

Bitdefender® ENTERPRISE

SECURITY FOR ENDPOINTS (CONSOLE DANS LE CLOUD)

Guide de démarrage rapide



Security for Endpoints (Console dans le Cloud)

Guide de démarrage rapide

Date de publication 2014.04.14

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.

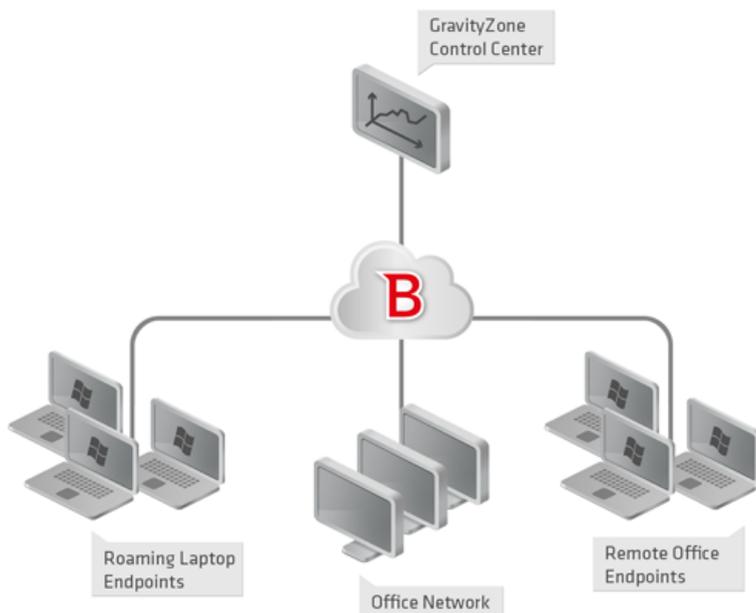


Table des matières

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. Installation et configuration	11
4.1. Préparation de l'Installation	11
4.2. Installer le service sur les ordinateurs	12
4.2.1. Installation locale	13
4.2.2. Installation à distance	16
4.3. Organisation des ordinateurs (Facultative)	20
4.4. Créer et affecter une politique de sécurité	21
5. Surveillance de l'état de sécurité	25
6. Analyse des ordinateurs administrés	27
7. Obtenir de l'aide	29
A. Configuration requise	30
A.1. Configuration requise pour Security for Endpoints	30
A.1.1. Systèmes d'exploitation pris en charge	30
A.1.2. Matériel	31
A.1.3. Navigateurs pris en charge	31
A.2. Fonctionnement de Network Discovery	32
A.2.1. Plus d'informations sur le service Explorateur d'ordinateurs de Microsoft	33
A.2.2. Configuration requise pour la découverte du réseau	33

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

Security for Endpoints peut être configuré et administré à l'aide de Control Center, une interface web hébergée par Bitdefender.

Suite à votre inscription pour une version d'essai ou à votre achat du service, vous recevrez un e-mail du Service Inscription de Bitdefender. L'e-mail contient vos informations de connexion.

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**.

