
Bitdefender ENTERPRISE
BITDEFENDER
SMALL OFFICE
SECURITY
Guide du rapporteur ››

Bitdefender Small Office Security
Guide du rapporteur

Date de publication 2014.12.17


Bitdefender

Table des matières

1. À propos de Small Office Security 1

2. Pour démarrer 3
2.1. Connexion au Control Center 3
2.2. Le Control Center en un coup d'œil 3
2.2.1. Données du tableau 5
2.2.2. Barres d'outils d'actions 6
2.2.3. Menu contextuel 6
2.3. Changer de mot de passe de connexion 6
2.4. Gérer votre compte 7

3. Tableau de bord de supervision 8
3.1. Actualiser les données du portlet 9
3.2. Modification des paramètres d'un portlet 9
3.3. Ajouter un nouveau portlet 9
3.4. Suppression d'un portlet 10
3.5. Réorganiser les portlets 11

4. Notifications 12
4.1. Types de notifications 12
4.2. Afficher les notifications 13
4.3. Supprimer des notifications 15
4.4. Configurer les paramètres de notification 15

5. Utilisation des rapports 18
5.1. Types de rapports disponibles 18
5.2. Création de rapports 21
5.3. Afficher et gérer des rapports planifiés 23
5.3.1. Afficher les rapports 24
5.3.2. Modifier les rapports planifiés 25
5.3.3. Supprimer les rapports planifiés 26
5.4. Enregistrer des rapports 26
5.4.1. Exportation de rapports 27
5.4.2. Télécharger des Rapports 27
5.5. Envoyer des rapports par e-mail 28
5.6. Impression des rapports 28

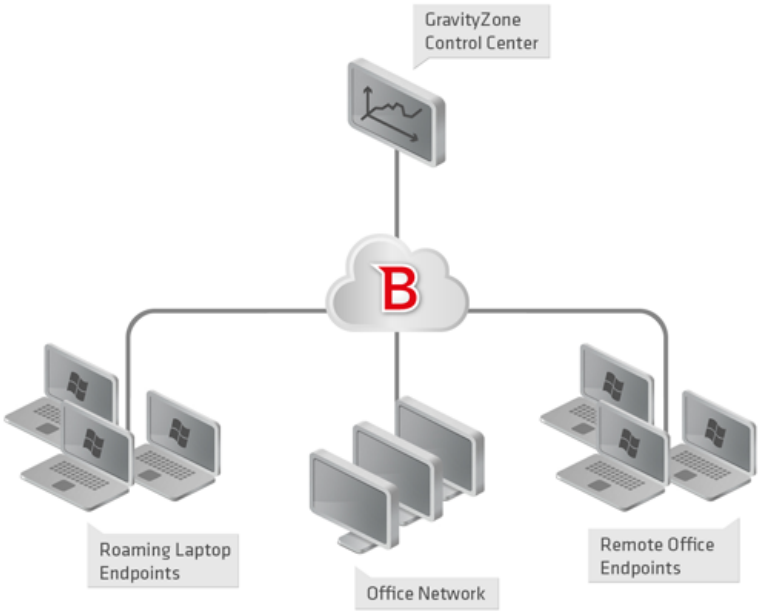
6. Journal d'activité de l'utilisateur 29

7. Obtenir de l'aide 31

Glossaire 32

1. À propos de Small Office Security

Small Office Security 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 Small Office Security

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 solutions BitdefenderSmall Office Security 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

