installer le client avec le rôle Endpoint Security Relay sur l'ordinateur cible. Endpoint Security Relay est un rôle spécial qui installe un serveur de mise à jour sur la machine cible avec Endpoint Security, lequel peut être utilisé pour mettre à jour tous les autres clients du réseau, faisant diminuer ainsi la consommation de bande passante entre les machines clientes et le Control Center.
- Sélectionnez les modules de protection que vous voulez installer. Veuillez noter que seule la protection antimalware est disponible pour les systèmes d'exploitation serveurs.
- Dans le champ **Langue**, sélectionnez la langue souhaitée pour l'interface du client.
- Sélectionnez **Analyser avant l'installation** si vous souhaitez vous assurer que les ordinateurs sont sains avant d'y installer Endpoint Security. Une analyse rapide dans

le Cloud sera réalisée sur les ordinateurs correspondants avant de commencer l'installation.

- Endpoint Security est installé dans le répertoire d'installation par défaut sur les ordinateurs sélectionnés. Sélectionnez **Utiliser le chemin d'installation personnalisé** si vous souhaitez installer Endpoint Security à un emplacement différent. Dans ce cas, saisissez le chemin souhaité dans le champ correspondant. Utilisez les conventions Windows lorsque vous saisissez le chemin (par exemple, D:\folder). Si le dossier spécifié n'existe pas, il sera créé lors de l'installation.
- Lors de l'installation silencieuse, l'ordinateur fait l'objet d'une analyse antimalware. Un redémarrage du système peut être nécessaire pour terminer la désinfection de malwares.

Sélectionnez **Redémarrer automatiquement (si nécessaire)** afin de vous assurer que les malwares détectés ont été complètement supprimés avant l'installation. Sinon, l'installation peut échouer.

- Vous pouvez, si vous le souhaitez, définir un mot de passe pour empêcher les utilisateurs de supprimer la protection. Sélectionnez **Mot de passe de désinstallation** et indiquez le mot de passe souhaité dans les champs correspondants.
- Cliquez sur **Suivant**.
- En fonction du rôle du client (Poste de travail ou Endpoint Security Relay), sélectionnez l'entité via laquelle les clients communiqueront :
 - **Cloud Bitdefender**, si vous souhaitez mettre à jour les clients directement à partir d'Internet.
 - **Endpoint Security Relay**, si vous souhaitez mettre à jour les clients via les postes de travail Endpoint Security Relay installés dans votre réseau. Dans ce cas, tous les postes de travail avec le rôle Endpoint Security Relay détectés dans votre réseau apparaîtront dans le tableau ci-dessous. Sélectionnez le Endpoint Security Relay que vous souhaitez utiliser pour les mises à jour clientes.

7. Cliquez sur **Suivant**.

8. Dans la section **Admin. des authentifications**, indiquez les identifiants d'administration requis pour l'authentification à distance sur les postes de travail sélectionnés.

Vous pouvez ajouter les identifiants requis en saisissant l'utilisateur et le mot de passe de tous les systèmes d'exploitation cibles.



Note

Un message d'avertissement s'affiche tant que vous n'avez sélectionné aucun identifiant. Cette étape est obligatoire pour installer à distance Endpoint Security sur les ordinateurs.

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. 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 indiquez le nom d'un compte d'utilisateur de domaine (par exemple, domaine\utilisateur ou utilisateur@domaine.com).



Note

Les identifiants spécifiés sont enregistrés automatiquement dans votre Administrateur des authentifications afin que vous n'ayez pas à les saisir la prochaine fois.

- b. Cliquez sur le bouton **+ Ajouter**. Le compte est ajouté à la liste des identifiants.
- c. Cochez la case correspondant au compte que vous souhaitez utiliser.

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

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

5.5. Fonctionnement de Network Discovery

Security for Endpoints comprend un mécanisme de découverte du réseau automatique destiné à détecter les ordinateurs du groupe de travail.

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

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

La commande Net view

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



Important

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

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

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

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

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

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

Pour une visibilité complète du réseau, Endpoint Security doit être installé sur au moins un ordinateur de chaque groupe de travail ou domaine de votre réseau. Idéalement, Endpoint Security devrait être installé sur au moins un ordinateur de chaque sous-réseau.

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

Présentation rapide du service Explorateur d'ordinateurs :

- Fonctionne indépendamment d'Active Directory.

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

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

5.5.2. Configuration requise pour la découverte du réseau

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

- Les ordinateurs doivent faire partie d'un groupe de travail ou d'un domaine et être connectés via un réseau local IPv4. Le service Explorateur d'ordinateurs ne fonctionne pas sur les réseaux IPv6.
- Plusieurs ordinateurs dans chaque groupe LAN (groupe de travail ou domaine) doivent exécuter le service Explorateur d'ordinateurs. Les contrôleurs principaux de domaine doivent également exécuter le service.
- NetBIOS sur TCP/IP (NetBT) doit être activé sur les ordinateurs. Le pare-feu local doit autoriser le trafic NetBT.
- Le partage de fichiers doit être activé sur les ordinateurs. Le pare-feu local doit autoriser le partage de fichiers.
- Une infrastructure WINS (Windows Internet Name Service) doit être installée et opérationnelle.
- Pour Windows Vista et les versions ultérieures, la découverte du réseau doit être activée (**Panneau de configuration > Centre Réseau et partage > Modifier les paramètres de partage avancés**).

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

- DNS Client
- Function Discovery Resource Publication
- SSDP Discovery
- UPnP Device Host

- Dans les environnements avec plusieurs domaines, il est recommandé d'établir des relations d'approbation entre les domaines afin que les ordinateurs puissent accéder aux listes de parcours d'autres domaines.

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

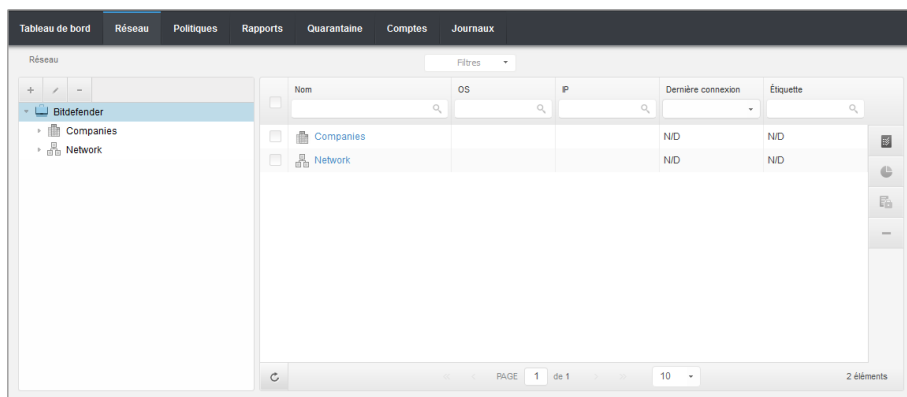


Note

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

6. Gestion des ordinateurs

La page **Réseau** comporte plusieurs fonctionnalités pour explorer et administrer les ordinateurs disponibles. La vue **Réseau** consiste en une interface à deux panneaux affichant l'état en temps réel de tous les objets du réseau :



La Page Réseau

1. Le panneau de gauche affiche la structure arborescente du réseau disponible.



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 l'arborescence du réseau. 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. Cliquez sur le nom de l'objet pour faire apparaître une fenêtre contenant plus de précisions.
- Utilisez la [barre d'outils d'actions](#) à droite du tableau pour effectuer certaines opérations pour chaque objet du réseau (telles qu'exécuter des tâches, créer des rapports, affecter des politiques et supprimer).

- [Actualiser les données du tableau.](#)

La section **Réseau** vous permet également de gérer les [packages d'installation](#) et la [liste de tâches](#) pour chaque type d'objet du réseau.

Pour afficher les ordinateurs sous votre compte, allez sur la page **Réseau** et sélectionnez le groupe du réseau souhaité dans la partie gauche de la page.







Vous pouvez voir le réseau informatique disponible dans le panneau de gauche et des informations sur chaque ordinateur dans le panneau de droite.

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

- [Vérifier l'état de l'ordinateur.](#)
- [Organiser les ordinateurs dans des groupes.](#)
- [Afficher des informations sur un ordinateur.](#)
- [Trier, filtrer et rechercher des ordinateurs.](#)
- [Exécuter des tâches sur des ordinateurs.](#)
- [Créer des rapports rapides.](#)
- [Affecter des politiques.](#)
- [Supprimer des ordinateurs de l'inventaire du réseau.](#)

6.1. Vérifier l'état de l'ordinateur

Chaque ordinateur est représenté sur la page du réseau par une icône spécifique à son état. Afficher l'état de l'ordinateur et les icônes correspondantes dans le tableau suivant :




Icône	État
	Ordinateur, Administré, Aucun problème, En ligne
	Ordinateur, Administré, Avec des problèmes de sécurité, En ligne,
	Ordinateur, Administré, Aucun problème, Hors Connexion
	Ordinateur, Administré, Avec des problèmes de sécurité, Hors Connexion
	Non administré
	Supprimé

Pour plus d'informations, reportez-vous à :

- « [Ordinateurs administrés, non administrés et supprimés](#) » (p. 32)
- « [Ordinateurs en ligne et hors connexion](#) » (p. 33)
- « [Ordinateurs avec des problèmes de sécurité](#) » (p. 34)



6.1.1. Ordinateurs administrés, non administrés et supprimés

Les ordinateurs peuvent avoir différents états d'administration :

-  **Administrés** - ordinateurs sur lesquels la protection Endpoint Security est installée.
-  **Non administrés** - ordinateurs détectés sur lesquels la protection Endpoint Security n'est pas encore installée.
-  **Supprimés** - les ordinateurs que vous avez supprimés de Control Center. Pour plus d'informations, reportez-vous à « [Supprimer des ordinateurs de l'inventaire du réseau](#) » (p. 56).

6.1.2. Ordinateurs en ligne et hors connexion

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 Endpoint Security 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 normalement en ligne, même quand ils sont verrouillés ou que l'utilisateur est déconnecté.

- Endpoint Security n'a pas de connectivité avec Bitdefender Control Center ou avec le Endpoint Security Relay affecté :
 - L'ordinateur peut être déconnecté du réseau.
 - Un routeur ou un pare-feu du réseau peut bloquer la communication entre Endpoint Security et Bitdefender Control Center ou le Endpoint Security Relay affecté.
- Endpoint Security a été désinstallé manuellement de l'ordinateur, alors que l'ordinateur n'avait pas de connectivité avec Bitdefender Control Center ou avec le Endpoint Security Relay affecté. Normalement, lorsqu'Endpoint Security est désinstallé manuellement d'un ordinateur, Control Center est informé de cet événement et l'ordinateur est signalé comme étant non administré.
- Endpoint Security 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 **Administrés (Postes de travail)** et **Administrés (Endpoint Security Relay)** dans la catégorie **Sécurité** 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.


6.1.3. Ordinateurs avec des problèmes de sécurité

L'état de sécurité concerne uniquement les ordinateurs administrés. Consultez l'icône de l'état affichant un symbole d'avertissement pour identifier les ordinateurs présentant des problèmes de sécurité :

-  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 d'Endpoint Security a expiré.
- Endpoint Security n'est pas à jour.
- Des malwares ont été détectés.

Si vous remarquez un ordinateur avec des problèmes de sécurité, cliquez sur son nom pour afficher la page **Détails de l'ordinateur**. Vous pouvez identifier les problèmes de sécurité par l'icône . Consultez l'info-bulle de l'icône pour plus d'informations. D'autres enquêtes locales peuvent être nécessaires.

6.2. Organiser les ordinateurs dans des groupes

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

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

Sous le groupe **Réseau** appartenant à votre entreprise vous pouvez [créer](#), [supprimer](#), [renommer](#) et [déplacer](#) des groupes d'ordinateurs dans une structure arborescente personnalisée.



Important

Veillez noter ceci :

- 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 au-dessus 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 ordinateurs 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 le groupe **Réseau** 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**.

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 groupes et des utilisateurs partout à l'intérieur de la hiérarchie du groupe **Réseau**. 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 qu'une autre politique lui ait été affectée. Pour plus d'informations sur l'héritage de la politique, reportez-vous à « [Affecter des politiques à des objets du réseau](#) » (p. 70).

Supprimer des groupes

Un groupe ne peut pas être supprimé s'il contient au moins un ordinateur. Déplacez tous les ordinateurs 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 ordinateurs individuels.

Pour supprimer un groupe :

1. Sélectionnez le groupe vide dans le panneau de droite 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**.

6.3. Afficher des informations sur un ordinateur

Vous pouvez obtenir des informations détaillées sur chaque ordinateur à partir de la page **Réseau** y compris l'OS, l'IP, la date et l'heure auxquelles il a été vu pour la dernière fois, etc.

Pour obtenir des informations sur un ordinateur :

1. Allez sur la page **Réseau**.
2. Sélectionnez le groupe du réseau souhaité dans le panneau de gauche.
Tous les ordinateurs du groupe sélectionné apparaissent dans le tableau du panneau de droite.
3. Vous pouvez identifier facilement l'état de l'ordinateur en consultant l'icône correspondante. Pour plus d'informations, reportez-vous à « [Vérifier l'état de l'ordinateur](#) » (p. 32).
4. Consultez les informations affichées sur les colonnes pour tous les ordinateurs :
 - **Nom** : nom de l'ordinateur
 - **OS** : système d'exploitation installé sur l'ordinateur.
 - **IP** : adresse IP de l'ordinateur.
 - **Dernière connexion** : date et heure auxquelles l'ordinateur a été vu en ligne pour la dernière fois.

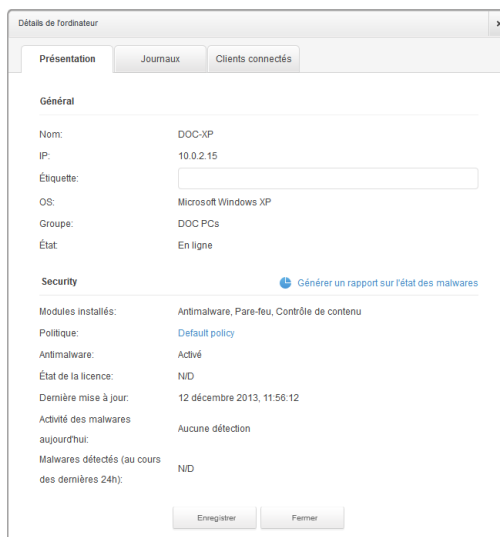


Note

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** : l'étiquette ajoutée à l'ordinateur dans la fenêtre **Détails de l'ordinateur**.

5. Cliquez sur le nom de l'ordinateur administré qui vous intéresse. La fenêtre **Détails de l'ordinateur** apparaît :



Détails de l'ordinateur

- L'onglet **Présentation** indique les informations suivantes :
 - Informations générales sur l'ordinateur telles que son nom, adresse IP, système d'exploitation, groupe parent et état actuel. Vous pouvez également affecter une étiquette à l'ordinateur. Vous pouvez donc rechercher et filtrer les ordinateurs par étiquette à l'aide du champ de recherche de la colonne Étiquette du tableau de droite de la page **Réseau**.
 - Informations de sécurité liées à Endpoint Security installé sur l'ordinateur sélectionné, telles que les modules installés, la politique affectée, l'état de l'antimalware, l'état de la licence, la dernière mise à jour et les malwares détectés au cours des dernières 24 heures. Vous pouvez également avoir un aperçu rapide du nombre de détections de malwares sur l'ordinateur pour la journée en cours.
 - Cliquez sur **Générer un rapport sur l'état des malwares** pour accéder aux options du rapport sur les malwares pour l'ordinateur sélectionné.

Pour plus d'informations, reportez-vous à « [Création de rapports](#) » (p. 122)




Note

Chaque propriété générant des problèmes de sécurité est signalée par l'icône . Consultez l'info-bulle de l'icône pour plus d'informations. D'autres enquêtes locales peuvent être nécessaires.

- Cliquez sur l'onglet **Journaux** pour voir des informations détaillées sur toutes les tâches d'analyse effectuées sur l'ordinateur. Cliquez sur le rapport d'analyse qui vous intéresse pour l'ouvrir dans une nouvelle page du navigateur.

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 .

Cliquez sur le bouton  **Actualiser** dans l'angle inférieur gauche du tableau pour mettre à jour la liste des journaux d'analyse.

6.4. Trier, filtrer et rechercher des ordinateurs

En fonction du nombre d'ordinateurs, le tableau des ordinateurs peut comporter plusieurs pages (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 zones de recherche sous les en-têtes de colonne ou le menu du **Filtres** en haut du tableau afin de filtrer les données affichées. Vous pouvez, par exemple, rechercher un ordinateur spécifique ou choisir d'afficher uniquement les ordinateurs administrés.

6.4.1. Trier des ordinateurs

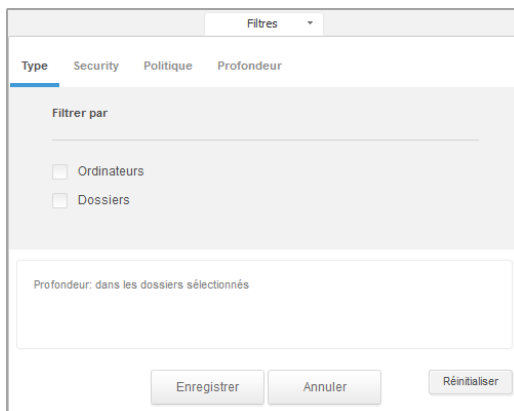
Pour trier les données en fonction d'une colonne spécifique, cliquez sur les en-têtes de la colonne. Par exemple, si vous souhaitez classer les ordinateurs par nom, cliquez sur l'en-tête **Nom**. Si vous cliquez de nouveau sur l'en-tête, les ordinateurs s'afficheront dans l'ordre inverse.