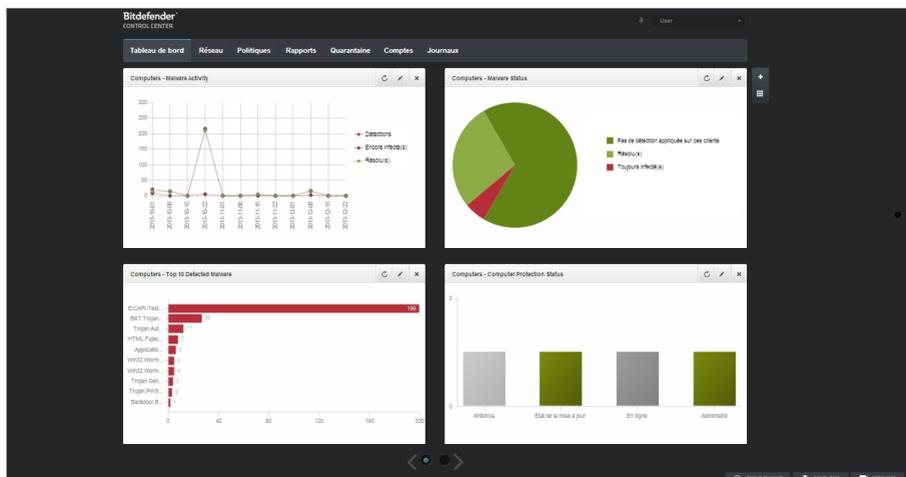


Note

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

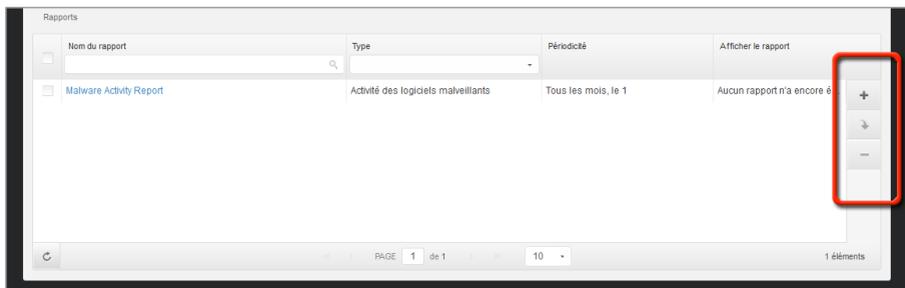
Pour que la console affiche des informations à jour, cliquez sur le bouton  **Actualiser** dans l'angle inférieur gauche du tableau.

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 :

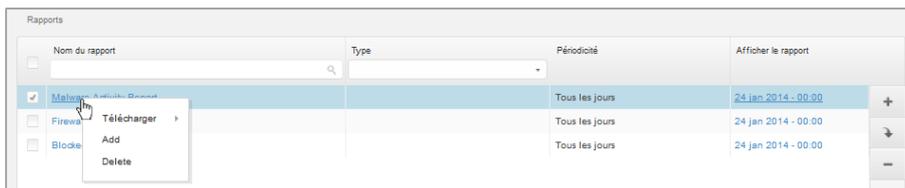
- Créer un nouveau rapport.
- Télécharger les rapports générés par un rapport planifié.
- Supprimer un rapport planifié.



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.

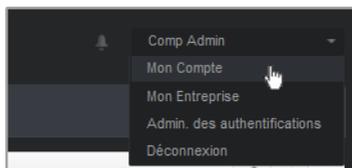


La page Rapports - Menu contextuel

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. Installation et configuration

L'installation et la configuration sont assez simples. Voici les étapes principales :

1. [Étape 1 - Préparation à l'installation](#)
2. [Étape 2 - Installation du service sur les ordinateurs.](#)
3. [Étape 3 - Organiser les ordinateurs en groupes \(facultatif\).](#)
4. [Étape 4 - Création et configuration d'une politique de sécurité](#)

Pour les deux premières étapes, les informations de connexion de l'ordinateur sont requises. Les deux autres étapes sont effectuées à partir de Control Center.

4.1. 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.

4.2. Installer le service sur les ordinateurs

Security for Endpoints est conçu pour les postes de travail, les ordinateurs portables et les serveurs fonctionnant sous Microsoft® Windows. Pour protéger des postes de travail avec Security for Endpoints, vous devez installer Endpoint Security (la solution 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.

Il y a deux méthodes d'installation :

- **Installation locale.** Téléchargez les packages d'installation à partir de Control Center sur les ordinateurs individuels, puis exécutez en local l'installation d'Endpoint Security. Une autre option consiste à télécharger le package, à l'enregistrer sur un partage réseau et à envoyer aux utilisateurs de l'entreprise des e-mails comprenant le lien vers le package, leur demandant de télécharger et d'installer la protection sur leur ordinateur. L'installation locale est guidée par un assistant.
- **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. La protection de Security for Endpoints peut ensuite être installée à distance à partir de la console sur les autres ordinateurs du réseau. L'installation à distance s'effectue en tâche de fond, sans que l'utilisateur ne le sache.

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. 13).

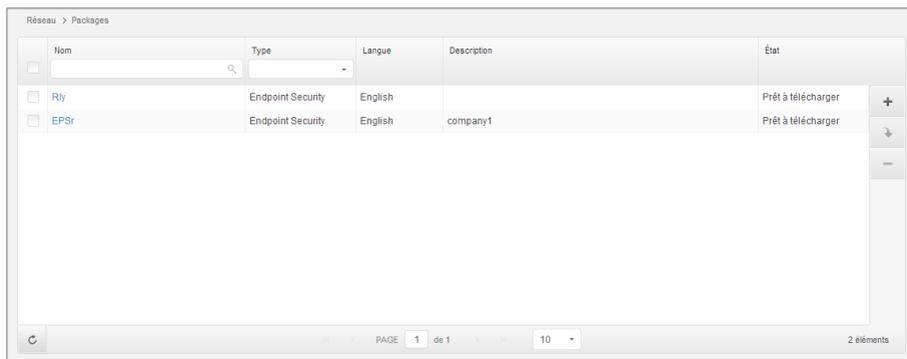
4.2.1. Installation locale

L'installation locale nécessite le téléchargement à partir de Control Center et l'exécution du package d'installation sur tous les ordinateurs cibles. Vous pouvez créer différents packages d'installation en fonction des besoins spécifiques à chaque ordinateur (par exemple, le chemin d'installation ou la langue de l'interface utilisateur).