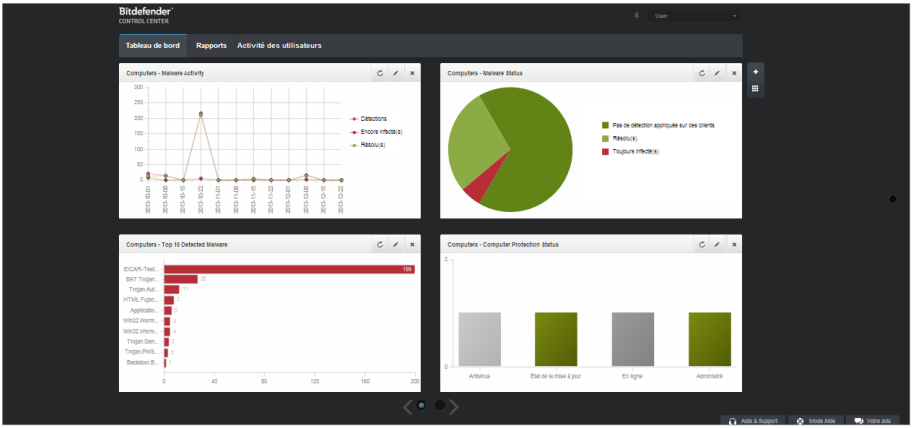
Pour se connecter au Control Center :

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.



Le tableau de bord

Les rapporteurs 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.

Rapports
Obtenir des rapports de sécurité sur les clients administrés.

Activité des utilisateurs
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.
- **Déconnexion**. Cliquez sur cette option pour vous déconnecter de votre compte.

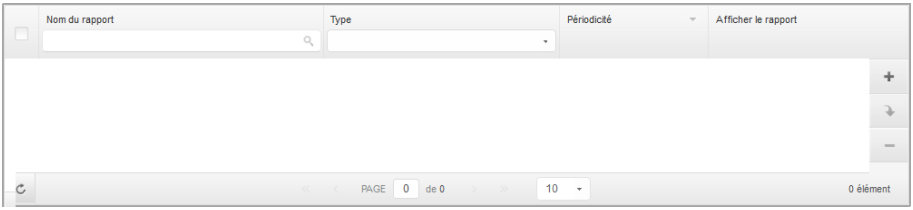
Vous trouverez les liens suivants dans l'angle inférieur droit de la console :

- **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 du 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 Small Office Security.

2.2.1. 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.

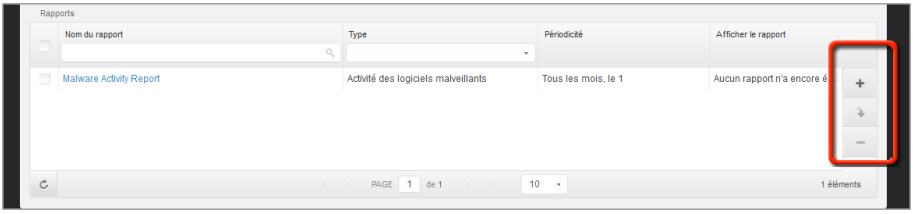
Actualiser les données du tableau

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

2.2.2. 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 :

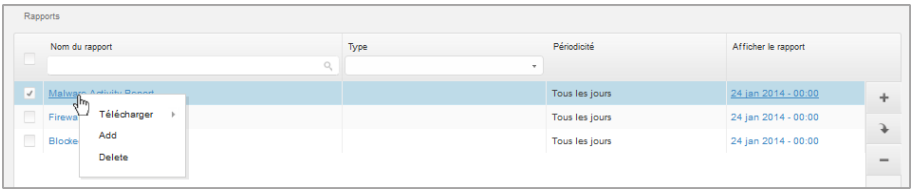
- Créer un nouveau rapport.
- Télécharger les rapports générés par un rapport planifié.
- Supprimer un rapport planifié.



La page Rapports - Barre d'outil d'actions

2.2.3. 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. Changer de mot de passe de connexion

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

Nous vous recommandons de réaliser les actions suivantes :

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

- Changez régulièrement de mot de passe de connexion.

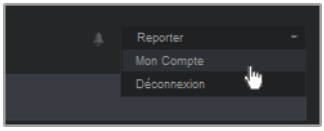
Pour changer le mot de passe de connexion :

1. 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 appliquer les modifications.