Trier des ordinateurs

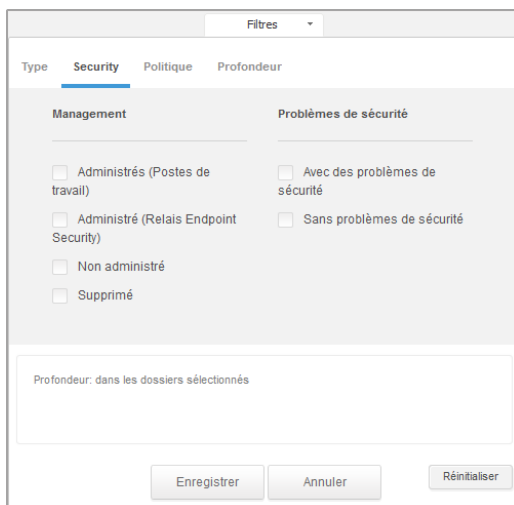
6.4.2. Filtrer des ordinateurs

1. Sélectionnez le groupe souhaité dans le panneau de gauche.
2. Cliquez sur le menu **Filtres** situé au-dessus du tableau.
3. Sélectionnez les critères de filtrage comme suit :
 - **Type**. Sélectionnez le type d'entités que vous souhaitez afficher (ordinateurs, dossiers ou les deux).



Ordinateurs - Filtrer par type

- **Sécurité.** Choisissez d'afficher les ordinateurs par état d'administration et de sécurité.



Ordinateurs - Filtrer par sécurité

- **La politique.** Sélectionnez le modèle de politique à partir duquel vous souhaitez filtrer les ordinateurs ainsi que l'état d'attribution de la politique (Affecté ou En attente).

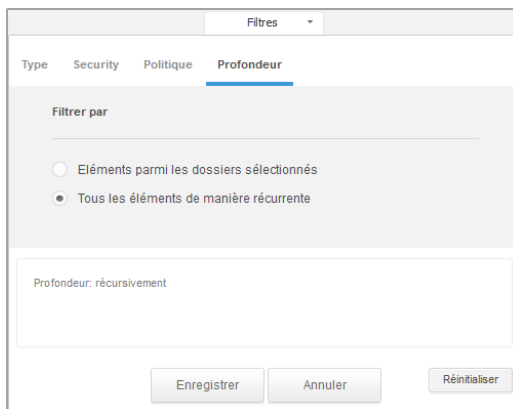


The screenshot shows the 'Filtres' (Filters) window in the Bitdefender console. The 'Politique' (Policy) tab is selected. The window contains the following elements:

- Navigation tabs: Type, Security, **Politique**, Profondeur.
- Modèle: A dropdown menu.
- État: Two checkboxes, 'Affecté' and 'En attente', both of which are currently unchecked.
- Profondeur: A text input field containing the text 'récursivement'.
- Buttons: 'Enregistrer' (Save), 'Annuler' (Cancel), and 'Réinitialiser' (Reset).

Ordinateurs - Filtrer par politique

- **Profondeur.** Lorsque les réseaux informatiques ont une 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 dans ses sous-groupes.



The screenshot shows the 'Filtres' (Filters) window in the Bitdefender console with the 'Profondeur' (Depth) tab selected. The window contains the following elements:

- Navigation tabs: Type, Security, Politique, **Profondeur**.
- Filtrer par: A section with two radio button options:
 - Eléments parmi les dossiers sélectionnés
 - Tous les éléments de manière récurrente
- Profondeur: A text input field containing the text 'récursivement'.
- Buttons: 'Enregistrer' (Save), 'Annuler' (Cancel), and 'Réinitialiser' (Reset).

Ordinateurs - Filtrer par profondeur



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.

6.4.3. 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	OS	IP	Dernière connexion	Étiquette
<input type="checkbox"/> WIN-TAU6HBSO3TQ	Windows	192.168.1.3	N/D	N/D

Recherche d'ordinateurs

6.5. Exécuter des tâches sur des ordinateurs

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. 42)
- « [Installer Client](#) » (p. 49)
- « [Modifier le programme d'installation](#) » (p. 52)
- « [Désinstaller Client](#) » (p. 53)
- « [Mettre à jour le client](#) » (p. 53)
- « [Redémarrer votre ordinateur.](#) » (p. 54)
- « [Découverte du réseau](#) » (p. 54)

Vous pouvez choisir de créer des tâches individuellement pour chaque ordinateur ou pour des groupes d'ordinateurs. Vous pouvez par exemple installer à distance Endpoint Security 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 uniquement **Installer le client**, 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.

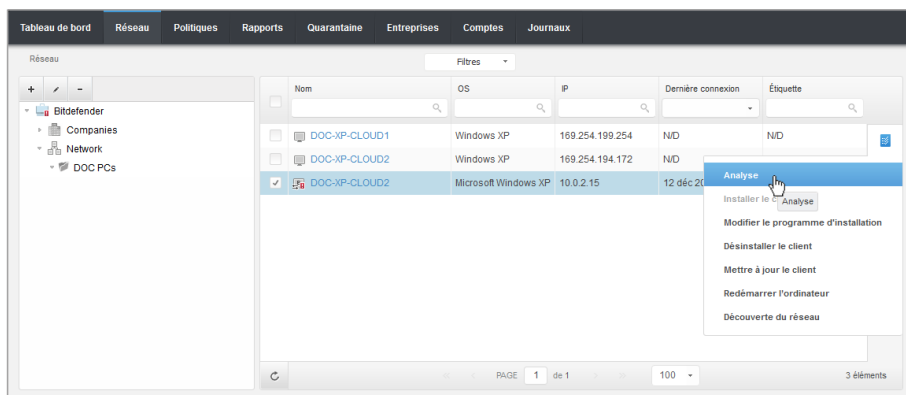
Une fois créée, la tâche commencera à s'exécuter immédiatement sur les ordinateurs en ligne. Si un ordinateur est hors ligne, la tâche s'exécutera dès qu'il sera de nouveau en ligne.

Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à [Viewing and Managing Tasks](#).

6.5.1. Analyse

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

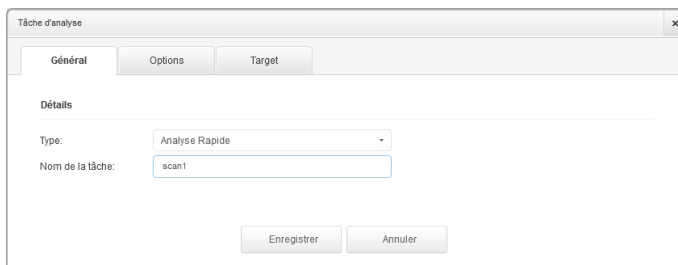
1. Allez sur la page **Réseau**.
2. Sélectionnez le groupe souhaité dans le panneau de gauche. Tous les ordinateurs du groupe sélectionné apparaissent dans le tableau du panneau de droite.
3. Cochez les cases correspondant aux ordinateurs que vous souhaitez analyser.
4. Cliquez sur le bouton  **Tâche** à droite du tableau et sélectionnez **Analyser**.



Tâche Analyse des ordinateurs

Une fenêtre de configuration s'affichera.

5. 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 ordinateurs - Configurer les paramètres généraux

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

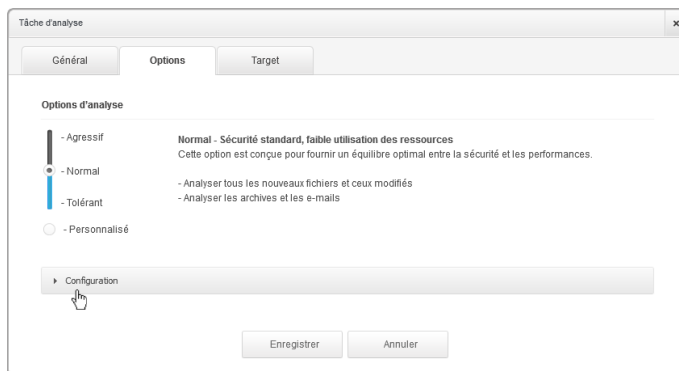
- **Quick Scan** utilise l'analyse dans le Cloud pour détecter les malwares présents sur le système. La réalisation d'une analyse rapide dure généralement moins d'une minute et n'utilise qu'une petite partie des ressources du système dont a besoin une analyse antivirus classique.



Note

L'analyse rapide détecte uniquement les malwares présents, sans appliquer aucune action. Si des malwares sont détectés lors d'une Analyse rapide, vous devez exécuter une tâche Analyse Complète du Système pour supprimer les malwares détectés.

- L'**Analyse Complète** analyse l'ensemble de votre ordinateur afin de détecter tous les types de malwares menaçant sa sécurité : virus, spywares, adwares, rootkits et autres.
- **Analyse personnalisée** vous permet de sélectionner les emplacements à analyser et de configurer les options d'analyse. Pour définir une tâche personnalisée :
 - 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 allez dans la section **Configuration**.



Tâche Analyse des ordinateurs

Voici les options proposées :

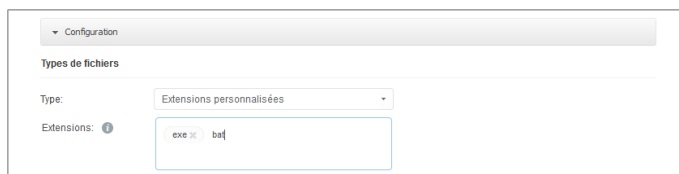
- **Types de fichiers.** Utilisez ces options pour spécifier les types de fichiers que vous souhaitez analyser. Vous pouvez configurer Endpoint Security afin qu'il analyse tous les fichiers (quelle que soit l'extension des fichiers), ou uniquement les fichiers d'applications ou certaines extensions de fichiers que vous considérez dangereuses. L'analyse de tous les fichiers consultés offre une protection maximale, alors que l'analyse des applications offre uniquement une analyse 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 « [Liste des types de fichier d'Application](#) » (p. 145).

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.



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'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 dans les archives.** 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 informatique nécessaire pour faire démarrer le processus de boot. Quand un virus infecte le secteur de boot, 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 masqués à l'aide de ce logiciel.
 - **Rechercher les keyloggers.** Sélectionnez cette option pour rechercher les logiciels [keyloggers](#).
 - **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.
- **Actions.** En fonction du type de fichier détecté, les actions suivantes sont menées automatiquement :

- **Quand un fichier infecté est détecté.** Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la Base de Données de Signatures de Codes Malveillants Bitdefender.Endpoint Security 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, Endpoint Security tente 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 détectés en tant que fichiers suspects par l'analyse heuristique. B-HAVE étant une technologie d'analyse heuristique, Endpoint Security ne peut pas être certain que le fichier est réellement infecté par des malwares. 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.

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 supprime 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 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 « [Utilisation des variables du système](#) » (p. 145)
- c. 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.

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

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

Tâche Analyse des ordinateurs - Définir des exclusions

Vous pouvez choisir d'utiliser des exclusions globales pour une analyse spécifique ou de définir des exclusions explicites pour chaque analyse. Pour plus d'informations sur les exclusions, reportez-vous à « [Exclusions](#) » (p. 93).

6. Cliquez sur **Enregistrer** pour créer la tâche d'analyse. Un message de confirmation s'affichera.
7. Vous pouvez afficher et gérer la tâche sur la page **Réseau > Tâches**. Pour plus d'informations, reportez-vous à [Viewing and Managing Tasks](#).

6.5.2. Installer Client

Pour protéger vos postes de travail avec Security for Endpoints, vous devez installer Endpoint Security sur chacun d'entre eux.



Avertissement

- Le premier ordinateur sur lequel vous installez la protection doit avoir le rôle Endpoint Security Relay, vous ne pourrez sinon pas déployer Endpoint Security sur les autres ordinateurs du réseau.
- L'ordinateur avec le rôle Endpoint Security Relay doit être allumé et en ligne pour que les clients communiquent avec Control Center.

Lorsque vous aurez installé un client Endpoint Security avec un rôle Endpoint Security Relay dans un réseau, celui-ci détectera automatiquement les ordinateurs non protégés de ce réseau.

La protection Security for Endpoints peut ensuite être installée sur ces 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 Security for Endpoints sur des logiciels de sécurité existants 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 Endpoints sur un ou plusieurs ordinateurs :


1. Allez sur la page **Réseau**.
2. Sélectionnez le groupe du réseau 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 ordinateurs non administrés. Cliquez sur le bouton **Filtres** et sélectionnez les options suivantes : **Non**

administré dans la catégorie **Sécurité** et **Tous les éléments de manière récurrente** dans la catégorie **Profondeur**.

3. Sélectionnez les entités (ordinateurs ou groupes d'ordinateurs) sur lesquelles vous souhaitez installer la protection.
4. Cliquez sur le bouton  **Tâches** à droite du tableau et sélectionnez **Installer le client**. L'assistant **Installer le client** apparaît.
5. Configurer les options d'installation :
 - Sélectionnez le rôle que vous souhaitez que le client ait :
 - **Poste de travail**. Sélectionnez cette option si vous souhaitez installer le client sur un poste de travail standard.
 - **Endpoint Security Relay**. Sélectionnez cette option pour installer le client avec le rôle Endpoint Security Relay sur l'ordinateur cible. Endpoint Security Relay est un rôle spécial qui installe un serveur de mise à jour sur la machine cible avec Endpoint Security, lequel peut être utilisé pour mettre à jour tous les autres clients du réseau, faisant diminuer ainsi la consommation de bande passante entre les machines clientes et le Control Center.
 - Sélectionnez les modules de protection que vous voulez installer. Veuillez noter que seule la protection antimalware est disponible pour les systèmes d'exploitation serveurs.
 - Dans le champ **Langue**, sélectionnez la langue souhaitée pour l'interface du client.
 - Sélectionnez **Analyser avant l'installation** si vous souhaitez vous assurer que les ordinateurs sont sains avant d'y installer Endpoint Security. Une analyse rapide dans le Cloud sera réalisée sur les ordinateurs correspondants avant de commencer l'installation.
 - Endpoint Security est installé dans le répertoire d'installation par défaut sur les ordinateurs sélectionnés. Sélectionnez **Utiliser le chemin d'installation personnalisé** si vous souhaitez installer Endpoint Security à un emplacement différent. Dans ce cas, saisissez le chemin souhaité dans le champ correspondant. Utilisez les conventions Windows lorsque vous saisissez le chemin (par exemple, D:\folder). Si le dossier spécifié n'existe pas, il sera créé lors de l'installation.
 - Lors de l'installation silencieuse, l'ordinateur fait l'objet d'une analyse antimalware. Un redémarrage du système peut être nécessaire pour terminer la désinfection de malwares.

Sélectionnez **Redémarrer automatiquement (si nécessaire)** afin de vous assurer que les malwares détectés ont été complètement supprimés avant l'installation. Sinon, l'installation peut échouer.

- Vous pouvez, si vous le souhaitez, définir un mot de passe pour empêcher les utilisateurs de supprimer la protection. Sélectionnez **Mot de passe de désinstallation** et indiquez le mot de passe souhaité dans les champs correspondants.
 - Cliquez sur **Suivant**.
 - En fonction du rôle du client (Poste de travail ou Endpoint Security Relay), sélectionnez l'entité via laquelle les clients communiqueront :
 - **Cloud Bitdefender**, si vous souhaitez mettre à jour les clients directement à partir d'Internet.
 - **Endpoint Security Relay**, si vous souhaitez mettre à jour les clients via les postes de travail Endpoint Security Relay installés dans votre réseau. Dans ce cas, tous les postes de travail avec le rôle Endpoint Security Relay détectés dans votre réseau apparaîtront dans le tableau ci-dessous. Sélectionnez le Endpoint Security Relay que vous souhaitez utiliser pour les mises à jour clientes.
6. Cliquez sur **Suivant**.
7. Dans la section **Admin. des authentifications**, indiquez les identifiants d'administration requis pour l'authentification à distance sur les postes de travail sélectionnés.

Vous pouvez ajouter les identifiants requis en saisissant l'utilisateur et le mot de passe de tous les systèmes d'exploitation cibles.



Note

Un message d'avertissement s'affiche tant que vous n'avez sélectionné aucun identifiant. Cette étape est obligatoire pour installer à distance Endpoint Security sur les ordinateurs.

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. 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 indiquez le nom d'un compte d'utilisateur de domaine (par exemple, `domaine\utilisateur` ou `utilisateur@domaine.com`).



Note

Les identifiants spécifiés sont enregistrés automatiquement dans votre Administrateur des authentifications afin que vous n'ayez pas à les saisir la prochaine fois.


- b. Cliquez sur le bouton **+ Ajouter**. Le compte est ajouté à la liste des identifiants.
- c. Cochez la case correspondant au compte que vous souhaitez utiliser.

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 [Viewing and Managing Tasks](#).

6.5.3. Modifier le programme d'installation

Pour modifier les modules de protection installés sur un ou plusieurs ordinateurs :

1. Allez sur la page **Réseau**.
2. Sélectionnez le groupe souhaité dans le panneau de gauche. Tous les ordinateurs du groupe sélectionné apparaissent dans le tableau du panneau de droite.
3. Cochez les cases correspondant aux ordinateurs administrés sur lesquels vous souhaitez changer les modules de protection installés.
4. Cliquez sur le bouton  **Tâche** à droite du tableau et sélectionnez **Modifier le programme d'installation**.
5. Dans la section **Modules**, sélectionnez uniquement les modules de protection que vous souhaitez installer :

Antimalware

Le module Antimalware protège le système contre tous les types de malwares (virus, chevaux de Troie, spywares, rootkits, adwares, etc.).