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**.



La page Packages

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

The screenshot shows the 'Endpoint Security' configuration window. On the left, there is a sidebar with 'Options' and 'Avancé'. The main area is titled 'Détails' and contains the following sections:

- Détails:** 'Nom: *' (text input: EPS-FR), 'Description:' (text input: Endpoint Security FR).
- Général:** 'Role:' (dropdown: Endpoint Security Relay), 'Société:' (dropdown: Sélectionner une entreprise).
- Modules à installer:** Three checkboxes are checked: 'Antimalware', 'Pare-feu', and 'Contrôle de contenu'.
- Configuration:** 'Langue:' (dropdown: Français), 'Analyser avant l'installation' (checked), 'Utiliser le chemin d'installation personnalisé' (unchecked), 'Mot de passe de désinstallation' (unchecked). Below these are 'Mot de passe:' (button: Cliquez ici pour changer le m...) and 'Confirmer:' (button: Veuillez saisir de nouveau le...).
- A warning icon and text: 'Endpoint Security by Bitdefender désinstalle automatiquement les autres logiciels de sécurité.'
- Buttons at the bottom right: 'Suivant >' and '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.

Télécharger et installer Endpoint Security

1. Connectez-vous à <https://gravityzone.bitdefender.com/> à l'aide de votre compte à partir de l'ordinateur sur lequel vous souhaitez installer la protection.
2. Accédez à la page **Réseau > Packages**.
3. Sélectionnez l'entreprise appropriée dans la liste sous l'en-tête de la colonne **Société**. Seuls les packages disponibles pour l'entreprise sélectionnée s'afficheront.
4. Sélectionnez le package d'installation d'Endpoint Security que vous souhaitez télécharger.
5. 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. Notez que deux versions sont disponibles pour Windows : l'une pour les systèmes 32 bits et l'autre pour les systèmes 64 bits. Veillez à utiliser la version adaptée à l'ordinateur sur lequel vous l'installez.
6. Enregistrez le fichier sur l'ordinateur.
 7. Exécutez le package d'installation.



Note

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

8. 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.

4.2.2. 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.

Pour faciliter le déploiement, Security for Endpoints comprend un mécanisme de découverte du réseau automatique qui permet de détecter les ordinateurs dans le même réseau. Les ordinateurs détectés sont affichés en tant qu'**ordinateurs non administrés** sur la page **Réseau**.

Pour activer le Network Discovery et l'installation à distance, vous devez déjà avoir installé Endpoint Security sur au moins un ordinateur du réseau. Cet ordinateur sera utilisé pour analyser le réseau et installer Endpoint Security sur les ordinateurs non protégés. Quelques minutes peuvent être nécessaires pour que les autres ordinateurs du réseau deviennent visibles dans Control Center.

Configuration requise pour l'installation à distance

Pour que la découverte du réseau fonctionne, certaines conditions doivent être remplies. Pour en savoir plus, reportez-vous à « [Fonctionnement de Network Discovery](#) » (p. 32).

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.

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

Pour exécuter une tâche d'installation à distance :