2.4. 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

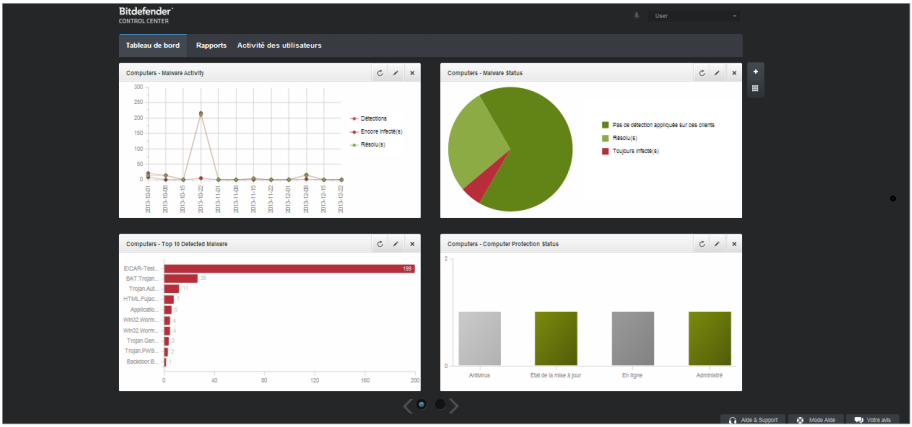
2. Sous **Détails du compte**, corrigez ou actualisez les détails de votre compte.
   - **Prénom & Nom .** Indiquez votre nom complet.
   - **E-mail.** Ceci est votre Login et votre e-mail de contact. Des rapports et d'importantes notifications de sécurité sont envoyés à cette adresse. Des notifications 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 les informations horaires en fonction du fuseau horaire sélectionné.
   - **Langue.** Choisissez dans le menu la langue d'affichage de la console.
   - **Temps imparti à la session.** Sélectionnez la période d'inactivité avant que votre session utilisateur n'expire.
4. Cliquez sur **Enregistrer** pour appliquer les modifications.

Note
Vous ne pouvez pas supprimer votre propre compte.

3. 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 :

- Le Control Center dispose de plusieurs portlets prédéfinis sur le tableau de bord.
- Chaque portlet du tableau de bord comprend un rapport détaillé en arrière-plan, accessible d'un simple clic sur le graphique.
- Il existe plusieurs types de portlets comprenant différentes informations sur la protection des 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. 18).
- 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.

3.1. Actualiser les données du portlet

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

3.2. 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.

3.3. 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. 18).
4. Sous l'onglet **Cibles**, sélectionnez les objets et les groupes du réseau à inclure.
5. Cliquez sur **Enregistrer**.

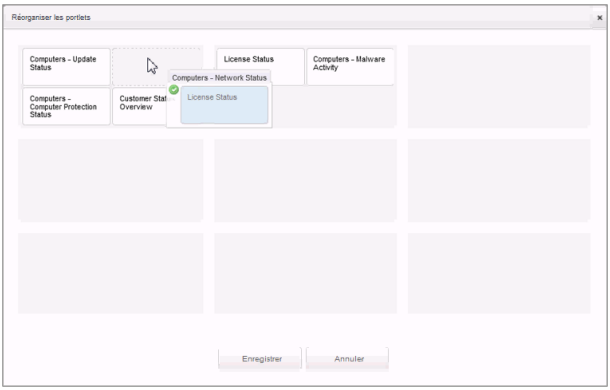
3.4. Suppression d'un portlet

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 paramères.

3.5. Réorganiser les portlets

Vous pouvez réorganiser les portlets du tableau de bord en fonction de vos besoins. Pour réorganiser les portlets :

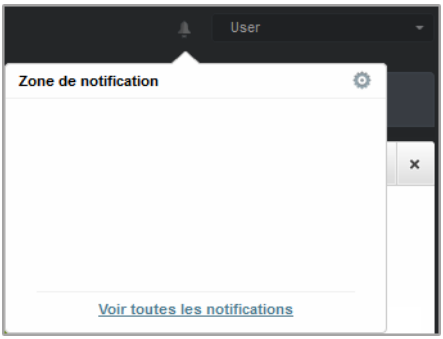
1. Allez sur la page **Tableau de bord**.
2. Cliquez sur le bouton **Réorganiser les portlets** à droite du tableau de bord. La fenêtre de la disposition des portlets s'affiche.
3. Glissez-déposez chaque portlet à l'emplacement de votre choix.
4. Cliquez sur **Enregistrer**.