Pare-feu

Le pare-feu protège votre ordinateur contre les tentatives de connexions entrantes et sortantes non autorisées.

Contrôle de contenu

Le module Contrôle de contenu vous aide à contrôler l'accès des utilisateurs à Internet et aux applications. Veuillez noter que les paramètres configurés du Contrôle de contenu s'appliqueront à tous les utilisateurs qui se connecteront aux ordinateurs cibles.



Note


Veuillez noter que seule la protection antimalware est disponible pour les systèmes d'exploitation serveurs.

6. Cochez l'option **Redémarrer si nécessaire** pour permettre à l'ordinateur de redémarrer automatiquement pour terminer l'installation.
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 [Viewing and Managing Tasks](#).

6.5.4. Désinstaller Client

Pour désinstaller à distance la protection Security for Endpoints sur un ou plusieurs ordinateurs :

1. Allez sur la page **Réseau**.
2. Sélectionnez le groupe souhaité dans le panneau de gauche. Tous les ordinateurs du groupe sélectionné apparaissent dans le tableau du panneau de droite.
3. Cochez les cases correspondant aux ordinateurs sur lesquels vous souhaitez désinstaller la protection Security for Endpoints.
4. Cliquez sur le bouton  **Tâche** à droite du tableau et sélectionnez **Désinstaller le client**.
5. Une fenêtre de configuration apparaît, vous permettant de choisir de conserver les éléments en quarantaine sur la machine cliente.
6. Cliquez sur **Enregistrer** pour créer 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 [Viewing and Managing Tasks](#).



Note


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

6.5.5. 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 **Détails de l'ordinateur**. Pour plus d'informations, reportez-vous à « [Ordinateurs avec des problèmes de sécurité](#) » (p. 34).

Un client non à jour présente un problème de sécurité. Dans ce cas, vous devriez exécuter une mise à jour du client 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 à distance sur les ordinateurs administrés :

1. Allez sur la page **Réseau**.
2. Sélectionnez le groupe souhaité dans le panneau de gauche. Tous les ordinateurs du groupe sélectionné apparaissent dans le tableau du panneau de droite.
3. Cochez les cases des ordinateurs sur lesquels vous souhaitez exécuter une mise à jour du client.
4. Cliquez sur le bouton  **Tâche** à droite du tableau et sélectionnez **Mettre à jour le client**.
5. Vous devrez confirmer votre action en cliquant sur **Oui**. 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 [Viewing and Managing Tasks](#).


6.5.6. Redémarrer votre ordinateur.

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 le groupe souhaité dans le panneau de gauche. Tous les ordinateurs du groupe sélectionné apparaissent dans le tableau du panneau de droite.
3. Cochez les cases correspondant aux ordinateurs que vous souhaitez faire redémarrer.
4. Cliquez sur le bouton  **Tâche** à droite du tableau et sélectionnez **Redémarrer l'ordinateur**.
5. 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.
6. 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 [Viewing and Managing Tasks](#).

6.5.7. Découverte du réseau

La découverte du réseau est effectuée automatiquement toutes les heures par Endpoint Security avec le rôle Endpoint Security Relay. Cependant, vous pouvez exécuter une tâche de découverte du réseau manuellement à partir de Control Center à tout moment, en commençant par toute machine protégée par Endpoint Security.


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

1. Allez sur la page **Réseau**.
2. Sélectionnez le groupe d'ordinateurs souhaité dans le panneau de gauche. Tous les ordinateurs du groupe sélectionné apparaissent dans le tableau du panneau de droite.
3. Cochez les cases correspondant aux ordinateurs avec lesquels vous souhaitez effectuer la découverte du réseau.

4. Cliquez sur le bouton  **Tâche** à droite du tableau et sélectionnez **Découverte du réseau**.
5. Une 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 [Viewing and Managing Tasks](#).

6.6. 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 le groupe souhaité 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.
3. Cochez les cases correspondant aux ordinateurs que vous souhaitez inclure dans le rapport.
4. Cliquez sur le bouton  **Rapport** à droite du tableau et sélectionnez le type de rapport dans le menu. Les rapports d'activité contiennent uniquement des données de la semaine précédente. Pour plus d'informations, reportez-vous à « [Types de rapports disponibles](#) » (p. 119).
5. Configurer les options de rapports. Pour plus d'informations, reportez-vous à « [Création de rapports](#) » (p. 122)
6. 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.

6.7. Affecter des politiques

Les paramètres de sécurité sur les ordinateurs sont administrés à l'aide de [politiques](#).

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



Note

Vous pouvez afficher ou modifier les paramètres de sécurité pour les ordinateurs administrés ou pour les groupes. Pour faciliter cette tâche, vous pouvez [filtrer](#) le contenu du tableau uniquement par ordinateurs administrés.

Pour afficher la politique affectée à un ordinateur spécifique :

1. Allez sur la page **Réseau**.

2. Sélectionnez le groupe souhaité dans le panneau de gauche. Tous les ordinateurs du groupe sélectionné apparaissent dans le tableau du panneau de droite.
3. Cliquez sur le nom de l'ordinateur administré qui vous intéresse. Une fenêtre détails apparaîtra.
4. Dans la section **Sécurité**, cliquez sur le nom de la politique en cours pour afficher ses paramètres.
5. 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 tous les autres ordinateurs auxquels on a affecté la même politique.

Pour plus d'informations sur la modification des politiques de l'ordinateur, reportez-vous à « [Politiques de l'ordinateur](#) » (p. 72).

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

1. Allez sur la page **Réseau**.
2. Sélectionnez le groupe souhaité dans le panneau de gauche. Tous les ordinateurs du groupe sélectionné apparaissent dans le tableau du panneau de droite.
3. Cochez la case de l'ordinateur ou du groupe souhaité. Vous pouvez sélectionner un ou plusieurs objets du même type du même niveau uniquement.
4. Cliquez sur le bouton  **Politique** à droite du tableau.
5. Effectuez la configuration nécessaire dans la fenêtre **Attribution de la politique**. Pour plus d'informations, reportez-vous à « [Affecter des politiques à des objets du réseau](#) » (p. 70).

6.8. Supprimer des ordinateurs de l'inventaire du réseau

Si vous ne prévoyez pas d'administrer certains ordinateurs détectés, vous pouvez choisir de les exclure de l'inventaire du réseau. Vous pouvez également supprimer définitivement les ordinateurs exclus de l'inventaire du réseau.

6.8.1. Exclure des ordinateurs de l'inventaire du réseau

Pour exclure des ordinateurs de l'inventaire du réseau :

1. Allez sur la page **Réseau**.
2. Sélectionnez le groupe souhaité dans le panneau de gauche. Tous les ordinateurs du groupe sélectionné apparaissent dans le tableau du panneau de droite.
3. Cochez la case correspondant à l'ordinateur que vous souhaitez exclure.

4. Cliquez sur le bouton **Supprimer** à droite du tableau. Vous devrez confirmer votre action en cliquant sur **Oui**.



Note

Si vous supprimez un ordinateur administré, Endpoint Security sera automatiquement désinstallé de celui-ci.

Une fois que vous avez supprimé un ordinateur, vous ne pouvez plus le voir dans le tableau. Les ordinateurs supprimés existent toujours dans la base de données de Security for Endpoints (Console dans le Cloud) mais ils ne sont plus visibles.

Vous pouvez souhaiter administrer de nouveau certains ordinateurs supprimés. Vous devez dans ce cas afficher les ordinateurs supprimés et installer Endpoint Security sur ceux qui vous intéressent. Pour afficher les ordinateurs supprimés, cliquez sur le menu **Filtres** situé au-dessus du tableau, allez dans l'onglet **Sécurité**, sélectionnez l'option **Supprimé** puis cliquez sur **Enregistrer**.

The screenshot shows a 'Filtres' (Filters) dropdown menu. Under the 'Security' tab, there are two main sections: 'Management' and 'Problèmes de sécurité' (Security Issues). In the 'Management' section, the 'Supprimé' (Deleted) checkbox is checked. In the 'Problèmes de sécurité' section, the 'Sans problèmes de sécurité' (No security issues) checkbox is checked. Below these sections, there is a 'Profondeur' (Depth) section with the text 'dans les dossiers sélectionnés' (in selected folders). At the bottom of the filter menu, there are three buttons: 'Enregistrer' (Save), 'Annuler' (Cancel), and 'Réinitialiser' (Reset).

Ordinateurs - Filtrer par postes de travail supprimés




Note

Si vous réinstallez la protection sur un ordinateur exclu, il sera détecté comme étant administré et restauré dans le tableau.

6.8.2. Supprimer définitivement des ordinateurs

Pour supprimer définitivement des ordinateurs de l'inventaire du réseau :

1. Allez sur la page **Réseau**.
2. Sélectionnez le groupe souhaité dans le panneau de gauche. Tous les ordinateurs du groupe sélectionné apparaissent dans le tableau du panneau de droite.
3. Filtrez le contenu du tableau par ordinateurs **Supprimés**.
4. Cochez la case correspondant aux ordinateurs que vous souhaitez supprimer.
5. Cliquez sur le bouton  **Supprimer** à droite du tableau. Vous devrez confirmer votre action en cliquant sur **Oui**.

Les ordinateurs correspondants sont supprimés définitivement de la base de données de Security for Endpoints (Console dans le Cloud).



Avertissement

Vous ne pouvez pas restaurer un ordinateur ayant été supprimé définitivement de la base de données de Security for Endpoints (Console dans le Cloud).

6.9. Packages d'installation

Les packages de protection de Security for Endpoints (Console dans le Cloud) peuvent être installés sur les OS cibles du réseau en les déployant à partir du Control Center ou en téléchargeant le package d'installation et en l'exécutant sur les postes et les serveurs physiques du réseau.

Vous pouvez gérer les packages d'installation à partir de la page **Réseau > Packages**.

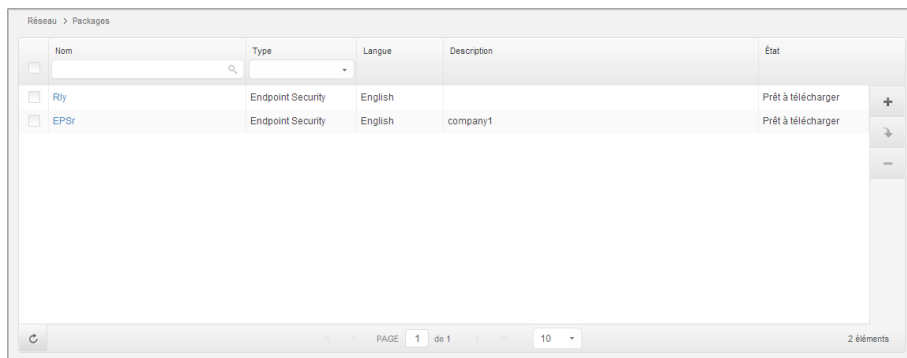
6.9.1. Créer des packages d'installation

Vous pouvez avoir besoin d'apporter certaines modifications aux packages d'installation, afin de mieux répondre aux besoins en sécurité.

Création de packages d'installation d'Endpoint Security

Pour créer un package d'installation d'Endpoint Security :

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



Réseau > Packages

<input type="checkbox"/>	Nom	Type	Langue	Description	État	
<input type="checkbox"/>	Rly	Endpoint Security	English		Prêt à télécharger	+
<input type="checkbox"/>	EPSr	Endpoint Security	English	company1	Prêt à télécharger	-

PAGE 1 de 1 10 2 éléments

La page Packages

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

Endpoint Security

Options

Avancé

Détails

Nom: * EPS-FR

Description: Endpoint Security FR

Général

Role: Endpoint Security Relay

Société: Sélectionner une entreprise

Modules à installer :

Antimalware ⓘ

Pare-feu ⓘ

Contrôle de contenu

Configuration

Langue: Français

Analyser avant l'installation

Utiliser le chemin d'installation personnalisé

Mot de passe de désinstallation

Mot de passe: Cliquez ici pour changer le m...

Confirmer: Veuillez saisir de nouveau le

Endpoint Security by Bitdefender désinstalle automatiquement les autres logiciels de sécurité.

Suivant > Annuler

Créer des packages Endpoint Security - Options


- Indiquez un nom et une description explicites pour le package d'installation que vous souhaitez créer.
- Sélectionnez le rôle de l'ordinateur cible :
 - Poste de travail.** Sélectionnez cette option pour créer le package pour un poste de travail standard.
 - Endpoint Security Relay.** Sélectionnez cette option pour créer le package pour un poste de travail avec le rôle Endpoint Security Relay. Endpoint Security Relay est un rôle spécial qui installe un serveur de mise à jour sur la machine cible avec Endpoint Security, lequel peut être utilisé pour mettre à jour tous les autres clients du réseau, faisant diminuer ainsi la consommation de bande passante entre les machines clientes et le Control Center.
- Sélectionnez l'entreprise où le package d'installation sera utilisé.
- Sélectionnez les modules de protection que vous voulez installer.

8. Dans le champ **Langue**, sélectionnez la langue souhaitée pour l'interface du client.
9. Sélectionnez **Analyser avant l'installation** si vous souhaitez vous assurer que les ordinateurs sont sains avant d'y installer Endpoint Security. Une analyse rapide dans le Cloud sera réalisée sur les ordinateurs correspondants avant de commencer l'installation.
10. Endpoint Security est installé dans le répertoire d'installation par défaut sur les ordinateurs sélectionnés. Sélectionnez **Utiliser le chemin d'installation personnalisé** si vous souhaitez installer Endpoint Security à un emplacement différent. Dans ce cas, saisissez le chemin souhaité dans le champ correspondant. Utilisez les conventions Windows lorsque vous saisissez le chemin (par exemple, `D:\folder`). Si le dossier spécifié n'existe pas, il sera créé lors de l'installation.
11. Vous pouvez, si vous le souhaitez, définir un mot de passe pour empêcher les utilisateurs de supprimer la protection. Sélectionnez **Mot de passe de désinstallation** et indiquez le mot de passe souhaité dans les champs correspondants.
12. Cliquez sur **Suivant**.
13. En fonction du rôle du package d'installation (Endpoint ou Endpoint Security Relay), sélectionnez l'entité auprès de laquelle les ordinateurs cibles se connecteront régulièrement pour mettre à jour le client :
 - **Cloud Bitdefender**, si vous souhaitez mettre à jour les clients directement à partir d'Internet.
 - **Endpoint Security Relay**, si vous souhaitez mettre à jour les clients via les postes de travail Endpoint Security Relay installés dans votre réseau. Dans ce cas, tous les postes de travail avec le rôle Endpoint Security Relay détectés dans votre réseau apparaîtront dans le tableau ci-dessous. Sélectionnez le Endpoint Security Relay que vous souhaitez utiliser pour les mises à jour clientes.
14. Cliquez sur **Enregistrer**.

Le nouveau package d'installation apparaîtra dans la liste de packages de l'entreprise cible.

6.9.2. Téléchargement de packages d'installation

Pour télécharger des packages d'installation d'Endpoint Security :

1. Identifiez-vous auprès de Control Center à partir de l'ordinateur sur lequel vous souhaitez installer la protection.
2. Accédez à la page **Réseau > Packages**.
3. Sélectionnez le package d'installation d'Endpoint Security que vous souhaitez télécharger.
4. Cliquez sur le bouton  **Télécharger** sur la partie droite du tableau et sélectionnez le type de programme d'installation que vous souhaitez utiliser. Deux types de fichiers d'installation sont disponibles :

- **Programme de téléchargement** . Le downloader commence par télécharger le kit d'installation complet sur les serveurs cloud de Bitdefender avant de lancer l'installation. Il est peu volumineux et peut être exécuté à la fois sur les systèmes 32 et 64 bits (ce qui facilite sa distribution). Il requiert par contre une connexion active à Internet.
- **Kit complet**. Le kit complet est à utiliser pour installer la protection sur les ordinateurs avec une connexion Internet lente ou sans connexion. Téléchargez ce fichier sur un ordinateur connecté à Internet puis transmettez-le à d'autres ordinateurs à l'aide de supports de stockage externes ou d'un partage réseau.



Note

Versions du kit complet disponibles :

- **OS Windows** : systèmes 32 et 64 bits
- **Mac OS X** : uniquement les systèmes 64 bits

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

5. Enregistrez le fichier sur l'ordinateur.

6.10. 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.

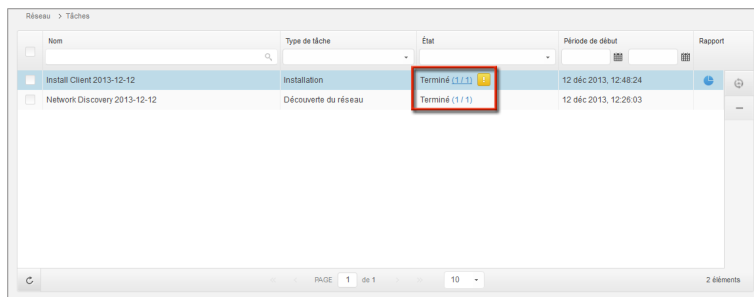
Vous pouvez effectuer les actions suivantes à partir de la page **Réseau > Tâches** :

- [Vérifier l'état d'une tâche](#)
- [Afficher les rapports sur les tâches](#)
- [Relancer des tâches](#)
- [Supprimer des tâches](#)

6.10.1. 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.