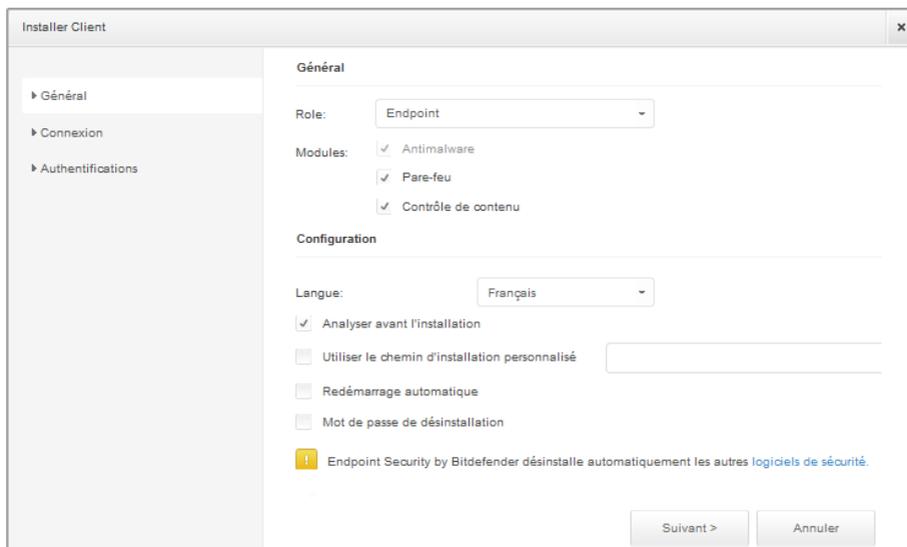
1. Connectez-vous et identifiez-vous sur le Control Center.
2. Allez sur la page **Réseau**.
3. Sélectionnez le groupe du réseau souhaité dans le panneau de gauche. Les entités contenues dans le groupe sélectionné apparaissent dans le tableau du panneau de droite.



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**.

4.3. Organisation des ordinateurs (Facultative)

Les réseaux d'entreprise s'affichent dans le panneau de gauche de la page **Réseau**. Il y a un groupe racine par défaut pour chacune de vos entreprises. Tous ses ordinateurs protégés ou détectés sont automatiquement placés dans ce groupe.

Si vous administrez un nombre important d'ordinateurs (des dizaines ou plus), vous aurez probablement besoin de les organiser dans des groupes. Organiser les ordinateurs dans des groupes vous aide à les gérer plus efficacement. L'un des principaux avantages est que vous pouvez utiliser des politiques de groupes pour répondre à différents besoins en sécurité.

Vous pouvez organiser les ordinateurs en créant des groupes sous le groupe de l'entreprise par défaut et en plaçant les ordinateurs dans le groupe approprié.

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, Gestion etc.).
- Besoins en sécurité (Ordinateurs de bureau, Portables, Serveurs etc.).
- Emplacement (siège, bureaux locaux, travailleurs à distance, bureaux à domicile etc.).



Note

- Les groupes créés peuvent 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 des 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 **Type > Ordinateurs** et **Profondeur > Tous les éléments de manière récurrente**.

Pour organiser le réseau d'un client en groupes :

1. Allez sur la page **Réseau**.
2. Dans le panneau de gauche, sous **Entreprises**, sélectionnez la société cliente que vous souhaitez administrer.

**Note**

Pour les entreprises partenaires sous votre compte ayant le droit de gérer des réseaux, sélectionnez le groupe **Réseaux**.

3. Cliquez sur le bouton **+ Ajouter un groupe** en haut du panneau de gauche.
4. Indiquez un nom explicite pour le groupe et cliquez sur **OK**. Le nouveau groupe apparaît sous la société correspondante.
5. Suivez les étapes précédentes pour créer des groupes supplémentaires.
6. Déplacez les ordinateurs du groupe racine vers le groupe approprié:
 - a. Cochez les cases correspondant aux ordinateurs que vous souhaitez déplacer.
 - b. Glissez-déposez votre sélection dans le groupe souhaité du panneau de gauche.

4.4. Créer et affecter une politique de sécurité

4.4. Créer et affecter une politique de sécurité

Une fois installée, la protection Security for Endpoints peut être configurée et gérée à partir de Control Center à l'aide des politiques de sécurité. Une politique précise les paramètres de sécurité à appliquer aux ordinateurs cibles.

Juste après l'installation, les ordinateurs se voient attribuer la politique par défaut, qui est préconfigurée avec les paramètres de protection recommandés. Pour consulter les paramètres de protection par défaut, allez sur la page **Politiques** et cliquez sur le nom de la politique par défaut. Vous pouvez modifier les paramètres de protection selon vos besoins et configurer également des fonctionnalités de protection supplémentaires en créant et en affectant des politiques personnalisées.

**Note**

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. Vous pouvez, par exemple, configurer différentes politiques pour les postes de travail de bureau, les portables et les serveurs. Une approche différente consiste à créer des politiques distinctes pour chaque réseau de votre client.

Voici ce que vous avez besoin de savoir au sujet des politiques :

- Les politiques sont créées sur la page **Politiques** et affectées aux postes de travail de la page **Réseau**.
- Les postes de travail peuvent uniquement avoir une politique active à la fois.
- Les politiques sont envoyées aux ordinateurs cibles immédiatement après leur création ou leur modification. Les paramètres devraient être appliqués aux postes de travail en moins d'une minute (à condition qu'ils soient en ligne). Si un ordinateur est hors 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.
- Les ordinateurs sous un compte entreprise peuvent être administrés avec des politiques à la fois par l'administrateur de l'entreprise et par le partenaire ayant créé le compte. Les politiques créées à partir du compte partenaire ne peuvent pas être modifiées à partir du compte entreprise.