Réorganisation des portlets du tableau de bord

4. 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.

4.1. Types de notifications

Voici la liste des types de notification disponibles :

Épidémie de malwares
Cette notification est envoyée aux utilisateurs qui ont, au moins, 5% de l'ensemble de leurs éléments administrés, infectés par le même malware.

Vous pouvez configurer le seuil de déclenchement antimalware dans la fenêtre **Paramètres**. Pour plus d'informations, reportez-vous à « Configurer les paramètres de notification » (p. 15).

La licence expire
Cette notification est envoyée trente, sept jours et un jour avant l'expiration de la licence.

La limite d'utilisation de la licence a été atteinte
Cette notification est envoyée lorsque toutes les licences disponibles ont été utilisées.

La limite de la licence est sur le point d'être atteinte
Cette notification est envoyée lorsque 90% des licences disponibles ont été utilisées.

Mise à jour disponible
Cette notification vous informe de la disponibilité d'une nouvelle mise à jour de Small Office Security.

Événement de l'Antiphishing
Cette notification vous informe à chaque fois que l'agent du poste de travail bloque l'accès à une page web de phishing connue. Cette notification fournit également des informations telles que le poste de travail ayant tenté d'accéder au site web dangereux (nom et IP), l'agent installé ou l'URL bloquée.

Événement du Pare-Feu
Cette notification vous informe à chaque fois que le module pare-feu d'un agent installé a empêché une analyse de ports ou une application d'accéder au réseau, selon la politique appliquée.

Événement de l'AVC/IDS
Cette notification est envoyée à chaque fois qu'une application potentiellement dangereuse est détectée et bloquée sur un poste de travail de votre réseau. Vous trouverez également des informations sur le type d'application dangereuse dont il s'agit, son nom et chemin d'accès.

Événement du Contrôle Utilisateur
Cette notification est déclenchée à chaque fois que l'activité d'un utilisateur comme sa navigation sur Internet ou une application logicielle est bloquée par l'endpoint client en raison de la politique appliquée.

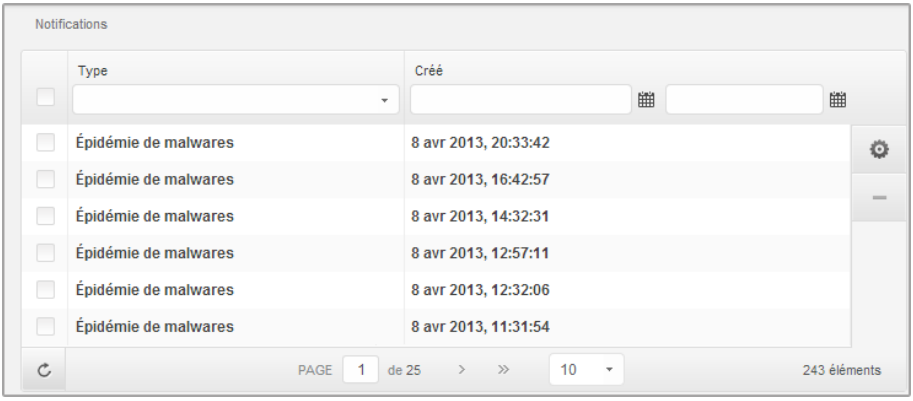
Événement des Données
Cette notification est envoyée à chaque fois que le trafic des données est bloqué sur un poste de travail en raison des règles de protection des données.

Événement des modules du produit
Cette notification est envoyée à chaque fois qu'un module de sécurité d'un agent installé est désactivé.

Événement Enregistrement du produit
Cette notification vous informe lorsque l'état d'activation d'un agent installé dans votre réseau a changé.

4.2. 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 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.

- 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.

4.3. 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.