Nom	Type de tâche	État	Période de début	Rapport
Install Client 2013-12-12	Installation	Terminé (1/1)	12 déc 2013, 12:48:24	
Network Discovery 2013-12-12	Découverte du réseau	Terminé (1/1)	12 déc 2013, 12:26:03	

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 :

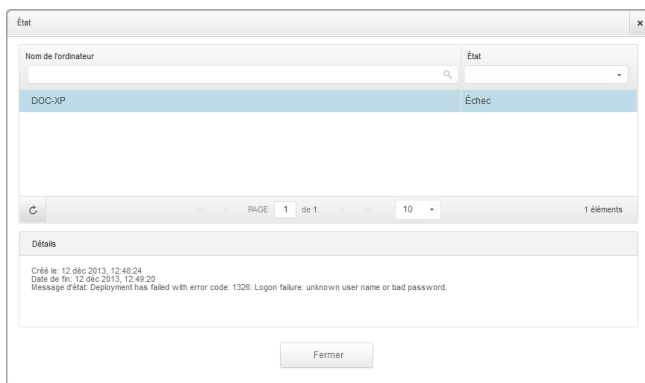
- **En attente**, lorsque aucune des sous-tâches n'a pas encore démarrée.
- **En cours**, lorsque toutes les sous-tâches sont en cours d'exécution. L'état de la tâche principale demeure "En cours" tant que la dernière sous-tâche n'a pas été effectuée.
- **Terminé**, lorsque toutes les sous-tâches sont 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.
- **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.
- **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.

Pour afficher les détails de chaque sous-tâche, sélectionnez-la et consultez la section **Détails** en bas du tableau.




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.

6.10.2. 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. Cochez la case correspondant à la tâche d'analyse qui vous intéresse.
3. 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. 119).

6.10.3. Relancer 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 relancer les tâches ayant échoué plutôt que d'en créer de nouvelles, en procédant comme suit :

1. Accédez à la page **Réseau > Tâches**.
2. Cochez les cases correspondant aux tâches ayant échoué.

3. Cliquez sur le bouton  **Relancer** à droite 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 **Relancer** est disponible uniquement lorsque toutes les sous-tâches sont terminées et exécutera uniquement les sous-tâches ayant échoué.

6.10.4. Supprimer des tâches

Pour éviter que la liste des tâches ne soit surchargée, nous vous recommandons de supprimer les tâches dont vous n'avez plus besoin.

1. Accédez à la page **Réseau > Tâches**.
2. Cochez la case correspondant à la tâche que vous souhaitez supprimer.
3. Cliquez sur le bouton  **Supprimer** à droite du tableau. Vous devrez confirmer votre action en cliquant sur **Oui**.



Avertissement

Supprimer une tâche en attente annulera également la tâche.

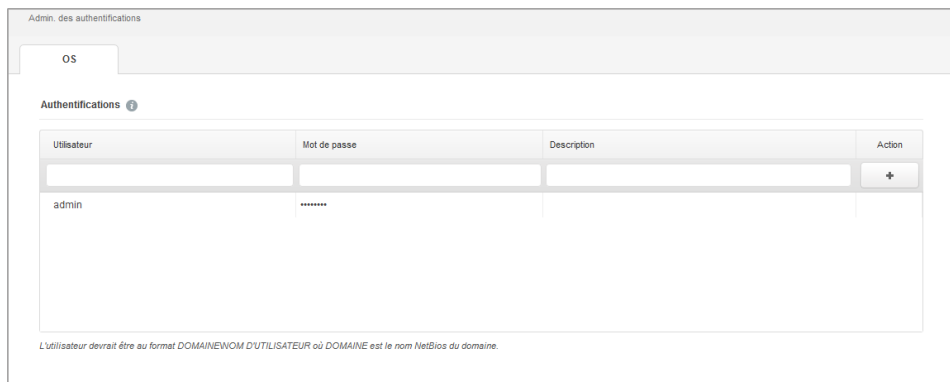
Si une tâche en cours est supprimée, toutes les sous-tâches en attente seront annulées. Dans ce cas, toutes les sous-tâches terminées ne peuvent pas être annulées.

6.11. Admin. des authentifications

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

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

6.11.1. Ajouter des identifiants dans l'Administrateur des authentifications



Admin. des authentifications

OS

Authentifications ⓘ

Utilisateur	Mot de passe	Description	Action
admin		+

L'utilisateur devrait être au format DOMAINE\NOM D'UTILISATEUR où DOMAINE est le nom NetBios du domaine.

Admin. des authentifications

1. Saisissez le nom d'utilisateur et le mot de passe d'un compte administrateur dans les champs correspondants. 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 indiquez le nom d'un compte d'utilisateur de domaine (par exemple, `domaine\utilisateur` ou `utilisateur@domaine.com`).
2. Cliquez sur le bouton **+** **Ajouter**. 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. 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 précise les paramètres de sécurité à appliquer aux ordinateurs.

Juste après l'installation, les ordinateurs de l'inventaire se voient attribuer la politique par défaut, qui est préconfigurée avec les paramètres de protection recommandés. Vous ne pouvez pas modifier ou supprimer la politique par défaut. Vous pouvez uniquement l'utiliser comme modèle pour la [création de nouvelles politiques](#).

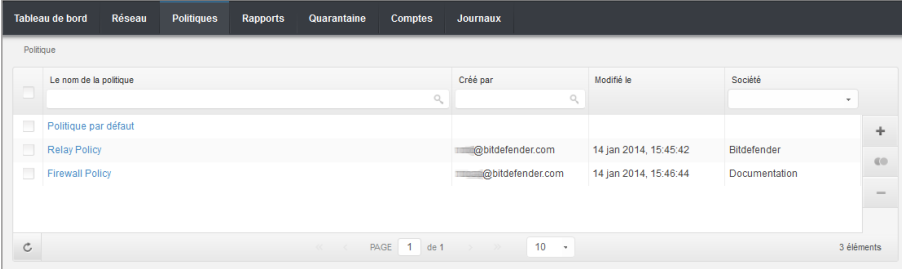
Vous pouvez créer autant de politiques que nécessaire en fonction des besoins en sécurité.

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 objets du réseau peuvent uniquement avoir une politique active à la fois.
- 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. Veuillez noter que seule la protection antimalware est disponible pour les systèmes d'exploitation serveurs.
- 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.

7.1. Administration des politiques

Vous pouvez afficher et gérer les politiques sur la page **Politiques**.



The screenshot shows the 'Politiques' page in the Bitdefender console. At the top, there is a navigation bar with tabs: 'Tableau de bord', 'Réseau', 'Politiques', 'Rapports', 'Quarantaine', 'Comptes', and 'Journaux'. Below the navigation bar, the 'Politiques' page is displayed. It features a search bar and a table with the following columns: 'Le nom de la politique', 'Créé par', 'Modifié le', and 'Société'. The table contains three rows of data:

Le nom de la politique	Créé par	Modifié le	Société
<input type="checkbox"/> Politique par défaut			
<input type="checkbox"/> Relay Policy	@bitdefender.com	14 Jan 2014, 15:45:42	Bitdefender
<input type="checkbox"/> Firewall Policy	@bitdefender.com	14 Jan 2014, 15:46:44	Documentation

At the bottom of the table, there is a pagination control showing 'PAGE 1 de 1' and a dropdown menu set to '10'. On the right side of the table, there are buttons for '+', '←', and '→'. At the bottom right of the page, it says '3 éléments'.

La page Politiques

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.

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 de deux façons : en ajouter une nouvelle ou dupliquer (cloner) une politique existante.

Pour créer une nouvelle politique :

1. Allez sur la page **Politiques**.
2. Choisissez la méthode de création de la politique :
 - **Ajouter une nouvelle politique.**
 - Cliquez sur le bouton **+ Ajouter** à droite 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** à droite du tableau.

3. Configurez les paramètres de la politique. Pour plus d'informations, reportez-vous à « [Politiques de l'ordinateur](#) » (p. 72).
4. Cliquez sur **Enregistrer** pour créer la politique et revenir à la liste des politiques.

7.1.2. 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. Recherchez la politique dans la liste et cliquez sur son nom pour la modifier.
3. Configurez les paramètres de la politique selon vos besoins. Pour plus d'informations, reportez-vous à « [Politiques de l'ordinateur](#) » (p. 72).
4. 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.

7.1.3. 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. Cliquez sur le nom de la politique. Cela ouvrira la page de la politique.
3. Indiquez un nouveau nom pour la politique.
4. Cliquez sur **Enregistrer**.



Note

Le nom de la politique est unique. Vous devez saisir un nom différent pour chaque nouvelle politique.

7.1.4. 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.



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 supprimer une politique :

1. Allez sur la page **Politiques**.
2. Cochez la case correspondante.
3. Cliquez sur le bouton **Supprimer** à droite du tableau. Vous devrez confirmer votre action en cliquant sur **Oui**.

7.1.5. Affecter des politiques à des objets du réseau

Une fois que vous avez défini les politiques nécessaires dans la section **Politiques**, vous pouvez les affecter aux objets du réseau dans la section **Réseau**.

La politique par défaut est attribuée au départ à tous les objets du réseau.



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**.

Pour affecter une politique :

1. Allez sur la page **Réseau**.
2. Cochez la case de l'objet du réseau souhaité. Vous pouvez sélectionner un ou plusieurs objets du même niveau uniquement.
3. Cliquez sur le bouton **Affecter une politique** sur la partie droite du tableau.

La fenêtre **Attribution de la politique** s'affiche:

Attribution de la politique

Options

Attribution

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
DOC	Default policy	Bitdefender

PAGE 1 de 1 10 1 éléments

Installation terminée Annuler

Paramètres de l'affectation de politique

4. Configurez les paramètres d'affectation de politique pour les objets sélectionnés :

- Afficher les affectations de politique actuelles pour les objets sélectionnés dans le tableau sous la section **Cibles**.
- **Affecter le modèle de politique suivant.** Sélectionnez cette option pour affecter les objets cibles avec une politique à partir du menu affiché à droite. Seules les politiques créées à partir de votre compte utilisateur sont disponibles dans le menu.
- **Hériter du niveau supérieur.** Sélectionnez l'option **Hériter du niveau supérieur** pour affecter les objets du réseau sélectionnés avec la politique du groupe parent.
- **Forcer l'héritage de la politique pour les objets.** Par défaut, chaque objet du réseau hérite la politique du groupe parent. Si vous changez la politique du groupe, tous les enfants du groupe seront affectés, à l'exception des membres du groupe pour lesquels vous avez expressément affecté une autre politique.

Sélectionnez l'option **Forcer l'héritage de la politique pour les objets** pour appliquer la politique sélectionnée à un groupe, y compris aux enfants du groupe auxquels on a affecté une autre politique. Dans ce cas, le tableau ci-dessous affichera les enfants du groupe sélectionné qui n'héritent pas de la politique du groupe.

5. Cliquez sur **Terminer** pour enregistrer et appliquer des modifications.

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.

Pour vérifier que la politique a bien été affectée, allez sur la page **Réseau** et cliquez sur le nom de l'objet qui vous intéresse pour afficher la fenêtre **Détails**. Consultez la section **Politique** pour afficher l'état de la politique actuelle. Lorsqu'elle est en attente, la politique n'a pas encore été appliquée à l'objet cible.

7.2. Politiques de l'ordinateur

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. Cliquez sur le nom de la politique. Cela ouvrira la page des paramètres de la politique.
3. Configurez les paramètres de la politique selon vos besoins. Les paramètres sont regroupés dans les catégories suivantes :
 - [Général](#)
 - [Antimalware](#)
 - [Pare-feu](#)
 - [Contrôle de contenu](#)

Vous pouvez sélectionner la catégorie des paramètres à l'aide du menu dans la partie gauche de la page.

4. 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. 68).

7.2.1. Général

Les paramètres généraux vous aident à gérer les options d'affichage de l'interface utilisateur, les options de communication, les préférences de mise à jour, la protection par mot de passe et d'autres paramètres d'Endpoint Security.

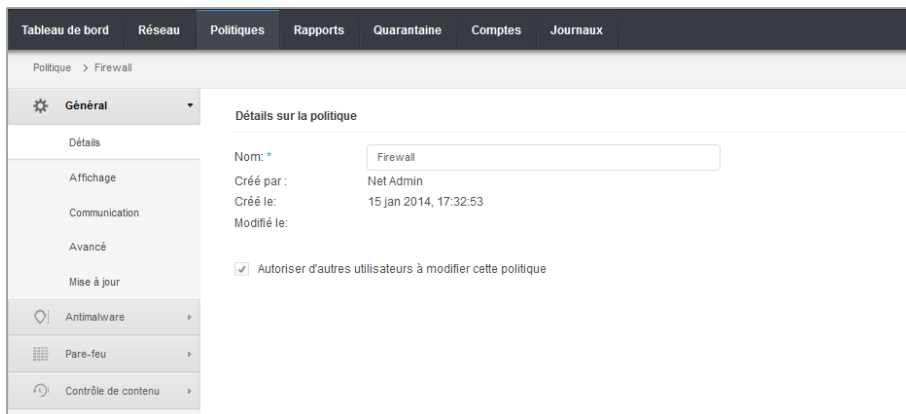
Les paramètres sont organisés dans les sections suivantes :

- [Détails](#)
- [Affichage](#)
- [Communication](#)
- [Avancé](#)
- [Mise à jour](#)

Détails

La page Détails présente des informations générales sur la politique :

- Le 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



Politiques de l'ordinateur

Vous pouvez renommer la politique en saisissant le nouveau nom dans le champ correspondant et en cliquant sur **enregistrer**. Les politiques doivent porter des noms explicites afin que vous, ou un autre administrateur, puissiez les identifier rapidement.

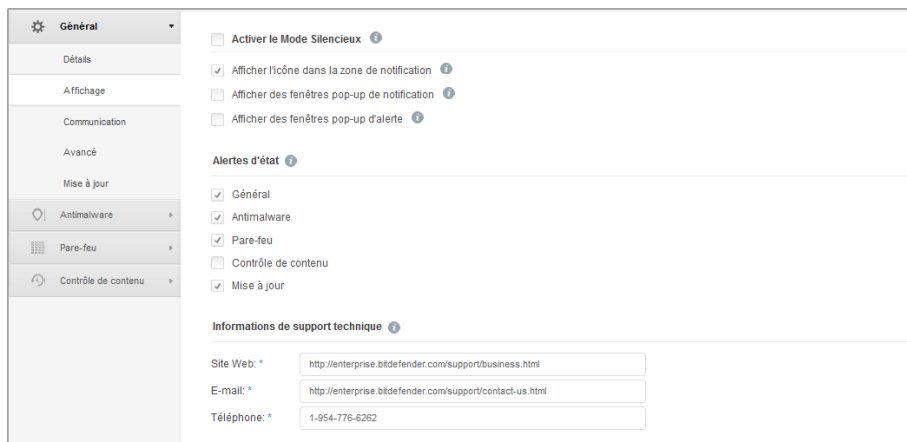


Note


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.

Affichage


Vous pouvez configurer dans cette section les options d'affichage de l'interface utilisateur.



Politiques de l'ordinateur - Paramètres d'affichage



- **Activer le 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 utilisateur dans Endpoint Security. 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  dans la zone de notification. 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 d'Endpoint Security ou la fenêtre **À propos de**. L'ouverture de la fenêtre **À propos de** lance automatiquement une mise à jour.
- **Afficher des fenêtres pop-up de notification.** Sélectionnez cette option pour signaler aux utilisateurs d'importants événements de sécurité tels que la détection de malwares et l'action appliquée via de petites fenêtres pop-up de notification. Les fenêtres pop-up disparaissent automatiquement après quelques secondes sans intervention de l'utilisateur.
- **Afficher des fenêtres pop-up d'alerte.** À la différence des fenêtres pop-up de notification, les fenêtres pop-up d'alertes demandent aux utilisateurs de spécifier une action. Si vous choisissez de ne pas afficher de pop-up d'alerte, Endpoint Security

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 Active Virus 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**
- **Alertes d'état.** Les utilisateurs sont informés de l'état de leur protection de deux façons :
 - La zone d'état de sécurité de la fenêtre principale affiche un message d'état approprié et change de couleur en fonction des problèmes détectés.
 - L'icône de Bitdefender  de la zone de notification change d'apparence lorsque des problèmes sont détectés.

L'état de la protection est déterminé en fonction des alertes d'état sélectionnées et se réfère aux problèmes de configuration de sécurité ou à d'autres risques de sécurité. Par exemple, si l'option **État de l'antimalware** est sélectionnée, les utilisateurs sont informés lorsqu'un problème lié à leur protection antimalware se produit (par exemple, si une analyse à l'accès est désactivée ou si une analyse système est en retard).

Sélectionnez les aspects de sécurité que vous souhaitez surveiller. Si vous ne souhaitez pas que les utilisateurs soient informés des problèmes existants, décochez toutes les cases.

- **Informations de support technique.** Vous pouvez personnaliser le support technique et les informations de contact disponibles dans Endpoint Security en complétant les champs correspondants. Les utilisateurs peuvent accéder à ces informations à partir de la fenêtre Endpoint Security en cliquant sur l'icône  dans l'angle inférieur droit (ou en faisant un clic droit sur l'icône Endpoint Security  de la zone de notification et en sélectionnant **À propos de**).

Communication

Lorsque plusieurs Endpoint Security Relay sont disponibles dans le réseau cible, vous pouvez affecter aux ordinateurs sélectionnés un ou plusieurs Endpoint Security Relay via une politique.

Pour affecter un Endpoint Security Relay aux ordinateurs cibles :

1. Dans le tableau **Affectation des serveurs de communication aux postes de travail**, cliquez sur le champ **Nom**. La liste des Endpoint Security Relays détectés dans votre réseau apparaît.