Pour créer une nouvelle politique :

1. Allez sur la page **Politiques**.
2. Cliquez sur le bouton **+ Ajouter** à droite du tableau. Cette commande crée une nouvelle politique à partir du modèle de politique par défaut.
3. Indiquez un nom explicite pour la politique. Lorsque vous choisissez un nom, prenez en compte l'objectif et la cible de la politique.
4. Configurez ensuite les paramètres de la politique. Les paramètres de sécurité par défaut sont recommandés dans la plupart des situations.
5. Cliquez sur **Enregistrer**. La nouvelle politique apparaît dans le tableau **Politiques**.

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

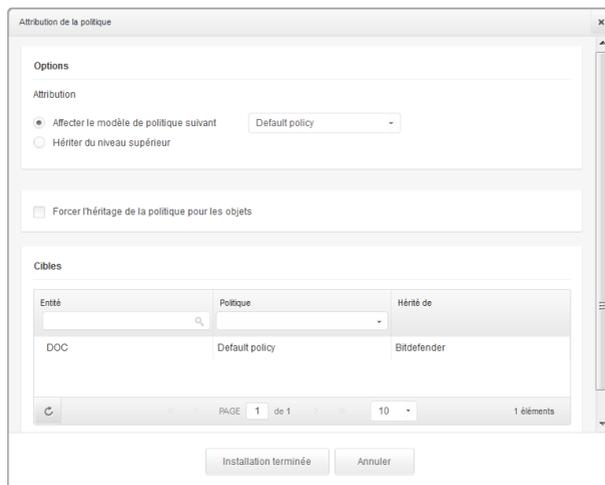
Vous pouvez affecter uniquement les politiques que vous avez créées. Pour affecter une politique créée par un autre utilisateur, vous devez commencer par la cloner sur la page **Politiques**.

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 :



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.

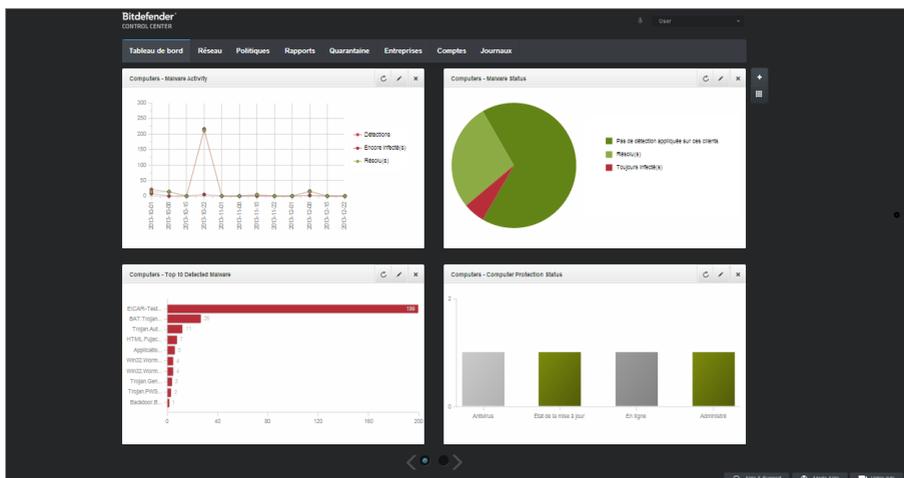
5. Cliquez sur **Terminer** pour enregistrer et appliquer des modifications.

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.

5. Surveillance de l'état de sécurité

Le principal outil de surveillance de Security for Endpoints est le tableau de bord de Control Center, une représentation visuelle personnalisable fournissant un aperçu rapide de la sécurité de votre réseau.



Le tableau de bord

Consultez régulièrement la page **Tableau de bord** pour voir des informations en temps réel sur l'état de sécurité du réseau.

Les portlets du tableau de bord affichent différentes informations de sécurité sous la forme de graphiques faciles à lire, vous permettant d'identifier rapidement tout problème susceptible de requérir votre attention.