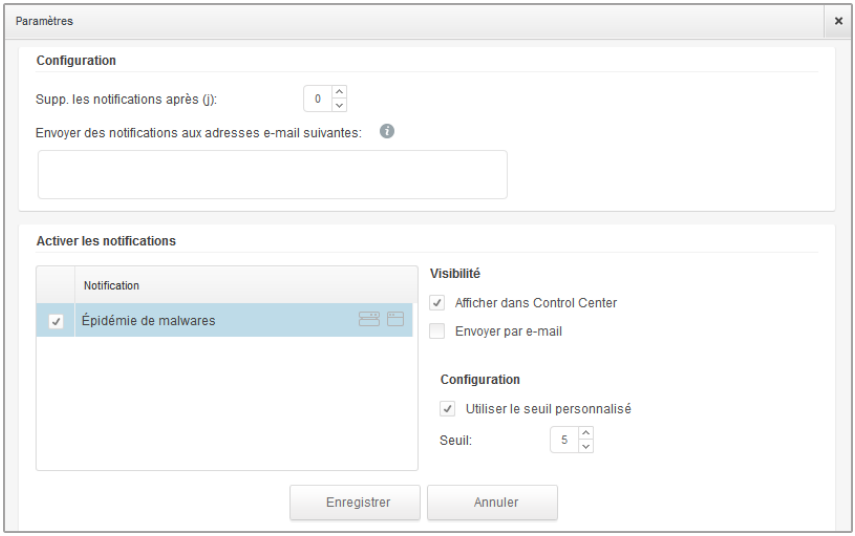
Vous pouvez également configurer la suppression automatique des notifications après un certain nombre de jours. Pour plus d'informations, reportez-vous à « Configurer les paramètres de notification » (p. 15).

4.4. 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. La section **Configuration** vous permet de définir les paramètres suivants :
   - Vous pouvez configurer la suppression automatique des notifications après un certain nombre de jours. Indiquez le nombre de jours souhaité dans le champ **Supp. les notifications après (j)**.
   - 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.
4. La section **Activer la notification** vous permet de choisir le type de notifications que vous souhaitez recevoir de la part de Small Office Security. Vous pouvez également configurer la visibilité et les options d'envoi séparément pour chaque type de notification.

   Sélectionnez le type de notification de votre choix dans la liste. Pour plus d'informations, reportez-vous à « Types de notifications » (p. 12). Lorsqu'un type de notification est sélectionné, vous pouvez configurer ses options spécifiques à droite :
   - **Afficher dans la console** spécifie que ce type d'événement est affiché dans Control Center, avec l'aide de l'icône **Zone de notification**.

- **Envoyer par e-mail** spécifie que ce type d'événement est également envoyé à certaines adresses e-mails. Dans ce cas, vous devez indiquer les adresses e-mail dans le champ correspondant, en appuyant sur `Entrée` après chaque adresse.

Note
La notification Épidémie de malwares est envoyée par défaut aux utilisateurs dont au moins 5% de l'ensemble de leurs éléments administrés sont infectés par le même malware. Pour modifier la sensibilité de la détection antimalware, sélectionnez l'option **Seuil de détection personnalisé** , puis entrez la valeur que vous souhaitez dans le champs **Seuil de déclenchement antimalware**.

5. Cliquez sur **Enregistrer**.

5. 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.

5.1. 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 des 24 dernières heures.

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)

Pour chaque menace détectée, vous pouvez cliquer sur les liens des colonnes de résultat de la désinfection pour afficher la liste des chemins d'accès aux fichiers et ordinateurs affectés. Par exemple, si vous cliquez sur le nombre de la colonne **Résolu(s)**, vous verrez les fichiers et ordinateurs sur lesquels la menace a été supprimée.

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)

Pour chaque ordinateur, vous pouvez cliquer sur les liens des colonnes de résultat de la désinfection pour afficher la liste des menaces et chemins d'accès aux fichiers affectés.

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.

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

Activité Antiphishing

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

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.

Données

Vous informe de l'activité du module Données d'Endpoint Security. Vous pouvez voir le nombre d'e-mails et 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).

État des modules du poste de travail

Fournit un aperçu de l'état des modules de protection d'Endpoint Security pour les ordinateurs sélectionnés. Vous pouvez voir quels modules sont actifs et lesquels sont désactivés ou non installés.