2. Sélectionnez une entité.

Affectation des serveurs de communication aux postes de travail

Priorité	Nom	IP	Nom personnalisé/IP	Actions
1	ECS 10.10.15.93	10.10.15.93		+ - ^ v
2	DOC-XP	10.0.2.15		+ - ^ v
	ERI-IT			
	RELAY 1A			

PAGE 1 de 1 10 2 éléments

Politiques de l'ordinateur - Paramètres de communication

3. Cliquez sur le bouton + **Ajouter** à droite du tableau.

Le Endpoint Security Relay est ajouté à la liste. Tous les ordinateurs cibles communiqueront avec Control Center via le Endpoint Security Relay spécifié.

4. Procédez de la même façon pour ajouter plusieurs Endpoint Security Relay, si possible.

5. Vous pouvez configurer la priorité des Endpoint Security Relay 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.

Avancé

Cette section vous permet de configurer les paramètres généraux et le mot de passe de désinstallation.

Configuration

Supprimer les événements de plus de

Envoyer les rapports de plantage à Bitdefender

Configuration du Mot de passe

Conserver les paramètres actuels

Activer le mot de passe

Mot de passe:

Retaper mot de passe:

Désactiver le mot de passe

Politiques de l'ordinateur - Paramètres avancés

- **Supprimer les événements de plus de (jours).** Endpoint Security 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 Endpoint Security. 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.
- **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 actuels** 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**.

Mise à jour

Cette rubrique vous permet de configurer les paramètres de mise à jour de Endpoint Security. Les mises à jour sont très importantes car elles permettent de contrer les nouvelles menaces.

Priorité	Serveur	Utiliser un proxy	Action
	Ajouter un emplacement	<input type="checkbox"/>	+
1	http://10.15.93.7074/	<input type="checkbox"/>	

Politiques de l'ordinateur - Options de mise à jour

- **Fréquence des MAJ (hrs).** Endpoint Security 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.

Pour modifier la fréquence des mises à jour automatiques, sélectionnez une option différente dans le menu. Veuillez noter que la mise à jour automatique ne peut pas être désactivée.

- **Reporter le redémarrage.** Certaines mises à jour requièrent un redémarrage du système pour s'installer et fonctionner correctement. En sélectionnant cette option, le programme continuera à fonctionner avec les anciens fichiers jusqu'au redémarrage de l'ordinateur, sans en informer l'utilisateur. Sinon, une notification dans l'interface utilisateur demandera à l'utilisateur de redémarrer le système lorsqu'une mise à jour le nécessitera.

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).

- **Paramètres du proxy.** Sélectionnez cette option si les ordinateurs se connectent à Internet (ou au serveur local de mise à jour) via un serveur proxy. Trois options permettent de définir les paramètres du proxy :
 - **Importer les paramètres proxy à partir du navigateur par défaut.** Endpoint Security peut importer les paramètres proxy des principaux navigateurs, y compris des dernières versions d'Internet Explorer, de Mozilla Firefox et d'Opera.

- **Détecter automatiquement le proxy réseau.** Endpoint Security utilise le protocole WPAD (Web Proxy Auto-Discovery - Découverte automatique de proxy Web) inclus dans Windows pour récupérer automatiquement les paramètres proxy à partir d'un fichier de configuration automatique du proxy (PAC) publié dans le réseau local. Si aucun fichier PAC n'est disponible, les mises à jour échoueront.
- **Utiliser les paramètres proxy personnalisés.** Si vous connaissez les paramètres proxy, sélectionnez cette option puis indiquez-les :
 - **Serveur** - saisissez l'adresse IP du serveur proxy.
 - **Port** - entrez le port utilisé pour se connecter au serveur proxy.
 - **Nom d'utilisateur** - entrez le nom d'utilisateur reconnu par le serveur proxy.
 - **Mot de passe** - saisissez le mot de passe valide de l'utilisateur dont le nom vient d'être indiqué.



Note

Modifier l'option de configuration du proxy écrasera les paramètres proxy existants dans Endpoint Security.

Vous devez également cocher la case **Utiliser un proxy** correspondant à l'emplacement des mises à jour sur lequel les paramètres s'appliquent (l'adresse du serveur de mise à jour Internet ou local).

Priorité	Serveur	Utiliser un proxy	Action
	Ajouter un emplacement	<input type="checkbox"/>	+
1	http://10.10.17.89:7074/	<input checked="" type="checkbox"/>	▼ ▲ -

Politiques de l'ordinateur - Emplacements des mises à jour

- **Emplacements des mises à jour.** Pour éviter de surcharger le trafic réseau externe, Endpoint Security est configuré pour se mettre à jour à partir de <http://upgrade.bitdefender.com>. Vous pouvez également ajouter d'autres adresses de serveurs de mise à jour à la liste et 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, le suivant est vérifié et ainsi de suite.

Pour configurer l'adresse de mise à jour locale :

1. Indiquez l'adresse du serveur local 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.

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.
4. Utilisez les flèches **^ Haut** / **▾ Bas** dans la colonne **Action** pour définir la première adresse de mise à jour locale de la liste. Placez le curseur de la souris sur la ligne correspondante pour que les flèches deviennent visibles.

Pour retirer un emplacement de la liste, placez le curseur dessus et cliquez sur le bouton **- Supprimer** correspondant. Bien que vous puissiez supprimer l'emplacement des mises à jour par défaut, cela n'est pas recommandé.

7.2.2. Antimalware

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 deux catégories :

- **Analyse à l'accès** : empêche les nouvelles menaces d'infecter le système.
- **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, Endpoint Security 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 de contenir l'infection. Quand un virus est en quarantaine, il ne peut faire aucun dégât car il ne peut ni être exécuté, ni être lu.

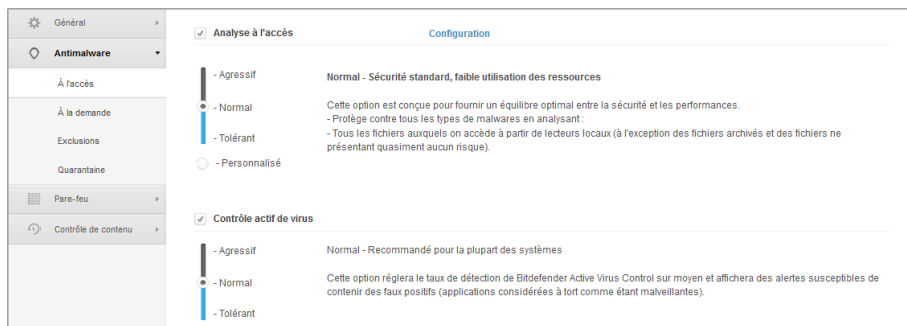
Les utilisateurs avancés peuvent configurer des exceptions d'analyse s'ils ne souhaitent pas que certains fichiers ou types de fichiers soient analysés.

Les paramètres sont organisés dans les sections suivantes :

- [À l'accès](#)
- [A la demande](#)
- [Exclusions](#)
- [Quarantaine](#)

À l'accès

Cette section vous permet de configurer les deux composants de la protection antimalware en temps réel :



Politiques de l'ordinateur - Paramètres à l'accès

- [Analyse à l'accès](#)
- [Contrôle actif de virus](#)

Paramètres de l'analyse à l'accès

L'analyse à l'accès empêche que de nouveaux malwares n'entrent dans le système - elle analyse les fichiers à l'accès (lorsqu'ils sont ouverts, déplacés, copiés ou exécutés), les e-mails envoyés et reçus et le trafic web.

Pour configurer l'analyse à l'accès :

1. Utilisez cette case pour activer ou désactiver l'analyse à l'accès. Si vous désactivez l'analyse à l'accès, les ordinateurs 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. Les utilisateurs avancés peuvent 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 sont décrites ci-après du premier au dernier onglet :

- **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'ordinateur 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 Endpoint Security afin qu'il analyse tous les fichiers à l'accès (quelle que soit l'extension des fichiers), uniquement les fichiers d'applications ou certaines extensions de fichiers que vous jugez dangereuses. L'analyse de tous les

fichiers auxquels on a accédé 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 « [Liste des types de fichier d'Application](#) » (p. 145).

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.

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.

- **Archives** Sélectionnez **Analyser à l'intérieur des archives** si vous souhaitez activer l'analyse à l'accès des fichiers archivés. L'analyse à l'intérieur des archives 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.
- **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 de boot. Quand un virus infecte le secteur de boot, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.
 - **Analyser 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.

- **Rechercher les keyloggers.** Les keyloggers enregistrent ce que vous tapez sur votre clavier et envoient des rapports sur Internet à une personne malveillante (un hacker). 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.
- **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.
- **Action d'analyse.** En fonction du type de fichier détecté, les actions suivantes sont menées automatiquement :

- **Action par défaut pour les fichiers infectés.** Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la Base de Données de Signatures de Codes Malveillants Bitdefender. Endpoint Security 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, Endpoint Security tente 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.

- **Action par défaut pour les fichiers suspects.** Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique. B-HAVE étant une technologie d'analyse heuristique, Endpoint Security ne peut pas être certain que le fichier est réellement infecté par des malwares. 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.

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.

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 supprime le risque d'une infection. Vous pouvez gérer les fichiers en quarantaine à partir de la page [Quarantaine](#) de la console.

Configuration d'Active Virus Control

Bitdefender Active Virus Control est une technologie de détection proactive innovante qui utilise des méthodes heuristiques de pointe pour détecter de nouvelles menaces potentielles en temps réel.

Active Virus Control surveille en permanence les applications en cours d'exécution sur l'ordinateur, 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. Active Virus Control bloquera automatiquement le processus détecté.



Note

Pour plus d'informations, rendez-vous sur notre site web et consultez le [livre blanc sur la technologie Active Virus Control](#).

Pour configurer Active Virus Control :

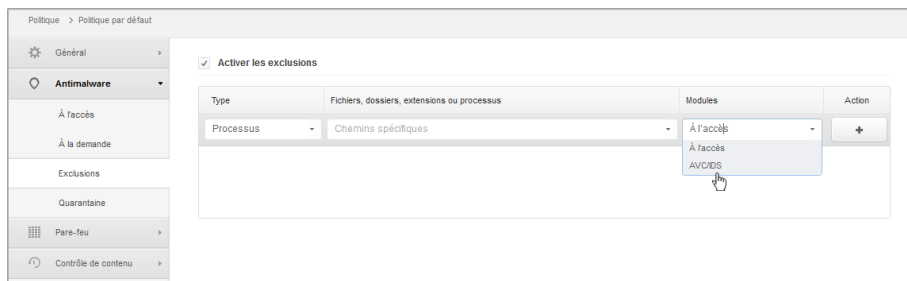
1. Utilisez cette case pour activer ou désactiver Active Virus Control. Si vous désactivez Active Virus Control, les ordinateurs seront vulnérables aux malwares inconnus.
2. Cliquez sur le niveau de sécurité qui correspond le mieux à vos besoins (Agressif, Normal ou Tolérant). Utilisez la description à droite de l'échelle pour faire votre choix.



Note

Si vous élevez le niveau de protection, Active Virus 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).

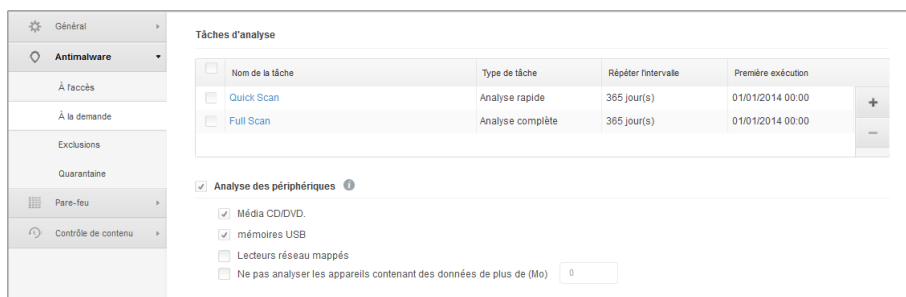
3. Nous vous recommandons de créer des règles d'exclusion pour les applications fréquemment utilisées ou connues afin d'éviter les faux positifs (applications légitimes détectées à tort comme étant malveillantes). Allez dans l'onglet **Exclusions** et configurez les **règles d'exclusion des processus AVC/IDS** pour les applications de confiance.



Politique de l'ordinateur - Exclusion des processus AVC/IDS

A la demande

Cette section vous permet de configurer les tâches d'analyse antimalware qui s'exécuteront régulièrement sur les ordinateurs cibles, en fonction de la planification que vous spécifiez.



Politiques de l'ordinateur - Tâches d'analyse à la demande

L'analyse s'effectue discrètement, en tâche de fond. L'utilisateur n'est averti du processus d'analyse en cours que par l'apparition d'une icône dans la barre des tâches.

Bien que ce ne soit pas obligatoire, nous vous recommandons de planifier l'exécution hebdomadaire d'une analyse complète sur tous les ordinateurs. Analyser les ordinateurs 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.

Il y a deux tâches d'analyse système par défaut que vous pouvez configurer si besoin :

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

Les options d'analyse des tâches, par défaut, sont préconfigurées et vous ne pouvez pas les modifier.

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 que vous le souhaitez. Une tâche d'analyse personnalisée vous permet de sélectionner les emplacements à analyser et de configurer les options d'analyse.

Pour créer et configurer une nouvelle tâche d'analyse personnalisée, 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.

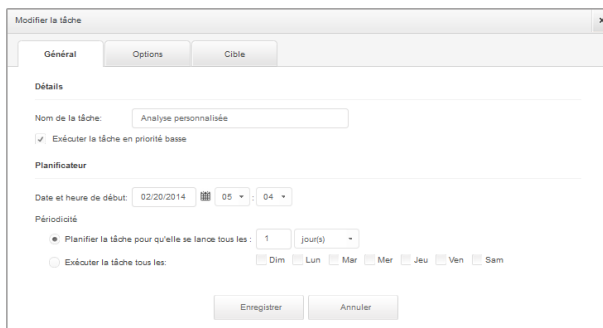
Pour retirer une tâche de la liste, sélectionnez la tâche et cliquez sur le bouton **- Supprimer** à droite du tableau.

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 dossiers à analyser.

Les options sont décrites ci-après du premier au dernier onglet :



Politiques de l'ordinateur - 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.
- **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.

Gardez à l'esprit que les ordinateurs doivent être allumés au moment de la planification. Les analyses planifiées ne s'exécuteront pas si l'ordinateur est éteint, en veille prolongée ou en veille ou si aucun utilisateur n'est connecté. Dans l'un de ces cas, l'analyse sera reportée intérieurement.

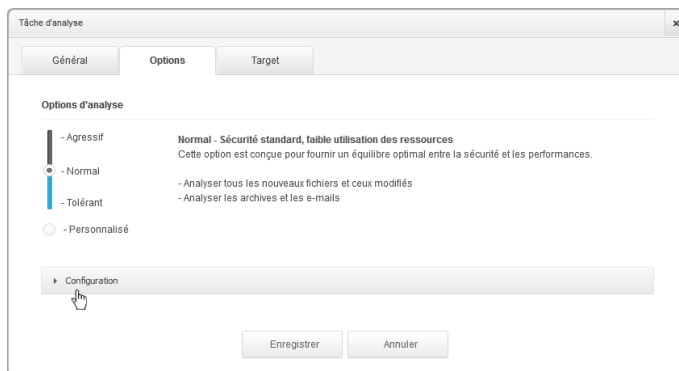


Note

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).

- **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 Analyse des ordinateurs

- **Types de fichiers.** Utilisez ces options pour spécifier les types de fichiers que vous souhaitez analyser. Vous pouvez configurer Endpoint Security afin qu'il analyse tous les fichiers (quelle que soit l'extension des fichiers), ou uniquement les fichiers d'applications ou certaines extensions de fichiers que vous considérez dangereuses. L'analyse de tous les fichiers consultés offre une protection maximale, alors que l'analyse des applications offre uniquement une analyse 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 « [Liste des types de fichier d'Application](#) » (p. 145).

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 dans les archives.** 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.



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 informatique nécessaire pour faire démarrer le processus de boot. Quand un virus infecte le secteur de boot, 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 masqués à l'aide de ce logiciel.
 - **Rechercher les keyloggers.** Sélectionnez cette option pour rechercher les logiciels [keyloggers](#).
 - **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.

- **Actions.** En fonction du type de fichier détecté, les actions suivantes sont menées automatiquement :

- **Action par défaut pour les fichiers infectés.** Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la Base de Données de Signatures de Codes Malveillants Bitdefender.Endpoint Security 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, Endpoint Security tente 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.

- **Action par défaut pour les fichiers suspects.** Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique.B-HAVE étant une technologie d'analyse heuristique, Endpoint Security ne peut pas être certain que le fichier est réellement infecté par des malwares. 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 :

Ignorer

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.

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 supprime 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.

- **Exclusions.** Vous pouvez choisir d'utiliser des exclusions globales pour une analyse spécifique ou de définir des exclusions explicites pour chaque analyse. Pour plus d'informations sur les exclusions, reportez-vous à « [Exclusions](#) » (p. 93).

Analyse des périphériques

Vous pouvez configurer Endpoint Security pour détecter et analyser automatiquement les périphériques de stockage externe quand ils sont connectés à l'ordinateur. Les périphériques détectés appartiennent à l'une des catégories suivantes :

- CD/DVD
- Des mémoires USB, tels que des clés flash et des disques durs externes
- Lecteurs réseau mappés
- 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. Merci de prendre en compte qu'aucune action ne peut être prise sur les fichiers infectés détectés sur les CD / DVD ou sur les lecteurs réseau mappés qui sont limités à un accès Lecture.




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 > Affichage**, 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 > Affichage** .
- Une icône d'analyse  apparaît dans la **barre des tâches**. L'utilisateur peut double-cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

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**
- **Lecteurs réseau mappés**
- **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.