Voici ce que vous avez besoin de savoir sur la gestion de votre tableau de bord :

- Control Center dispose de plusieurs portlets prédéfinis sur le tableau de bord. Vous pouvez ajouter plus de portlets à l'aide du bouton **+** **Ajouter un portlet** sur la partie de droite du tableau de bord.
- Chaque portlet du tableau de bord comprend un rapport détaillé en arrière-plan, accessible d'un simple clic sur le graphique.
- Les informations affichées par les portlets se rapportent uniquement aux éléments du réseau relatif à votre compte. Vous pouvez personnaliser les informations qu'affiche un

portlet (type, fréquence des rapports, cibles) en cliquant sur l'icône  **Modifier le portlet** de sa barre de titre.

Vous pouvez par exemple configurer des portlets pour qu'ils affichent des informations sur une certaine société de votre réseau.

- 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.
- Cliquez sur les entrées de la légende du graphique, lorsque cela est possible, pour masquer ou afficher la variable correspondante sur le graphique.
- Vous pouvez réorganiser les portlets du tableau de bord afin qu'ils répondent mieux à vos besoins en cliquant sur le bouton  **Réorganiser les portlets** sur la partie de droite du tableau de bord. Vous pouvez ensuite glisser-déposer les portlets à l'emplacement de votre choix.
- Les portlets s'affichent en groupes de quatre. Utilisez le curseur en bas de la page pour naviguer entre les groupes de portlets.

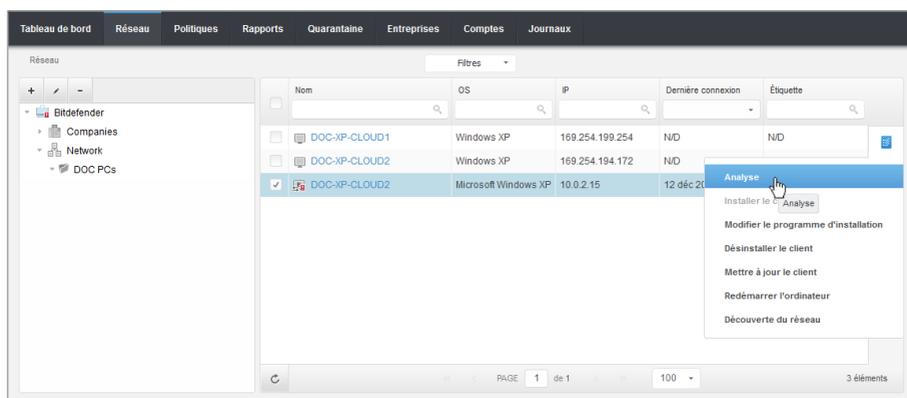
6. Analyse des ordinateurs administrés

Il y a trois façons d'analyser les ordinateurs protégés par Endpoint Security :

- L'utilisateur connecté à l'ordinateur peut lancer une analyse à partir de l'interface utilisateur Endpoint Security.
- Vous pouvez créer des tâches d'analyse planifiées à l'aide de la politique.
- Exécutez une tâche d'analyse immédiate à partir de la console.

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

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. Sélectionnez les entités que vous souhaitez analyser. Vous pouvez sélectionner certains ordinateurs administrés ou l'ensemble d'un groupe.
4. Cliquez sur le bouton  **Tâche** à droite du tableau et sélectionnez **Analyser**. Une fenêtre de configuration s'affichera.



Tâche Analyse des ordinateurs

5. Dans l'onglet **Général**, sélectionnez le type d'analyse à partir du menu **Type** :

- L'**Analyse rapide** recherche les malwares en cours d'exécution sur le système, sans prendre 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.
6. Cliquez sur **Enregistrer** pour créer la tâche d'analyse. Une message de confirmation s'affichera.



Note

Une fois créée, la tâche d'analyse commencera à s'exécuter immédiatement sur les ordinateurs en ligne.

Si un ordinateur est hors ligne, il sera analysé dès qu'il sera de nouveau en ligne.

7. Vous pouvez afficher et gérer les tâches sur la page **Réseau > Tâches**.

7. Obtenir de l'aide

Pour trouver des ressources d'aide supplémentaires ou pour obtenir de l'aide de Bitdefender :

- Cliquez sur le lien **Aide et Support**, dans l'angle inférieur droit de Control Center.
- Consultez notre [Centre d'assistance en ligne](#).

Pour contacter le support technique, merci d'utiliser ce [formulaire en ligne](#).

A. Configuration requise

A.1. Configuration requise pour Security for Endpoints

A.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

A.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.

A.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+

A.2. 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
\\SCIREFMN
\\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'envoie 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.

A.2.1. 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.

A.2.2. 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.