5.2. Création de rapports

Vous pouvez créer deux catégories de rapports :

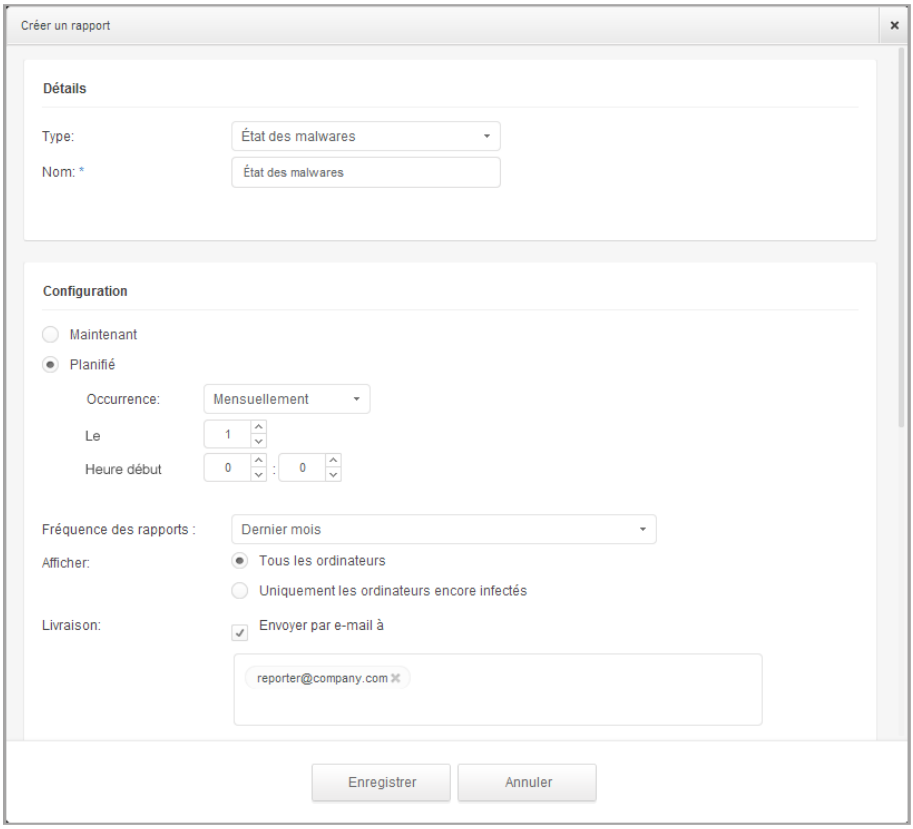
- **Les rapports instantanés.** Les rapports instantanés s'affichent automatiquement une fois que vous les avez générés.
- **Rapports planifiés.** Des rapports planifiés peuvent être configurés pour s'exécuter à l'heure et à la date spécifiées et une liste de tous les rapports planifiés apparaît sur 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**.
2. Cliquez sur le bouton **+ Ajouter** à droite du tableau. Une fenêtre de configuration s'affiche.



Options des Rapports Ordinateurs

3. Sélectionnez le type de rapport souhaité dans le menu. Pour plus d'informations, reportez-vous à « Types de rapports disponibles » (p. 18).
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 récurrence des rapports:
   - Sélectionnez **Maintenant** afin de créer un rapport.
   - Sélectionnez **Planifier** afin de configurer les rapports qui seront automatiquement générés, aux intervalles souhaités:
     – Par heure, à un intervalle horaire spécifique.
     – Tous les jours. Dans ce cas, vous pouvez aussi établir l'heure du début (heure et minutes).

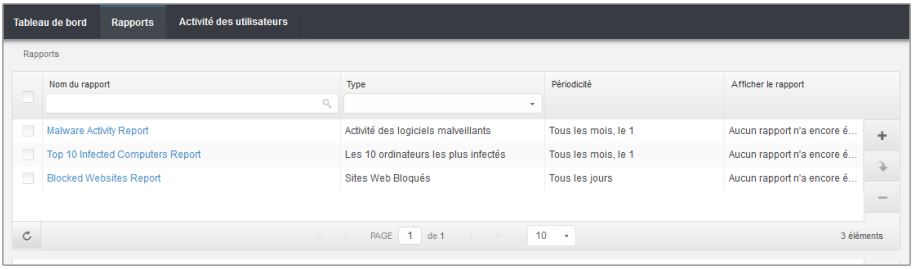
- Par semaine, à un jour précis de la semaine et à l'heure choisie (heure et minutes).
- Par mois, à n'importe quel jour du mois et à l'heure choisie (heure et minutes).