Note

Cette option s'applique uniquement aux CD/DVD et aux supports de stockage USB.

Exclusions

Cette section vous permet de configurer des règles d'exclusion d'analyse. Les exclusions peuvent s'appliquer à l'analyse à l'accès ou à la demande, ou aux deux. En fonction de l'objet de l'exclusion, il y a quatre types d'exclusions :

Type	Fichiers, dossiers, extensions ou processus	Modules	Action
Fichier	Chemins spécifiques	À la demande	+

Politiques de l'ordinateur - Exclusions de l'Antimalware

- **Exclusions de fichiers** : le fichier spécifié est exclu de l'analyse.
- **Exclusions du dossier** : tous les fichiers à l'intérieur du dossier spécifié et tous ses sous-dossiers sont exclus de l'analyse.
- **Exclusions d'extensions** - tous les fichiers ayant l'extension spécifiée sont exclus de l'analyse.
- **Exclusions de processus** : tout objet auquel accède le processus exclu est également exclu de l'analyse. Vous pouvez également configurer des exclusions de processus pour les technologies [Active Virus Control](#) et [Système de détection d'intrusion](#).



Important

Les exceptions d'analyse 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](#). 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.

Utilisez la case **Activer les exclusions** pour activer ou désactiver les exclusions.

Pour configurer une règle d'exclusion :

1. Sélectionnez le type d'exclusion dans le menu.
2. En fonction du type d'exclusion, spécifiez l'objet à exclure comme suit :
 - **Exclusions d'extensions.** Spécifiez une ou plusieurs extensions de fichier à exclure de l'analyse, en les séparant 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

Avant de choisir d'exclure des extensions, veillez à vous documenter pour savoir quelles sont celles qui sont les cibles principales des malwares.

- **Exclusions de fichiers, de dossiers et de processus.** Vous devez spécifier le chemin de l'objet exclu sur les ordinateurs cibles.
 - a. Choisissez dans le menu un emplacement prédéfini ou l'option **Chemins spécifiques**.
 - b. Si vous avez choisi un emplacement prédéfini, complétez le chemin selon vos besoins. Par exemple, pour exclure l'ensemble du dossier `Program Files`, il suffit de sélectionner l'emplacement prédéfini correspondant dans le menu. Pour exclure un dossier spécifique de `Program Files`, vous devez compléter le chemin en ajoutant une barre oblique inverse (\) et le nom du dossier. Pour les exclusions de processus, vous devez ajouter le nom du fichier exécutable de l'application.
 - c. Si vous avez choisi **Chemins spécifiques**, indiquez le chemin complet vers l'objet à exclure. 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. Sélectionnez les types d'analyse auxquels la règle s'appliquera. Certaines exclusions peuvent être pertinentes pour l'analyse à l'accès uniquement, certaines pour les analyses à la demande seulement, tandis que d'autres peuvent être recommandés pour les deux. Des exclusions de processus peuvent être configurées pour l'analyse à l'accès et pour les technologies [Active Virus Control](#) et [Système de détection d'intrusion](#)



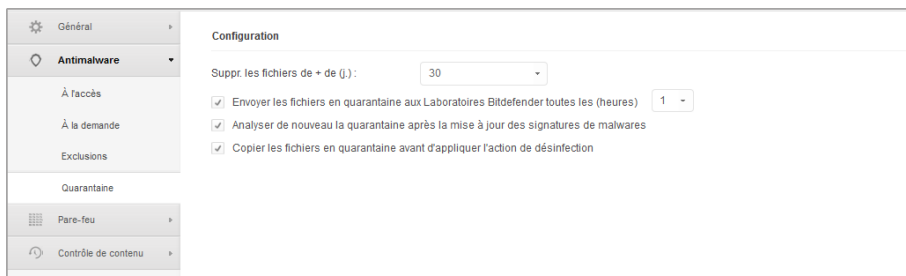
Note

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 Endpoint Security by Bitdefender**.

4. 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.

Quarantaine

Cette section vous permet de configurer les paramètres de la zone de quarantaine.



Politiques de l'ordinateur - Quarantaine

Vous pouvez configurer Endpoint Security pour qu'il exécute automatiquement les actions suivantes :

- **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)**
Maintenez cette option sélectionnée pour envoyer automatiquement les fichiers de la quarantaine aux laboratoires de Bitdefender. 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.

Par défaut, les fichiers en quarantaine sont automatiquement envoyés aux Laboratoires Bitdefender toutes les heures. Si vous souhaitez modifier cet intervalle, choisissez une option différente dans le menu.

- **Analyser de nouveau la quarantaine après la mise à jour des signatures de malwares.**
Maintenez cette option sélectionnée pour analyser automatiquement les fichiers en quarantaine après chaque mise à jour des signatures de 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**.

7.2.3. Pare-feu

Le pare-feu protège votre ordinateur 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.

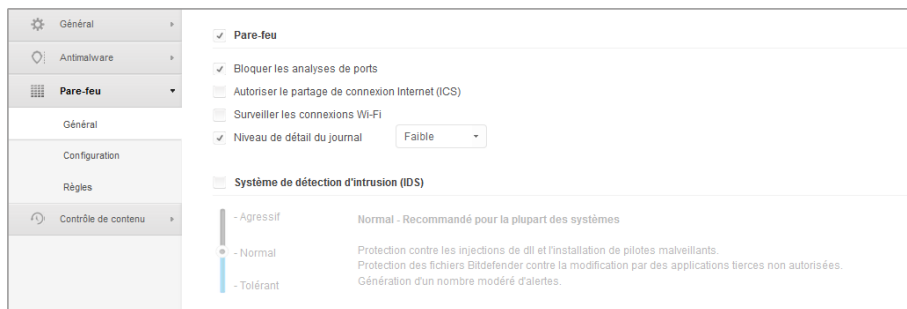
À chaque fois qu'une nouvelle connexion est créée, le pare-feu la détecte et compare les informations de l'adaptateur de la connexion aux informations des profils existants, en appliquant le profil correct. Pour des informations détaillées sur la manière dont les profils s'appliquent, consultez les [paramètres des réseaux](#).

Les paramètres sont organisés dans les sections suivantes :

- [Général](#)
- [Configuration](#)
- [Règles](#)

Général

Dans cette section, vous pouvez activer ou désactiver le pare-feu de Bitdefender et configurer les paramètres généraux.



Politiques de l'ordinateur - Paramètres généraux du pare-feu

- **Pare-feu.** Utilisez cette case pour activer ou désactiver le pare-feu. 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.** Endpoint Security 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.** Endpoint Security 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.).

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 soit détectée par le système de détection d'intrusion, merci d'ajouter une **règle d'exclusion du processus AVC/IDS** pour cette application, dans la section **Antimalware > Exclusions**.

Configuration

Le pare-feu applique automatiquement un profil en fonction du type de réseau. Vous pouvez spécifier les profils génériques à appliquer en fonction du type d'adaptateur et spécifier également des profils individuellement pour les réseaux de votre entreprise. Les paramètres sont organisés dans les tableaux suivants :

- [Réseaux](#)
- [Adaptateurs](#)

Nom	Type	Identification	MAC	IP	Action
					+

Type	Type de Réseau	Mode Furtif
Wired	Domicile / Bureau	Distant
Wireless	Public	Activé
Virtual	De confiance	Désactivé

Politiques de l'ordinateur - Paramètres du pare-feu

Paramètres des réseaux

Pour que le pare-feu fonctionne correctement, l'administrateur doit définir les réseaux qui seront gérés dans le tableau **Réseaux**. Les champs du tableau **Réseaux** sont décrits comme suit :

- **Nom.** Un nom permettant à l'administrateur de reconnaître le réseau dans la liste.
- **Type.** Sélectionnez dans le menu le type de profil affecté au réseau.
Endpoint Security applique automatiquement l'un des quatre profils de pare-feu à chaque connexion réseau détectée pour définir les options de filtrage de trafic de base. Les profils de pare-feu sont les suivants :
 - Réseau **de confiance**. Désactiver le Pare-feu pour l'adaptateur concerné.
 - Réseau **domestique/d'entreprise**. Autoriser tout le trafic vers et depuis les ordinateurs du réseau local.
 - Réseau **public**. Tout le trafic est filtré.
 - Réseau **non fiable**. Bloquer complètement le trafic réseau et Internet via l'adaptateur respectif.
- **Identification.** Sélectionnez dans le menu la méthode d'identification du réseau par Endpoint Security. Les réseaux peuvent être identifiés par trois méthodes : **DNS**, **Passerelle** et **Réseau**.
- **MAC.** Utilisez ce champ pour spécifier l'adresse MAC d'un serveur DNS spécifique.



Note

Ce champ est obligatoire si la méthode d'identification DNS est sélectionnée.

- **IP.** Utilisez ce champ pour définir des adresses IP spécifiques dans un réseau. Vous pouvez également utiliser un masque pour définir un sous-réseau complet.

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, Endpoint Security 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. Endpoint Security peut détecter trois types d'adaptateurs prédéfinis : **Câblé**, **Sans fil** et **Virtual** (Réseau privé virtuel).
- **Type de Réseau.** Décrit le profil de réseau affecté à un type d'adaptateur spécifique. Les types 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, Endpoint Security 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 dans lequel le type de réseau est considéré comme **Public** et les paramètres de furtivité sont réglés sur **Activé**. Si l'adresse IP du domaine dans lequel l'ordinateur est détecté se trouve dans l'un des réseaux associés à l'adaptateur, alors le niveau de confiance est considéré comme **Domicile/Bureau** et les paramètres de furtivité sont réglés sur **Activés à distance**. Si l'ordinateur n'est pas dans un domaine, cette condition n'est pas applicable.

- **Mode Furtif.** Masque l'ordinateur face aux logiciels malveillants et pirates du réseau et face à Internet. Configurez, si besoin, le Mode furtif pour chaque type d'adaptateur en sélectionnant l'une des options suivantes :
 - **Activé.** L'ordinateur n'est pas visible depuis le réseau local et Internet.
 - **Désactivé.** N'importe qui sur le réseau local ou sur Internet peut détecter l'ordinateur (via la commande ping).
 - **Distancé.** 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 pare-feu Domicile/Bureau** et **Public**.

Priorité	Nom	Type de règle	Réseau	Protocole	Permission
1	ICMP entrant	Application	Domicile / Bu...	ICMP	Autoriser
2	ICMPv6 entrant	Application	Domicile / Bu...	IPv6-ICMP	Autoriser
3	Connexions Bureau à distance entrantes	Connexion	Domicile / Bu...	TCP	Autoriser
4	Envoi d'e-mails	Connexion	Domicile / Bu...	TCP	Autoriser
5	HTTP navigation web	Application	Domicile / Bu...	TCP	Autoriser
6	Impression dans un autre réseau	Application	Domicile / Bu...	Tous	Refuser
7	Trafic Windows Explorer sur FTP	Application	Domicile / Bu...	TCP	Refuser
8	Trafic Windows Explorer sur HTTP	Application	Domicile / Bu...	TCP	Refuser

Politiques des ordinateurs - Paramètres des règles du pare-feu

Configuration

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 hackers pour perpétrer des attaques contre les réseaux informatiques. Par défaut, ce type de trafic est refusé.

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 dans un autre 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 ordinateurs. Cette configuration est cependant réservée aux administrateurs avec de fortes compétences réseaux.

Pour créer et configurer une nouvelle règle, cliquez sur le bouton **+ Ajouter** à droite du tableau. Reportez-vous à la rubrique suivante pour plus d'informations.

Pour retirer une règle de la liste, cliquez sur le bouton correspondant **- Supprimer** à droite 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** à droite 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
Autoriser	L'application spécifiée se verra autoriser l'accès réseau/Internet dans les circonstances spécifiées.
Refuser	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.

7.2.4. Contrôle de contenu

Utilisez le module Contrôle de contenu pour configurer vos préférences concernant le filtrage du contenu et la protection des données pour l'activité des utilisateurs y compris la navigation web, les applications de messagerie et logicielles. 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. Veuillez noter que les paramètres configurés du Contrôle de contenu s'appliqueront à tous les utilisateurs qui se connecteront aux ordinateurs cibles.

Les paramètres sont organisés dans les sections suivantes :

- [Trafic](#)
- [Web](#)
- [Données](#)
- [Applications](#)

Trafic


Configurez les préférences de sécurité du trafic à l'aide des paramètres sous les sections suivantes :

- [Options](#)
- [Analyse du trafic](#)
- [Exclusions de l'analyse du trafic](#)

Type	Entité exclue	Action
	Entité	+


Politiques de l'ordinateur - Contrôle de contenu - Trafic


Options

- **Analyse SSL.** Sélectionnez cette option si vous souhaitez que le trafic web SSL (Secure Sockets Layer) soit inspecté par les modules de protection Endpoint Security.
- **Afficher la barre d'outils du navigateur.** 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.
- **Search Advisor.** 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.

Analyse du trafic

Les e-mails entrants et le trafic web sont analysés en temps réel pour empêcher le téléchargement de malwares sur l'ordinateur. Les e-mails sortants sont analysés afin d'éviter que des malwares n'infectent d'autres ordinateurs. L'analyse du trafic web peut ralentir un peu la navigation sur Internet, mais elle bloquera les malwares 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.

Exclusions de l'analyse du trafic

Vous pouvez choisir de ne pas analyser une partie du trafic à la recherche de malwares lorsque les options d'analyse du trafic sont activées.

Pour définir une exception à l'analyse du trafic :

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.** Saisissez l'adresse IP pour laquelle vous ne souhaitez pas analyser le trafic entrant et sortant.
 - **URL.** Exclut de l'analyse les adresses Internet spécifiées. Pour exclure une URL de l'analyse :
 - Saisissez une URL spécifique telle que `www.exemple.com/exemple.html`
 - 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	Application des exceptions
<code>www.exemple*</code>	Chaque site web ou page web commençant par <code>www.exemple</code> (sans tenir compte de 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>	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

Syntaxe	Application des exceptions
	n'importe quel caractère unique. Ces sites Web pourraient inclure : <code>www.exemple1.com</code> ou <code>www.exempleA.com</code> .

- **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.

Web

Cette section vous permet de configurer vos préférences en matière de sécurité pour la navigation sur Internet.

Les paramètres sont organisés dans les sections suivantes :

- [Contrôle Web](#)
- [Antiphishing](#)

Contrôle Web

Le Contrôle Web vous permet d'autoriser ou d'interdire l'accès au Web à des utilisateurs ou des applications pendant des intervalles de temps spécifiés.

Les pages Web bloquées par le Contrôle Web 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 Web.



Politiques de l'ordinateur - Contrôle de contenu - Web

Utilisez ce bouton pour activer ou désactiver le **Contrôle Web**.

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.

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

Endpoint Security 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 Web 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. Sélectionnez **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 cliquant sur le bouton **Catégories** placé 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 le bouton **Catégories** pour étendre la section correspondante.
 - c. Recherchez la catégorie qui vous intéresse dans la liste et sélectionnez l'action souhaitée dans le menu.
4. Vous pouvez également choisir de **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. 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 Web.
- Les permissions **Autoriser** ne fonctionnent que lorsque l'accès à Internet est bloqué par le Contrôle Web alors que les permissions **Bloquer** ne fonctionnent que lorsque l'accès à Internet est autorisé par le Contrôle Web.
- Vous pouvez écraser la permission de la catégorie d'adresses Web individuelles en les ajoutant avec la permission opposée dans **Contrôle Web > 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 Web. Les utilisateurs pourront ainsi accéder à une page web spécifique même lorsque la navigation sur Internet est bloquée par le Contrôle Web.

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**.

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 par 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.

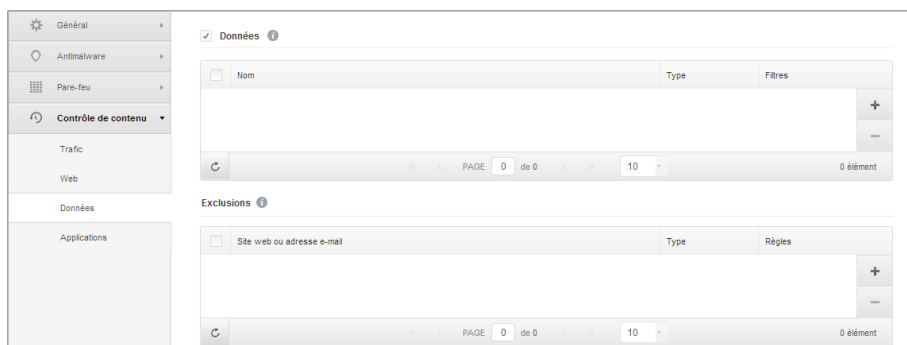
Si une page web légitime est détectée à tort comme étant une page de phishing et est bloquée, vous pouvez l'ajouter à la liste blanche afin de permettre aux utilisateurs d'y accéder. La liste ne doit contenir que des sites web de confiance.

Pour gérer les exceptions de l'antiphishing :

1. Cliquez sur **Exclusions**.
2. Saisissez l'adresse web et cliquez sur le bouton **+ Ajouter**.
Pour retirer une exception de la liste, placez le curseur dessus et cliquez sur le bouton **- Supprimer**.
3. Cliquez sur **Enregistrer**.

Données

La Protection des données empêche la divulgation non autorisée de données sensibles grâce à des règles définies par l'administrateur.



Politiques de l'ordinateur - Contrôle de contenu - Protection des données

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 que vous créez, Endpoint Security analyse le trafic web et de messagerie quittant l'ordinateur 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 Endpoint Security 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** à droite 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. 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.

Veillez à entrer au moins cinq caractères de manière à éviter un blocage par erreur d'e-mails et de pages Web.