6. Pour la plupart des types de rapport, vous devez spécifier l'intervalle de temps sur lequel les données se réfèrent. Le rapport affichera uniquement des données sur la période sélectionnée.
7. Plusieurs types de rapports fournissent des options de filtrage pour vous aider à trouver facilement les informations qui vous intéressent. Utilisez les options de filtrage sous le menu **Voir** pour obtenir uniquement les informations souhaitées.

   Par exemple, pour un rapport sur le **Statut des mises à jour**, vous pouvez choisir la liste des ordinateurs qui ont été mis à jour sur une période donnée, ou ceux qui nécessite d'être redémarrés afin de compléter la mise à jour.
8. **Livraison**. Pour recevoir un rapport planifié par e-mail, sélectionnez l'option correspondante. Entrez l'adresse e-mail souhaitée dans le champs ci-dessous.
9. **Sélectionner la cible**. Dérouler vers le bas afin de configurer le rapport. Sélectionnez le groupe sur lequel vous souhaitez exécuter le rapport.
10. Cliquez sur **Générer** pour créer un rapport instantané ou sur **Enregistrer** pour créer un rapport planifié.
    - 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**.

5.3. Afficher et gérer des rapports planifiés

Pour afficher et gérer les rapports planifiés, allez sur la page **Rapports**.



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.

5.3.1. 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.

5.3.2. Modifier les rapports planifiés

Note
Lorsqu'un rapport planifié est modifié, toutes les mises à jour sont appliquées à partir de la prochaine génération du rapport. Les rapports générés auparavant ne seront pas affectés par la modification.

Pour modifier les paramètres d'un rapport planifié :

1. Allez sur la page **Rapports**.
2. Cliquez sur le nom du rapport.
3. Modifiez les paramètres du rapport selon vos besoins. Vous pouvez modifier les options suivantes :
   - **Nom du rapport** Choisissez un nom de rapport explicite afin de l'identifier facilement. Lorsque vous choisissez un nom, prenez en compte le type et la cible du rapport, et, éventuellement, les options du rapport. Les rapports générés par un rapport planifié portent son nom.
   - **Récurrence des rapports (planifier)**. Vous pouvez planifier les rapports afin qu'ils soient automatiquement générés toutes les heures (par intervalle), tous les jours (à un horaire précis), toutes les semaines (à un jour et un horaire défini) ou tous les mois (un jour et un horaire précis du mois). En fonction de la planification sélectionnée, le rapport contiendra uniquement des données de la veille, de la semaine ou du mois précédent.

- **Configuration.**
  - Vous pouvez planifier les rapports afin qu'ils soient automatiquement générés toutes les heures (par intervalle), tous les jours (à un horaire précis), toutes les semaines (à un jour et un horaire défini) ou tous les mois (un jour et un horaire précis du mois). En fonction de la planification sélectionnée, le rapport contiendra uniquement des données de la veille, de la semaine ou du mois précédent.
  - Le rapport comprendra uniquement des données sur l'intervalle de temps sélectionné. Vous pouvez modifier l'intervalle dès la nouvelle génération du rapport.
  - La plupart des rapports fournissent des options de filtrage pour vous aider à trouver facilement les informations qui vous intéressent. Lorsque vous affichez le rapport dans la console, toutes les informations seront disponibles, quelles que soient les options sélectionnées. Si vous téléchargez ou envoyez le rapport par e-mail, seul le résumé du rapport et les informations sélectionnées figureront dans le fichier PDF. Les données du rapport seront uniquement disponibles au format CSV.
  - Vous pouvez également choisir de recevoir le rapport par e-mail.
- **Sélectionner la Cible.** L'option sélectionnée indique le type de cible du rapport actuel (les groupes ou les éléments individuels du réseau). Cliquez sur le lien correspondant pour afficher la cible du rapport actuel. Pour la changer, sélectionnez les groupes ou les éléments du réseau à inclure dans le rapport.

4. Cliquez sur **Enregistrer** pour appliquer les modifications.

5.3.3. 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.

5.4. 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.

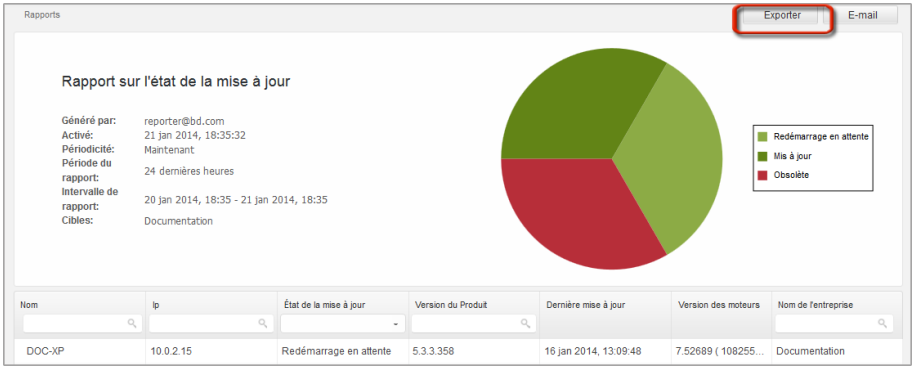
Il y a deux façons d'enregistrer les rapports :

- Exporter
- Télécharger

5.4.1. 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 - 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.

5.4.2. 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.

5.5. 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.

5.6. Impression des rapports

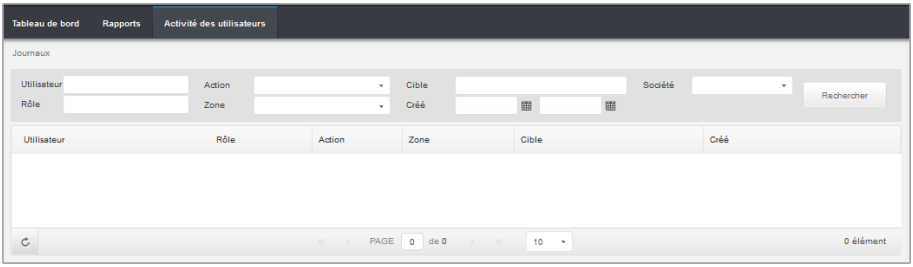
Le Control Center ne prend pas en charge actuellement la fonctionnalité du bouton imprimer. Pour imprimer un rapport, vous devez d'abord l'enregistrer sur votre ordinateur.

6. Journal d'activité de l'utilisateur

La Control Center enregistre toutes les opérations et actions effectuées par les utilisateurs. La liste des activités utilisateurs comprend les événements suivants, en fonction de votre niveau d'autorisation administrative :

- Connexion et déconnexion
- Créer, éditer, renommer et supprimer des rapports
- Ajouter et supprimer des portlets du tableau de bord

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



La page d'activité de l'utilisateur

Pour afficher les événements enregistrés qui vous intéressent, vous devez définir une recherche. Complétez les champs disponibles avec les critères de recherche et cliquez sur le bouton **Rechercher**. Tous les enregistrements correspondant à vos critères apparaîtront dans le tableau.

Les colonnes du tableau vous donnent les informations utiles sur les événements de la liste suivante :

- Le nom d'utilisateur de la personne ayant effectué l'action.
- Le rôle utilisateur.
- L'action ayant causée l'événement.
- Le type d'élément infecté par l'action.
- L'élément spécifique infecté.
- L'heure à laquelle l'événement s'est produit.

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

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

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

7. Obtenir de l'aide

Pour tout problème ou toute question concernant la Control Center, contactez un administrateur.

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 n'ont pas totalement pris connaissance 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'Iliade 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.