Important

Les données fournies sont stockées de manière chiffrée sur les ordinateurs 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**.

- d. 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.
- e. 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** à droite 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.



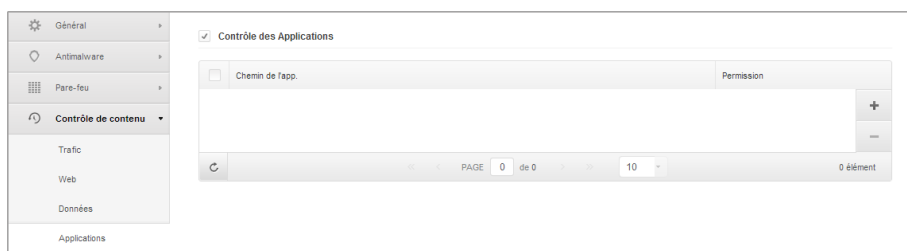
Note

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.

Applications

Cette section vous permet de configurer le Contrôle des applications. Le Contrôle des applications vous aide à bloquer complètement ou à limiter l'accès des utilisateurs aux applications sur leurs ordinateurs. Les jeux, logiciels de messagerie, comme d'autres catégories de logiciels (y compris malveillants) peuvent être bloqués de cette façon.




Politiques de l'ordinateur - Contrôle de contenu - Applications

Pour configurer le Contrôle des applications :

1. Utilisez le bouton pour activer le contrôle 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** à droite 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.

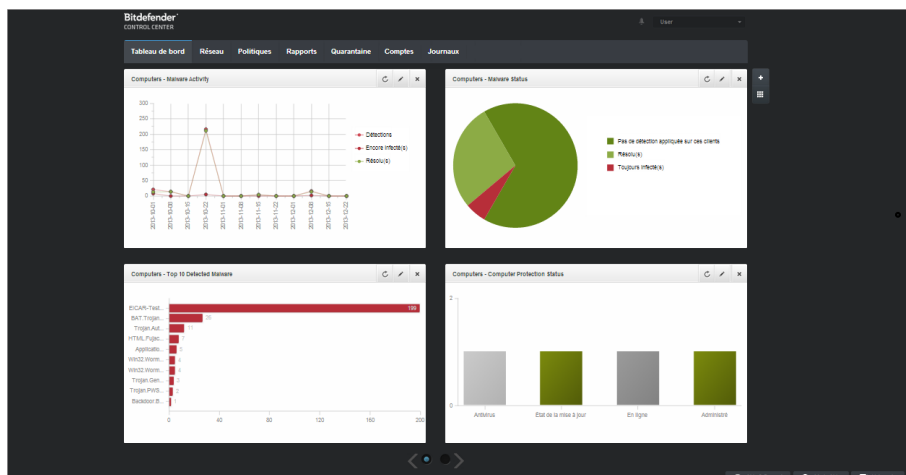
- Indiquez le chemin complet dans le champ de saisie. Il est recommandé d'utiliser les variables du système (le cas échéant) afin de s'assurer que le chemin soit valide sur tous les ordinateurs cibles.
- c. **Accéder au Planificateur.** Planifiez l'accès aux applications à certaines heures de la journée 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, cliquez sur le bouton correspondant  **Supprimer** à droite du tableau. Pour modifier une règle existante, cliquez sur le nom de l'application.

8. Tableau de bord de supervision

Le tableau de bord du Control Center est un écran personnalisable fournissant un aperçu rapide de la sécurité de tous les éléments protégés 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 :

- 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 éléments de votre réseau tels que l'état de la mise à jour, l'état des malwares, l'activité du pare-feu etc. Pour plus d'informations sur les types de portlet du tableau de bord, reportez-vous à « [Types de rapports disponibles](#) » (p. 119).
- Les informations affichées par les portlets se rapportent uniquement aux éléments du réseau relatif à votre compte. Vous pouvez personnaliser la cible de chaque portlet à l'aide de 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 le curseur en bas de la page pour naviguer entre les groupes de portlets.

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. Actualiser les données du portlet

Pour que le portlet affiche des informations à jour, cliquez sur l'icône  **Actualiser** sur sa barre de titre.


8.2. 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.

8.3. 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** à droite du tableau de bord. La fenêtre de configuration s'affiche.
3. Sous l'onglet **Détails**, configurez les informations du portlet :
 - Le type de rapport en arrière-plan
 - Un nom de portlet explicite
 - Fréquence des mises à jour

Pour plus d'informations sur les types de rapports disponibles, référez-vous à « [Types de rapports disponibles](#) » (p. 119).


4. Sous l'onglet **Cibles**, sélectionnez les objets et les groupes du réseau à inclure.
5. Cliquez sur **Enregistrer**.

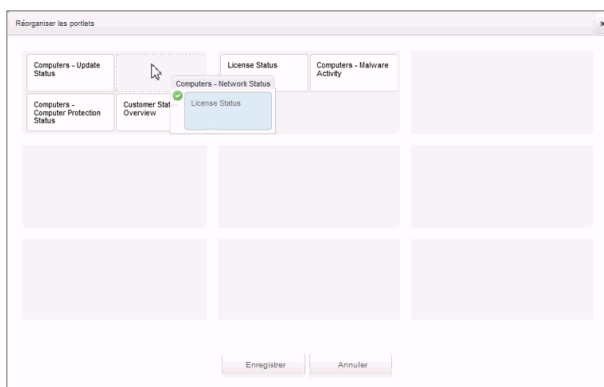
8.4. Suppression d'un portlet

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.

8.5. 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. Cliquez sur le bouton  **Réorganiser les portlets** à droite du tableau de bord. La fenêtre de la disposition des portlets s'affiche.
3. Glissez-déposez chaque portlet à l'emplacement de votre choix.
4. Cliquez sur **Enregistrer**.



Réorganisation des portlets du tableau de bord

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.
- Surveiller les incidents de sécurité et l'activité des malwares.
- 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 éléments du réseau administré.
- La liste des ordinateurs répondant à certains critères (par exemple, ceux dont la protection antimalware est désactivée.)

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 rapports disponibles

Voici la liste des types de rapports disponibles pour les ordinateurs :

État de la mise à jour

Vous indique l'état de la mise à jour de la protection Endpoint Security installée sur les ordinateurs sélectionnés. L'état de la mise à jour se réfère à la version du produit et à la version des moteurs (signatures).

Les filtres vous permettent de connaître facilement les clients ayant été ou non mis à jour au cours d'une période donnée.

État des malwares

Vous aide à découvrir combien et quels ordinateurs sélectionnés ont été affectés par des malwares pendant une période spécifique et comment les menaces ont été gérées.

Les ordinateurs sont regroupés en fonction des critères suivants :

- Ordinateurs sans détection (aucun malware n'a été détecté pendant la période spécifiée)
- Les ordinateurs avec des malwares résolus (tous les fichiers détectés ont bien été désinfectés ou placés dans la [quarantaine](#))
- Ordinateurs encore infectés par des malwares (certains des fichiers détectés dont l'accès a été refusé)

Activité des logiciels malveillants

Vous fournit des informations globales sur les malwares détectés pendant une certaine période sur les ordinateurs sélectionnés. Vous pouvez voir :

- Le nombre de détections (fichiers ayant été détectés comme infectés par des malwares)
- Le nombre d'infections résolues (les fichiers ayant été désinfectés avec succès ou placés en [quarantaine](#))
- Le nombre d'infections non résolues (fichiers n'ayant pas pu être désinfectés mais dont l'accès a été refusé ; par exemple, un fichier infecté stocké dans un format d'archive propriétaire)

État du réseau

Vous fournit des informations détaillées sur l'état de sécurité global des ordinateurs sélectionnés. Les ordinateurs sont regroupés en fonction des critères suivants :

- État des problèmes
- État de l'administration
- État de l'infection
- État de la protection antimalware
- État de la mise à jour du produit
- État de la licence
- L'état de l'activité du réseau de chaque ordinateur (en ligne/hors connexion). Si l'ordinateur est hors connexion lorsque le rapport est généré, vous verrez la date et l'heure auxquelles il a été vu en ligne pour la dernière fois par le Control Center.

État de la protection de l'ordinateur

Vous fournit différentes informations d'état au sujet des ordinateurs de votre réseau sélectionnés.

- État de la protection antimalware
- État de la mise à jour d'Endpoint Security
- 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.

Les 10 ordinateurs les plus infectés

Vous indique les 10 ordinateurs les plus infectés en fonction du nombre total de détections sur une période donnée pour les ordinateurs sélectionnés.



Note

Le tableau détails indique tous les malwares détectés sur les 10 ordinateurs les plus infectés.

Les 10 malwares les plus détectés

Vous indique les 10 principaux malwares détectés au cours d'une période donnée sur les ordinateurs sélectionnés.



Note

Le tableau détails indique tous les ordinateurs ayant été infectés par les 10 malwares les plus souvent détectés.

Activité du pare-feu

Vous informe de l'état du module Pare-feu d'Endpoint Security. Vous pouvez voir le nombre de tentatives de trafic bloquées et d'analyses de ports bloquées sur les ordinateurs sélectionnés.

Sites Web Bloqués

Vous informe de l'état du module Contrôle Web d'Endpoint Security. Vous pouvez voir le nombre de sites web bloqués sur les ordinateurs sélectionnés.

Applications Bloquées

Vous informe de l'état du module Contrôle des Applications d'Endpoint Security. Vous pouvez voir le nombre d'applications bloquées sur les ordinateurs sélectionnés.

Données

Vous informe de l'état du module Données d'Endpoint Security. Vous pouvez voir le nombre d'e-mails et de sites web bloqués sur les ordinateurs sélectionnés.

Activité Antiphishing

Vous informe de l'état du module Antiphishing d'Endpoint Security. Vous pouvez voir le nombre de sites web bloqués sur les ordinateurs sélectionnés.

Applications bloquées par l'Analyse Comportementale

Vous signale les applications bloquées par AVC (Active Virus Control) / IDS (Système de détection d'intrusion). Vous pouvez voir le nombre d'applications bloquées par AVC / IDS pour chaque ordinateur sélectionné. Cliquez sur le nombre d'applications bloquées pour l'ordinateur qui vous intéresse afin d'afficher la liste des applications bloquées et des informations à leur sujet (nom de l'application, raison pour laquelle elle a été bloquée, nombre de tentatives bloquées et date et heure de la dernière tentative bloquée).

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.** Des rapports planifiés peuvent être configurés pour s'exécuter à l'heure et à la date spécifiées et 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**.

The screenshot shows the configuration page for a 'Malware Activity Report'. The breadcrumb navigation is 'Rapports > Malware Activity Report'. The page is divided into several sections:

- Détails:**
 - Type: Activité des logiciels malveillants (dropdown menu)
 - Nom: Malware Activity Report (text input)
 - Cible: Documentation (text input) with a link 'Changer la cible' below it.
- Périodicité:**
 - Périodicité: Radio buttons for 'Maintenant', 'Tous les jours', 'Chaque semaine, tous les' (with a dropdown for frequency), and 'Chaque mois, le' (selected, with a dropdown for day '1').
- Options:**
 - Fréquence des rapports: Dernier mois (dropdown menu)
 - Afficher: Radio buttons for 'Tous les malwares' (selected) and 'Uniquement les malwares non résolus'.
 - Livraison: Checkmark for 'Envoyer par e-mail à' with an email input field containing 'reporter@bd.com'.

At the bottom, there are two buttons: 'Enregistrer' and 'Annuler'.

Options des Rapports Ordinateurs

2. Cliquez sur le bouton **+ Ajouter** à droite du tableau.
3. Sélectionnez le type de rapport souhaité dans le menu. Pour plus d'informations, reportez-vous à « [Types de rapports disponibles](#) » (p. 119).

4. 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.
5. Configurez la cible du rapport en cliquant sur le lien **Changer la cible**. Sélectionnez le groupe sur lequel vous souhaitez exécuter le rapport.
6. Configurer la périodicité du rapport (planification). Vous pouvez choisir de créer le rapport immédiatement (rapport instantané), ou planifiez des rapports quotidiens, hebdomadaires (un jour spécifique de la semaine) ou mensuels (un jour spécifique du mois).



Note

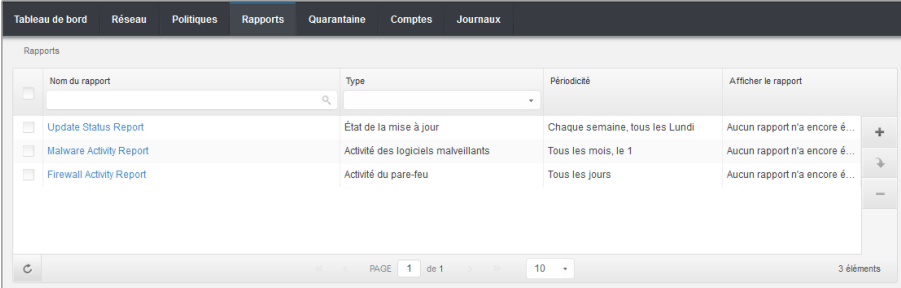
Les rapports planifiés sont générés à la date prévue immédiatement après 00:00 UTC (fuseau horaire par défaut de l'appliance GravityZone).

7. Configurer les options de rapports.
 - a. Pour la plupart des types de rapport, vous devez spécifier la fréquence des mises à jour. Le rapport comprendra uniquement des données sur la période sélectionnée.
 - b. 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 pour obtenir uniquement les informations souhaitées.

Par exemple, pour un rapport **État de la mise à jour**, vous pouvez choisir d'afficher uniquement la liste des ordinateurs mis à jour (ou, au contraire, ceux qui n'ont pas été mis à jour) pendant la période sélectionnée ou ceux ayant besoin de redémarrer pour que la mise à jour se termine.
 - c. Pour recevoir un rapport planifié par e-mail, sélectionnez l'option correspondante.
8. Cliquez sur **Générer** pour créer un rapport instantané ou sur **Enregistrer** pour créer un rapport planifié. Le bouton **Enregistrer** deviendra **Générer** si vous choisissez de créer un rapport instantané.
 - Si vous avez choisi de créer un rapport instantané, celui-ci apparaîtra immédiatement une fois que vous aurez cliqué sur **Générer**. Le temps nécessaire à la création des rapports peut varier en fonction du nombre d'ordinateurs administrés. Veuillez patienter le temps que le rapport demandé soit créé.
 - Si vous avez choisi de créer un rapport planifié, celui-ci apparaîtra dans la liste sur la page **Rapports**. Une fois que le rapport a été créé, vous pouvez le 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**.



The screenshot shows the 'Rapports' (Reports) page in the Bitdefender console. The page has a dark header with navigation tabs: 'Tableau de bord', 'Réseau', 'Politiques', 'Rapports', 'Quarantaine', 'Comptes', and 'Journaux'. Below the header, the 'Rapports' section is displayed. It features a table with the following columns: 'Nom du rapport' (Report Name), 'Type' (Type), 'Périodicité' (Frequency), and 'Afficher le rapport' (Show Report). The table contains three rows of reports:

Nom du rapport	Type	Périodicité	Afficher le rapport
Update Status Report	État de la mise à jour	Chaque semaine, tous les Lundi	Aucun rapport n'a encore é... +
Malware Activity Report	Activité des logiciels malveillants	Tous les mois, le 1	Aucun rapport n'a encore é... →
Firewall Activity Report	Activité du pare-feu	Tous les jours	Aucun rapport n'a encore é... -

At the bottom of the table, there is a pagination control showing 'PAGE 1 de 1' and a dropdown menu set to '10'. The total number of items is indicated as '3 éléments'.

La page Rapports

Tous les rapports planifiés s'affichent dans un tableau. Vous pouvez afficher les rapports planifiés générés et des informations utiles les concernant :

- Nom et type de rapport.
- Quand le rapport sera généré.



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.

Les données des rapports sont présentées dans un tableau de plusieurs colonnes fournissant différentes informations. Le tableau peut comporter plusieurs pages (seules 10 entrées par page sont affichées par défaut). Pour parcourir les pages "détails", utilisez les boutons en bas du tableau.

Pour trouver facilement ce que vous recherchez, utilisez les zones de recherche ou les options de filtrage sous les en-têtes de colonne.

Pour trier les données d'un rapport 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 effacer une zone de recherche, placez le curseur dessus et cliquez sur l'icône ✕ **Supprimer**.

Pour afficher les informations les plus récentes, cliquez sur l'icône ↻ **Actualiser** dans l'angle inférieur gauche 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.

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 ou groupes 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 détaillées sur chaque éléments du réseau administré.



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 pour faire apparaître les informations correspondantes dans le tableau se trouvant en-dessous du graphique.

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.
 - **Cible du rapport.** 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.


- **Périodicité du rapport (planification).** Vous pouvez configurer l'envoi automatique de rapport : quotidien, hebdomadaire (un jour spécifique de la semaine) ou mensuel (un jour spécifique du mois). En fonction de la planification sélectionnée, le rapport contiendra uniquement des données de la veille, de la semaine ou du mois précédent.
- **Options du rapport.** Le rapport comprendra uniquement des données de l'intervalle de mise à jour sélectionné. Vous pouvez modifier l'intervalle dès la nouvelle génération du rapport. Vous pouvez également choisir de recevoir le rapport par e-mail. 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.

4. Cliquez sur **Enregistrer** pour enregistrer 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 tous les rapports qu'il a générés 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** à droite du tableau.

9.4. 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](#)

9.4.1. Exportation de rapports

Pour exporter le rapport sur votre ordinateur :

1. Cliquez sur le bouton **Exporter** dans l'angle supérieur droit de la page du rapport.

Rapports

Exporter E-mail

Rapport sur l'état de la mise à jour

Généré par: reporter@bd.com
Activé: 21 jan 2014, 18:35:32
Périodicité: Maintenant
Période du rapport: 24 dernières heures
Intervalle de rapport: 20 jan 2014, 18:35 - 21 jan 2014, 18:35
Cibles: Documentation

Redémarrage en attente
Mis à jour
Obsolète

Nom	ip	État de la mise à jour	Versión du Produit	Dernière mise à jour	Versión des moteurs	Nom de l'entreprise
DOC-XP	10.0.2.15	Redémarrage en attente	5.3.3.358	16 jan 2014, 13:09:48	7.52689 (108255...	Documentation

Rapports - Option Exporter

2. Sélectionnez le format désiré du rapport :
 - Portable Document Format (PDF) ou
 - 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.

9.4.2. 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.

9.5. 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 consultez, cliquez sur le bouton **E-mail** dans l'angle supérieur droit de la page du rapport. 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 **Options > 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.

9.6. 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.

10. Quarantaine

Par défaut, Endpoint Security isole les fichiers suspects et les fichiers infectés par des malwares qui ne peuvent pas être désinfectés, dans une zone sécurisée nommée quarantaine. Quand un virus est en quarantaine, il ne peut faire aucun dégât car il ne peut ni être exécuté, ni être lu.

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.

Par défaut, des fichiers de la quarantaine sont automatiquement envoyés aux Laboratoires Bitdefender afin d'être analysés par les spécialistes des 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.

Le Control Center fournit des informations détaillées sur tous les fichiers placés en quarantaine, sur les éléments du réseau administrés depuis votre compte.

Pour consulter et gérer les fichiers de la quarantaine, allez sur la page **Quarantaine**.




La page Quarantaine

Des informations sur les fichiers en quarantaine sont affichées dans un tableau. Vous disposez des informations suivantes :

- Le nom de l'objet du réseau sur lequel la menace a été détectée.
- L'IP de l'objet du réseau sur lequel la menace a été détectée.
- Chemin vers le fichier infecté ou suspect sur l'élément du réseau où il a été détecté.
- Nom donné à la menace malware par les chercheurs de sécurité de Bitdefender.

- Heure à laquelle le fichier a été placé en quarantaine.
- Action en attente, requise par l'administrateur, à appliquer au fichier en quarantaine.

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

10.1. Navigation et Recherche

En fonction du nombre d'éléments administrés du réseau et de la nature des infections, le nombre de fichiers en quarantaine peut parfois être important. Le tableau peut comporter plusieurs pages (seules 10 entrées par page sont affichées 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 afin de 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.

10.2. 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.

Pour restaurer un ou plusieurs fichiers en quarantaine :

1. Allez sur la page **Quarantaine**.
2. Cochez les cases correspondant aux fichiers en quarantaine que vous souhaitez restaurer.
3. Cliquez sur le bouton  **Restaurer** à droite du tableau.
4. 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 dans le champ correspondant. 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, reportez-vous à « [Utilisation des variables du système](#) » (p. 145).

5. Cliquez sur **Restaurer** pour demander une restauration du fichier. Vous pouvez remarquer l'action en attente dans la colonne **Action**.

6. L'action requise est envoyée aux ordinateurs cibles immédiatement ou dès qu'ils sont connectés de nouveau. Une fois un fichier restauré, l'entrée correspondante disparaîtra du tableau Quarantaine.

10.3. 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 objets administrés du réseau.

Pour modifier l'intervalle de suppression automatique des fichiers en quarantaine :


1. Allez sur la page **Politiques**.
2. Trouvez la politique affectée aux objets du réseau sur lesquels vous souhaitez modifier le paramètre et cliquez sur son nom.
3. Allez dans la section **Antimalware > Quarantaine**.
4. Sélectionnez dans le menu la fréquence de la suppression automatique souhaitée.
5. Cliquez sur **Enregistrer** pour enregistrer les modifications.

10.4. Supprimer les 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. Suivez ces conseils lors de la suppression des fichiers en quarantaine :

- 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.
- Vous pouvez supprimer en toute sécurité :
 - Les fichiers d'archive sans importance.
 - Les fichiers d'installation infectés.

Pour supprimer un ou plusieurs fichiers en quarantaine :

1. Allez sur la page **Quarantaine**.
2. Vérifiez la liste des fichiers en quarantaine et cochez les cases correspondant à ceux que vous souhaitez supprimer.
3. Cliquez sur le bouton  **Supprimer** à droite du tableau. Vous pouvez remarquer l'état en attente dans la colonne **Action**.

4. 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.

11. Journal d'activité de l'utilisateur

La Control Center enregistre toutes les opérations et actions effectuées par les utilisateurs. La liste des journaux 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
- Créer, éditer, renommer et supprimer des comptes d'utilisateur
- Supprimer ou déplacer des ordinateurs 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, éditer, renommer, affecter et supprimer des politiques

Pour consulter les enregistrements de l'activité de l'utilisateur, allez sur la page **Journaux**.

Utilisateur	Rôle	Action	Zone	Cible	Créé
-------------	------	--------	------	-------	------

La page Journaux


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.

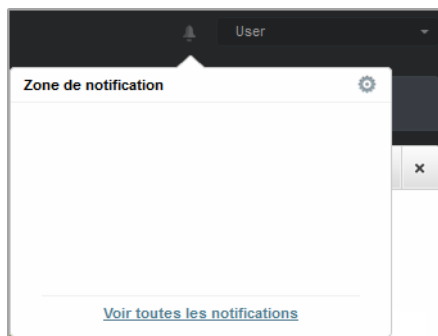
Pour trier les événements en fonction d'une colonne, cliquez simplement sur l'en-tête de cette colonne. Cliquez de nouveau sur l'en-tête de colonne pour inverser l'ordre de tri.

Pour afficher des informations détaillées sur un événement, sélectionnez-le et consultez la section sous le tableau.


Pour afficher les informations les plus récentes, cliquez sur le bouton  **Actualiser** dans l'angle inférieur gauche du tableau.

12. 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 dans l'angle supérieur droit de l'interface du Control Center.



Zone de notification

Lorsqu'un nouvel événement est détecté dans le réseau, la zone de notification affiche une icône rouge  indiquant le nombre d'événements venant d'être détectés. Cliquer sur l'icône affiche la liste des événements détectés.

12.1. 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.

Mise à jour disponible

Vous informe de la disponibilité d'une nouvelle mise à jour de Security for Endpoints (Console dans le Cloud).

La licence expire

Cette notification est envoyée 30 jours avant et 7 jours avant l'expiration de la licence, ainsi que le jour où celle-ci expire.


La limite de la licence est sur le point d'être atteinte

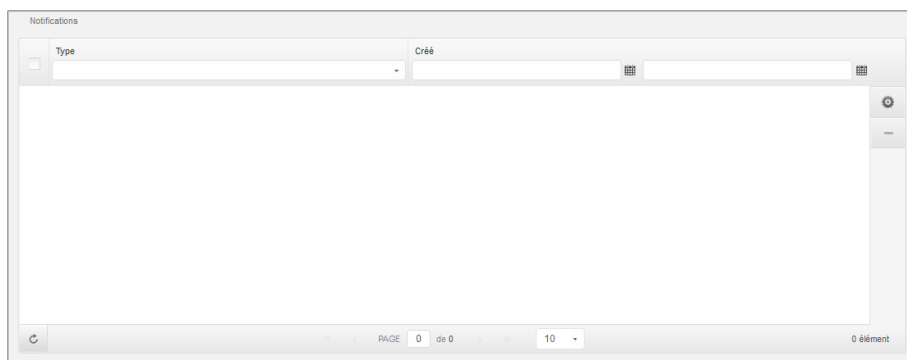
Cette notification est envoyée lorsque 90% des licences disponibles ont été utilisées.

La limite d'utilisation de la licence a été atteinte

Cette notification est envoyée lorsque toutes les licences disponibles ont été utilisées.

12.2. Afficher les notifications

Pour afficher les notifications, cliquez sur le bouton  **Zone de notification** puis cliquez sur **Voir toutes les notifications**. Un tableau contenant toutes les notifications s'affiche.



La page Notifications

En fonction du nombre de notifications, le tableau des notifications peut comporter plusieurs pages (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 zones de recherche sous les en-têtes de colonne ou le menu du filtre en haut du tableau, afin de filtrer les données affichées. Vous pouvez par exemple rechercher un type de notification spécifique ou choisir d'afficher uniquement les notifications générées au cours d'un intervalle donné.

- 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.

12.3. Supprimer des notifications



Pour supprimer des notifications :

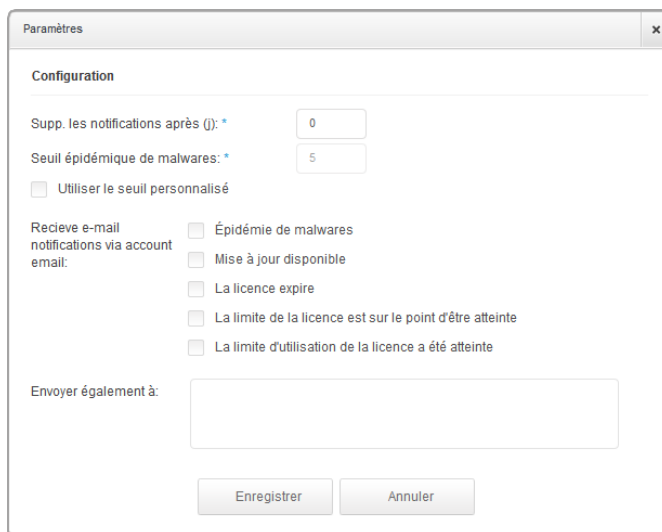
1. Cliquez sur le bouton  **Zone de notification** à droite de la barre de menus puis cliquez sur **Voir toutes les notifications**. Un tableau contenant toutes les notifications s'affiche.
2. Sélectionnez les notifications que vous voulez supprimer.
3. Cliquez sur le bouton  **Supprimer** à droite du tableau.

12.4. 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  **Zone de notification** à droite de la barre de menus puis cliquez sur **Voir toutes les notifications**. Un tableau contenant toutes les notifications s'affiche.
2. Cliquez sur le bouton  **Configurer** à droite du tableau. La fenêtre **Paramètres de notification** apparaît.



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. Sélectionnez les types de notification souhaités dans la liste. Pour plus d'informations, reportez-vous à « [Types de notifications](#) » (p. 135)
4. Vous pouvez également choisir d'envoyer les notifications par e-mail à certaines adresses e-mail. Saisissez les adresses e-mail dans le champ prévu à cet effet, en appuyant sur Entrée après chaque adresse.
5. Cliquez sur **Enregistrer**.

13. 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 vous 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.

13.1. Centre de support de Bitdefender

Le Centre de support de Bitdefender, disponible à l'adresse suivante <http://www.bitdefender.fr/support>, est l'endroit où vous trouverez 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 la base de connaissances
- Forum du Support Bitdefender
- Documentation du produit

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 la base de connaissances

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>.

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 <http://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.

Documentation du produit

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

Vous pouvez consulter et télécharger la version la plus récente de la documentation sur les produits Bitdefender pour entreprises dans [Centre de Support](#) > Documentation.

13.2. Demande d'aide

Vous pouvez nous contacter pour nous demander de l'aide grâce à notre Centre de support en ligne :

1. Allez à <http://www.bitdefender.fr/site/Main/nousContacterBusiness/>.
2. Utilisez le formulaire de contact pour faire une demande par e-mail ou accéder aux autres options de contact disponibles.

13.3. Utiliser l'Outil de Support

L'Outil de Support Security for Endpoints (Console dans le Cloud) 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.

Pour utiliser l'Outil de Support :

1. Téléchargez l'Outil de Support et diffusez-le aux ordinateurs affectés. Pour télécharger l'Outil de Support :
 - a. Connectez-vous au Control Center en utilisant votre compte.
 - b. Cliquez sur le lien **Aide et Support**, dans l'angle inférieur droit de la console.
 - c. Les liens de téléchargement sont disponibles dans la section **Support**. Deux versions sont disponibles : l'une pour les systèmes 32 bits et l'autre pour les systèmes 64 bits. Vérifiez que vous utilisez la version correcte lorsque vous exécutez l'Outil de Support sur un ordinateur.
2. Exécuter l'Outil de Support localement sur chacun des ordinateurs affectés.
 - a. Cochez la case d'accord et cliquez sur **Suivant**.
 - b. Compléter le formulaire de soumission avec les données nécessaires :
 - i. Indiquez votre adresse e-mail.
 - ii. Saisissez votre nom.
 - iii. Sélectionnez votre pays dans le menu correspondant.
 - iv. Décrivez le problème que vous avez rencontré.
 - v. Vous pouvez également essayer de reproduire le problème avant de commencer à recueillir des données. Dans ce cas, procédez comme suit :
 - A. Activez l'option **Essayer de reproduire le problème avant la soumission**.
 - B. Cliquez sur **Suivant**.
 - C. Sélectionnez le type de problème que vous avez rencontré .
 - D. Cliquez sur **Suivant**.
 - E. Reproduisez le problème sur votre ordinateur. Une fois cela effectué, revenez dans l'Outil de support et sélectionnez l'option **J'ai reproduit le problème**.
 - c. Cliquez sur **Suivant**. L'Outil de Support recueille des informations sur le produit, liées aux autres applications installées sur la machine et à la configuration matérielle et logicielle.
 - d. Patientez jusqu'à la fin du processus.
 - e. Cliquez sur **Terminer** pour fermer la fenêtre. Une archive zip a été créée sur votre bureau.

Envoyez l'archive zip avec votre demande au représentant du support de Bitdefender à l'aide du formulaire du ticket de support par e-mail sur la page **Aide et Support** de la console.

13.4. Contacts

Une communication efficace est la clé d'une relation réussie. Au cours des dix 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.

13.4.1. Adresses Web

Ventes : bitdefender@editions-profil.eu

Centre de support : <http://www.bitdefender.fr/support>

Documentation : documentation@bitdefender.com

Distributeurs Locaux : <http://www.bitdefender.fr/partenaires/trouver-un-partenaire.html>

Partner Program: partners@editions-profil.eu

Relations Presse : communication@editions-profil.eu

Virus Submissions: virus_submission@bitdefender.com

Spam Submissions: spam_submission@bitdefender.com

Report Abuse: abuse@bitdefender.com

Site web : <http://www.bitdefender.fr/>

13.4.2. 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.

France

Editions Profil

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 : supportpro@editions-profil.eu

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

Centre de support : <http://www.bitdefender.fr/support/professionnel.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 Internet : <http://www.bitdefender.es>

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

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 : <http://www.bitdefender.com/support/business.html>

Allemagne

Bitdefender GmbH

Airport Office Center

Robert-Bosch-Straße 2

59439 Holzwickede

Deutschland

Téléphone (services administratif et commercial) : +49 (0)2301 91 84 222

Téléphone (support technique) : +49 (0)2301 91 84 444

Ventes : vertrieb@bitdefender.de

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

Centre de support : <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 (0) 8451-305096

E-mail : info@bitdefender.co.uk

Ventes : sales@bitdefender.co.uk

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

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

Roumanie

BITDEFENDER SRL

DV24 Offices, Building A

24 Delea Veche Street

024102 Bucharest, Sector 2

Fax : +40 21 2641799

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

Ventes : sales@bitdefender.ro

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

Centre de support : <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/world>

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

A. Annexes

A.1. Liste des types de fichier d'Application

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; accdba; accdb; 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; fpx; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; lacdba; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpv; 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; 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; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

A.2. Utilisation des 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 :

- **Windows XP :**
C:\Documents and Settings\{username}\Application Data
- **Windows Vista/7 :**
C:\Users\{username}\AppData\Roaming

%HOMEPATH%

Les dossiers utilisateurs.Chemin typique :

- **Windows XP :**
\Documents and Settings\{username}
- **Windows Vista/7 :**
\Users\{username}

%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.

Glossaire

Adware

Les adwares sont souvent associés à des applications gratuites mais exigeant leur acceptation par l'utilisateur. Ces adwares 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 « pop up » publicitaires peuvent devenir contrariants et dans certains cas dégrader les performances du système. De plus, les informations collectées peuvent mettre en péril la vie privée des utilisateurs qui ne s'étaient pas complètement rendu compte des termes de l'accord de licence.

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.

Backdoor

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.

Code malveillant

« 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.

Cookies

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.

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.

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.

Hameçonnage

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.

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.

Keylogger

Application qui enregistre tout ce qui est tapé.

Les keyloggers 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 de sécurité sociale).

Ligne de commande

Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.

Logiciel espion

Tout type de logiciel récupérant les informations des utilisateurs via leur connexion Internet à leur insu, généralement à des fins publicitaires. Les spywares sont généralement cachés dans des logiciels sharewares ou freewares pouvant être téléchargés sur Internet. Notons toutefois que la plupart des applications sharewares ou freewares ne comportent pas de spywares. Une fois installé, le spyware 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 spywares 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 spywares 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.

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. Les deux navigateurs les plus populaires sont Netscape Navigator et Microsoft Internet Explorer. Les deux sont des navigateurs graphiques, ce qui signifie qu'ils peuvent

afficher aussi bien le graphisme que le texte. De plus, les navigateurs les plus modernes peuvent visionner les informations multimédia, y compris le son et la vidéo, bien qu'ils exigent des modules d'extension (plugins) pour certains formats.

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.

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.

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 de boot 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.

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 de boot

Virus qui infecte le secteur de boot d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus de boot 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.

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 : fax, imprimante, modem, volume, etc. Double-cliquez ou faites un clic-droit sur une icône pour afficher les options.